On chains of monoids and their representation rings

Maithreya Sitaraman

Submitted in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
under the Executive Committee
of the Graduate School of Arts and Sciences

COLUMBIA UNIVERSITY

2022

Abstract

On chains of monoids and their representation rings

Maithreya Sitaraman

We present some results about chains of monoids $S_0 \hookrightarrow S_1 \hookrightarrow S_2..$ and their associated representation rings, with particular emphasis to behavior as the index n (viz. S_n) varies. A rich supply of such chains of monoids can be found via specializations of diagrammatic algebras or variations of diagrammatic algebras, where the inclusions involve the addition of loose strands. This thesis comprises of original results along three themes associated with the above:

(1) Identifying a certain polynomial property featuring operators on representation rings, and a characterization of chains of groups $G_0 \hookrightarrow G_1 \hookrightarrow G_2..$ which satisfy this polynomial property.
(2) Understanding the induced action on homology from topological actions of the chain of Temperley-Lieb monoids $\mathrm{TL}_1 \hookrightarrow \mathrm{TL}_2 \hookrightarrow \mathrm{TL}_3 ...$. Making the analogy to classical representation stability.
(3) Identifying chains of diagrammatic monoids $S_0 \hookrightarrow S_1 \hookrightarrow S_2..$ on which cryptographic protocols resist linear attacks. Explicitly computes lower bounds on the dimensions of all representations of various truncations of diagrammatic monoids.

Table of Contents

Acknowledgements

First and foremost, I must thank my advisor Mikhail Khovanov for the guidance he has provided over the last few years, and also for his encouragement whenever things have gotten difficult. Furthermore, I am thankful for the creative freedom that he lent me to pursue numerous dead-ends, and patiently waited as I inevitably came to the conclusion that he was correct. Secondly, I must thank my other collaborators Sun Woo Park and Daniel Tubbenhauer, both of whom played a key role in forming and working through many of the mathematical ideas in this thesis. Sun Woo Park and I jointly wrote the paper upon which Chapter 1 is based. Mikhail Khovanov, Daniel Tubbenhauer and I jointly wrote the paper upon which Chapter 3 is based. I am thankful for their valuable insights and stimulating discussions.

To my wife Sowmya,
together with whom I grow
and attempt to maneuver
the world

Chapter 1

Introduction

In this thesis, we present original results about chains of monoids $S_0 \hookrightarrow S_1 \hookrightarrow S_2 \ldots$. across three themes. In this introduction, we will aim to summarize the motivation, the problem statement, the most relevant existing literature, and our novel results.

Theme 1: On a polynomial property involving chains of representation rings

Motivation:

The chains of symmetric groups

$$S_0 \hookrightarrow S_1 \hookrightarrow S_2 \hookrightarrow \ldots$$

and more generally the chain of wreath products

$$H^0 \rtimes S_0 \hookrightarrow H^1 \rtimes S_1 \hookrightarrow H^2 \rtimes S_2 \hookrightarrow H^3 \rtimes S_3 \ldots$$

satisfy the Heisenberg algebra property on the level of their representation rings. That is,

$$\operatorname{Res}\operatorname{Ind} - \operatorname{Ind}\operatorname{Res} = M\,\mathrm{Id}$$

for a constant M. This is well known and well studied from both classical and modern perspectives, see for example [52], [45], [47], [53]:

It is also well known (see for example Corollary 1.4.11 of [17]) that the Heisenberg algebra structures leads to a natural polynomial property associated with Induction and Restriction operators, namely:

Property. $(*)$ *For every* $l \in \mathbb{Z}_{\geq 0}$ *there exists a polynomial* f_l *such that* $\mathrm{Ind}^l \mathrm{Res}^l = f_l(\mathrm{Ind}\,\mathrm{Res})$.

It is therefore natural to study the above polynomial property in and of itself, without the extra Heisenberg algebra structure. It is also natural to wonder if there are other examples of chains of groups

$$G_0 \hookrightarrow G_1 \hookrightarrow G_2 \hookrightarrow G_3 ...$$

whose induction and restriction operators also satisfy this polynomial property.

The problem statement:

Characterize chains of groups

$$G_0 \hookrightarrow G_1 \hookrightarrow G_2 \hookrightarrow G_3 ...$$

whose induction and restriction operators also satisfy the following polynomial property:

Property. $(*)$ *For every* $l \in \mathbb{Z}_{\geq 0}$ *there exists a polynomial* f_l *such that* $\mathrm{Ind}^l \mathrm{Res}^l = f_l(\mathrm{Ind}\,\mathrm{Res})$.

The most relevant existing literature:

The only known examples of chains of groups that satisfy the Heisenberg algebra property $(\mathrm{Res}\,\mathrm{Ind} - \mathrm{Ind}\,\mathrm{Res} = M\,\mathrm{Id})$ are chains of wreath products. It is proved in [18] that if

$M = 1$ or M is prime, then the only such chains are chains of wreath products. It is further conjectured in [18] that the only such chains are chains of wreath products for M arbitrary. This is especially relevant to our paper since our main result can be viewed as a partial answer to a generalization of the conjecture in [18].

The other literature on dual graded graphs is also especially relevant ([9] [10] [17]). In [9], the authors consider towers of algebras satisfying certain axioms, and prove that their Grothendieck rings have dual graded graph structures. They then appeal to [17], which, given a dual graded graph structure, uses combinatorial arguments to express the $\mathrm{Ind}^l \mathrm{Res}^l$ operator as a polynomial in the Ind Res operator. In this paper, we pursue this question from a representation theoretic perspective, examine the representation theoretic consequences of the above polynomial property, and explore necessary conditions for such a polynomial property to hold. This yields results of a very different flavor from [9] [10] and [17]. Nevertheless, the main corollary of our work (Corollary 2.3.18) can be restated using the language of dual graded graphs as (under the relevant hypotheses): "Ind and Res operators have recurrent commutation relation if and only if they have linear commutation relation", which we believe is a significant result in the world of dual graded graphs.

Our novel results:

The main results of this chapter are characterizations of chains of groups which satisfy the Property $(*)$ above and their associated polynomials. More specificially, the main theorem of the chapter is Theorem 2.3.17, which shows that the family of polynomials is determined by two parameters which can easily be read off from the orders of the group. Furthermore, a corollary of the main theorem, Corollary 2.3.18, shows that Ind Res and Res Ind satisfy a simple linear equation in terms of those two parameters.

Theme 2: On topological actions of the Temperley-Lieb monoids

Motivation:

Our original motivations came from the world of representation stability. Given a chain of monoids

$$M_0 \hookrightarrow M_1 \hookrightarrow M_2 \hookrightarrow ...$$

a natural question to consider is whether there is a natural theory of representation stability associated with such a chain. Originally, representation considered only the chain of symmetric groups:

$$S_0 \hookrightarrow S_1 \hookrightarrow S_2 \hookrightarrow ...$$

To learn about representation stability, we recommend that the reader take a look at [60] and [46]. Since then, this field has expanded to a whole host of algebraic objects. Regarding chains of diagrammatic algebras: there has been some work in recent years. We refer the reader to [43]. Diagrammatics and representation stability have also been uttered in the same breadth in a different sense: In [6], the authors produce a functor from the category of FI-modules modulo finite length FI-modules to the abelian envelope of the Deligne category. For the Temperley-Lieb algebra in particular, the representation stability of Temperley-Lieb algebras has also debatably been considered in [39], where the author considers representations of TL(∞), and classifies "link state representations" which are indecomposable or irreducible. However, note that the author of [39] does not make any suggestion regarding what families of TL(∞)-representations could be considered stable.

In any case, topological actions and representation stability go hand in hand, and this

motivates a study of topological actions. Indeed, the homology of natural families of spaces provides rich examples of representation stability. The foundational paper on representation stability [46] shows, for instance, that the homology of configuration spaces is representation-stable. We are able to prove an analogue of this theorem for the chain of Temperley-Lieb monoids (see Corollary 3.5.14).

Nevertheless, while our original motivations came from the world of representation stability, topological actions and the induced representation structure of homology is an interesting subject to think of in and of itself, even without representation stability lurking in the background. In particular, it is interesting to think about how homology groups decompose as representations of TL_n, which is what our main theorem for this theme is about (see Theorem 3.4.17).

The problem statement:

Given a space X that carries an action of the Temperley-Lieb monoid TL_n, and given $k \in \mathbb{Z}_{\geq 0}$ how does the homology $H_k(X)$ decompose as a TL_n representation? Furthermore, is there a notion of topological stability and representation stability for TL_n such that a topologically stable chain of spaces results in representation-stable chain of homology groups?

The most relevant existing literature:

To our knowledge, topological actions of the Temperley-Lieb monoids have not been studied before in any capacity. However, we strongly recommend the paper [44] which includes a wonderful treatment of the representation theory of Temperley-Lieb algebras from a diagrammatic perspective. Some of the foundational diagrammatic constructions

and intuition that make our proofs possible are derived from that paper. For representation stability, our Corollary 3.5.14 can be thought of as an analogy to the celebrated result of [46] that the homology of configuration spaces is representation-stable. For other perspectives related to the representation stability of Temperley-Lieb algebras, we would like to point the reader to [43] and [39].

Our novel results:

The main theorem of our paper is Theorem 3.4.17, which, under certain hypotheses, gives a formula to explicitly decompose the homology of a space X upon which TL_n acts as a TL_n representation. The explicit decomposition is in terms of the filtration associated with the space X (Definition 3.3.8), which is a novel definition introduced in this paper and can be read off from the space X with ease.

Theme 3: On cryptographic efficacy and representation gap of diagrammatic monoid chains

Motivation:

Some of the most important cryptographic protocols in use today are based on *commutative groups* and deliver a gold standard for cryptography. On the other hand, *noncommutative group-based* and *monoid-based* protocols seem to be less understood and in many cases admit efficient attacks.

There has been many ideas and there is an extensive literature on constructing cryptographic protocols from noncommutative groups and monoids, see e.g. [1] and references therein. Examples of such are Magyarik–Wagner public key protocol [58],

Anshel–Anshel–Goldfeld key exchange [25], Ko–Lee et al. key exchange protocol [29] and Shpilrain–Zapata public key protocols [48]. In [40, Section 4] there is a big list of various protocols.

However, as shown by Myasnikov and Roman'kov [40], these protocols can be successfully attacked if S admits small nontrivial representations. This is called a *linear decomposition attack* or *linear attack*, for short. One of the consequences of linear attacks is that finite noncommutative groups may not be suited for cryptographic purposes as they admit nontrivial representations of moderate size. For a toy example, the symmetric group S_n has $n!$ elements, but admits a faithful $(n-1)$-dimensional representation. The dimension of this representation is logarithmic in the size of the group, and the symmetric group would be a poor choice for various standard noncommutative group protocols.

It is therefore valuable to find non-commutative monoids which have no small nontrivial simple representations. Thus, we are interested to find non-commutative monoids which have a large "representation gap" (See Definition 4.1.25). Since cryptography intrinsically uses monoid chains rather than monoids, we are interested in chains of monoids

$$S_{(0)} \hookrightarrow S_{(1)} \hookrightarrow S_{(2)} \hookrightarrow ...$$

such that the representation gap of $S_{(n)}$ grows fast in n. We are able to show that truncations of various diagrammatic monoids provides us with a supply of such monoids that resist linear attacks.

The problem statement:

Can we find chains of non-commutative monoids

$$S_{(0)} \hookrightarrow S_{(1)} \hookrightarrow S_{(2)} \hookrightarrow ...$$

whose representation gap grows fast in n and therefore resist linear attacks?

The most relevant existing literature:

The linear attack, as outlined by Myasnikov and Roman'kov [40], is in many ways the foundation for the motivation of our investigation. There are also many cryptographic protocols outlined there for an interested reader to take a look.

The main structural tool we use in this paper to prove our results is Green's theory of cells (Green's relations). The classical description using Green's relations can be found in many (older and newer) sources e.g. [20], [41] or [55]. The cell based discussion is not so easy to find in the literature, see however [21] or [57].

Our novel results:

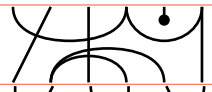
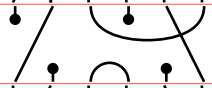
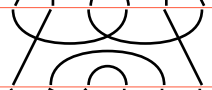
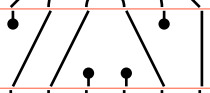
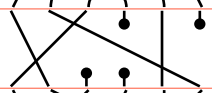
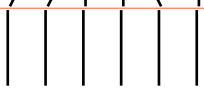
Most of the monoids which we will use can be obtained as hom-subsets of the *set-theoretical partition category*. We will use matchings from n bottom to n top points of the following types (all of these are classical example, see e.g. [23] or [22] for summaries):

- The *partition monoid* Pa_n of all diagrams of partitions of a $2n$-element set.
- The *rook-Brauer monoid* RoBr_n consisting of all diagrams with components of size $1, 2$;
- The *Brauer monoid* Br_n consisting of all diagrams with components of size 2;
- The *rook monoid* Ro_n consisting of all diagrams with components of size $1, 2$, and all

partitions have at most one component at the bottom and at most one at the top;

- The *symmetric group* S_n consisting of all matchings with components of size 1;
- *Planar* versions of these: pPa_n, $\mathrm{pRoBr}_n = \mathrm{Mo}_n$, $\mathrm{pBr}_n = \mathrm{TL}_n$, pRo_n and $\mathrm{pS}_n \cong 1$ (the latter denotes the *trivial monoid*). The planar rook-Brauer monoid is also called *Motzkin monoid*, the planar Brauer monoid is also known as the *Temperley–Lieb monoid*, and the planar symmetric group is trivial.

After suitable truncations, many of the above have large representation gaps. The table below summarizes our results. The "Big reps" column refers to representation gap after appropriate cell truncation. Hereby * means that they have such representations but still come with an aftertaste (such as being semisimple in some cases), $_c$ means conjectural (everything is proved except for results regarding potential nontrivial extensions of the trivial representations) and EX means excluded from the discussion due to triviality. This is explained in more details in Conclusion 4.4.11 and Conclusion 4.5.27.

Symbol	Diagrams	Big reps	Symbol	Diagrams	Big reps
pPa_n		YES*	Pa_n		YES$^*_c$
Mo_n		YES$_c$	RoBr_n		YES$^*_c$
TL_n		YES	Br_n		YES*
pRo_n		YES*	Ro_n		YES*
pS_n		EX	S_n		NO

. (1.0.0.1)

The left half of the table above contains *planar* monoids, the right half *symmetric* monoids. We discuss all of these monoids and their representation gaps.

Chapter 2

On a polynomial property involving chains of representation rings

This chapter is based on the paper [42], which is joint work with Sun Woo Park.

Let G be any finite group, and let $R(G)$ be the vector space of representations of G over an algebraically closed field $\mathbf{k}$, whose basis is given by the set of irreducible representations of G. Given a chain of groups $G_0 \leq G_1 \leq G_2 \leq \cdots$, we form the corresponding chain of vector spaces of their representations, together with induction and restriction operators.

$$R(G_0) \underset{\text{Res}}{\overset{\text{Ind}}{\rightleftarrows}} R(G_1) \underset{\text{Res}}{\overset{\text{Ind}}{\rightleftarrows}} R(G_2) \underset{\text{Res}}{\overset{\text{Ind}}{\rightleftarrows}} \cdots$$

Note that Ind and Res are considered as maps of vector spaces rather than maps of rings. This is because restrictions respect tensor products, whereas inductions do not. Denote by Res^l the operator which restricts representations from G_n to G_{n-l}, and denote by Ind^l the respective operator.

In this chapter, we pursue the following natural structural question: "What happens if the $\text{Ind}^l \text{Res}^l$ operator is a polynomial in the $\text{Ind}\,\text{Res}$ operator over the representation ring $R(G_n)$ of G_n?". In the special case where the chain of group rings form a tower of algebras (i.e. there is an injection $\mathbb{C}[G_k] \otimes \mathbb{C}[G_l] \to \mathbb{C}[G_{k+l}]$), then it is known that such a polynomial property will hold, see for example [9] [10] [17]. In [9], the authors consider towers of algebras satisfying certain axioms, and prove that their Grothendieck rings have dual graded graph structures. They then appeal to [17], which, given a dual graded graph structure, uses combinatorial arguments to express the $\text{Ind}^l \text{Res}^l$ operator as a polynomial in the $\text{Ind}\,\text{Res}$ operator. In this chapter, we pursue this question from a representation

theoretic perspective, examine the representation theoretic consequences of the above polynomial property, and explore necessary conditions for such a polynomial property to hold. This yields results of a very different flavor from [9] [10] and [17].

Throughout this chapter, we denote by Property $(*)$ the constraint that the operator $\mathrm{Ind}^l \mathrm{Res}^l$ is a polynomial in terms of the $\mathrm{Ind}\,\mathrm{Res}$ operator for any l.

Property 2.0.1. $(*)$ *For every $l \in \mathbb{Z}_{\geq 0}$ there exists a polynomial f_l such that* $\mathrm{Ind}^l \mathrm{Res}^l = f_l(\mathrm{Ind}\,\mathrm{Res})$.

This chapter is devoted to finding rigid numerical constraints on the chains of groups $\{G_i\}$ that satisfy Property $(*)$. The main result of this chapter (Theorem 2.3.17) shows that representation theoretic perspective allows us to rigidly determine the polynomials f_l by using two integral parameters B and C. For the reader's convenience, we state it below:

Theorem 2.0.2 (Polynomials are determined by two parameters)**.** *Let $\{G_n\}_{n\geq 0}$ be a non-constant chain of groups with surjective restriction operators (surjective chain of groups) which satisfies Property $(*)$; that is, there exists polynomials $\{f_l\}_{l\geq 1}$ such that* $\mathrm{Ind}^l \mathrm{Res}^l = f_l(\mathrm{Ind}\,\mathrm{Res})$. *Let $a_n = \frac{|G_n|}{|G_{n-1}|}$. Then:*

(1) $\{a_n\}_{n\in\mathbb{Z}_{\geq 0}}$ is an infinite set. Moreover, there exist two parameters $B \in \mathbb{Z}_{\geq 0}$ and $C \in \mathbb{Z}$ such that for all n, $a_n = Ba_{n-1} + C$.

(2) The two parameters B and C from Part (2) completely determine the polynomials $\{f_l\}_{l\in\mathbb{Z}_{\geq 0}}$. The polynomial f_l can be expressed in terms of these parameters as:

$$f_l(X) = \frac{1}{B^{\frac{l(l-1)}{2}}} X(X-C)(X-[1+B]C)(X-[1+B+B^2]C)...(X-[1+B+....+B^{l-2}]C)$$

For instance, all polynomials are uniquely determined by the polynomial of $\mathrm{Ind}^2\,\mathrm{Res}^2$ (i.e f_2), and that f_2 takes the form $f_2(X) = \frac{1}{B}X(X-C)$ where $B \in \mathbb{Z}_{\geq 0}$ and $C \in \mathbb{Z}$. Furthermore, B and C can be easily read off from the orders of the groups $\{G_i\}$.

While previous research such as [52] and [61] present algebraic structures that induction and restriction operators respect, our theorem, on the other hand, explicitly demonstrates rigid constraints which prevent induction and restriction operators from respecting certain algebraic structures. It can be viewed as a partial answer to a generalization of a Conjecture by Christian Gaetz as follows: The collection of chains of groups satisfying property $(*)$ includes that of dual towers of groups, a family of group chains which satisfy the Heisenberg algebra property. Gaetz [18] conjectured that the numerical constraints the desired polynomial relation satisfy forces the chain of groups to be a chain of wreath products. He proves the conjecture in the special case when the scaling factor is either 1 or is a prime. Since the Heisenberg algebra property implies Property $(*)$ but not vice versa, our main result can be viewed as a partial answer to a generalization of the conjecture by Gaetz.

It should be noted that a corollary of our work (see Corollary 2.3.18) is that, in the language of dual graded graphs (see [17]), Ind and Res operators have a recurrent commutation relation if and only if they have linear commutation relation. In [9] and [10], the authors assume conditions that imply a linear commutation relation and deduce a recurrent commutation relation. However, in the context of "surjective chains of groups", we are able to prove the converse (the harder direction). This is a novel aspect of our chapter which is not addressed in the literature. For the reader's convenience, we state Corollary 2.3.18 below:

Corollary 2.0.3. *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups which satisfies*

Property $(*)$. *Then there exist constants* B *and* C *such that*

$$\mathrm{Res}\,\mathrm{Ind} - B\,\mathrm{Ind}\,\mathrm{Res} = C\,Id$$

That is, the language of dual graded graphs (see [17]), Ind *and* Res *operators have recurrent commutation relation if and only if they have linear commutation relation.*

2.1 Setup and notation

We work with chains of groups $G_0 \leq G_1 \leq G_2 ...$ and their corresponding chains of representation rings over $\mathbb{C}$:

$$R(G_0) \underset{\text{Res}}{\overset{\text{Ind}}{\rightleftarrows}} R(G_1) \underset{\text{Res}}{\overset{\text{Ind}}{\rightleftarrows}} R(G_2) \underset{\text{Res}}{\overset{\text{Ind}}{\rightleftarrows}} ...$$

that are surjective, in the sense that

Definition 2.1.1 (Surjective Chain)**.** A surjective chain of groups $\{G_n\}_{n\geq 0}$ is a sequence of groups such that:

(1) $G_{n-1} \leq G_n$ for all n

(2) $\mathrm{Res} : R(G_n) \to R(G_{n-1})$ is a surjective linear map for all n

Remark: The condition that $\mathrm{Res} : R(G_n) \to R(G_{n-1})$ is a surjection is equivalent by Frobenius reciprocity to the condition that $\mathrm{Ind} : R(G_{n-1}) \to R(G_n)$ is an injection. To see this, simply note that: Res is not surjective $\iff$ there exists some nonzero representation $w \in R(G_{n-1})$ which is perpendicular to the image of Res $\iff$ there exists a basis $\{x_1, .., x_n\}$ of $R(G_n)$ such that $\langle \mathrm{Res}(x_i), w\rangle = 0$ for all i $\iff$ there exists a basis $\{x_1, .., x_n\}$ of $R(G_n)$ such that $\langle x_i, \mathrm{Ind}(w)\rangle = 0$ for all i $\iff$ $\mathrm{Ind}(w) = 0$ for some nonzero w $\iff$ Ind is not injective.

Remark: We note that the construction of chains of representation rings of $\{G_n\}_{n\geq 0}$ is analogous to the construction of the Grothendieck ring of the tower of algebras $\bigoplus_{n\geq 0}\mathbb{C}G_n$. The only difference is that the Grothendieck ring is a $\mathbb{Z}$-module, while we consider the representation ring as a $\mathbb{C}$-vector space. We refer to Section 2 of [9] and Section 3 of [10] for the conditions on the tower of algebras $\bigoplus_{n\geq 0}\mathbb{C}G_n$. However, we also note that the conditions on surjective chains of groups $\{G_n\}_{n\geq 0}$ are different from those on the tower of algebras provided in [9] and [10]. One of the axioms [9] and [10] assume is that the external multiplication $\mathbb{C}G_m \otimes \mathbb{C}G_n \to \mathbb{C}G_{m+n}$ is an injection. This is a rigid condition on the level of algebras. However, the only condition we have on the level of algebras is the fact that $\mathbb{C}[G_n]$ is a subalgebra of $\mathbb{C}[G_{n+1}]$, which is a weak condition. We do, however, impose a condition on the level of representation rings (rather than the level of algebras) that the restriction operator is surjective. In [9] and [10], Mackey's theorem implies the existence of a Hopf algebra structure on the level of representation rings with multiplication $m : \overline{R} \otimes \overline{R} \to \overline{R}$ given by $\mathrm{Ind}_{G_m \times G_n}^{G_{m+n}}$ and comultiplication $\Delta : \overline{R} \to \overline{R} \otimes \overline{R}$ given by $\sum_{k+l=n} \mathrm{Res}_{G_k \times G_l}^{G_{k+l}}$. Our surjectivity condition need not imply such a Hopf algebra structure.

Let $\bar{R}\{l\}$ denote the subchain of the chain of representation rings comprising of all components of degree $\geq l$, i.e $\bar{R}\{l\} = \bigoplus_{i=l}^{\infty} R(G_i)$. We now consider the family of grading-preserving linear operators $\{\mathrm{Ind}^l \mathrm{Res}^l : \bar{R}\{l\} \to \bar{R}\{l\}\}_{l\in\mathbb{Z}_{\geq 0}}$, where $\mathrm{Ind}^l \mathrm{Res}^l : R(G_n) \to R(G_n)$ is the operator which restricts a representation l steps down and then induces the resulting expression l steps up. That is:

$$\mathrm{Ind}^l \mathrm{Res}^l \restriction_{R(G_n)} := \begin{cases} \mathrm{Ind}_{G_{n-l}}^{G_n} \mathrm{Res}_{G_{n-l}}^{G_n} & \text{if } n \geq l \\ \text{not defined} & \text{if } n < l \end{cases}$$

This construction allows us to understand the overarching question of this chapter: "What happens if the $\mathrm{Ind}^l \mathrm{Res}^l$ operator is a polynomial in the $\mathrm{Ind}\,\mathrm{Res}$ operator?". There exists a polynomial over $\mathbb{Q}$ (in fact, over $\mathbb{Z}$ as seen from Section 4) depending on l, $f_l(X) = c_0 + c_1X + c_2X^2 + ... + c_dX^d$ such that for any $n \geq l$ and any representation $u \in R(G_n)$,

$$\mathrm{Ind}^l \mathrm{Res}^l(u) = c_0u + c_1 \mathrm{Ind}\,\mathrm{Res}(u) + c_2 \mathrm{Ind}\,\mathrm{Res}\,\mathrm{Ind}\,\mathrm{Res}(u) + ... + c_d(\mathrm{Ind}\,\mathrm{Res})^d(u)$$

where multiplication on the right hand side is of course composition. In addition, $\mathrm{Ind}^l \mathrm{Res}^l \restriction_{R(G_n)}$ and $\mathrm{Ind}\,\mathrm{Res} \restriction_{R(G_n)}$ are matrices for every $n \geq l$, and the property above states that there exists a single polynomial f_l such that for all $n \geq l$, the matrix $\mathrm{Ind}^l \mathrm{Res}^l \restriction_{R(G_n)}$ is equal to f_l applied to the matrix $\mathrm{Ind}\,\mathrm{Res} \restriction_{R(G_n)}$.

The operators Ind and Res are considered as maps of vector spaces rather than maps of rings, the reason being that although restrictions respect tensor products, inductions do not. In this chapter, we are interested in obtaining information from restrictions, and so it is of the utmost importance that the restriction maps above are surjective. The restriction from the symmetric group to the alternating group $\mathrm{Res} : R(S_n) \to R(A_n)$ is an example of a restriction which is not surjective, and we wish to exclude such cases. Since we think of operators like $\mathrm{Ind}\,\mathrm{Res}$ as linear maps, we like to denote them by capital letters. Since we think of representations as vectors, we denote them by small letters. The following table of notation outlines the notation used in this chapter:

Notation	**What it denotes**
Lower case letters such as u, w, x, y	Representations living in some $R(G_n)$
Lower case letters with a tilde such as $\tilde{w}$	If $w \in R(G_k)$, $\tilde{w}$ is a lift of w by Restriction that lives in $R(G_n)$ for some $n > k$. That is, $\mathrm{Res}^{n-k}(\tilde{w}) = w$
Ind^k	The k-step induction operator $\mathrm{Ind}_{G_n}^{G_{n+k}}$ for all n
Res^k	The k-step restriction operator $\mathrm{Res}_{G_n}^{G_{n+k}}$ for all n
X	The operator $\mathrm{Ind}\,\mathrm{Res}$
δ_h	The column of the character table of G_n associated with the conjugacy class $[h]$. As a vector in $R(G_n)$, $\delta_h = \sum_{\text{irreps } u} \chi_u(h)u$
t_n or t	The trivial representation of the group G_n
s_n or s	The sign representation of the symmetric group S_n
v_n or v	The standard representation of the symmetric group S_n
$\wedge^2_n$ or $\wedge^2$	The representation of the symmetric group S_n corresponding to the young diagram $(n-2,1,1)$
p_n or p	The representation of the symmetric group S_n corresponding to the young diagram $(n-2,2)$
b_n or b	The representation of the symmetric group S_n corresponding to the young diagram $(n-3,3)$.
r_n or r	The representation of the symmetric group S_n corresponding to the young diagram $(n-3,2,1)$.
$\mathbb{M}(G,u)$	The McKay graph associated to a group G and its representation u
$[h]_n$, $[\tau]_n$	Conjugacy classes of h and τ when considered as an element of G_n

Table 2.1: Table of notation

2.2 Motivating examples

In this section we will introduce the motivating examples of chains which satisfy Property $(*)$, namely symmetric groups and (more generally) wreath products. Both of these chains have the additional Heisenberg-algebra property as defined below:

Property 2.2.1 (Heisenberg algebra property)**.** *A chain of groups $\{G_n\}_{n\geq 0}$ is said to satisfy the Heisenberg algebra property with scaling $M \in \mathbb{Z}_{\geq 0}$ if:*

$$\operatorname{Res}\operatorname{Ind} - \operatorname{Ind}\operatorname{Res} = M\,\mathrm{Id}$$

It is well known that:

Proposition 2.2.2. *Let H be any finite group.*

(a) *The chain of wreath products $\{H^n \rtimes S_n\}_{n\in\mathbb{Z}_{\geq 0}}$ is a surjective chain.*

(b) *The chain of wreath products $\{H^n \rtimes S_n\}_{n\in\mathbb{Z}_{\geq 0}}$ satisfies the Heisenberg algebra property with scaling $|H|$.*

In particular, setting $H = \{1\}$, the chain of symmetric groups satisfies the Heisenberg algebra property with $M = 1$. It remains to show that Heisenberg algebra property implies Property $(*)$. This is also a well known fact; for instance, the reader may see for example Corollary 1.4.11 of [17]. Nevertheless, for the reader's convenience, we now provide a self-contained proof of this fact:

Lemma 2.2.3 (Heisenberg property implies the polynomial property)**.** *Suppose* $\{G_n\}_{n\geq 0}$ *is a chain of groups which satisfies the Heisenberg algebra property with scaling* M*. Then, for every* $l \in \mathbb{Z}_{\geq 0}$*:*

$$\operatorname{Ind}^l \operatorname{Res}^l = f_l(\operatorname{Ind}\operatorname{Res})$$

where f_l *is the polynomial given by* $f_l(X) = X(X-M)(X-2M)...(X-(l-1)M)$*. In particular,* $\{G_n\}_{n\geq 0}$ *satisfies Property* $(*)$*.*

Proof. The statement clearly holds when $l = 1$. Suppose the statement holds for $l = k$. Then the following relation holds.

$$\begin{aligned}
\operatorname{Ind}^{k+1} \operatorname{Res}^{k+1} &= \operatorname{Ind}^k(\operatorname{Ind}\operatorname{Res})\operatorname{Res}^k \\
&= \operatorname{Ind}^k(\operatorname{Res}\operatorname{Ind} - M)\operatorname{Res}^k \\
&= \operatorname{Ind}^k(\operatorname{Res}\operatorname{Ind}\operatorname{Res}^k - M\operatorname{Res}^k) \\
&= \operatorname{Ind}^k(\operatorname{Res}(\operatorname{Res}\operatorname{Ind} - M)\operatorname{Res}^{k-1} - M\operatorname{Res}^k) \\
&= \operatorname{Ind}^k(\operatorname{Res}^2\operatorname{Ind}\operatorname{Res}^{k-1} - 2M\operatorname{Res}^k) \\
&= \cdots \\
&= \operatorname{Ind}^k(\operatorname{Res}^k\operatorname{Ind}\operatorname{Res} - kM\operatorname{Res}^k) \\
&= \operatorname{Ind}^k\operatorname{Res}^k(\operatorname{Ind}\operatorname{Res} - kM) \\
&= X(X-M)(X-2M)\cdots(X-kM)
\end{aligned}$$

□

Therefore, chains of wreath products satisfy Property $(*)$, and thus serve as motivating examples for the rest of the chapter. For interesting computations using the power of Property $(*)$ when applied to wreath products, we refer the reader to Section 2.4. In the next section, we will study the interplay between Property $(*)$ and representation theory,

and the structural limitations that representation theory provides to chains satisfying Property $(*)$. The first few results from the next section will be used in the computations of Section 2.4.

2.3 Constraints on surjective chains satisfying Property $(*)$

The goal of this section is to show that surjective chains that satisfy Property $(*)$ behave very rigidly, and therefore Property $(*)$ is a very rare property. The chain of wreath products is therefore a very special chain. A trivial example of such a chain of groups is the constant chain at a fixed group G, i.e set $G_n = G$ for all n. Here, induction and restriction are both the identity and so clearly $\mathrm{Ind}^l \mathrm{Res}^l = \mathrm{Ind}\,\mathrm{Res}$. Thus, if we set $f_l(X) = X$ for all l, then we have that $\mathrm{Ind}^l \mathrm{Res}^l = f_l(\mathrm{Ind}\,\mathrm{Res})$. However, this example is not very interesting, and we will henceforth restrict our attention to non-constant chains which satisfy Property $(*)$.

2.3.1 Character theoretic properties of surjective chains of groups

We will now present a theorem that gives a formula for character table columns in terms of the representation theory of smaller groups of our chain and the $\mathrm{Ind}\,\mathrm{Res}$ operator. It is incredibly useful from a computational perspective, but moreover, it will serve as a foundational result for the rest of the chapter. Though the idea involves original ideas, the proof is short and self-contained.

Theorem 2.3.1. (Extracting character information from the polynomial property). Let $\{G_n\}_{n\geq 0}$ be a surjective chain of groups and $l \in \mathbb{Z}_{\geq 0}$ is such that $\mathrm{Ind}^l \mathrm{Res}^l = f_l(\mathrm{Ind}\,\mathrm{Res})$ for some polynomial f_l. Let $\alpha \in G_k \hookrightarrow G_{k+l}$, and let $\delta_\alpha \in R(G_{k+l})$ be the character column of

α, that is: $\delta_\alpha = \sum_{\text{irreps } u \text{ of } G_{k+l}} \chi_u(\alpha) u$. For each representation w of G_k, let $\tilde{w}$ denote a lift to G_{k+l}, i.e an element of $R(G_{k+l})$ such that $\mathrm{Res}^l(\tilde{w}) = w$. Then:

$$\delta_\alpha = f_l(\mathrm{Ind}\,\mathrm{Res}) \left(\sum_{\text{irreps } w \text{ of } G_k} \chi_w(\alpha) \cdot \tilde{w} \right)$$

Proof. Observe that since $\alpha \in G_k \hookrightarrow G_n$, and since restrictions preserve character values, we have that for every $u \in R(G_n)$, $\chi_u(\alpha) = \chi_{\mathrm{Res}\, u}(\alpha)$. Now we replace this global restriction operator with the local $\mathrm{Ind}\,\mathrm{Res}$ operator as follows:

$$\begin{aligned}
\chi_{\mathrm{Res}^{n-k}\, u}(\alpha) &= \sum_{\text{irreps } w \text{ of } G_k} \langle \mathrm{Res}^{n-k}\, u, w \rangle \chi_w(\alpha) \\
&= \sum_{\text{irreps } w \text{ of } G_k} \chi_w(\alpha) \langle u, \mathrm{Ind}^{n-k}\, w \rangle \\
&= \sum_{\text{irreps } w \text{ of } G_k} \chi_w(\alpha) \langle u, \mathrm{Ind}^{n-k}\, \mathrm{Res}^{n-k}\, \tilde{w} \rangle \\
&= \sum_{\text{irreps } w \text{ of } G_k} \chi_w(\alpha) \langle u, f_l(\mathrm{Ind}\,\mathrm{Res}) \tilde{w} \rangle \\
&= \langle f_l(\mathrm{Ind}\,\mathrm{Res}) \left(\sum_{\text{irreps } w \text{ of } G_k} \chi_w(\alpha) \tilde{w} \right), u \rangle
\end{aligned}$$

In the above, the second line followed from Frobenius reciprocity, the third line was from the definition of the lift $\tilde{w}$, and the fourth line was from our hypothesis.

We therefore have that $\langle \delta_\alpha, u \rangle = \langle \sum_{\text{ irreducible representations } w \text{ of } G_k} \chi_w(\alpha) f_l(\mathrm{Ind}\,\mathrm{Res}) \tilde{w}, u \rangle$ for all u. We therefore conclude that:

$$\delta_\alpha = f_l(\text{Ind}\,\text{Res})\left(\sum_{\text{irreducible representations } w \text{ of } G_k} \chi_w(\alpha)\tilde{w}\right)$$

which proves the result. □

A couple of remarks about the theorem:

(1) Deducing character theory via the above theorem: The theorem reduces the problem of computing the character column δ_α of G_n to a problem in G_k. The Ind Res operator allows us to linear algebraically compute character columns via the provided formulae. We see that information about G_k appears in the formula via the lifts $\tilde{w}$ - we only need to lift representations of G_k (which are a relatively small number of representations for $k << n$). There are systematic lifting procedures that enable one to easily construct lifts $\tilde{w}$ for symmetric groups and wreath products, see Section 2.4 for further discussions.

(2)

This theorem can be thought of as a way to compute characters using ring structure: Because $U \otimes Ind(W) = \text{Ind}(\text{Res}(U) \otimes W)$, we can take $W = t$ (the trivial representation of the subgroup) and $U = u$ (some arbitrary representation of our group) to obtain that: $u \otimes \text{Ind}(t) = \text{Ind}\,\text{Res}(u)$. That is:

Observation 2.3.2. Let $H \leq G$ be a subgroup and let t be the trivial representation of H. Then we have the following equality of operators:

$$\text{Ind}_H^G \,\text{Res}_H^G = \text{Ind}_H^G(t)\otimes$$

Therefore, in light of the above observation, Ind Res can be thought of as the element

$\mathrm{Ind}(t)$ in the representation ring $(R(G_n), \otimes)$. Our theorem gives expressions for the character table columns in terms of a polynomial in $\mathrm{Ind}\,\mathrm{Res}$ which translates to sums of tensor powers of $\mathrm{Ind}(t)$.

As one may observe, the key component of Theorem 2.3.1 is the idea of taking lifts of representations. Given an irreducible representation w in $R(G_k)$, we want to construct a lift $\tilde{w} \in R(G_n)$ such that $\mathrm{Res}^{n-k} \tilde{w} = w$. This is possible because, for surjective chains, restriction is surjective by definition. Note that symmetric groups and wreath products form surjective chains since the branching rule is surjective. For such chains, it is possible to lift an irreducible representation from $R(G_k)$ to $R(G_n)$ for all n. This is not a cumbersome process since there are only $k!$ representations to lift, which is relatively insignificant when $k << n$.

2.3.2 Proving the conjugacy class constraint

The goal of this subsection is to prove a family of constraints that our polynomials $\{f_l\}_{l \in \mathbb{N}}$ must satisfy that is indexed by conjugacy classes. We will call the constraint corresponding to a conjugacy class $[h]$ as the $[h]$-class constraint. One constraint that will turn out to be extremely important to us is the $[e]$-class constraint, which we will simply call "the identity class constraint". The feature of our method which allows us to recover conjugacy class information is that our method allows us to directly obtain the global structure of the character column, rather than obtaining individual character values separately. We begin with the following Lemma, which is very close to the conjugacy class which we will ultimately prove in this subsection:

Lemma 2.3.3. *Let $\{G_n\}_{n \geq 0}$ be a surjective chain that satisfies Property $(*)$. Let $h \in G_{n-l}$ for some $l < n \in \mathbb{N}$. Then, f_l satisfies the constraint:*

$$f_l\left(\frac{|G_n| \cdot |[h]_n \cap G_{n-1}|}{|G_{n-1}| \cdot |[h]_n|}\right) = f_l(\chi_{\mathrm{Ind}(t)}(h)) = \frac{|G_n| \cdot |[h]_{n-l}|}{|G_{n-l}| \cdot |[h]_n|}$$

Proof. For ease of notation, set $k = n - l$. By Theorem 2.3.1,

$$\delta_h = f_l(\mathrm{Ind}\,\mathrm{Res})\left(\sum_{\text{irreducible representations } w \text{ of } G_k} \chi_w(h)\tilde{w}\right)$$

Write $X = \mathrm{Ind}(t)\otimes = \mathrm{Ind}\,\mathrm{Res}$ (by Observation 2.3.2). Since the trivial representation t has real character, $\mathrm{Ind}(t)$ also has real character and is therefore self-dual. The adjoint of a representation with respect to the $\mathrm{Hom}(\cdot,\cdot)$ bilinear form and the $\otimes$ multiplication is the dual representation. Therefore, by self-duality of X, we know that $\langle Xu_1, u_2\rangle = \langle u_1, Xu_2\rangle$ for any $u_1, u_2 \in R(G_n)$. Knowing that conjugacy classes can be recovered from L^2 norms, we compute:

$$\begin{aligned}
||\delta_h||^2 &= \langle f_l(X)\left(\sum_{\text{irreps } w \text{ of } G_k} \chi_w(h)\tilde{w}\right), \delta_h\rangle \\
&= \sum_{\text{irreps } w \text{ of } G_k} \chi_w(h)\langle f_l(X)\tilde{w}, \delta_h\rangle \\
&= \sum_{\text{irreps } w \text{ of } G_k} \chi_w(h)\langle \tilde{w}, f_l(X)\delta_h\rangle \\
&= \sum_{\text{irreps } w \text{ of } G_k} \chi_w(h) f_l(\chi_X(h))\bar{\chi_w}(h) \\
&= f_l(\chi_X(h)) \cdot \sum_{\text{irreps } w \text{ of } G_k} |\chi_w(h)|^2 \\
&= f_l(\chi_X(h)) \cdot ||\delta_h^{(k)}||^2
\end{aligned}$$

where $\delta_h^{(k)}$ is the character column of G_k corresponding to h, i.e

$\delta_h^{(k)} = \sum_{\text{irreps } w \text{ of } G_k} \chi_w(h) w \in R(G_k)$. In the above computation, the first line followed from Theorem 2.3.1, the third line followed from self-duality of X, and the fourth line partly followed from the fact that $\text{Res}(\tilde{w}) = w$ and so their characters coincide at h.

Translating L^2 norms into conjugacy classes, we see that:

$$\begin{aligned} f_l(\chi_X(h)) &= \frac{||\delta_h||^2}{||\delta_h^{(k)}||^2} \\ &= \frac{\left(\frac{|G_n|}{|[h]_n|}\right)}{\left(\frac{|G_k|}{|[h]_k|}\right)} \\ &= \frac{|G_n| \cdot |[h]_k|}{|G_k| \cdot |[h]_n|} \end{aligned}$$

To complete the proof, simply note that since $X = \text{Ind}(t)$, the induced character formula tells us that:

$$\begin{aligned} \chi_{\text{Ind}(t)}(h) &= \frac{1}{|G_{n-1}|} \sum_{g \in G_n \text{ s.t } ghg^{-1} \in G_{n-1}} \chi_t(ghg^{-1}) \\ &= \frac{1}{|G_{n-1}|} \sum_{h' \in [h]_n \cap G_{n-1}} |\{g \in G_n \,|\, gh'g^{-1} = h'\}| \cdot 1 \\ &= \frac{1}{|G_{n-1}|} \sum_{h' \in [h]_n \cap G_{n-1}} |C_{G_n}(h')| \\ &= \frac{1}{|G_{n-1}|} \sum_{h' \in [h]_n \cap G_{n-1}} \frac{|G_n|}{|[h']_n|} \text{ (by orbit-stabilizer)} \\ &= \frac{|G_n|}{|G_{n-1}|} \cdot \frac{|[h]_n \cap G_{n-1}|}{|[h]_n|} \end{aligned}$$

This completes the proof of the Lemma. □

We now prove a theorem which is a slight change from the Lemma above. We wish to replace $[h]_n \cap G_{n-1}$ with $[h]_{n-1}$. That is, we require G_{n-1} to control its own fusion in G_n.

Theorem 2.3.4. (The conjugacy class constraint). Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups which satisfies Property $(*)$; that is, there exists polynomials $\{f_l\}_{l\geq 1}$ such that $\mathrm{Ind}^l \mathrm{Res}^l = f_l(\mathrm{Ind}\,\mathrm{Res})$. Then, for any $n \geq l$ and $h \in G_{n-l}$, f_l satisfies the conjugacy class constraint

$$f_l\left(\frac{|G_n| \cdot |[h]_{n-1}|}{|G_{n-1}| \cdot |[h]_n|}\right) = f_l(\chi_{\mathrm{Ind}(t)}(h)) = \frac{|G_n| \cdot |[h]_{n-l}|}{|G_{n-l}| \cdot |[h]_n|}$$

where $[h]_j$ denotes the conjugacy class of $h \in G_j$.

Proof. By Lemma 2.3.3, it suffices to prove that $[h]_n \cap G_{n-1} = [h]_{n-1}$. Note that if two elements of G_{n-1} are conjugate in G_{n-1}, they are automatically conjugate in G_n and so $[h]_{n-1} \subseteq [h]_n \cap G_{n-1}$. We need to show that this is actually an equality. Suppose it were not. Then, there is some $h' \in G_{n-1}$ such that $h' \in [h]_n \cap G_{n-1}$ but $h' \notin [h]_{n-1}$. Since $h' \notin [h]_{n-1}$, choose any class function $\phi : G_{n-1} \to \mathbb{C}$ such that $\phi(h) \neq \phi(h')$. This class function cannot be in the image of Res, since for any class function $\psi : G_n \to \mathbb{C}$, $\mathrm{Res}(\psi)(h') = \psi(h') = \psi(h) = \mathrm{Res}(\psi)(h)$. Thus, Res is not surjective, which is a contradiction. □

Out of all these constraints, the most important constraint is the identity class constraint, obtained by taking $h = e$, and it is worth stating it separately:

Proposition 2.3.5 (The identity class constraint)**.** *Let $\{G_n\}_{n\geq 0}$ be a surjective chain of groups that satisfies Property $(*)$. For each $n \in \mathbb{Z}_{\geq 0}$, let $a_n = \frac{|G_n|}{|G_{n-1}|}$. Then:*

$$f_l(a_n) = a_n a_{n-1} \ldots a_{n-l+1}$$

Proof. Setting $h = e$ in Theorem 2.3.4, and observing that $[e]_m = 1$ for all m, we see that:

$$f_l\left(\frac{|G_n|}{|G_{n-1}|}\right) = \frac{|G_n|}{|G_{n-l}|}$$

which can be rewritten as:

$$f_l(a_n) = a_n a_{n-1} ... a_{n-l+1}$$

□

Recovering conjugacy class information for symmetric groups

For convenience, we use $X = \text{Ind}(t)$ as the permutation representation of G_n over the coset $[G_n : G_{n-1}]$.

Consider a permutation τ. Let S_k be the smallest symmetric group that τ lives in, i.e. the non-fixed elements of τ are relabeled as $\{1, \cdots, k\}$. The number of fixed points that τ has when acting on $\{1, ..., n\}$ is $n - k$, and so $\chi_X(\tau) = n - k$. Since $(n-k)_{n-k} = (n-k)!$, and since $\frac{\#S_n}{\#S_k} = \frac{n!}{k!}$, Theorem 2.3.4 informs us that:

$$\#[\tau]_n = \frac{n!}{k!(n-k)!}\#[\tau]_k = \binom{n}{k}\#[\tau]_k$$

That is, we have recovered something that we already knew: Since the conjugates of τ are obtained by first choosing $n - k$ fixed points and then choosing an element of the cycle type of τ on the remaining k points, we have that the size of the conjugacy class of τ should be the number of ways to choose $n - k$ fixed points multiplied by $\#[\tau]_k$.

2.3.3 The collection of all a_n is necessarily infinite

Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain that satisfies Property $(*)$. Recall that $a_n := \frac{|G_n|}{|G_{n-1}|}$. Why might we want $\{a_n\}_{n\in\mathbb{N}}$ to be an infinite set? The reason is that the infinitude of $\{a_n\}_{n\in\mathbb{N}}$ allows us to use analytic arguments in conjunction with the identity class constraint to deduce very rigid properties that our polynomials must satisfy. Notice that if $\{G_n\}_{n\geq 0}$ is a constant chain (i.e $G_n = G$ for all n), then $a_n = 1$ for all n and $\{G_n\}_{n\geq 0}$ satisfies Property $(*)$ with $f_l(X) = X$ for all l. Therefore, the non-constancy of $\{G_n\}_{n\geq 0}$ is a prerequisite for infinitude of $\{a_n\}_{n\in\mathbb{N}}$. Our goal of this subsection is to prove the following Lemma:

Lemma 2.3.6 (Infinitude of $\{a_n\}_{n\in\mathbb{N}}$)**.** *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups satisfying Property $(*)$. Define $a_n = \frac{|G_n|}{|G_{n-1}|}$. Then: $\{a_n\}_{n\in\mathbb{N}}$ is an infinite set.*

We will prove our goal in 3 steps.

Lemma 2.3.7 (Step 1)**.** *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups such that $\mathrm{Ind}^2\,\mathrm{Res}^2 = f_2(\mathrm{Ind}\,\mathrm{Res})$ for some polynomial f_2. Suppose that $h_1, h_2 \in G_{n-1} \hookrightarrow G_n$ are such that $\chi_{\mathrm{Ind}(t_{n-2})}(h_1) \neq \chi_{\mathrm{Ind}(t_{n-2})}(h_2)$. Let t_i denote the trivial representation of G_i. Then,*

$$\chi_{\mathrm{Ind}(t_{n-1})}(h_1) \neq \chi_{\mathrm{Ind}(t_{n-1})}(h_2)$$

Proof. By the proof of Theorem 2.3.4, we know that every group G_k of our chain controls its own fusion. Since $f_2(X) = \mathrm{Ind}^2(t)$, we have that for any $h \in G_{n-1} \hookrightarrow G_n$, $f_2(\chi_{\mathrm{Ind}(t_{n-1})}(h)) = \chi_{\mathrm{Ind}^2(t_{n-2})}(h)$. By the induced character formula, we have that:

$$
\begin{aligned}
f_2(\chi_{\mathrm{Ind}(t_{n-1})}(h)) &= \chi_{\mathrm{Ind}^2(t_{n-2})}(h) \\
&= \chi_{\mathrm{Ind}(\mathrm{Ind}(t_{n-2}))}(h) \\
&= \frac{1}{|G_{n-1}|} \sum_{g\in G_n \text{ such that } ghg^{-1}\in G_{n-1}} \chi_{\mathrm{Ind}(t_{n-2})}(ghg^{-1}) \\
&= \frac{1}{|G_{n-1}|} \sum_{g\in G_n \text{ such that } ghg^{-1}\in G_{n-1}} \chi_{\mathrm{Ind}(t_{n-2})}(h) \\
&= \chi_{\mathrm{Ind}(t_{n-2})}(h) \cdot \frac{1}{|G_{n-1}|} \sum_{g\in G_n \text{ such that } ghg^{-1}\in G_{n-1}} 1 \\
&= \chi_{\mathrm{Ind}(t_{n-2})}(h) \cdot \chi_{\mathrm{Ind}(t_{n-1})}(h)
\end{aligned}
$$

In the above computation, the third line followed from the induced character formula, and the fourth line followed from the fact that G_{n-1} controls its own fusion.

Now, suppose $h_1, h_2 \in G_{n-1} \hookrightarrow G_n$ such that $\chi_{\mathrm{Ind}(t_{n-1})}(h_1) = \chi_{\mathrm{Ind}(t_{n-1})}(h_2)$. Observe that $\chi_{\mathrm{Ind}(t_{n-1})}(h_1) \neq 0$ because h_1 fixes $eG_{n-1} \in G_n/G_{n-1}$. Then, $\frac{f_2(\chi_{\mathrm{Ind}(t_{n-1})}(h_1))}{\chi_{\mathrm{Ind}(t_{n-1})}(h_1)} = \frac{f_2(\chi_{\mathrm{Ind}(t_{n-1})}(h_2))}{\chi_{\mathrm{Ind}(t_{n-1})}(h_2)}$. So, we conclude that $\chi_{\mathrm{Ind}(t_{n-2})}(h_1) = \chi_{\mathrm{Ind}(t_{n-2})}(h_2)$, which proves the contrapositive statement of the Lemma and therefore completes the proof. □

Lemma 2.3.8 (Step 2)**.** *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups such that $\mathrm{Ind}^2 \mathrm{Res}^2 = f_2(\mathrm{Ind}\,\mathrm{Res})$ for some polynomial f_2. Then, $\mathrm{Ind}(t) \in R(G_n)$ has at least n distinct character values.*

Proof. We proceed by induction on n. For $n = 1$ there is nothing to show since every representation must have at least one character value.

Suppose it is true that $\mathrm{Ind}(t_{n-2})$ has $n-1$ distinct character values, say $\chi_{\mathrm{Ind}(t_{n-2})}(h_1), \chi_{\mathrm{Ind}(t_{n-2})}(h_2), ..., \chi_{\mathrm{Ind}(t_{n-2})}(h_{n-1})$. By Lemma 2.3.7, $\chi_{\mathrm{Ind}(t_{n-1})}(h_1), \chi_{\mathrm{Ind}(t_{n-1})}(h_2), ..., \chi_{\mathrm{Ind}(t_{n-1})}(h_{n-1})$ are $n-1$ distinct character values of

$\mathrm{Ind}(t_{n-1})$. Moreover, each of these character values are nonzero because if $h_i \in G_{n-1}$, then h_i fixes the identity coset. By Burnside's Lemma, because the action of G_n on $\{G_n / G_{n-1}\}$ is a transitive action, there must exist some $g \in G_n$ such that $\chi_{\mathrm{Ind}(t_{n-1})}(g) = 0$. Thus, $0, \chi_{\mathrm{Ind}(t_{n-1})}(h_1), \chi_{\mathrm{Ind}(t_{n-1})}(h_2), ..., \chi_{\mathrm{Ind}(t_{n-1})}(h_{n-1})$ are n distinct character values of $\mathrm{Ind}(t_{n-1})$ and we have therefore proved the result. □

Observation 2.3.9 (Step 3)**.** The number of distinct character values of $\mathrm{Ind}(t)$ is at most a_n

Proof. Since the character values of $\mathrm{Ind}(t)$ are the number of fixed points, they are integers. Moreover $\dim(\mathrm{Ind}(t)) = a_n$ is the maximal character value □

Using Steps 1, 2, and 3, we can prove the infinitude of $\{a_n\}_{n\in\mathbb{N}}$ which is the main goal of this section. Recall the statement:

Lemma 2.3.10. (Infinitude of $\{a_n\}_{n\in\mathbb{N}}$). Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups satisfying Property $(*)$. Define $a_n = \frac{|G_n|}{|G_{n-1}|}$. Then: $\{a_n\}_{n\in\mathbb{N}}$ is an infinite set.

Proof. By Lemma 2.3.8, we have that the number of distinct character values of $\mathrm{Ind}(t) \in R(G_n)$ is $\geq n$. But by Observation 2.3.9, the number of distinct character values of $\mathrm{Ind}(t) \in R(G_n)$ is $\leq a_n$. This is only compatible if $a_n \geq n$ for every n. In particular, $a_n \to \infty$ as $n \to \infty$. □

2.3.4 Description of f_l in terms of the two parameters B and C

Now that we have established that $\{a_n\}_{n\in\mathbb{N}}$ is an infinite collection, we are ready to use the identity class constraint (Proposition 2.3.5) together with analytic methods to deduce

results. The end goal of this subsection is to prove Theorem 2.3.17. We begin with a simple observation:

Observation 2.3.11 (Bounding degrees of f_l)**.** Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups satisfying Property $(*)$. Then, f_l has degree at most l.

Proof. We first prove that f_2 has degree at most 2. Suppose there are infinitely many $n \in \mathbb{N}$ such that $a_{n-1} > a_n$. Then $a_n^2 < f_2(a_n) = a_n a_{n-1}$ for infinitely many n. Because $a_n \to \infty$ as $n \to \infty$, there also exist infinitely many $n \in \mathbb{N}$ such that $a_{n-1} \leq a_n$. For such n's, $f_2(a_n) \leq a_n^2$. Then the polynomial $f_2(X) - X^2$ has infinitely many local extrema, a contradiction. Thus there exists only finitely many $n \in \mathbb{N}$'s such that $a_{n-1} > a_n$. In particular, there exists a fixed positive integer M such that for all $n \geq M$, $a_{n-1} \leq a_n$. Since $f_2(a_n) = a_n a_{n-1} \leq a_n^2$ for all sufficiently large n, we obtain that f_2 has degree at most 2. The proof for f_l immediately follows because for all $n \geq M$, $f_l(a_n) = a_n \cdots a_{n-l+1} \leq a_n^l$. □

We also deduce the following Lemma, which is an interesting and important stepping stone:

Lemma 2.3.12 (Smaller polynomials divide larger polynomials)**.** *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups satisfying Property $(*)$. Then: f_{l-1} divides f_l for every l.*

Proof. Recall that $a_n = \frac{|G_n|}{|G_{n-1}|}$. By the Identity class constraint (Proposition 2.3.5):

$$f_l(a_n) = a_n a_{n-1} ... a_{n-l+1} = f_{l-1}(a_n) a_{n-l+1}$$

We therefore have that, for all $n \in \mathbb{N}$, $\frac{f_l(a_n)}{f_{l-1}(a_n)} = a_{n-l+1} \in \mathbb{Z}$. The condition that $a_{n-l+1} \in \mathbb{N}$ is just a consequence of Lagrange's theorem since $G_{n-l} \leq G_{n-l+1}$.

By the divisor theorem on $\mathbb{Q}[X]$, we can write $f_l = f_{l-1}q + r$ where r is a polynomial of degree less than f_{l-1}. Thus, we may write:

$$\frac{f_l}{f_{l-1}} = q + \frac{r}{f_l}$$

Suppose for contradiction that r is nonzero.

Choose $\epsilon > 0$ such that for all integers $a \in \mathbb{Z}$, either $q(a) \in \mathbb{Z}$ or $|q(a) - \mathbb{Z}| \geq \epsilon$. Let us first show that such an ϵ exists. For pedagogical reasons, first consider the case in which $q = \frac{c}{d}X^p$ for $c, d \in \mathbb{Z}$. Observe that for $a \in \mathbb{Z}$ either $q(a) \in \mathbb{Z}$ or $|q(a) - \mathbb{Z}| \geq \frac{1}{d}$. For such a polynomial q, we may take $\epsilon = \frac{1}{d}$. In general, write $q = \frac{c_p}{d_p}X^p + \frac{c_{p-1}}{d_{p-1}}X^{p-1} + ... + \frac{c_0}{d_0}$. For such a polynomial, we may take $\epsilon = \frac{1}{\prod_{i=0}^{p} d_p}$.

Choose ϵ as in the previous paragraph. For large values of n, (say $n > N$), we can assert that $0 < |(\frac{r}{f_l})(a_n)| < \epsilon$. The first inequality is simply because r is nonzero. The second inequality is because the degree of f_l is strictly larger than the degree of r, and $a_n \to \infty$ as $n \to \infty$ (Lemma 2.3.10).

Take any $n > N$. Then we have that: either $q(a_n) \in \mathbb{Z}$ or $|q(a_n) - \mathbb{Z}| \geq \epsilon$, and $0 < (\frac{r}{f_l})(a_n) < \epsilon$. Therefore, we have that:

$$(q + \frac{r}{f_l})(a_n) \notin \mathbb{Z}$$

Therefore,

$$(\frac{f_l}{f_{l-1}})(a_n) \notin \mathbb{Z}$$

for this n, and this is a contradiction since we remarked earlier that $\frac{f_l}{f_{l-1}}(a_n) \in \mathbb{Z}$ for all n.

We therefore must have that $r = 0$, i.e f_{l-1} divides f_l. □

An immediate and useful application of the two above results is the following:

Observation 2.3.13 (Determining f_2)**.** Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups satisfying Property $(*)$. Then, there exist constants $A, C \in \mathbb{Q}$ such that

$$f_2(X) = AX(X - C)$$

Proof. Since $\mathrm{Ind}^1 \mathrm{Res}^1 = \mathrm{Ind}\,\mathrm{Res}$, we have that $f_1(X) = X$. By the Lemma 2.3.12, f_1 must divide f_2, and by Observation 2.3.11, f_2 is either a degree 1 polynomial or a degree 2 polynomial. Thus, we must have that either $f_2(X) = AX$, or $f_2(X) = AX(X - C)$ for some constants $A, C \in \mathbb{Q}$. If the former is true, then by the identity class constraint (Proposition 2.3.5), $a_n a_{n-1} = f_2(a_n) = Aa_n$ for all n, and thus, $a_{n-1} = A$ is a constant for all n, thereby contradicting the infinitude of $\{a_n\}_{n\in\mathbb{N}}$ (Lemma 2.3.10). Thus,

$$f_2(X) = AX(X - C)$$

. □

We therefore observe the following recursion formula:

Observation 2.3.14 (Recursion of $\{a_n\}_{n\in\mathbb{N}}$)**.** Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups satisfying Property $(*)$. Then, there exist constants $A, C \in \mathbb{Q}$ such that

$$a_n = \frac{1}{A} a_{n-1} + C$$

Proof. Using the identity lass constraint (Proposition 2.3.5) for f_2 above, we see that $a_n a_{n-1} = A a_n (a_n - C)$. The observation follows. □

Thus far, we do not have any restrictions on $A, C \in \mathbb{Q}$. The following proposition shows that $\frac{1}{A}$ and C must both be integers.

Proposition 2.3.15 ($C, \frac{1}{A} \in \mathbb{Z}$)**.** *Suppose $\{a_n\}$ is a sequence of positive integers such that $a_n = \frac{1}{A} a_{n-1} + C$ for fixed rational numbers A and C. Suppose also that $a_n \to \infty$ as $n \to \infty$. Then $A = \frac{1}{B}$ for some positive integer B and an integer C.*

Proof. Write $A = \frac{p}{q}$ where $(p, q) = 1$, and write $C = \frac{c}{d}$ for $(c, d) = 1$. By repeatedly applying the identity $a_n = \frac{1}{A} a_{n-1} + C$, we observe that a_n can be expressed as the following equation in terms of a_1:

$$\begin{aligned} a_n &= \frac{1}{A^{n-1}} \left(a_1 + CA + CA^2 + \cdots + CA^{n-1} \right) \\ &= \frac{q^{n-1}}{p^{n-1}} \left(a_1 + C \left(\frac{p}{q} + \cdots + \frac{p^{n-1}}{q^{n-1}} \right) \right) \end{aligned}$$

We then obtain that:

$$a_n d p^{n-1} = a_1 d q^{n-1} + cpq^{n-2} + \cdots + cp^{n-1}$$

Now, suppose that $p \geq 2$. Since $(p, q) = 1$, taking the above equation mod p^i for all $0 \leq i \leq n-1$ and dividing by suitable powers of q^j gives:

$$
\begin{aligned}
a_1 d &\equiv 0 \bmod p \\
a_1 dq &\equiv -cp \bmod p^2 \\
a_1 dq^2 &\equiv -c(p^2 + pq) \bmod p^3 \\
&\vdots \\
a_1 dq^{n-2} &\equiv -c(p^{n-2} + \cdots + pq) \bmod p^{n-1}
\end{aligned}
$$

Since q^j is a unit in $\mathbb{Z}/p^i\mathbb{Z}$, we also obtain:

$$
\begin{aligned}
a_1 d &\equiv 0 \bmod p \\
a_1 d &\equiv -c\frac{p}{q} \bmod p^2 \\
a_1 d &\equiv -c\left(\frac{p^2}{q^2} + \frac{p}{q}\right) \bmod p^3 \\
&\vdots \\
a_1 d &\equiv -c\left(\frac{p^{n-2}}{q^{n-2}} + \cdots + \frac{p}{q}\right) \bmod p^{n-1}
\end{aligned}
$$

But notice that $a_1 d$ is a fixed integer. Then there exists an integer k such that $a_1 d < p^k$. Therefore, taking sufficiently large n, we obtain that

$$
-c\left(\frac{p^{k-2}}{q^{k-2}} + \cdots + \frac{p}{q}\right) \equiv -c\left(\frac{p^{k-1}}{q^{k-1}} + \frac{p^{k-2}}{q^{k-2}} + \cdots + \frac{p}{q}\right) \bmod p^n
$$

In particular,

$$
c\frac{p^{k-1}}{q^{k-1}} \equiv 0 \bmod p^n
$$

Hence, $c \equiv 0 \bmod p^{n-k-1}$.

From this relation, we first show that $A = \frac{1}{q}$. If $c = 0$, then $C = 0$. Therefore, $a_n = \frac{1}{A}a_{n-1} = \frac{q}{p}a_{n-1}$. This is a contradiction because a_n is a positive integer for all $n \in \mathbb{N}$. If $c \neq 0$. Then the equivalence $c \equiv 0 \bmod p^{n-k-1}$ is a contradiction because it holds for arbitrarily large n while c is a fixed integer.

Hence, $p = 1$ so $A = \frac{1}{q}$ for some integer $q \in \mathbb{Z}$. We can fix $B = q$. Note that we in fact require that B is positive because $\{a_n\}_{n\in\mathbb{N}}$ is a sequence of positive integers. Next, we recall that $a_n = \frac{1}{A}a_{n-1} + C$. Since a_n, a_{n-1}, and $\frac{1}{A} = B$ are integers, we require that C is an integer. □

If we concatenate the theory we have built thus far, we notice that we have proved Part (1) of Theorem 2.3.17. We may use this to strengthen Observation 2.3.11 as follows:

Lemma 2.3.16 (f_l has degree l)**.** *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups satisfying Property $(*)$. Then, f_l is a polynomial of degree l.*

Proof. By the Identity class constraint (Proposition 2.3.5),

$$f_l(a_n) = a_n a_{n-1}...a_{n-l+1} = a_n \cdot a_n \frac{a_{n-1}}{a_n} \cdot a_n \frac{a_{n-2}}{a_{n-1}} \frac{a_{n-1}}{a_n} ... \cdot a_n \frac{a_{n-l+1}}{a_{n-l+2}} \frac{a_{n-l+2}}{a_{n-l+3}} .. \frac{a_{n-1}}{a_n}$$

Now observe that by Part (1) of Theorem 2.3.17, $\frac{a_m}{a_{m+1}} = \frac{a_m}{Ba_m+C} = \frac{1}{B+\frac{C}{a_m}}$ for every m, and thus we obtain that for m large:

$$\frac{1}{B} - \epsilon \leq \frac{a_m}{a_{m+1}} \leq \frac{1}{B} + \epsilon$$

In particular, for m large:

$$\left(\frac{1}{B}-\epsilon\right)^{\frac{(l-1)(l)}{2}} a_n^l \leq f_l(a_n) \leq \left(\frac{1}{B}+\epsilon\right)^{\frac{(l-1)(l)}{2}} a_n^l$$

and thus f_l has degree l by the Infinitude of $\{a_n\}_{n\in\mathbb{N}}$ (Lemma 2.3.10). □

We are now ready to prove Theorem 2.3.17 in its full entirety. For the reader's convenience, we will state the theorem below:

Theorem 2.3.17. (Polynomials are determined by two parameters). Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups which satisfies Property $(*)$; that is, there exists polynomials $\{f_l\}_{l\geq 1}$ such that $\operatorname{Ind}^l \operatorname{Res}^l = f_l(\operatorname{Ind}\operatorname{Res})$. Let $a_n = \frac{|G_n|}{|G_{n-1}|}$. Then:

(1) $\{a_n\}_{n\in\mathbb{N}}$ is an infinite set. Moreover, there exists two parameters $B \in \mathbb{N}$ and $C \in \mathbb{Z}$ such that for all n, $a_n = Ba_{n-1} + C$.

(2) The two parameters B and C from Part (2) completely determine the polynomials $\{f_l\}_{l\in\mathbb{N}}$. f_l can be expressed in terms of these parameters as:

$$f_l(X) = \frac{1}{B^{\frac{l(l-1)}{2}}} X(X-C)(X-[1+B]C)(X-[1+B+B^2]C)...(X-[1+B+....+B^{l-2}]C)$$

Proof. (1) follows directly from Lemma 2.3.10, Observation 2.3.14 and Proposition 2.3.15. It therefore remains to prove (2).

We prove the formula in (2) by induction on l. When $l = 1$, we have $f_1(X) = X$, which satisfies the formula prescribed by the proposition. Suppose that f_l satisfies the formula prescribed by the proposition. Since f_l divides f_{l+1} (Lemma 2.3.12) and f_l has degree l and f_{l+1} has degree $l+1$ (Lemma 2.3.16), we may write:

$$\frac{f_{l+1}(X)}{f_l(X)} = B_{l+1}(X - C_{l+1})$$

for some $B_{l+1}, C_{l+1} \in \mathbb{Q}$.

Evaluating the above expression at a_n and applying the Identity class constraint (Proposition 2.3.5) to simplify the left hand side, we see that:

$$a_{n-l} = B_{l+1}(a_n - C_{l+1})$$

Since $a_{n-1} = \frac{1}{B}(a_n - C)$, we have that:

$$a_{n-l} = \frac{1}{B^l}\left(a_n - C(1 + B + \cdots + B^{l-1})\right)$$

Comparing expressions, we see that $B_{l+1} = \frac{1}{B^l}$ and $C_{l+1} = C(1 + B + \cdots + B^{l-1})$. Thus:

$$\begin{aligned} f_{l+1}(X) &= \frac{1}{B^l} \cdot \frac{1}{B^{\frac{l(l-1)}{2}}} X(X - C)(X - [1 + B]C)(X - [1 + B + B^2]C)...(X - [1 + B + ... + B^{l-1}]C) \\ &= \frac{1}{B^{\frac{(l+1)(l)}{2}}} X(X - C)(X - [1 + B]C)(X - [1 + B + B^2]C)...(X - [1 + B + ... + B^{l-1}]C) \end{aligned}$$

which completes the inductive step. □

Some remarks about the theorem:

(1) Relation to results via dual graded graphs: We note that one can prove analogous formulae by viewing Grothendieck rings of towers of algebras $\bigoplus_{n\geq 0} \mathbb{C}G_n$ as a dual graded graph, see in particular Theorem 1.1 and Theorem 7.2 of [9] and Theorem 3.7 of [10]. However, our result is fundamentally different, since those results assume that we have an injection $\mathbb{C}[G_k] \otimes \mathbb{C}[G_l] \to \mathbb{C}[G_n]$, which is a strong condition that

automatically implies a linear recurrence relation, see Theorem 3.2 and Theorem 7.4 of [9]. Those papers then deduce the polynomial relation from the linear recurrence relation using Section 1.4 of [17]. In contrast, the goal of our theorem is to assume a polynomial recurrence relation, and from this deduce that a linear recurrence relation must hold, thereby addressing a converse direction. The arguments we use also have a very different flavor from those used in [9], [10], and [17], since our arguments are fundamentally representation theoretic, whereas those papers extensively use combinatorial properties of towers of algebras.

(2) The two parameter family: A consequence of Theorem 2.3.17 is that whenever a surjective chain satisfies Property $(*)$, the polynomials f_l belong to a two-parameter family of polynomials and the parameters are integers (B and C). This is certainly a very rigid constraint. Moreover, by Lemma 2.2.3, we know that there exist chains for $B = 1$ and any positive integer C. Furthermore, any given f_k determines f_l because f_k uniquely determines the two parameters B and C as shown in Part (2) of Theorem 2.3.17. It is a natural question to ask whether it is possible to have C to be non-positive. In fact, if G_0 is trivial, then C must be positive.

(3) Reading off polynomials from three successive values: a_n, a_{n+1}, a_{n+2}: Observe that the orders of four consecutive groups $G_{n-1}, G_n, G_{n+1}, G_{n+2}$ determines f_l for all l. This suggests that the sequence $\{f_l\}_{l\in\mathbb{N}}$ behaves very rigidly. Indeed, note that
$a_{n+1} = Ba_n + C \implies C = a_{n+1} - Ba_n$, and thus,
$a_{n+2} = Ba_{n+1} + C = (B+1)a_{n+1} - Ba_n \implies B(a_{n+1} - a_n) = (a_{n+2} - a_{n+1})$, and thus B is uniquely determined, since one can show that $a_{n+1} \neq a_n$ for non-constant chains. And likewise C is uniquely determined.

(4) Predicting the polynomials for wreath products from dimensions: For the chain of

wreath products $\{H^n \rtimes S_n\}_{n\in\mathbb{Z}_{\geq 0}}$, $a_n = n|H|$. One may observe that $a_n = a_{n-1} + |H|$. The constants B and C in Theorem 2.3.17 are then 1 and $|H|$ respectively, and Theorem 2.3.17 therefore implies that if $\{H^n \rtimes S_n\}_{n\in\mathbb{N}}$ satisfies Property $(*)$, then $f_l(X) = X(X - |H|)(X - 2|H|)...(X - (l-1)|H|)$.

As a corollary of the above result, we obtain a result which has importance in the world of dual graded graphs (see [17] for a rigorous treatment of the subject).

Corollary 2.3.18. *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups which satisfies Property $(*)$. Then there exist constants B and C such that*

$$\text{Res Ind} - B\,\text{Ind Res} = C\,Id$$

That is, the language of dual graded graphs (see [17]), Ind *and* Res *operators have recurrent commutation relation if and only if they have linear commutation relation.*

2.3.5 If $G_0 = \{e\}$, the roots of f_l correspond to characters values of $\text{Ind}(t) \in G_l$

In this subsection, we will consider the special and important case when $G_0 = \{e\}$. The reason why this situation is special and insightful is that G_0 has only one representation, the trivial representation, which we always know how to lift. This allows us to apply our character column techniques from Theorem 2.3.1 to deduce special information. Our goal is to prove:

Theorem 2.3.19. *Let $\{G_n\}_{n\geq 0}$ be a non-constant surjective chain of groups which satisfies Property $(*)$. Suppose further that $G_0 = \{e\}$. Then, the roots of f_l are precisely the non-identity character values of $X = \text{Ind}(t) \in R(G_l)$ (i.e the character values other than $\dim(\text{Ind}(t))$).*

A couple of remarks about the theorem:

(1) Positivity of C: Theorem 2.3.19 shows that if G_0 is trivial, then the integer C from Theorem 2.3.17 has to be positive. We do not know of any examples of chains for which C is negative, and a reasonable question for the future would be to ask whether or not C is forced to be positive.

(2) Predicting the polynomials f_l: We may use Theorem 2.3.19 to predict the polynomials f_l. For example, consider the chain of symmetric groups $\{S_n\}_{n\in\mathbb{N}}$. Since $S_1 = \{e\}$, Theorem 2.3.19 informs us that the roots of the polynomial f_l are precisely the non-identity eigenvalues of $X = \mathrm{Ind}(t) \in R(S_{l+1})$. These eigenvalues are the characters of the permutation representation of S_{l+1}, which are obtained by counting fixed points of the S_{l+1} action on $\{1, 2, ..., l+1\}$. The possible number of fixed points a non-identity permutation can have belongs to $\{1, 2, 3, .., l-1\}$, and we therefore know that f_l is a multiple of the falling factorial polynomial $X(X-1)...(X-(l-1))$. Dimension counting is enough to show that this multiple is 1.

(3) Generalization to wreath products: The aforementioned argument can be generalized to the chain of wreath products $\{H^n \rtimes S_n\}_{n\in\mathbb{N}}$ as well. We thank the reviewer for pointing out this example. Suppose that H acts on a set S. Let $K < H$ be a point stabilizer. Then the permutation representation $\mathrm{Ind}_{H^{n-1}\rtimes S_{n-1}\times K}^{H^n\rtimes S_n} t$ is the permutation representation of $H^n \rtimes S_n$ acting imprimitively on $H \times \{1, \cdots, n\}$. This is because the group $H^n \rtimes S_n$ acts imprimitively on the set $S \times \{1, \cdots, n\}$ with blocks $S \times \{k\}$ for $k \in \{1, \cdots, n\}$, and the point stabilizer for this action is $H^{n-1} \rtimes S_{n-1} \times K$. Because H acts regularly on itself, the possible number of fixed points a non-identity permutation can have belongs to $\{|H|, 2|H|, \cdots, (n-2)|H|, n|H|\}$.

We will now prove the statement of Theorem 2.3.19.

Lemma 2.3.20 (Non-identity character values are roots)**.** *Suppose that* $\{G_n\}_{n\geq 0}$ *is a surjective chain of groups that satisfies Property* $(*)$ *with the additional property that* $G_0 = \{e\}$*. Consider* $\mathrm{Ind}(t) \in G_l$*. Then,* $\chi_{\mathrm{Ind}(t)}(\alpha)$ *is a root of* f_l *for every* $\alpha \in G_l$ *other than* $\alpha = e$*.*

Proof. Consider $e \in \{e\} = G_0$. Observe that Theorem 2.3.1 informs us that:

$$\delta_e = \chi_t(e) f_l(X)\tilde{e} = f_l(X)\tilde{t} = f_l(X)t$$

Consider another character column δ_α such that $\alpha \neq e$. Observe that this is an eigenvector of X with eigenvalue $\chi_{\mathrm{Ind}(t)}(\alpha)$. Indeed, this is a simple consequence of the fact that $\mathrm{Ind}\,\mathrm{Res} = \mathrm{Ind}(t)\otimes$. It might be worth mentioning that the fact that character columns are eigenvectors for $\mathrm{Ind}\,\mathrm{Res}$ with the above eigenvalues is also observed in [2] and is given more prominence there.

So, we then have that:

$$0 = \langle \delta_e, \delta_\alpha \rangle = \langle f_l(X)t, \delta_\alpha \rangle = \langle t, f_l(\chi_{\mathrm{Ind}(t)}(\alpha))\delta_\alpha \rangle = f_l(\chi_{\mathrm{Ind}(t)}(\alpha))\delta_\alpha(t) = f_l(\chi_{\mathrm{Ind}(t)}(\alpha))$$

□

It might be worth to remark that If we had used $\alpha = e$ with the above reasoning, then we have obtained that:

$$|G_l| = \langle \delta_e, \delta_e \rangle = f_l(\frac{|G_l|}{|G_{l-1}|}) = f_l(a_l)$$

which is simply the Identity class constraint (Proposition 2.3.5) in the special case where $G_0 = \{e\}$.

Now we prove the converse:

Lemma 2.3.21 (Roots are non-identity character values)**.** *Suppose that $\{G_n\}_{n\geq 0}$ is a surjective chain of groups that satisfies Property $(*)$ with the additional property that $G_0 = \{e\}$. Then, any root of f_l is an eigenvalue of* $\mathrm{Ind}(t) \in R(G_l)$.

Proof. Let γ be a root of $f_l(X)$. Then $f_l(X)$ is divisible by $X - \gamma$. By Theorem 2.3.1, $\delta_e = f_l(X)$, and thus, for any $\alpha \neq e$:

$$0 = \langle \delta_e, \delta_\alpha \rangle = \langle f_l(X), \delta_\alpha \rangle = \langle X - \gamma, \frac{f_l(X)}{X - \gamma} \delta_\alpha \rangle$$

Therefore, if $\frac{f_l(X)}{X-\gamma}\delta_\alpha$ is nonzero for some α, then it is an eigenvector of X with eigenvalue γ.

If $\frac{f_l(X)}{X-\gamma}\delta_\alpha$ is the zero vector for all $\alpha \neq e$, then:

$$0 = \langle \frac{f_l(X)}{X - \gamma} \delta_\alpha, t \rangle = \langle \frac{f_l(X)}{X - \gamma}, \delta_\alpha \rangle$$

Hence, $\frac{f_l(X)}{X-\gamma}$ is orthogonal to all δ_α's. Because $\{\delta_\alpha\}$ forms an orthogonal basis of the space $R(G_l)$, $\frac{f_l(X)}{X-\gamma}$ is a scalar multiple of δ_e. This is impossible since we would have that $\frac{f_l(X)}{X-\gamma} = \lambda f_l(X)$ but the degrees on both sides of the equation are not equal. Therefore,

there must exist some α such that $\frac{f_l(X)}{X-\gamma}\delta_\alpha$ is nonzero, and this is an eigenvector of X with eigenvalue γ. □

We have thus proved Theorem 2.3.19.

2.4 Examples

As examples, we present how Property (∗) can be utilized to excavate the representation theoretic properties of chains of symmetric groups and wreath products.

2.4.1 Chains of symmetric groups

The chain of symmetric groups is a chain of wreath products with $H = \{e\}$,. The chain of symmetric groups satisfies the Heisenberg algebra property (Property 2.2.1) with scaling 1. That is, the chain of symmetric groups satisfies Property (∗) with $f_l(X) = (X)_l$, where $(X)_l$ is the falling factorial polynomial. In this subsection, we will exhibit some formulae for symmetric group character columns using Theorems 2.3.1 and 2.3.17.

Theorem 2.4.1. *Let* $X = \operatorname{Ind}\operatorname{Res} = \operatorname{Ind}(t)\otimes$ *be the* Ind Res *operator on the chain* $\{S_n\}$.

(a) *The polynomial* f_l *is given by*

$$f_l = X(X-1)(X-2)...(X-(l-1))$$

(b) *The non-identity character values of* Ind t *in the symmetric group* S_n *is the set* $\{0, 1, \cdots, n-1\}$.

(c) *Let* $\tau \in S_k \hookrightarrow S_n$. *The character column* δ_τ *as an element of* $R(S_n)$ *is given by:*

$$\delta_\tau = X(X-1)...(X-(n-k)+1)\left(\sum_{irreps\ w\ of\ S_k} \chi_w(\tau)\tilde{w}\right)$$

Throughout this subsection, we will abbreviate the Young diagrams corresponding to representations of S_n as indicated in Table 2.1.

A systematic lifting procedure for symmetric groups

We start with a description of a systematic lifting process required for an effective implementation of Theorem 2.3.1 to chains of symmetric groups.

(a) Let w_1 and w_2 be two partitions of an integer k, represented as Young diagrams. The partial order $<$ on irreducible representations of S_k can be obtained from comparing the partitions of k by the number of boxes in their young diagrams below the first row. That is, set $w_1 < w_2$ if w_1 contains fewer boxes below the first row than w_2.
(b) We begin with an irreducible representation w of S_k. Extend the first row of u by attaching $n-k$ boxes to the first row. The result is a representation w' of S_n
(c) Observe that $\mathrm{Res}^{n-k}(w')$ contains exactly one copy of w in its decomposition, corresponding to removing the boxes in the first row.
(d) Observe that all of the other representations of S_k that appear $\mathrm{Res}^{n-k}(u')$ are $< w$ with respect to the ordering in (a)
(e) We therefore can apply an inductive process using $<$.

> **Remark:** It is interesting to note that the procedure we describe in (b) is the same procedure that is used in [13] to construct the FI-module generated by a given irreducible representation. Let w be a representation of S_k, and in the notation of [13], let $V(w)_n$ be the representation obtained by adding $n-k$ boxes to the top row of w. The combinatorial procedure of restricting w to S_k involves polynomial choices, and it is therefore the coefficients which describe the restriction to S_k in terms of the irreducible representations of S_k are polynomials in n. It follows that the characters

$V(w)_n$ are polynomials in n. Exploiting this fact, the authors of [13] show that polynomial stability is a feature of finitely generated FI modules. In this chapter, the usefulness of this polynomial property is simply the observation that the coefficients that appear in our lifts are polynomials in n, and thus, in particular, we may simultaneously lift a representation to S_n for every $n \geq k$.

An example of a lifting procedure:

Consider the irreducible representation $p_5 = \ydiagram{3,2} \in R(S_5)$. We first attach on $n-5$ boxes to the top row of p_5 to get a Young diagram p_n, say the representation $p_9 = \ydiagram{7,2}$ for S_9. By restricting this representation, we obtain one copy of p_5 as well as other representations over S_5:

(•) There are $\binom{n-5}{1}$ ways of obtaining $v_5 = \ydiagram{4,1}$ (since we may choose one step out of $n-5$ steps to remove a box from the second row)

(•) And similarly, there are $\binom{n-5}{2}$ ways of of getting the trivial representation t_5. Thus, p_5 lifts to

$$\begin{aligned}
\tilde{p_5} &= p_n - \binom{n-5}{1}\tilde{v_5} - \binom{n-5}{2}\tilde{t_5} \\
&= p_n - (n-5)(v_n - (n-5)t_n) - \frac{(n-5)(n-6)}{2}t_n \\
&= p_n - (n-5)v_n + \frac{1}{2}(n-5)(n-4)t_n
\end{aligned}$$

where we have used that $\tilde{v_5} = v_n - (n-5)t_n$, which can be checked easily since $\mathrm{Res}(v_n) = t_{n-1} + v_{n-1}$.

Note that there are also other ways to obtain the lift of p_5. The lift of $v_5 \in R(S_5)$ to S_n is

given by

$$\tilde{v}_5 = v_n - (n-5)\tilde{t}_5$$

where $\tilde{t}_5$ is the unique lift of the trivial character t_5. The lift of $p_5 \in R(S_5)$ to S_n can be obtained as:

$$\tilde{p}_5 = p_n - (n-5)\tilde{v}_5 - \binom{n-5}{2}\tilde{t}_5 = p_n - (n-5)v_n + \frac{1}{2}(n-5)(n-4)t_n$$

It should be clear from this example that we can simultaneously lift a representation of S_k to every S_n.

Formula for δ_e

Let us turn our focus to computing the character column at the identity $\delta_e = \mathbb{C}[S_n] = \sum_u \dim(u)u \in R(S_n)$. Observe that $e \in S_1$, and there is only one representation of S_1, the trivial representation $t_1 \in R(S_1)$, which lifts to $t \in R(S_n)$. (We will frequently commit these kinds of notational abuse, where we denote representations $w_n \in R(S_n)$ as simply w.) Since $\chi_t(e) = 1$, we therefore conclude from the above formula that:

$$\delta_e = X(X-1)...(X-(n-1)+1)t = X(X-1)...(X-(n-2))t$$

Remark: If we think of $X = \mathrm{Ind}(t)$ and think of the above as tensor products, we may notice that tensoring with the trivial representation does nothing, and so one might rewrite the above as:
$\delta_e = X(X-1)...(X-(n-1)+1)t = X(X-1)...(X-(n-2))$. However, one should be careful to not interpret the above as a matrix. It is a vector. To avoid confusion, we will therefore stick to the first convention.

Formula for $\delta_{(12)}$

$(12) \in S_2 \hookrightarrow S_n$, and S_2 has two representations t_2 and s_2. t_2 lifts to t and s_2 lifts to s. Moreover, $\chi_{t_2}((12)) = 1$ and $\chi_{s_2}((12)) = -1$. We therefore see that the character column of S_n that corresponds to the conjugacy class of (12) is:

$$\delta_{(12)} = X(X-1)...(X-(n-3))(t-s)$$

Formula for $\delta_{(123)}$

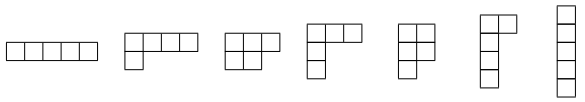
$(123) \in S_3 \hookrightarrow S_n$, and S_3 has three representations t_3, s_3, and v_3. t_3 lifts to t, s_3 lifts to s, and v_3 lifts to $v-(n-3)t$ (since $\mathrm{Res}(v_n) = t_{n-1} + v_{n-1}$). Observe that to compute the lift of v_3, we made use of our systematic lifting procedure. Observe that for representations of S_3, $\chi_{t_3}(123) = \chi_{s_3}(123) = 1$, and $\chi_{v_3}(123) = -1$. Thus,

$$\begin{aligned}\delta_{(123)} &= X(X-1)...(X-(n-4))(t+s-(v-(n-3)t)) \\ &= X(X-1)...(X-(n-4))((n-2)t+s-v)\end{aligned}$$

Formula for $\delta_{(12345)}$

Rather than going systematically, we thought it might be more instructive to provide one example of a "slightly larger conjugacy class". $(12345) \in S_5 \hookrightarrow S_n$. The representations of

S_5 and their respective abbreviations are given as follows:



t_5 v_5 p_5 $\wedge^2_5$ s_5p_5 s_5v_5 s_5

For each of these representations, we get a representation of S_n by stacking $n-5$ boxes to the top row of the Young diagram, and we will abuse notation a little by abbreviating representations of S_n, see Table 2.1 for further details.

Our first step is to compute lifts. Define $R(S_5)_{\geq 0} := \{\text{irreps } w \text{ of } S_5 \,|\, \chi_w(12) \geq 0\}$. For $w \in R(S_5)_{\geq 0}$, we will lift w via our systematic lifting procedure. For any other representation w' over S_5, we may observe that $s_5 w' \in R(S_5)_{\geq 0}$ and $\tilde{w'} = s_5 \cdot (\tilde{s_5 w'})$. We then obtain the lifts of representations as shown in Table 2.2.

Representation	**Lift**
t_5	t
v_5	$v-(n-5)t$
p_5	$p-(n-5)v+\frac{1}{2}(n-5)(n-4)t$
$\wedge^2_5$	$\wedge^2-(n-5)v+\frac{1}{2}(n-5)(n-4)t$
s_5p_5	$sp-(n-5)sv+\frac{1}{2}(n-5)(n-4)s$
s_5v_5	$sv-(n-5)s$
s_5	s

Table 2.2: Table of lifts for representations of S_5

From the character table for S_5, we know that $\chi_{t_5}(12345) = \chi_{s_5}(12345) = \chi_{\wedge^2_5}(12345) = 1$, $\chi_{p_5}(12345) = \chi_{s_5p_5}(12345) = 0$, $\chi_{v_5}(12345) = \chi_{s_5v_5}(12345) = -1$. Therefore,

$$\sum_{\text{irreps } w \text{ of } S_5} \chi_w(12345)\tilde{w}$$
$$= t + s + \wedge^2 - (n-5)v + \frac{1}{2}(n-5)(n-4)t - (v - (n-5)t) - (sv - (n-5)s)$$
$$= \frac{1}{2}(n-3)(n-4)t - (n-4)v + \wedge^2 - sv + (n-4)s$$

Therefore:

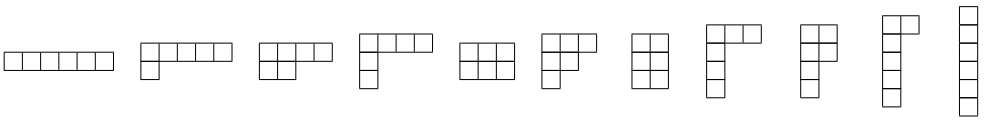
$$\delta_{(12345)} = X(X-1)...(X-(n-6))(\frac{1}{2}(n-3)(n-4)t - (n-4)v + \wedge^2 - sv + (n-4)s)$$

Table of formulae for character columns coming from permutations in S_k for $k \leq 5$

Table 2.3 summarizes what have done, and provides the formula for δ_τ for all permutations $\tau \in S_k$ for $k \leq 5$.

Computing the character column $\delta_{(123)}$ of S_6

In this example, we explicitly compute the character column $\delta_{(123)}$ of S_6. The representations of S_6 and the corresponding abbreviations are given as follows.



t_6 v_6 p_6 $\wedge^2_6$ b_6 r_6 s_6b_6 $s_6\wedge^2_6$ s_6p_6 s_6v_6 s_6

Consider the McKay graph $\mathbb{M}(S_6, X)$, which describes the irreducible decomposition of tensor products of representations of S_6. The vertices of the graph $\mathbb{M}(G, V)$ are the

Permutation τ	**Formula for** δ_τ (for every $n > k$)
e	$X(X-1)...(X-(n-2))t$
(12)	$X(X-1)...(X-(n-3))(t-s)$
(123)	$X(X-1)...(X-(n-4))((n-2)t+s-v)$
(12)(34)	$X(X-1)...(X-(n-5))((n^2-5n+5)t-(2n-7)v+2p-sv+(n-4)s)$
(1234)	$X(X-1)...(X-(n-5))((n-3)(t-s)-(v-sv))$
(123)(45)	$X(X-1)...(X-(n-6))(\frac{(n-3)(n-4)}{2}(t-s)-(n-4)(v-sv)+(p-sp))$
(12345)	$X(X-1)...(X-(n-6))(\frac{(n-3)(n-4)}{2}t-(n-4)v+\wedge^2-sv+(n-4)s)$

Table 2.3: Table of formulae for character columns obtained from permutations in $S_k \leq S_5$

irreducible representations of G, and the number of edges from U to W are $\langle U \otimes V, W \rangle$. The McKay graph serves as a visual aid for constructing the matrix $X = \operatorname{Ind}\operatorname{Res}$. In addition, counting paths and estimating numbers of paths on the McKay graph might play a crucial role in combinatorial or probabilistic extensions of this chapter.

We may easily construct the McKay graph $\mathbb{M}(S_6, X)$ using the Branching Rule. For example,

$$\operatorname{Ind}\operatorname{Res}(\ydiagram{3,2,1}) = \operatorname{Ind}(\ydiagram{3,2} + \ydiagram{4,1}) = (\ydiagram{3,2,1} + \ydiagram{3,3} + \ydiagram{3,2,1}) + (\ydiagram{5,1} + \ydiagram{4,2} + \ydiagram{4,1,1})$$

and therefore, $Xp_6 = 2p_6 + v_6 + b_6 + \wedge^2_6 + r_6$. The reader may verify that we obtain the following graph as shown in Figure 2.1, where the subscripts indicating that these are representations over S_6 are abbreviated.

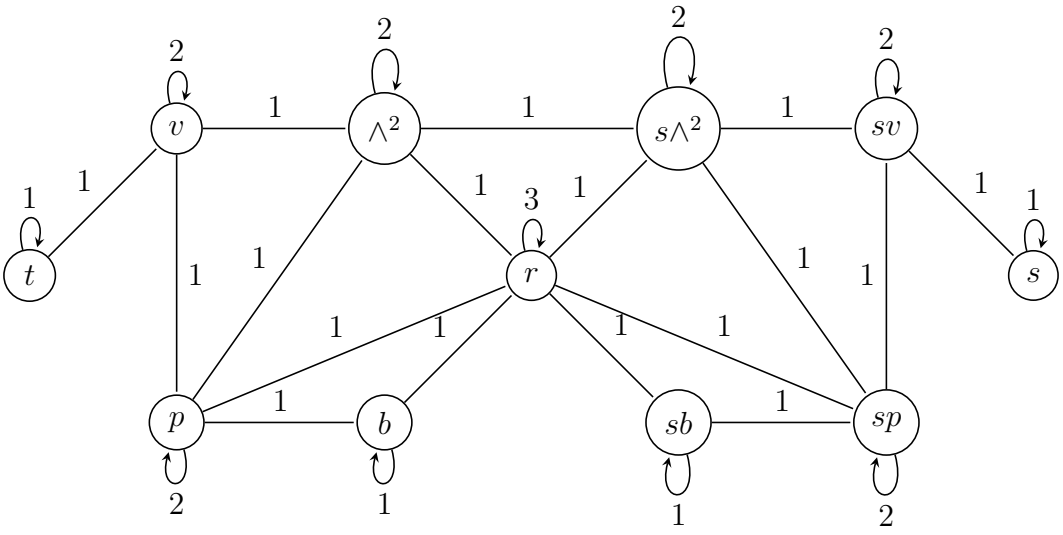


Figure 2.1: McKay graph $\mathbb{M}(S_6, X)$

X is then the following transition matrix of the Mckay graph:

$$X = \begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 2 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 3 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1
\end{pmatrix}$$

Theorem 2.3.1 thus implies that:

$$\begin{aligned}\delta_{(123)} &= X(X-1)....(X-(n-4))((n-2)t+s-v) \\ &= X(X-1)....(X-(n-4)) \times \begin{pmatrix} n-2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}^T\end{aligned}$$

Substituting the matrix X, we derive the character column of the conjugacy class (123) for S_6:

$$\delta_{(123)} = \begin{pmatrix} 1 & 2 & 0 & 1 & -1 & -2 & -1 & 1 & 0 & 2 & 1 \end{pmatrix}^T$$

2.4.2 Chains of wreath products

Let H be a finite group. We give a quick review of the representation theory of wreath products $H^n \rtimes S_n$. We will introduce notation which, in our opinion, is both conceptually clear and computationally ideal. We refer the reader to [5], [34], [37], and [53] for more details. A representation of the wreath product $H^n \rtimes S_n$ is denoted by a $2 \times d$ array

$$\begin{pmatrix} U_1 & U_2 & ... & U_d \\ \lambda_1 & \lambda_2 & ... & \lambda_d \end{pmatrix} := \mathrm{Ind}_{H^n \rtimes (S_{k_1} \times \cdots \times S_{k_d})}^{H^n \rtimes S_n} (U_1^{\otimes k_1} \otimes \lambda_1) \otimes \cdots \otimes (U_d^{\otimes k_d} \otimes \lambda_d),$$

where U_i is an irreducible representation of H, and λ_i is a representation of S_{k_i}. The specific order of the irreducible representations $\{U_i\}_{i=1}^n$ of H is fixed. The irreducible representations of the wreath product $H^n \rtimes S_n$ can be denoted by:

$$\left\{ \begin{pmatrix} U_1 & U_2 & ... & U_d \\ \lambda_1 & \lambda_2 & ... & \lambda_d \end{pmatrix} | \{U_i\}_{i=1}^d \text{ are distinct irreps of } H, \lambda_i \text{ is an irrep of } S_{k_i} \text{ for each } i \right\}$$

.

The action of $H^n \rtimes S_n$ on the array $\begin{pmatrix} U_1 & U_2 & ... & U_d \\ \lambda_1 & \lambda_2 & ... & \lambda_d \end{pmatrix}$ is as follows: H^n and $S_{k_1} \times ... \times S_{k_d}$ both act on $U_1 \otimes U_2 \otimes .. \otimes U_d$; H^n acts on each factor and $S_{k_1} \times ... \times S_{k_d}$ permutes the factors according to the representation $\lambda_1 \otimes ... \otimes \lambda_d$ (Note that λ_i is a representation of S_{k_i} for each i).

The branching rule, which plays a crucial role for us, is easy to state using our array notation:

$$\text{Ind}\left(\begin{pmatrix} U_1 & U_2 & ... & U_d \\ \lambda_1 & \lambda_2 & ... & \lambda_d \end{pmatrix} \right) = \sum_{i=1}^{d} \dim(U_i) \cdot \begin{pmatrix} U_1 & ... & U_i & ... & U_d \\ \lambda_1 & ... & \text{Ind}(\lambda_i) & ... & \lambda_d \end{pmatrix}$$

$$\text{Res}\left(\begin{pmatrix} U_1 & U_2 & ... & U_d \\ \lambda_1 & \lambda_2 & ... & \lambda_d \end{pmatrix} \right) = \sum_{i=1}^{d} \dim(U_i) \cdot \begin{pmatrix} U_1 & ... & U_i & ... & U_d \\ \lambda_1 & ... & \text{Res}(\lambda_i) & ... & \lambda_d \end{pmatrix}$$

We recall that the irreducible representations of S_n are represented by Young diagrams. The branching rules for induction and restriction are given by adding or removing a box from the given diagram.

The reader should take note that there is a subtle point in the above rule: namely that we may restrict a Young diagram with only 1 box to a Young diagram with 0 boxes, and

thereby removing the corresponding column. Likewise, when inducing a representation whose Young diagram does not have a full set of columns, we may add additional columns of boxes where necessary. Adopting these notations, one can prove the following two facts about chains of wreath products, the proof of which we omit.

Proposition 2.4.2. *Let H be any finite group.*

(a) *The chain $\{H^n \rtimes S_n\}_{n\in\mathbb{N}}$ is a surjective chain.*

(b) *The chain $\{H^n \rtimes S_n\}_{n\in\mathbb{N}}$ satisfies the Heisenberg algebra property with scaling $|H|$.*

For any group H, it is well known that the chain of wreath products $\{H^n \rtimes S_n\}_{n\in\mathbb{N}}$ satisfies the Heisenberg algebra property with scaling $|H|$. It should be noted that the only known examples of chains of groups that satisfy the Heisenberg algebra property are chains of wreath products. It is proved in [18] that if $M = 1$ or M is prime, then the only such chains are chains of wreath products. It is further conjectured in [18] that the only such chains are chains of wreath products for M arbitrary.
The statement of the main results can be applied to chains of wreath products as follows:

Theorem 2.4.3. *Let H be any finite group. Let $X = \operatorname{Ind}\operatorname{Res} = \operatorname{Ind}(t)\otimes$ be the* $\operatorname{Ind}\operatorname{Res}$ *operator on the chain of wreath products $\{H^n \rtimes S_n\}$.*

(a) *The polynomial f_l is given by*

$$f_l(X) = X(X - |H|)(X - 2|H|)...(X - (l-1)|H|)$$

(b) *The non-identity character values of* $\operatorname{Ind} t$ *in the wreath product $H^n \rtimes S_n$ is the set $\{0, |H|, \cdots, (n-1)|H|\}$.*

(c) *Let $\alpha \in H^k \rtimes S_k \hookrightarrow H^{k+l} \rtimes S_{k+l}$, and let $\delta_\alpha \in R(H^{k+l} \rtimes S_{k+l})$ be the character column of α, that is: $\delta_\alpha = \sum_{irreps\ u\ of\ H^{k+l} \rtimes S_{k+l}} \chi_u(\alpha)u$. For each representation w of G_k, let*

$\tilde{w}$ denote a lift to G_{k+l}, i.e an element of $R(G_{k+l})$ such that $\mathrm{Res}^l(\tilde{w}) = w$. Then:

$$\delta_\alpha = \mathrm{Ind}\,\mathrm{Res}(\mathrm{Ind}\,\mathrm{Res} - |H|)(\mathrm{Ind}\,\mathrm{Res} - 2|H|)...(\mathrm{Ind}\,\mathrm{Res} - (l-1)|H|)\left(\sum_{irreps\ w\ of\ H^k \rtimes S_k} \chi_w(\alpha)\cdot\tilde{w}\right)$$

A systematic lifting procedure for wreath product representations

As shown for chains of symmetric groups, we begin with a blueprint of the systematic lifting of representations for chains of wreath products.

(a) For a Young diagram λ let $B(\lambda)$ denote the number of boxes of λ and let $B'(\lambda)$ denote the number of boxes of λ below the top row.
(b) Define the partial ordering $<$ on the irreducible representations of $H^k \rtimes S_k$ by the following rule:

$$\begin{pmatrix} U_1 & U_2 & ... & U_d \\ \lambda_1 & \lambda_2 & ... & \lambda_d \end{pmatrix} < \begin{pmatrix} U_1 & U_2 & ... & U_d \\ \mu_1 & \mu_2 & ... & \mu_d \end{pmatrix}$$ if either of the following holds:

(1) $B'(\lambda_1) < B'(\mu_1)$ and $B(\lambda_i) \leq B(\mu_i)$ for all $i \geq 2$.

(2) $B'(\lambda_1) \leq B'(\mu_1)$, $B(\lambda_i) \leq B(\mu_i)$ for all $i \geq 2$, and $B(\lambda_i) < B(\mu_i)$ for at least one $i \geq 2$.

where a subtle point is that we allow $\mu_i = 0$ or $\lambda_i = 0$ (the Young diagram with 0 boxes), since the branching rule of representations of symmetric groups allows us to restrict a Young diagram with only one box to obtain the Young diagram with 0 boxes, which corresponds to removing the corresponding column.
(c) We begin with a representation $w = \begin{pmatrix} U_1 & U_2 & ... & U_d \\ \mu_1 & \mu_2 & ... & \mu_d \end{pmatrix}$ of $H^k \rtimes S_k$. Extend the first row of μ_1 by attaching $n-k$ boxes to the first row, and call the resulting Young diagram

μ_1'. Consider the element

$$w' = \frac{1}{\dim(U_1)^{n-k}} \begin{pmatrix} U_1 & U_2 & ... & U_d \\ \mu_1' & \mu_2 & ... & \mu_d \end{pmatrix} \in R(H^n \rtimes S_n)$$

(d) Observe that $\mathrm{Res}^{n-k}(w')$ contains exactly one copy of w in its decomposition, corresponding to removing the boxes in the first row of μ_1.

(e) Observe that all of the other representations of S_k that appear $\mathrm{Res}^{n-k}(u')$ are $< w$ with respect to the ordering in (a)

(f) We therefore can apply an inductive process using $<$.

An example to illlustrate the procedure above:

Let 1 and -1 be the representations of $\mathbb{Z}/2\mathbb{Z}$. Denote by t_i and s_i the trivial and the sign representations of S_i. We will lift the representation $\begin{pmatrix} 1 & -1 \\ t_1 & t_1 \end{pmatrix} \in R(\left(\mathbb{Z}/2\mathbb{Z}\right)^2 \rtimes S_2)$ to $R(\left(\mathbb{Z}/2\mathbb{Z}\right)^n \rtimes S_n)$ via our systematic lifting procedure. The first step is to consider the representation $\begin{pmatrix} 1 & -1 \\ t_{n-1} & t_1 \end{pmatrix} \in R(\left(\mathbb{Z}/2\mathbb{Z}\right)^n \rtimes S_n)$, and observe that:

$$\mathrm{Res}^{n-2} \begin{pmatrix} 1 & -1 \\ t_{n-1} & t \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ t_1 & t_1 \end{pmatrix} + (n-2) \begin{pmatrix} 1 \\ t_2 \end{pmatrix}$$

since there are $\binom{n-2}{1} = (n-2)$ ways to remove a box from the second column (one way for each step).

Since $\begin{pmatrix} 1 \\ t_2 \end{pmatrix}$ is the trivial representation, which lifts to the trivial representation $\begin{pmatrix} 1 \\ t_n \end{pmatrix}$, we conclude that:

$$\begin{pmatrix} 1 & -1 \\ t_1 & t_1 \end{pmatrix} \text{ lifts to } \begin{pmatrix} 1 & -1 \\ t_{n-1} & t_1 \end{pmatrix} - (n-2)\begin{pmatrix} 1 \\ t_n \end{pmatrix}$$

Character columns of $(\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n$

We will let ± 1 denote both the elements and the representations of the group $\mathbb{Z}/2\mathbb{Z}$, but it will be clear when we are referring to which. As before, denote by t_i and s_i the trivial and the sign representations of S_i. $\mathbb{Z}/2\mathbb{Z} \rtimes S_1 \cong \mathbb{Z}/2\mathbb{Z}$ has two representations, $\begin{pmatrix} 1 \\ t_1 \end{pmatrix}$ and $\begin{pmatrix} -1 \\ t_1 \end{pmatrix}$. The representation $\begin{pmatrix} 1 \\ t_1 \end{pmatrix}$ is the trivial representation which lifts to the trivial representation $\begin{pmatrix} 1 \\ t_n \end{pmatrix} \in R((\mathbb{Z}/2\mathbb{Z})^n \rtimes S_n)$. $\begin{pmatrix} -1 \\ t_1 \end{pmatrix}$ lifts to $\begin{pmatrix} -1 \\ t_n \end{pmatrix}$.

The characters of representations of $\mathbb{Z}/2\mathbb{Z} \rtimes S_1$ are:

$$\chi_{\begin{pmatrix} 1 \\ t_1 \end{pmatrix}}((1), e) = \chi_{\begin{pmatrix} 1 \\ t_1 \end{pmatrix}}((-1), e) = \chi_{\begin{pmatrix} -1 \\ t_1 \end{pmatrix}}((1), e) = 1$$

$$\chi_{\begin{pmatrix} -1 \\ t_1 \end{pmatrix}}((-1), e) = -1$$

Therefore,

$$\delta_e = X(X-2)(X-4)...(X-2(n-2))\left(\begin{pmatrix}1\\t_n\end{pmatrix}+\begin{pmatrix}-1\\t_n\end{pmatrix}\right)$$

$$\delta_{((-1,1,1,...,1),e)} = X(X-2)(X-4)...(X-2(n-2))\left(\begin{pmatrix}1\\t_n\end{pmatrix}-\begin{pmatrix}-1\\t_n\end{pmatrix}\right)$$

To obtain character columns $\delta_{((-1,-1,1,...,1),e)}$, $\delta_{((1,1,1,...,1),(12))}$, and $\delta_{((-1,1,1,...,1),(12))}$, we refer to the character table of $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2$, given as in Table 2.4.

	e	$((-1,1),e)$	$((-1,-1),e)$	$((1,1),(12))$	$((-1,1),(12))$
$\begin{pmatrix}1\\t_2\end{pmatrix}$	1	1	1	1	1
$\begin{pmatrix}1 & -1\\t_1 & t_1\end{pmatrix}$	2	0	-2	0	0
$\begin{pmatrix}1\\s_2\end{pmatrix}$	1	1	1	-1	-1
$\begin{pmatrix}-1\\t_2\end{pmatrix}$	1	-1	1	1	-1
$\begin{pmatrix}-1\\s_2\end{pmatrix}$	1	-1	1	-1	1

Table 2.4: Character table for $(\mathbb{Z}/2\mathbb{Z})^2 \rtimes S_2$

Given any one dimensional representation U of H, the branching rule of representations of wreath products imply that $\begin{pmatrix}U\\t_k\end{pmatrix} \in R(H^k \rtimes S_k)$ lifts to $\begin{pmatrix}U\\t_n\end{pmatrix} \in R(H^n \rtimes S_n)$ and

$\begin{pmatrix} U \\ s_k \end{pmatrix} \in R(H^k \rtimes S_k)$ lifts to $\begin{pmatrix} U \\ s_n \end{pmatrix} \in R(H^n \rtimes S_n)$. Therefore, all lifts except for the lift of $\begin{pmatrix} 1 & -1 \\ t_1 & t_1 \end{pmatrix}$ can be obtained. This can be done via the proposed systematic lifting procedure, and we obtain that $\begin{pmatrix} 1 & -1 \\ t_1 & t_1 \end{pmatrix}$ lifts to $\begin{pmatrix} 1 & -1 \\ t_{n-1} & t_1 \end{pmatrix} - (n-2)\begin{pmatrix} 1 \\ t_n \end{pmatrix}$.

Therefore, we have:

$$\begin{aligned}
&\delta_{((-1,-1,1,\ldots,1),e)} \\
&= X(X-2)\ldots(X-2(n-3)) \cdot \left[(2n-3)\begin{pmatrix} 1 \\ t_n \end{pmatrix} - 2\begin{pmatrix} 1 & -1 \\ t_{n-1} & t_1 \end{pmatrix} + \begin{pmatrix} 1 \\ s_n \end{pmatrix} + \begin{pmatrix} -1 \\ t_n \end{pmatrix} + \begin{pmatrix} -1 \\ s_n \end{pmatrix} \right]
\end{aligned}$$

$$\delta_{((1,1,1,\ldots,1),(12))} = X(X-2)\ldots(X-2(n-3)) \cdot \left[\begin{pmatrix} 1 \\ t_n \end{pmatrix} - \begin{pmatrix} 1 \\ s_n \end{pmatrix} + \begin{pmatrix} -1 \\ t_n \end{pmatrix} - \begin{pmatrix} -1 \\ s_n \end{pmatrix} \right]$$

$$\delta_{((-1,1,1,\ldots,1),(12))} = X(X-2)\ldots(X-2(n-3)) \cdot \left[\begin{pmatrix} 1 \\ t_n \end{pmatrix} - \begin{pmatrix} 1 \\ s_n \end{pmatrix} - \begin{pmatrix} -1 \\ t_n \end{pmatrix} + \begin{pmatrix} -1 \\ s_n \end{pmatrix} \right]$$

Character columns of $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$

We compute character columns of $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$ for $\delta_e, \delta_{((-1,1,1),e)}$, $\delta_{((-1,-1,1),e)}$, $\delta_{((1,1,1),e)}$, and $\delta_{((-1,1,1),(12))}$ as an example. Using the branching rule, we compute the matrix X can be written as follows with respect to the following basis of irreducible representations:

$$\left\{\begin{pmatrix}1\\t_3\end{pmatrix},\begin{pmatrix}1\\s_3\end{pmatrix},\begin{pmatrix}1\\v_3\end{pmatrix},\begin{pmatrix}1&-1\\t_2&t_1\end{pmatrix},\begin{pmatrix}1&-1\\s_2&t_1\end{pmatrix},\begin{pmatrix}1&-1\\t_1&t_2\end{pmatrix},\begin{pmatrix}1&-1\\t_1&s_2\end{pmatrix},\begin{pmatrix}-1\\t_3\end{pmatrix},\begin{pmatrix}-1\\s_3\end{pmatrix},\begin{pmatrix}-1\\v_3\end{pmatrix}\right\}$$

$$X=\begin{pmatrix}1&0&1&1&0&0&0&0&0&0\\0&1&1&0&1&0&0&0&0&0\\1&1&2&1&1&0&0&0&0&0\\1&0&1&2&1&1&1&0&0&0\\0&1&1&1&2&1&1&0&0&0\\0&0&0&1&1&2&1&1&0&1\\0&0&0&1&1&1&2&0&1&1\\0&0&0&0&0&1&0&1&0&1\\0&0&0&0&0&0&1&0&1&1\\0&0&0&0&0&1&1&1&1&2\end{pmatrix}$$

We then have:

$$\begin{aligned}\delta_e &= X(X-2)\times\begin{pmatrix}1&0&0&0&0&0&0&1&0&0\end{pmatrix}^T\\&=\begin{pmatrix}1&1&2&3&3&3&3&1&1&2\end{pmatrix}^T\end{aligned}$$

$$\begin{aligned}\delta_{((-1,1,1),e)} &= X(X-2)\begin{pmatrix}1&0&0&0&0&0&0&-1&0&0\end{pmatrix}^T\\&=\begin{pmatrix}1&1&2&1&1&-1&-1&-1&-1&-2\end{pmatrix}^T\end{aligned}$$

$$\delta_{((-1,-1,1),e)} = X \times \begin{pmatrix} 3 & 1 & 0 & -2 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}^T$$
$$= \begin{pmatrix} 1 & 1 & 2 & -1 & -1 & -1 & -1 & 1 & 1 & 2 \end{pmatrix}^T$$

$$\delta_{((1,1,1),(12))} = X \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \end{pmatrix}^T$$
$$= \begin{pmatrix} 1 & -1 & 0 & 1 & -1 & 1 & -1 & 1 & -1 & 0 \end{pmatrix}^T$$

$$\delta_{((-1,1,1),(12))} = X \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \end{pmatrix}^T$$
$$= \begin{pmatrix} 1 & -1 & 0 & 1 & -1 & -1 & 1 & -1 & 1 & 0 \end{pmatrix}^T$$

Chapter 3

On topological actions of the Temperley-Lieb monoids

This chapter is based on the paper [49].

The Temperley-Lieb algebra $\mathrm{TL}_n(\delta)$ specialized at $\delta = 1$ is an interesting monoid, which we will simply call TL_n. In this chapter, we will study topological actions of the chain of Temperley-Lieb monoids $\{\mathrm{TL}_n\}_{n\in\mathbb{N}}$. Given a CW-complex X, a topological action of TL_n on X is a map:

$$(\mathrm{TL}_n, \cdot) \mapsto (\mathrm{Hom}(X, X), \circ)$$

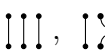
where $(\mathrm{Hom}(X, X), \circ)$ is of course the monoid of continuous maps from X to itself, under composition. Given a topological action $(\mathrm{TL}_n, \cdot) \mapsto (\mathrm{Hom}(X, X), \circ)$, the induced action on (co)homology is representation, i.e we get a map $\mathrm{TL}_n(1) \to \mathrm{End}(H_k(X))$ for any k. We will ultimately be able to explicitly deduce how homology groups of our space decompose as representations of the Temperley-Lieb monoids. The main theorem of this Chapter is Theorem 3.4.17, and does exactly this.

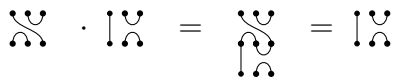
Once we understand topological actions, we also define representation stability and topological stability of the Temperley-Lieb monoid chain. Recall that a celebrated theorem in the foundational paper on FI modules (i.e [46] (Church, Ellenberg, Farb), Section 6) shows that the homology of configuration spaces is a finitely generated FI-module. Thinking of configuration spaces as the notion of topological stability for symmetric groups, we then prove an analogous result for the chain of Temperley-Lieb monoids.

3.1 Quick review: Temperley-Lieb algebras and their representation theory

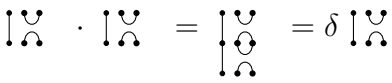
3.1.1 The definition of Temperley-Lieb algebras

The Temperley-Lieb algebra $\mathrm{TL}_n(\delta)$ is the algebra of all crossingless matchings from n points to n points, where multiplication is concatenation, circles are evaluated to $\delta \in$ some field $\mathbb{K}$, and addition is formal. In the current Chapter, since we are interested in monoids, we focus on the the case when $\delta = 1$.

For example, $\mathrm{TL}_3(\delta)$ is the algebra comprising of formal linear combinations of the elements:  . Multiplication is given by, for example:



and



$\mathrm{TL}_n(\delta)$ admits the very useful presentation given by:

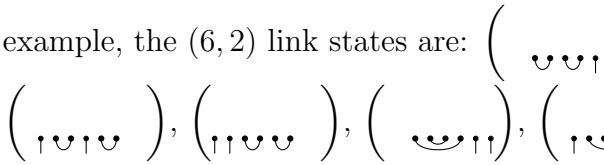
$$\begin{cases} u_i^2 = \delta \cdot u_i \text{ for all } i \in \{1, 2, ..., n-1\} & \text{(the idempotent relation)} \\ u_i u_{i+1} u_i = u_i \text{ for all } i \in \{1, 2, ..., n-2\} & \text{(the upper neighbor relation)} \\ u_i u_{i-1} u_i = u_i \text{ for all } i \in \{2, ..., n-1\} & \text{(the lower neighbor relation)} \\ u_i u_j = u_j u_i \text{ whenever } |i-j| \geq 2 & \text{(the long-distance relation)} \end{cases}$$

Here u_i the diagram which comprises of a single cup and cap at position i, and straight

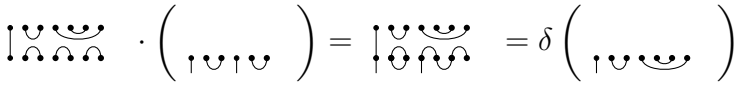
lines elsewhere. For example, $u_2 \in \mathrm{TL}_5$ is given by the diagram 

3.1.2 Link state representations of Temperley-Lieb algebras

Link state representations are an important class of representations of $\mathrm{TL}_n(\delta)$. When $\mathrm{TL}_n(\delta)$ is semisimple (i.e $\delta \neq q + q^{-1}$ for q a root of unity), then every representation of $\mathrm{TL}_n(\delta)$ is a direct sum of link-state representations. When δ is not semisimple, there are whole host of other representations, but we will not talk about these in this Subsection. The reader may refer to [7] (Belletete, Ridout, Saint-Aubin) for a classification of indecomposables. The reader may also refer to [44] for a more comprehensive treatment of link state representations.

For p an integer $\leq \frac{n}{2}$, an (n, p) link state is a collection p cups and $n - 2p$ lines. For example, the $(6, 2)$ link states are:  .

Let M_n be the set $\bigcup_{p=1}^{\lfloor \frac{n}{2} \rfloor} \{(n, p) \text{ link states}\}$. Abusing notation slightly, let us also let M_n denote the $\mathbb{K}$-linear span of that set. M_n admits an action of TL_n by concatenating an element of TL_n with a link state and evaluated any circles to δ. If $\delta = 1$, this becomes a well defined action on the set M_n. For the moment, we take δ arbitrary and present an example to illustrate the action:



M_n admits a natural filtration as follows: action by a Temperley-Lieb element can only increase the number of cups a link state has, it can never decrease the number of cups of a link state. For example, in the above example, the action increases the number of cups from 2 to 3. So, let $M_{n,p} = \bigcup_{q\geq p}^{\lfloor \frac{n}{2} \rfloor}\{(n,q) \text{ link states}\}$.

Then, TL_n action respects the filtration

$$M_{n,0} \supset M_{n,1} \supset M_{n,2} \supset ... \supset M_{n,\lfloor \binom{n}{2} \rfloor}$$

Therefore, it is natural to define the representations $V_{n,p} = M_{n,p} \Big/ M_{n,p+1}$ when $p < \lfloor \binom{n}{2} \rfloor$ and $V_{n,\lfloor \binom{n}{2} \rfloor} = M_{n,\lfloor \binom{n}{2} \rfloor}$. $\{V_{n,p}\}$ are then well defined representations of TL_n. The representation $V_{n,p}$ is called the standard representation of $\mathrm{TL}_n(\delta)$ of (n,p) link states. It is a fact that when $\mathrm{TL}_n(\delta)$ is semisimple (i.e $\delta \neq q + q^{-1}$ for q a root of unity), $\{V_{n,p}\}_{p\in\{0,1,2,...,\lfloor \binom{n}{2} \rfloor\}}$ form a complete set of irreducible representations of $\mathrm{TL}_n(\delta)$.

3.2 An example of a topological action

Consider three 3-tori, A_1, A_2 and A_3. We glue A_1 and A_3 along a copy of $S^1 \subset A_1, A_3$. We choose a point $*$ on this copy of S^1, and we glue A_2 to $*$. Call the resulting space X. Pictorially, the topological space we have constructed is as below:

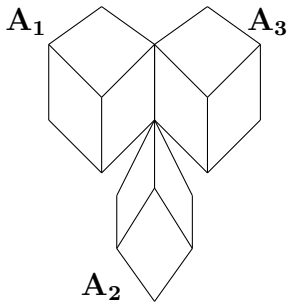


Figure 3.1: This space will admit an action of TL_4. The 3-tori A_1 and A_3 are glued together along a copy of S_1. The 3-torus A_2 is glued to a single point in that copy of S^1.

The above space admits an action of TL_4. TL_4 is generated by u_1, u_2, u_3 subject to the relations $u_1^2 = u_1$, $u_2^2 = u_2$, $u_3^2 = u_3$, $u_1u_2u_1 = u_1$, $u_3u_2u_3 = u_2$ and $u_2u_1u_2 = u_2u_3u_2 = u_2$. Now, we are going to let each u_i be a particular retraction onto A_i. The retractions are pictorially defined below:

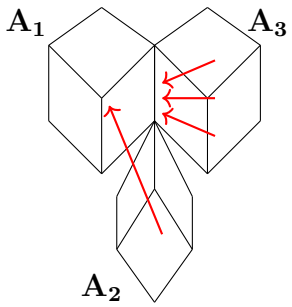


Figure 3.2: u_1 is a retraction onto A_1 where A_2 is mapped isomorphically in a way that preserves $*$, and A_3 is projected onto S_1

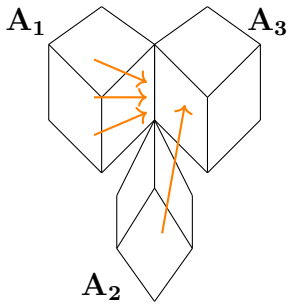


Figure 3.3: u_3 is a retraction onto A_3 where A_2 is mapped isomorphically in a way that preserves $*$, and A_1 is projected onto S_1

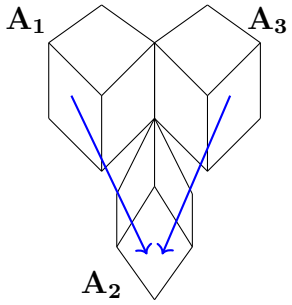
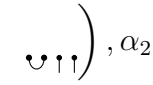
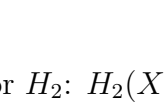
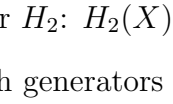


Figure 3.4: u_2 is a retraction onto A_2 where both A_1 and A_3 are mapped isomorphically in a way that preserves $*$, such that the isomorphism is the inverse of the corresponding isomorphisms induced by u_1 and u_3

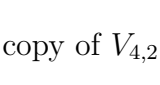
Since each u_i is a retraction, $u_i^2 = u_i$ for each i. Since the isomorphism that goes from A_2 to A_1 is the inverses of the isomorphism that goes from A_1 to A_2, we have that $u_1u_2u_1 = u_1 \circ id = u_1$. Likewise, we have that $u_3u_2u_3 = u_2$ and $u_2u_1u_2 = u_2u_3u_2 = u_2$. Thus, this is a well defined action of TL_4 on X.

Now, how does the homology of X decompose as representations of TL_n?

$H_3(X)$ is the easiest to see: it is three dimensional, spanned by classes α_1, α_2 and α_3, where

α_i is the class associated with A_i. Based on the action described above, we can see that $u_1\alpha_1 = u_1\alpha_2 = \alpha_1$, $u_1\alpha_3 = 0$, $u_2\alpha_1 = u_2\alpha_2 = u_2\alpha_3 = \alpha_2$, and $u_3\alpha_2 = u_3\alpha_3 = \alpha_3$ and $u_3\alpha_1 = 0$. Thus, as a TL_4 representation, $H_3(X) \cong V_{4,1}$, where the isomorphism is given by $\alpha_1 \mapsto$  , $\alpha_2 \mapsto$  , $\alpha_3 \mapsto$  .

Next for H_2: $H_2(X)$ has dimension 9, where $3 = \binom{3}{2}$ dimensions come from each 3-torus. For each generators $\alpha \in H_2(A_1)$, consider $u_2\alpha \in H_2(A_2)$ and $u_3u_2(\alpha) \in H_2(A_3)$. In a very similar spirit as we did for H_3, we can check that each such triple gives rise to a copy of $V_{4,1}$. Thus, we have that $H_2(X) \cong V_{4,1}^{\oplus 3}$ as a TL_4 representation.

Lastly, consider H_1, which is the most interesting of the three: The common copy of S^1 gives a common generator of $H_1(A_1)$ and $H_1(A_3)$. Call this generator α. $u_2\alpha \in H_1(A_2)$. The two dimensional vector space spanned by α and $u_2\alpha$ is closed under TL_4 action and gives a copy of $V_{4,2}$ under the isomorphism $\alpha \mapsto$  , $u_2\alpha \mapsto$. Other than this copy, there are two other generators of $H_1(A_1)$ and by applying isomorphisms and clubbing triples, we see that each such generator gives rise to a copy of $V_{4,1}$. We therefore conclude that $H_1(X) \cong V_{4,2} \oplus V_{4,1}^{\oplus 2}$.

Thus, to summarize, as TL_4 representations, homology groups decompose as:

$$H_3(X) \cong V_{4,1}$$

$$H_2(X) \cong V_{4,1}^{\oplus 3}$$

$$H_1(X) \cong V_{4,2} \oplus V_{4,1}^{\oplus 2}$$

3.3 Describing topological actions of Temperley-Lieb algebras

3.3.1 Topological translation of the Temperley-Lieb relations

The first natural step to study such an action would be to look at the relations of $(\mathrm{TL}_n, \cdot)$ (with respect to a natural presentation), and translate what these relations mean in topological language. We will use the most common presentation of $(\mathrm{TL}_n, \cdot)$, namely generated by $u_1, ..., u_{n-1}$ subject to the relations:

$$\begin{cases} u_i^2 = u_i \text{ for all } i \in \{1, 2, ..., n-1\} & \text{(the } \delta\text{-idempotent relation)} \\ u_i u_{i+1} u_i = u_i \text{ for all } i \in \{1, 2, ..., n-2\} & \text{(the upper neighbor relation)} \\ u_i u_{i-1} u_i = u_i \text{ for all } i \in \{2, ..., n-1\} & \text{(the lower neighbor relation)} \\ u_i u_j = u_j u_i \text{ whenever } |i-j| \geq 2 & \text{(the long-distance relation)} \end{cases}$$

We now will translate each of the three relations into topological language:

Lemma 3.3.1 (Translating the idempotent relation)**.** *Each u_i maps to a retraction map.*

Proof. The idempotents in $(\mathrm{Hom}(X, X), \circ)$ are precisely retractions. □

We will denote the retraction map by r_i, and the subspace onto which r_i retracts by A_i.

Lemma 3.3.2 (Translating the neighbor relation)**.** *$r_{i\pm1} \restriction_{A_i}: A_i \to A_{i\pm1}$ and $r_i \restriction_{A_{i\pm1}}: A_{i\pm1} \to A_i$ are homeomorphisms. Moreover, these two homeomorphisms are inverses of each other.*

Proof. The neighbor relation tells us that $u_i u_{i\pm1} u_i = u_i$, and this therefore, $r_i r_{i\pm1} r_i = r_i$. Since $r_i(x) = x$ for every $x \in A_i$, we conclude that for every $x \in A_i$ $r_i r_{i\pm1}(x) = x$. That is,

$r_i r_{i\pm1} = id_{A_i}$. This tells us that $r_i \restriction_{A_{i\pm1}}$ and $r_{i\pm1} \restriction_{A_i}$ are inverses of each other, and thus, in particular they are both homeomorphisms. □

Remark 3.3.3. It is natural to wonder whether Lemma 3.3.2 is equivalent to the neighbor relation, or whether it is a weaker statement. Even though we only needed to take $x \in A_i$, it turns out that Lemma 3.3.2 is in fact equivalent to the neighbor relation. The reason is that assuming the Lemma 3.3.2 holds, and given any $x \in X$, $r_i(x) \in A_i$ and thus, applying the Lemma to $r_c(x)$, we deduce that $r_i r_{i\pm1} r_i(x) = r_i(x)$. Since x was arbitrary, we deduce the Temperley-Lieb relation. This justifies the fact that we called it a translation.

Lemma 3.3.4 (Translating the long-distance relation)**.** *If $|i-j| \geq 2$, then $r_i \restriction A_j$ is a retraction onto $A_i \cap A_j$.*

Proof. The long-distance relation tells us that $u_i u_j = u_j u_i$. Therefore, $r_i r_j = r_j r_i$.
$r_i(x) \in A_i$ tautologically for every $x \in X$. Moreover, for $x \in A_j$,
$r_i \restriction_{A_j}(x) = r_i r_j(x) = r_j r_i(x) \in A_j$. Therefore, $r_i \restriction A_j$ is a retraction onto $A_i \cap A_j$. □

At this point, the reader should be able to form some kind of sketchy picture in their heads for how topological actions of Temperley-Lieb algebras behave.

3.3.2 The full intersection

In this Subsection we will describe properties of the full intersection $A_1 \cap A_2 \cap ... \cap A_{n-1}$. The main result of this Section is that any point in a neighbor intersection must in fact lie in the full intersection. This will serve as one of the key foundational stones for the rest of the chapter.

Lemma 3.3.5 (neighbor intersection = full intersection)**.** *Suppose that* $x \in A_i \cap A_{i+1}$. *Then, in fact,* $x \in A_1 \cap A_2 \cap ... \cap A_{n-1}$

Proof. By symmetry and induction, it suffices to show that $x \in A_{i+2}$. The trick now is to look at the "cycle map" $r_i r_{i+1} r_{i+2}$.

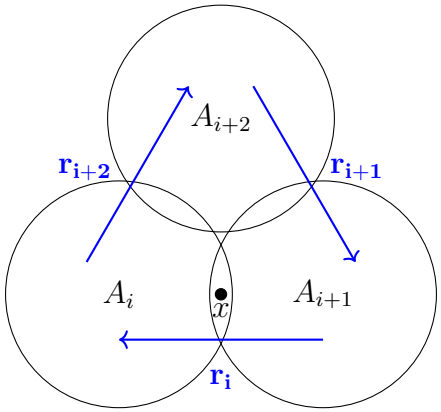


Figure 3.5: A schematic of the cycle map

Since $x \in A_i$, it follows by Lemma 3.3.4 that $r_{i+2}(x) \in A_i \cap A_{i+2}$. Therefore, on one hand, by Lemma 3.3.2

$$r_i r_{i+1} r_{i+2} x = (r_i r_{i+1})(r_{i+2}(x)) = id_{A_i} r_{i+2}(x) = r_{i+2}(x) \in A_{i+2}$$

On the other hand, by associativity of multiplication, Lemma 3.3.2, and the fact that $x \in A_{i+1}$

$$r_i r_{i+1} r_{i+2}(x) = r_i(r_{i+1} r_{i+2})(x) = r_i id_{A_{i+1}} x = r_i(x) = x$$

Therefore, comparing the two expressions,

$$x = r_{i+2}(x) \in A_{i+2}$$

□

A corollary of Lemma 3.3.5, stated and proved below, is that all the A_is must have some point in common. This is an important property that topological spaces carrying a TL_n action have. The reader might be able to use this property to rule out some of the sketchy pictures that have in their head.

Corollary 3.3.6 (Full intersection is nonempty)**.** *Let X a connected CW complex upon which TL_n acts. Then, $A_1 \cap ... \cap A_{n-1} \neq \emptyset$.*

Proof. Consider the subspaces $A_1 \cup A_3 \cup ...$ and $A_2 \cup A_4 \cup ...$ are closed spaces, since they are the unions of finitely many closed spaces.

By Lemma 3.3.5, if these spaces intersect, then $A_1 \cap ... \cap A_{n-1} \neq \emptyset$, and thus, if we suppose that the corollary were false, we must have that the subspaces $A_1 \cup A_3 \cup ...$ and $A_2 \cup A_4 \cup ...$ are disjoint. But then this is a separation of X via two closed subspaces, and so X is not connected, a contradiction. □

Throughout, we will denote the full intersection $A_1 \cap ... \cap A_{n-1}$ by Q, and it will play an important role going forward. We will see later that Q need not be a retract (Example 3.3.9).

3.3.3 Long-distance intersections of the same cardinality are isomorphic

By Lemma 3.3.5, every intersection is either the full intersection Q or is a long-distance intersection, i.e is of the form $A_{i_1} \cap ... \cap A_{i_d}$ where $|i_k - i_l| \geq 2$ for any $k \neq l$. The natural next step is to enquire about the structural properties of the collection of long-distance intersections. The Lemma that follows shows us that the homeomorphism class of a long-distance intersection only depends on the number of subspaces intersected.

Lemma 3.3.7 (Intersections of the same cardinality are homeomorphic)**.** *Let $i_1, .., i_m$ and $j_1, ..., j_m$ be such that $|i_k - i_l| \geq 2$, $|j_k - j_l| \geq 2$ for all k, l. Then,*

$$A_{i_1} \cap ... \cap A_{i_m} \cong A_{j_1} \cap ... \cap A_{j_m}$$

That is, the homeomorphism class of a long-distance intersection only depends on the number of spaces that intersect. Moreover, ordering indices so that $i_1 < ... < i_m$, this isomorphism from $A_1 \cap A_3 \cap A_5 ... \cap A_{2m-1}$ to $A_{i_1} \cap .. \cap A_{i_m}$ is explicitly given by the following map:

$$r_{i_1} r_{i_1 - 1} ... r_1 r_{i_2} r_{i_2 - 1} ... r_3 ... r_{i_m} r_{i_m - 1} ... r_{2m-1} \restriction_{A_1 \cap A_3 ... \cap A_{2m-1}} : A_1 \cap A_3 ... \cap A_{2m-1} \cong A_{i_1} \cap .. \cap A_{i_m}$$

Proof. Start with $A_1 \cap A_3 \cap ... \cap A_{2m-1}$. We will show that any $A_{i_1} \cap ... \cap A_{i_m}$ is homeomorphic to $A_1 \cap A_3 \cap ... \cap A_{2m-1}$. We order indices so that $i_1 < ... < i_m$. Then, observe that $i_m \geq 2m - 1$. Consider $r_{i_m} r_{i_m - 1} ... r_{2m-1}$. We claim that $r_{i_m} r_{i_m - 1} ... r_{2m-1} \restriction A_1 \cap A_3 \cap ... \cap A_{2m-1}$ is a homeomorphism from $A_1 \cap A_3 \cap ... \cap A_{2m-1}$ to $A_1 \cap A_3 \cap ... \cap A_{2m-3} \cap A_{i_m}$.

First, observe that the range is indeed correct: Analogous to the proof of Lemma 3.3.4, the

image of $r_{i_m}r_{i_m-1}...r_{2m-1} \restriction_{A_1\cap...\cap A_{2m-1}}$ is contained in each A_{2k-1} for $k < m$, since, for $x \in A_1 \cap ... \cap A_{2m-1}$,

$r_{i_m}r_{i_m-1}...r_{2m-1}(x) = r_{i_m}r_{i_m-1}...r_{2m-1}r_{2k-1}(x) = r_{2k-1}r_{i_m}r_{i_m-1}...r_{2m-1}(x) \in A_{2k-1}$.

Moreover, the image is contained in A_{i_m} since the image of r_{i_m} is A_{i_m}. In order to see that $A_1 \cap A_3 \cap ... \cap A_{2m-3} \cap A_{i_m}$ is the full image and that the map is a homeomorphism onto the image, we may write down the inverse, which is $r_{2m-1}r_{2m}...r_{i_m} \restriction_{A_1\cap A_3\cap...\cap A_{2m-3}\cap A_{i_m}}$. The reason why this is an inverse is that:

$$\begin{aligned} r_{2m-1}r_{2m}...r_{i_m}r_{i_m}r_{i_m-1}...r_{2m-1} &= r_{2m-1}r_{2m}...r_{i_m}^2 r_{i_m-1}...r_{2m-1} \\ &= r_{2m-1}r_{2m}...r_{i_m-1}r_{i_m}r_{i_m-1}...r_{2m-1} \\ &= r_{2m-1}r_{2m}...r_{i_m-2}r_{i_m-1}r_{i_m-2}...r_{2m-1} \\ &= ... \\ &= r_{2m-1}^2 \\ &= r_{2m-1} \end{aligned}$$

and $r_{2m-1} \restriction A_{2m-1} = id_{A_{2m-1}}$.

Therefore, we have shown that

$$A_1 \cap A_3 \cap ... \cap A_{2m-1} \cong A_1 \cap A_3 \cap ... \cap A_{2m-3} \cap A_{i_m}$$

Repeating this process by moving A_{2k-1} to i_k for $k < m-1, m-2$ etc.. we deduce that

$$A_1 \cap A_3 \cap ... \cap A_{2m-1} \cong A_{i_1} \cap ... \cap A_{i_m}$$

□

3.3.4 The filtration of retracts

Lemma 3.3.7 tells us that no particular intersection is special - the intersections are all homeomorphic to intersections of the form $A_1 \cap A_3 \cap ... \cap A_{2m-1}$. This motivates us to give importance to the following filtration:

Definition 3.3.8. (Filtration of retracts) Let X be a topological space upon which TL_n acts. We define the filtration of retracts associated to X, denoted by $\mathcal{F}(X)$ to be the filtration:

$$A_1 \supseteq A_1 \cap A_3 \supseteq ... \supseteq A_1 \cap A_3 \cap ... A_{2.\lceil \frac{n-1}{2} \rceil - 1} \supseteq Q$$

We will often denote $A_1 \cap A_3 \cap ... \cap A_{2p-1}$ by R_p

Each R_p in the above definition is a retract, and the retraction map is given by $r_1 r_3 r_5 .. r_{2p-1}$, as can be seen using the argument from the proof of Lemma 3.3.4. However, Q need not be a retract, as the following examples show:

Example 3.3.9. (Counterexamples to demonstrate that Q need not be a retract)

(1) For a simple counterexample, take $n = 3$, the filtration $S^2 \supset \{x, -x\}$, and consider glueing two copies of S^2 to each other via the two points $\{x, -x\}$. Then, this is a valid space upon which TL_3 acts: u_1 preserves the first copy of S^2 and sends the second copy of S^2 to the first copy isomorphically; likewise, u_2 preserves the second copy of S^2 and sends the second copy of S^2 to the first copy isomorphically. But $Q = \{x, -x\}$, which is not a retract of S^2 since it is disconnected.

(2) For a slightly more interesting example, take $n = 4$ and consider the filtration $T^2 \supset S^1 \supset \{x, -x\}$, where x and $-x$ are two antipodal points of S^1. We construct the space as follows: Let $A, B, C = T^2$. Glue C to A by identifying copies of S^1. Lastly, take two opposite points on the common equator of A and C, choose two points on B, and glue B to those two points via the two points on B. The action of TL_4 is as follows: u_1 preserves A, sends B isomorphically to A, and retracts C to S^1, u_2 sends both A and C isomorphically to B while preserving B, and u_3 preserves C, sends B isomorphically to C, and retracts A to S^1. Once again, $Q = \{x, -x\}$, which is not a retract of T^2.

Remark 3.3.10. The above filtration $\mathcal{F}$ is arguably the most important definition in this chapter, for two reasons:
(1) Theorem 3.4.17 will show that the representation structure of homology groups of a TL_n space will only depend on the filtration $\mathcal{F}$.
(2) $\mathcal{F}$ will provide us a natural way to define topological stability (Definition 3.5.12).

3.3.5 Wedging along Q

To get a better understanding of how TL_n actions look, we ignore "superfluous parts of our space upon which there is no action". To do this, we define the notion of a surjective action:

Definition 3.3.11 (Surjective action)**.** Let X be a space on which TL_n acts. Each u_i is sent to a retraction onto some subspace A_i. We say that the action is surjective if

$$X = \bigcup_{i=1}^{n-1} A_i$$

Equivalently, a surjective action is one, such that, for any $y \in X$, there exists some $x \in X$ and $a \in \mathrm{TL}_n$ such that $a \cdot x = y$, hence the name surjective.

We then observe that we may construct TL_n-spaces by taking $n-1$ copies of A, $A_1, .., A_{n-1}$ and glue them to one another in a suitable way. Note that by Corollary 3.3.6, the total intersection $A_1 \cap ... \cap A_{n-1} = Q \neq \emptyset$. Furthermore, note that by Lemma 3.3.5, the only nontrivial intersections other than the full intersection are long-distance intersections. We therefore may observe that:

Observation 3.3.12 (Wedging along Q)**.** Let X be a space on which TL_n acts. Then, X is a quotient

$$X \cong A_1 \vee_Q A_2 \vee_Q ... \vee_Q A_n \,/_\sim$$

where $\sim$ is a relation which does not involve neighbors A_i and A_{i+1} for any i. In the above statement, $\vee_Q$ denotes the wedge along Q, which is notation to describe the procedure of taking a disjoint union of copies of A and gluing them all along Q.

3.4 Homology groups as TL_n-representations

This Section is the most substantial part of the Chapter. We build up to and prove Theorem 3.4.17, which is the main theorem of this Chapter.

3.4.1 Topological lemmas

The goal of this Subsection is to prove the topological Lemmas which are required to prove Theorem 3.4.17. Before we start, we will remark that, given an intersection $A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_p}$ such that $|i_t - i_s| \geq 2$ for $t \neq s$, $A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_p}$ is a retract, and therefore $i_* : H_k(A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_p}) \to H_k(X)$ is an injection. In light of this, given

$\alpha \in H_k(X)$, we will use the shorthand notation $\alpha \in H_k(A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_p})$ to denote $\alpha \in i_* H_k(A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_p})$. Note that we cannot use such shorthand for Q because Q need not be a retract. With this notation in mind, we begin with a simple but important observation.

Observation 3.4.1 (Homology classes in commuting retractions must live in their intersection)**.** Let X be a space, and let $r : X \to R$, $r' : X \to R'$ be commuting retractions. Suppose that there is $\alpha \in H_k(R)$ and $\alpha' \in H_k(R')$ such that $\alpha \sim \alpha'$ (i.e they are homologous in X). Then, there is some $\beta \in R \cap R'$ such that $\alpha, \alpha' \sim \beta$.

Proof. Since r and r' commute, $r'r$ is a retraction onto $R \cap R'$ (Lemma 3.3.4). Therefore, observe that $(rr')_* \alpha \in H_k(R \cap R')$.

Moreover, since $\alpha \sim \alpha'$, $(rr')_* \alpha = (rr')_* \alpha' = r_*(r')_* \alpha' = r_* \alpha' = r_* \alpha = \alpha$. Therefore, we see that $\alpha \sim (rr')_* \alpha$. Setting $\beta = (rr')_* \alpha$, we are done. □

The next definition provides topological framework we will henceforth work in. In particular, it requires that each A_i is a finite CW-subcomplex. One might naively expect that any retract of a finite CW-subcomplex is a finite CW-subcomplex, but this is false. In fact, there are retracts of finite CW-complexes which are not even CW-complexes. If we ask for homotopy equivalences (allowing ourselves to push up the dimension if necessary), then every retract is homotopy equivalent to a countable CW-complex, but as far as finiteness goes the answer remains false, and the entire issue is quite subtle and is the subject of Wall's finiteness obstruction, which is an algebraic K-theoretic invariant (see for example [15] (Ferry, Ranicki) for a survey, or [59] (Wall) for the original paper). Therefore, to avoid topological subtleties (so our proofs flow smoothly), we set in stone a favorable topological framework once and for all:

Definition 3.4.2 (Topological framework in which we work)**.** We say that a space X is a finite-CW surjective TL_n-space if it is a finite CW-complex which admits a surjective action of TL_n, with the additional property that each A_i is a finite subcomplex.

Now, we will prove a crucial lemma of this chapter. Much of the topological content behind Theorem 3.4.17 is concentrated in the lemma below.

Lemma 3.4.3 (Homological version of "neighborhood intersection = full intersection")**.** *Let X be a finite-*CW *surjective* TL_n*-space. Suppose that $\alpha \in H_k(A_i)$ and $\alpha \in H_k(A_{i+1})$. Then, $\alpha \in i_* H_k(Q)$.*

Proof. Since $\alpha \in H_k(A_i), H_k(A_{i+1})$, it follows that $(u_i)_*\alpha = (u_{i+1})_*\alpha = \alpha$. By the proof of Lemma 3.3.5 (i.e via the "cycle map trick"), we may see that $(u_j)_*\alpha = \alpha$ for all j. This at least should make it believable that $\alpha \in i_* H_k(Q)$. However, to show this requires a little work, which we shall now do.

WLOG, suppose i is odd and $i+1$ is even. Let $\alpha_o = (u_i)_*\alpha \in H_k(A_i)$ and likewise let $\alpha_e = (u_{i+1})_*\alpha \in H_k(A_{i+1})$. The subscripts o and e denote "odd" and "even" respectively. Since $\alpha_o \sim \alpha_e$, there exists a $k+1$ cells $f_1 : D_1 \to X, .., f_m : D_m \to X$ and constants $\{c_j\}_{j=1}^m$ such that $\sum_{j=1}^m c_j \partial f_j(D_j) = \alpha_e - \alpha_o$. Since $X = \bigcup_i A_i$, We may further divide the disks D_j into three types:

(1) Those disks D_j such that $\partial f(D_j)$ is entirely contained in $A_1 \cup A_3 \cup A_5 \cup ...$

(2) Those disks D_j such that $\partial f(D_j)$ is entirely contained in $A_2 \cup A_4 \cup A_6 \cup ...$

(3) Those disks D_j such that $\partial f(D_j)$ is neither entirely contained in $A_1 \cup A_3 \cup A_5 \cup ...$ nor is entirely contained in $A_2 \cup A_4 \cup A_6 \cup ....$

Thus, we may write:

$$a_e - a_o = \sum_{j=1}^{m} c_j \partial f_j(D_j) = \sum_{j \text{ of type (1)}} c_j \partial f_j(D_j) + \sum_{j \text{ of type (2)}} c_j \partial f_j(D_j) + \sum_{j \text{ of type (3)}} c_j \partial f_j(D_j)$$

and therefore:

$$(a_e - \sum_{j \text{ of type (2)}} c_j \partial f_j(D_j)) - (a_o + \sum_{j \text{ of type (1)}} c_j \partial f_j(D_j)) = \sum_{j \text{ of type (3)}} c_j \partial f_j(D_j)$$

Now, notice that $(a_e - \sum_{j \text{ of type (2)}} c_j \partial f_j(D_j)) \sim a_e$ since the latter term consists of boundaries, and moreover is contained entirely in $A_2 \cup A_4 \cup A_6 \cup ....$ Likewise $(a_o + \sum_{j \text{ of type (1)}} c_j \partial f_j(D_j)) \sim a_o$ and is entirely contained in $A_1 \cup A_3 \cup A_5 \cup ....$ Thus, we may replace a_e with $(a_e - \sum_{j \text{ of type (2)}} c_j \partial f_j(D_j))$ and a_o with $(a_o + \sum_{j \text{ of type (1)}} c_j \partial f_j(D_j)) \sim a_o$. In this manner, we may therefore ignore terms of type (1) and (2) and assume that all disks are of type (3).

Thus, it remains to consider disks of type (3). To this end, let $f : D = D^{k+1} \to X$ be a disk of type (3). It will be useful for us to think about closures, and therefore set $D = D^{\bar{k}+1}$ and set $\bar{f} : \bar{D} \to X$. For notational simplicity, we will denote $\bar{f}$ simply by f. Consider $D_o := f^{-1}(A_1 \cup A_3 \cup A_5 \cup ....)$ and $D_e := f^{-1}(A_2 \cup A_4 \cup A_6 \cup ....)$. $f(D_o) = f(D) \cap (A_1 \cup A_3 \cup A_5 \cup ....)$ is the intersection of finite CW complexes (due to Definition 3.4.2), and is thus a finite CW complex. Similarly, $f(D_e)$ is a finite CW complex. Since f is a homeomorphism on the interior of D, and continuous on the boundary, we therefore have that D_o and D_e are finite CW complexes. In particular, $H_k(D_o), H_k(D_e), H_0(D_o), H_0(D_e)$ are all finitely generated, and this is the fact which we will use. For $D = D_j$, we will denote the corresponding odd and even parts by $D_o(j)$ and $D_e(j)$ respectively. Our strategy for the proof is then as follows:

- We will show that we may choose the $k+1$ cell $f : D^{k+1} \to X$ such that, if P is a

path component of D_o or D_e, then $H_k(P) = 0$.

- Consider the set $PC = \{P \mid P \text{ is a path component of either } D_o \text{ or } D_e\}$. For each $P \in PC$, we will consider $\alpha_P = f \restriction_{\partial D \cap P} \colon P \to X$, and we will observe that α_P can be viewed as an element of $H_k(X)$. Observe then that $f \restriction_{\partial D} = \sum_P \alpha_P$.

- We will show that each $\alpha_P \in i_* C_k(Q)$, where $C_*(Q)$ is the cellular chain complex of Q.

- Let $PC_o = \{P \mid P \text{ is a path component of } D_o\}$ and let $PC_e = \{P \mid P \text{ is a path component of } D_e\}$. We will note that $\alpha_e - \alpha_o = \sum_j \sum_{P \in PC_e(j)} \alpha_P + \sum_j \sum_{P \in PC_o(j)} \alpha_P$. Since each $\alpha_P = f \restriction_{\partial D \cap P}$, it then follows that $\alpha_e = \sum_j \sum_{P \in PC_e(j)} \alpha_P$ and likewise $\alpha_o = \sum_j \sum_{P \in PC_o(j)} \alpha_P$. Since each $\alpha_P \in i_* C_k(Q)$, we then have that $\alpha_e, \alpha_o \in i_* H_k(Q)$.

Let us now proceed to prove the Lemma via the strategy above. We first want to show that we may choose the $k+1$ cell $f : D^{k+1} \to X$ such that, if P is a path component of D_o or D_e, then $H_k(P) = 0$. The idea behind this fact is the following: if we suppose that there is a k-dimensional "hole", take a homology or homology class "surrounding this hole", and observe that this has a representative which lives in $D_o \cap D_e = f^{-1}Q$. This will allow us to "fill the hole". And by finiteness, we may "fill all the holes one by one". After "filling all the holes", the resulting P will have the property we desire. Now we begin the formal argument: WLOG let P be a path component of D_o. We have seen that $H_k(D_o)$ is finitely generated. By surjectivity of action, $D_o \cup D_e = D$, and thus we in fact have that $H_k(D_o)$ has a finite generating set comprising of elements comprising of maps $S^k \to D_o \cap D_e = f^{-1}Q \subset D_o$. Take a member β of this generating set. Observe that $f_*\beta \in i_* H_k(Q)$, and therefore, in particular, $f_*\beta \in H_k(A_1)$. Since D is contractible, $f_*\beta = 0$ in $H_k(X)$, and since A_1 is a retract, $H_k(A_1) \hookrightarrow H_k(X)$ is an injection, and we have that $f_*\beta = 0$ in $H_k(A_1)$. That is, there exists some $k+1$ cell $e : D^{k+1} \to A_1 \subset A_1 \cup A_3 \cup A_5 ...$, such that $\partial e(D^{k+1}) = \beta$. Let D' denote the disk which β bounds. We therefore modify f

by replacing $f \restriction_{D'}$ with $e \restriction_{D^{k+1}}$. The map remains continuous because we have not modified the boundary. Call this new map $f' : D \to X$ and let $D'_o = (f')^{-1}(A_1 \cup A_3 \cup A_5 ...)$. Observe that $H_k(D'_o) = H_k(D_o) \,/_{\beta}$, since β is killed in D'_o and none of the other generators are affected. Therefore, since $H_k(D_o)$ is finitely generated, we may continue in this manner and "fill all the holes" one by one, so that, for every path component P of D_o and D_e, $H_k(P) = 0$.

The following figure (for $k + 1 = 2$) illustrates the procedure which we have described:

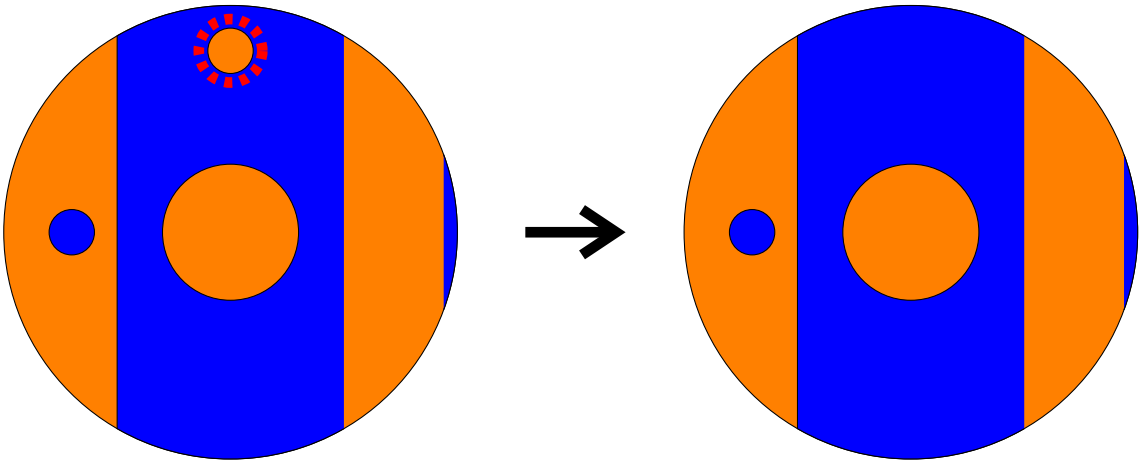


Figure 3.6: A schematic of D. The blue portion is D_o and the orange portion is D_e. The intersection of the two colors is $D \cap f^{-1}Q$ - In principle $f^{-1}Q$ can occupy nonzero volume, but we have not depicted this possibility for simplicity. The dashed red line is the representative of β, which is wrapped around one of the blue circles. We apply the procedure above to "fill the hole" which β surrounds.

After completing the above procedure, the resulting disk D is divided into connected components P of D_o and D_e, each of which satisfies $H_k(P) = 0$. Since D_e and D_o are closed, any point in D_e which is not contained in D_e° must be contained in D_o. Therefore, the collection $PC = \{P \,|\, P \text{ is a connected component of } D_e \text{ or } D_o\}$ forms a solid partition of D. Note that there a natural partial ordering on { connected components P } given by "containment". This can be formalized via a height function

$\mathrm{ht} : \{$ connected components $P \} \to \mathbb{Z}_{\geq 0}$. We define (recursively):

$$\mathrm{ht}(P) = \min\{d \in \mathbb{Z}_{\geq 0} \mid \text{there exists } P_1, ..., P_r \text{ with } \mathrm{ht}(P_i) \leq d-1 \text{ for all } i \text{ such that } P \cup \bigcup_{i=1}^{r} P_i \text{ is contractible}\}$$

In particular, note that $\mathrm{ht}(P) = 0 \iff P$ is contractible. Proceeding as per our proof strategy, we now need to show that $f \restriction_{P \cap \partial D}$ can naturally be interpreted as an element $\alpha_P \in i_* C_k(Q)$. We will now do this inductively:

The base case: For $\mathrm{ht}(P) = 0$, P is contractible. There exists at least one connected component P which is contractible (this is because finiteness of $H_0(D_o), H_0(D_e)$ disallows infinite nests. We must take the "innermost component"). Since P is a contractible subspace of D, it is homeomorphic to a disk, and thus $f \restriction_P : P \to X \in H_k(X)$ defined s $k+1$ cell in $H_{k+1}(X)$. Set $\alpha_P := f \restriction_{P \cap \partial D} \in C_k(X)$. Note that $\partial f \restriction_P$ comprises of $P \cap \partial D$ together with a portion of the boundary that is contained entirely in $D_o \cap D_e = f^{-1}Q$. Therefore, since $\partial f(P) = 0 \in H_k(X)$, we conclude that $\alpha_P = i_* C_k(Q)$. This completes the base case. Here is a schematic to illustrate what we have done:

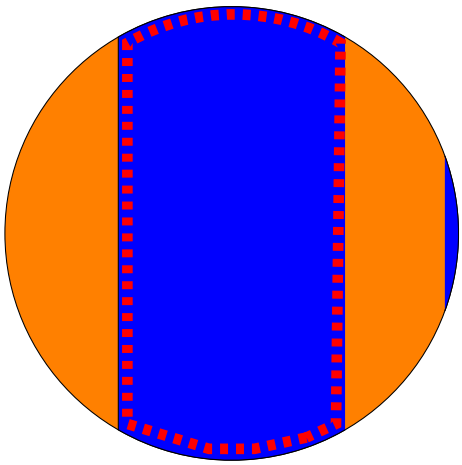


Figure 3.7: Here, P is the large blue component, and the red dashed line is its boundary. Observe that the boundary comprises of a portion of the boundary of D and the remaining portion is a portion in $D_o \cap D_e = f^{-1}Q$ (i.e "blue intersection orange").

The inductive step: For the inductive step, take a connected component P with $\mathrm{ht}(P) = d$. Observe that there are some components $P'_1, ..., P'_l$ such that $\mathrm{ht}(P'_i) < d$ for all i and $P \cup \bigcup_{i=1}^{l} P'_i$ is contractible (these are the components which "P surrounds"). Therefore, applying the argument from our base case, we conclude that $\alpha_{(P \cup \bigcup_{i=1}^{l} P'_i)} \in i_* C_k(Q)$. But observe that $\alpha_{(P \cup \bigcup_{i=1}^{l} P'_i)} = \alpha_P - \sum_i c_{P'_i} \alpha_{P'_i}$ for some constants $c_{P'_i}$. By our inductive hypothesis, $\alpha_{P'_i} \in i_* C_k(Q)$ for each i, and thus, we conclude that $\alpha_P \in i_* C_k(Q)$. We have completed the inductive procedure.

To conclude the proof of Lemma 3.4.3, we note that since $\partial D = \sum_P \alpha_P$ for each D, we put everything together to conclude that:

$$\alpha_e - \alpha_o = \sum_j \sum_{P \in PC(j)} \alpha_P = \sum_{P \in PC_e(j)} \alpha_P + \sum_j \sum_{P \in PC_o(j)} \alpha_P$$

It then follows that $\alpha_e = \sum_j \sum_{P \in PC_e(j)} \alpha_P$ and likewise $\alpha_o = \sum_j \sum_{P \in PC_o(j)} \alpha_P$. Since each $\alpha_P \in i_* C_k(Q)$ and $\alpha_e, \alpha_o \in H_k(X)$ (i.e are cycles), we then have that $\alpha_e, \alpha_o \in i_* H_k(Q)$. So,

$\alpha \in i_* H_k(Q)$. □

Example 3.4.4. (Example to demonstrate that the surjectivity of action was necessary for Lemma 3.4.3)

In our proof of Lemma 3.4.3, we heavily exploited the fact that the action was surjective (Definition 3.3.11), since the surjectivity of the action allowed us to write $D = D_o \cup D_e$, which is what allowed us to ensure that α was homologous to an element of $f(D_o \cap D_e) = Q$.

The following simple example shows why the surjective action hypothesis was necessary: Take a cylinder $C = S^1 \times [0,1]$, and consider $S^1 \vee S^1 \subset C$. We may then construct a non-surjective action of TL_3 on the cylinder, where u_1 and u_2 retract onto the first and second copy of S^1 respectively. If we set α_1 to be the generator of the first copy of S^1 and α_2 to be the generator of the second copy of S^1, we see that $\alpha_1 \sim \alpha_2$ (are homologous) but in fact $u_1(C) \cap u_2(C) = \{*\}$, and thus $\alpha_1, \alpha_2 \notin i_* H_1(Q)$. What goes wrong here is that the disk whose boundary is $\alpha_2 - \alpha_1$ cannot be decomposed as $D = D_o \cup D_e$.

We now define the notion of a minimal intersection. This notion as has a twofold importance:
(1) We will use it in Subsection 3.4.3 motivate the map that identifies the cyclic module generated by a homology class with the standard representation
(2) It is the conceptual reason for the injectivity of that map.

Definition 3.4.5. Let X be a finite-CW surjective TL_n-space. Given a homology class $\alpha \in H_k(X)$, and given $\{i_1, .., , i_m\}$ such that $|i_j - i_l| \geq 2$ for all $j \neq l$, we say that $A_{i_1} \cap ... \cap A_{i_m}$ is a minimal intersection containing α if:

(1) α lies in the image $H_k(A_{i_1} \cap ... \cap A_{i_m}) \hookrightarrow H_k(X)$

(2) Given any $l \notin \{i_1, ..., i_m\}$, α does not lie in the image $H_k(A_{i_1} \cap ... \cap A_{i_m} \cap A_l) \hookrightarrow H_k(X)$.

Furthermore, if $\alpha \in i_* H_k(Q)$, we say that the minimal intersection containing α is Q.

The utility of minimal intersections is that they have a uniqueness property, which we will see by exploiting Observation 3.4.1 and Lemma 3.4.3.

Lemma 3.4.6 (Uniqueness of minimal intersection containing a given homology class)**.** *Let X be a finite* CW*-complex. Take $\alpha \in H_k(X)$. Suppose that $A_{i_1} \cap ... \cap A_{i_p}$ is a minimal intersection containing α. Then, no other minimal intersection contains α.*

Proof. Suppose for contradiction that α is contained in two minimal intersections $A_{i_1} \cap ... \cap A_{i_p}$ and $A_{j_1} \cap ... \cap A_{j_q}$.

Suppose first that there exists some m such that $|j_m - i_l| \geq 2$ for all l. Then, observe that since $\alpha \in H_k(A_{j_m})$, $u_{j_m}\alpha = \alpha$. But on the other hand, observe that $u_{j_m}\alpha \in H_k(A_{i_1} \cap ... \cap A_{i_p} \cap A_{j_m})$ by Observation 3.4.1. Therefore, $\alpha \in H_k(A_{i_1} \cap ... \cap A_{i_p} \cap A_{i_m}))$, which contradicts minimality of the intersection $A_{i_1} \cap ... \cap A_{i_p}$.

The remaining case is when, for each j_m, there is some i_l such that $|j_m - i_l| \leq 1$. In particular, this implies that there is some i such that $\alpha \in A_i$ and $\alpha \in A_{i+1}$. We then conclude by Lemma 3.4.3 that the minimal intersection containing α is Q. □

An easy reformulation of the above into a form which is useful is:

Corollary 3.4.7. *If $\alpha, \beta \in H_k(X)$ are such that $A_{i_1} \cap ... \cap A_{i_m}$ is the minimal intersection containing α and $A_{j_1} \cap ... \cap A_{j_d}$ is the minimal intersection containing β, with $\{i_1, .., i_m\} \neq \{j_1, .., j_d\}$, then $\alpha \neq \beta$.*

We end this Section with a simple observation:

Observation 3.4.8 (Isomorphisms preserve the null-homologous property)**.** Suppose that $\beta \in H_k(A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_q})$. Suppose that j is such that $|j - i_s| \leq 1$ for some s. Then,

$$u_j\beta = 0 \iff \beta = 0$$

Proof. $u_j \restriction_{(A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_q})}$ is an isomorphism onto its range. □

3.4.2 The reason to consider $X/_Q$

Let X be a finite CW TL_n-space. By Definition 3.4.2, each A_i is a finite subcomplex, and therefore, $Q = A_1 \cap A_2 \cap ... \cap A_{n-1}$ is a finite subcomplex. Therefore, the $X/_Q$ is a finite CW subcomplex. This is important, because it is required for the results of Subsection 3.4.1 to hold.

Moreover, $X/_Q$ carries over the TL_n-action from X:

Observation 3.4.9 (The TL_n-action on $X/_Q$ is well defined)**.** The TL_n-action on X gives rise to a well defined TL_n-action on $X/_Q$.

Proof. Let G be a monoid. Given a G-space X, a subspace Y and an action of G gives rise to a well defined action on X/Y if and only if $G \cdot Y \subseteq Y$. In our case, TL_n fixes every point of Q, and thus in particular $\mathrm{TL}_n \cdot Q = Q$. It follows that the TL_n-action on X gives rise to a well defined TL_n-action on X/Q. □

In Subsection 3.4.1, all our results worked for arbitrary Q. Thus, in principle, we should be able to understand TL_n-spaces for arbitrary Q. However, it turns out that for Q arbitrary, we have much less control over the TL_n-representation structure of $H_*(X)$. This can be heuristically seen as follows: since TL_n fixes Q, the interesting portions of the action are away from Q. What this ends up meaning is that we have very little control which homology classes of X go into Q after an action by an element of TL_n.

Therefore, when Q is nontrivial, it does not seem possible to understand, in a clean manner, the decomposition of $H_*(X)$ as a TL_n-module. The saving grace is that all the "interesting action" happens outside Q anyway. In the future, we will therefore study the TL_n-space X/Q rather than X, and we will be able to obtain a beautiful and clean description of $H_*(X/Q)$ as a TL_n-representation. However, for now, we will provide an example of why it is much harder to fully describe $H_*(X)$ as a TL_n-module when Q is nontrivial:

Example 3.4.10. Let $A_1, A_2, A_3, A_4 = S^1 \vee S^1$ for each i, set $Q = S^1$, and set $X = A_1 \vee_Q A_2 \vee_Q A_3 \vee_Q A_4$, as depicted below:

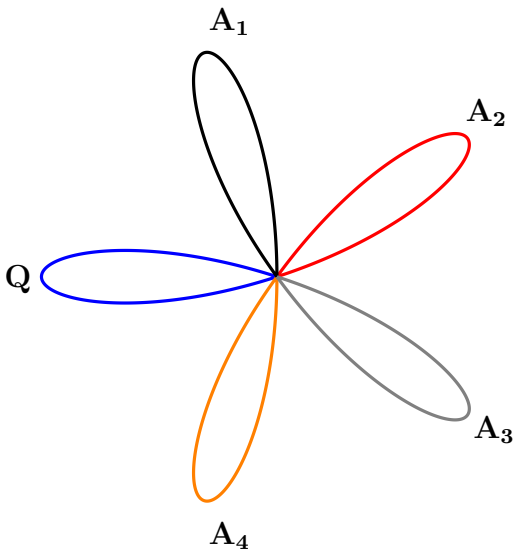


Figure 3.8: The blue copy of S^1 is Q. The blue and black copies together make A_1, the blue and red copies together make A_2, the blue and gray copies together make A_3, and the blue and orange copies together make A_4. We will describe the maps u_1, u_2, u_3, u_4 below, which will make X into a TL_5-space.

Let u_1, u_2, u_3, u_4 act as follows: Each u_i acts on $A_{i\pm1}$ by fixing the copy of S^1 corresponding to Q, and taking the other copy of S^1 isomorphically to the corresponding copy of S^1 in A_i. Let S^1_Q denote the copy of S^1 which makes up Q, and for each i, let $(S^1)_i$ denote the copy of S^1 of A_i which does not live in Q. We define the long distance maps as follows:

$$u_1((S^1)_3) = u_1((S^1)_4) = (S^1)_Q$$
$$u_2((S^1)_4) = \{*\}$$
$$u_3((S^1)_1) = (S^1)_Q$$
$$u_4((S^1)_1) = u_4((S^1)_2) = \{*\}$$

That is, u_2 and u_4, when applied long distance, retract to $\{*\}$ rather than the whole of S^1_Q. Let us observe that this is a well defined TL_n-action. Neighbor relations (Lemma 3.3.2) hold because the maps, when restricted to neighboring copies of S^1, have been chosen to be

mutually compatible isomorphisms. What remains to be checked are the long-distance relations. There are three cases to consider:

(1) To show that $u_1u_4 = u_4u_1$: Indeed, observe that if $x \in A_1$, then both maps act on x by the trivial map to $\{*\}$, if $x \in A_4$, both maps act on x surjections to S^1_Q, if $x \in A_2$, then both maps act on x by the trivial map to $\{*\}$, and if $x \in A_3$, then both maps act on x by surjections to S^1_Q.

(2) To show that $u_1u_3 = u_3u_1$: Observe that for every $x \in X$, both maps act on x via surjection maps to S^1_Q.

(3) To show that $u_2u_4 = u_4u_2$: Observe that for every $x \in X$, both maps act on x via surjection maps to S^1_Q.

Therefore, the above action of TL_5 on X is well defined. However, the TL_5-representation structure of $H_1(X)$ is rather strange, since we have very little control of the long-distance maps into Q. For instance, the representation structure of $H_1(X)$ could not be read off from the filtration $\mathcal{F} = S^1 \vee S^1 \supseteq S^1 \supseteq S^1 ...$ because we could have taken, for example, all long distance maps to be trivial maps onto $\{*\}$ away from Q (note that Q must be fixed), and this would have given us another TL_5-space with the same filtration but with a different representation structure for $H_1(X)$ (the new representation structure would be given by $V_{5,1} \oplus [1]$, where $[1]$ the one dimensional representation of TL_5 wherein every element of TL_n fixes the spanning vector; $[1]$ requires $\delta = 1$ to be well defined).

However, notice that if we consider our original action on X, and consider X/Q, then in fact $H_1(X/Q)$ has a very nice description as a TL_5-representation: indeed - it is just $V_{5,1}$, the standard representation spanned by $(5,1)$-link states! In fact, we will show in

Subsection 3.4.4 that the representation structure of $H_k(X/Q)$ can be read off from the filtration $\mathcal{F}$, and has a nice decomposition in terms of standard representations.

The above example shows why $H_k(X)$ does not necessarily behave well as a TL_n-representation (but $H_k(X/Q)$ does!), and this justifies us to consider X/Q as the central object of study from now on. The key property that X/Q) has is that the full intersection is $\{*\}$, i.e $A_1/Q \cap A_2/Q \cap ... \cap A_{n-1}/Q$. We will denote TL_n-spaces which have this property by Y instead of X.

3.4.3 The cyclic module generated from a p-intersection

As reasoned in Subsection 3.4.2, we will henceforth focus our attention to X/Q. X/Q is a TL_n-space whose full intersection is $\{*\}$. Thus, studying X/Q is equivalent to studying a TL_n-space Y with $Q = \{*\}$ - this latter perspective will make notation easier since we do not have to write quotients everywhere. In this Subsection, we will use the topological lemmas from Subsection 3.4.1 to deduce a key stepping stone to Theorem 3.4.17.

Before we delve into the theorem, we will remind the reader about a standard construction one encounters when studying the representation theory of Temperley-Lieb algebras, especially from a diagrammatic perspective:

Definition 3.4.11. Given any element of TL_n, we may construct this element by placing two link states "back to back". Given link states v and w, we will denote this construction by $vw^* \in \mathrm{TL}_n$ (here w is reflected and placed below v. This construction is often alternatively denoted by $|v\ w|$, as in [44] (Ridout, Saint-Aubin)).

For example

We now state and prove the theorem of this Subsection:

Theorem 3.4.12 (Cyclic module generated from a p-intersection)**.** *Let Y be a finite-*CW *surjective* TL_n*-space, with the additional property that $Q = \{*\}$. Consider*
$R_p = A_1 \cap A_3 \cap ... \cap A_{2p-1}$*. Suppose that:*
(1) $0 \neq \alpha \in H_k(R_p, \mathbb{Z}) \hookrightarrow H_k(Y, \mathbb{Z})$*.*
(2) If $\{1, 3, 5, ..., 2p-1\} \subsetneq \{i_1, ..., i_d\}$*,* $a \in \mathrm{TL}_n$ *and* $a \cdot \alpha \in H_k(A_{i_1} \cap ... \cap A_{i_d})$*, then* $a \cdot \alpha = 0$*.*
(3) m is the smallest natural number such that $m\alpha = 0$ (i.e m records torsion, $m = \infty$ if there is no torsion).
Then, the cyclic submodule of $H_k(Y, \mathbb{Z})$ generated by α is the standard representation with coefficients that record the torsion:

$$\mathrm{TL}_n \cdot \alpha = \begin{cases} V_{n,p} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} & \text{if } m < \infty \\ V_{n,p} & \text{if } m = \infty \end{cases}$$

In particular, if $\mathbb{K}$ is a field containing $\mathbb{Q}$, then, for $\alpha \in H_k(Y, \mathbb{K})$, $\mathrm{TL}_n \cdot \alpha = V_{n,p}$ is the standard representation over $\mathbb{K}$.

Proof. For simplicity, we will assume that $\mathbb{K}$ is a field containing $\mathbb{Q}$ and $\alpha \in H_k(Y, \mathbb{K})$, since this is where all the content of the above statement is. The result over $\mathbb{Z}$ is easy to deduce from the statement for $\mathbb{K}$, and we will remark in the end why the result over $\mathbb{Z}$ holds.

We construct the map $h : V_{n,p} \to TL_n \cdot \alpha$ by:

We must show that this gives rise to a well defined map $h : V_{n,p} \to TL_n \cdot \alpha$, and that this map is injective and surjective.

Motivation and connection with Subsection 3.4.1: Assume for the moment that h is well defined. We begin with the following observation which is the motivation for constructing the map above, and will also help us to prove injectivity later on:

Let $v \in V_{n,d}$ be a nonzero link state with length one cups ⌣ at positions $i_1, .., i_q$ (and no other positions). Then, the minimal intersection containing $h(v)$ is $A_{i_1} \cap ... \cap A_{i_q}$.

To see this, first observe that $h(v)$ is contained in this intersection since each u_{i_j} fixes $h(v)$, and thus $h(v) = u_{i_j} h(v) \in H_k(A_j)$. Thus, by Lemma 3.4.1, $h(v) = u_{i_1} u_{i_2} ... u_{i_q} h(v) \in H_k(A_{i_1} \cap ... \cap A_{i_q})$. Next note that any other u_j does not fix v. Suppose that we still have that $u_j h(v) = h(v)$ despite the fact that u_j does not fix v. If $|j - i_s| \leq 1$ for some s, then by Lemma 3.4.3 we must have that $h(v) \in H_k(Q)$ and since $Q = \{*\}$, we have that $h(v) = 0$. Since every link state is a cyclic generator of $V_{n,p}$ (since none of them lie in the kernel of the bilinear form, see for example [44] (Ridout, Saint-Aubin), the proof of Proposition 3.3), there is some $a \in \mathrm{TL}_n$ such that $av = ($ ⌣⌣ ··· ⌣||| ··· | $)$. But then, $0 = ah(v) = h(av) = h($ ⌣⌣ ··· ⌣||| ··· | $) = \alpha$, a contradiction. Therefore, $|j - i_s| \geq 2$ for every k. If v has loose strands in positions j and $j+1$, $u_j v = 0$ in which case $u_j h(v) = h(u_j v) = h(0) = 0$. $h(v)$ cannot be in $H_k(A_j)$, because if it was, $h(v) = u_j h(v) = 0$, and once again, we may exploit cyclicity to see that $\alpha = 0$, a contradiction. The only remaining case is when u_j "breaks a nest". This is best explained by means of an example, which easily generalizes:

Suppose that

$u_7 h($  $) = h($  $)$

That is,

$h($  $) = h($  $)$

Applying u_6 to both sides, we have that

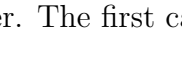
$h($  $) = h($  $)$

But the left hand side is in $H_k(A_1)$, while the right hand side is in $H_k(A_2)$. By Lemma 3.4.3, we must have that both are in $i_*H_k(Q)$, and are therefore both zero, since $Q = \{*\}$. By cyclicity, $\alpha = 0$, a contradiction. This establishes the fact that, for a link state v, the minimal intersection of $h(v)$ can be read off from the position of the length 1 cups of v. This motivates the construction of the above map. We now prove well-definedness:

Well definedness: We must show that if $a, b \in \mathrm{TL}_n$ are such that

$a\Big($ $\Big) = b\Big($ $\Big)$

then in fact $a\alpha = b\alpha$.

There are two cases to consider. The first case is when $a\Big($  $\Big) = 0 \in V_{n,p}$. In this case, if we think of the link state in M_n (see Subsection 3.5.1 if the notation is unclear), it has more than p cups. Such a link state can be taken to the link state comprising of $q > p$ cups followed by $n - q$ loose strands by a sequence of neighbor retractions in the sense of Observation 3.4.8. Call the product of neighbor retractions a'. Then, in light of Observation 3.4.1, $a'a\alpha = 0$ by hypothesis of our Theorem, since

$a'a\alpha \in H_k(R_p \cap A_{2p+1})$. Therefore, by Observation 3.4.8, $a\alpha = 0$. Similarly, since $b\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right) = 0$, we have that $b\alpha = 0$. So, $a\alpha = 0 = b\alpha$.

The remaining case is when $a\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right) \neq 0$. In this case, we observe the following important equivalence which is intrinsic to $V_{n,p}$:

$$0 \neq a\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right) = b\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right) \iff au_1u_3u_5...u_{2p-1} = bu_1u_3u_5...u_{2p-1}$$

If we assume this equivalence to be true, note that we are done, because then we have that $au_1u_3u_5...u_{2p-1}\alpha = bu_1u_3u_5...u_{2p-1}\alpha$, and since $\alpha \in H_k(R_p)$, each of u_1, u_3, u_5 etc fix α, and so we have that $a\alpha = b\alpha$. So, it remains to see why the above equivalence is true.

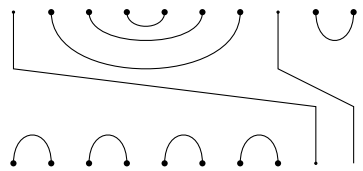
Consider a. First, observe that

$$a\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right) = au_1u_3...u_{2p-1}\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right)$$

As a shorthand, write $a' = au_1u_3...u_{2p-1}$. Write $a' = vw^*$, as in Definition 3.4.11. Since we have added $u_1u_3...u_{2p-1}$ to the end of a', and since we have assumed that $a\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right) \neq 0$, we must have that $w = \left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right)$. Next, observe that since the last $n - 2p$ loose strands are not affected by w, we must have that $v = a'\left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow\right)$. Thus, we have that

$$a' = [a' \left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow \right)] \cdot \left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow \right)^*$$
$$= [b' \left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow \right)] \cdot \left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow \right)^*$$
$$= b'$$

For an example, $a' = b'$ might look like:



Well definedness follows.

Surjectivity: Surjectivity is easy and follows from cyclicity. Given $a \cdot \alpha \in \mathrm{TL}_n \cdot \alpha$, observe that $a \left(\quad \cup\cup \cdots \cup\uparrow\uparrow \cdots \uparrow \right) \mapsto a \cdot \alpha$

Injectivity: We must show that if $v, w \in V_{n,p}$ are distinct link states then $h(v)$ and $h(w)$ are nonhomologous. If v and w do not have length one cups $\cup$ in the same locations, then the minimal intersections of $h(v)$ and $h(w)$ are different due to the observation we made in the "Motivation:" part of this proof, and thus $h(v) \neq h(w)$ by Corollary 3.4.7. Otherwise, v and w have their length one cups in the same locations. Then, since $v \neq w$, there is some length one cup such that the nesting around this cup in v is more than in w. One then can multiply by an outermost (with respect to the nesting) u_i to make $u_i v$ have length one cups at different positions as $u_i w$, and thus $h(u_i v) \neq h(u_i w)$, and thus $u_i h(v) \neq u_i h(w)$, and so $h(v) \neq h(w)$. The procedure for choosing u_i is not mysterious, and is best illustrated by an

example:

$v =$  , $w =$ 

Observe that the length one cups of v are both are positions 3 and 8. Thus, $h(v), h(w) \in A_3 \cap A_8$. But observe that the nesting around the length one cup at 3 is larger for v than w. Therefore, we choose u_5. Observe that

$u_5 v =$  , $u_5 w =$ 

Notice therefore that $h(u_5 v) \in H_k(A_1)$ but $h(u_5 w) \notin H_k(A_1)$. Thus, $u_5 h(v) = h(u_5 v) \neq h(u_5 w) = u_5 h(w)$ and thus, $h(v) \neq h(w)$.

Torsion: Simply note that this module is just obtained by action on a set, and formal linearity. Therefore, torsion of α carries over verbatim to the coefficients of $V_{n,p}$. □

3.4.4 The representation structure of $H_*(X/Q)$ can be read off from its filtration

Recall that in Definition 3.3.8, we associated a filtration of retracts $\mathcal{F}$ to a given TL_n-space. In this Subsection, we will present the proof of Theorem 3.4.17, which demonstrates how the representation structure of $H_*(X/Q)$ can be read off from its filtration $\mathcal{F}$. As before, instead of working with X/Q, we will, for notational convenience, work with a TL_n-space Y with $Q = \{*\}$.

Before we can state and prove Theorem 3.4.17, we need to introduce a few combinatorial notions which will appear in the statement of the theorem. Firstly, we need to introduce notation regarding compositions of an integer:

Definition 3.4.13 (Notation for compositions)**.** Given $m \in \mathbb{N}$, we will denote the collection of compositions of m by $\text{Comp}(m)$. If the reader needs reminding, a composition of m is an ordered way to sum up to m. So, for example, $\text{Comp}(3) = \{(1,1,1),(2,1),(1,2),(3)\}$.

We will denote compositions by λ, since compositions can be viewed as generalizations of partitions. We will denote the number of rows of a given composition λ by $\text{row}(\lambda)$ - i.e $\text{row}(\lambda)$ is the number of terms in the sum.

One of the first results one encounters when learning the representation theory of Temperley-Lieb algebras is that $\dim V_{n,p} = \binom{n}{p} - \binom{n}{p-1}$ (See for example, [44] (Ridout, Saint-Aubin), Section 2). This dimension is often denoted $d_{n,p}$, and we shall also denote it by $d_{n,p}$. Keeping this in mind, and motivated by the definitions of various families of symmetric functions, we arrive at the following definition:

Definition 3.4.14 (Defining d^r_λ)**.** Let $\lambda = (i_1, ..., i_l)$ be a composition of m. For each $1 \leq c \leq l$, set $d^r_{\lambda,c} = d_{r-2\sum_{j=1}^{c-1} i_j, i_c}$. We then set

$$d^r_\lambda = \prod_{c=1}^{l} d^r_{\lambda,c}$$

We present an example for the reader to better understand the definition of d^r_λ.

Example 3.4.15. (Elucidating the definition of d^r_λ) Consider $r = 8$. Noting that $\text{Comp}(3) = (1,1,1),(2,1),(1,2),(3)$, we have:

$$d^8_{(1,1,1)} = d_{8,1}d_{6,1}d_{4,1}$$
$$d^8_{(2,1)} = d_{8,2}d_{4,1}$$
$$d^8_{(1,2)} = d_{8,1}d_{6,2}$$
$$d^8_{(3)} = d_{8,3}$$

The above example would have made the definition of d_λ clear to the reader. We now present a simple combinatorial Lemma which will help us prove our theorem. The Lemma describes how the various d^r_λ are related.

Lemma 3.4.16 (How different d^r_λ are related)**.** *Let $\mu = (i_1, .., i_l) \in \mathrm{Comp}(m)$. Let $t \in \mathbb{N}$. Let $\lambda = (t, \mu)$ denote the composition of $m + t$ given by $(t, i_1, ..., i_l)$. Then,*

$$d^r_{(t,\mu)} = d_{r,t} \cdot d^{r-t}_\mu$$

Proof. We compute directly:

$$\begin{aligned} d^r_{(t,\mu)} &= d_{r-0,t} \cdot \prod_{c=1}^{\mathrm{row}(\mu)} d_{r-2(t+\sum_{j=1}^{c-1} i_j),i_c} \\ &= d_{r,t} \cdot \prod_{c=1}^{\mathrm{row}(\mu)} d_{(r-2t)-2\sum_{j=1}^{c-1} i_j,i_c} \\ &= d_{r,t} \cdot d^{r-2t}_\mu \end{aligned}$$

□

We now prove the main theorem of this chapter, Theorem 3.4.17, which gives an explicit

formula for reading off the representation structure of homology from the associated filtration.

Theorem 3.4.17. *Let Y be a finite-*CW *surjective* TL_n*-space, with the additional property that $Q = \{*\}$. Let $\mathcal{F} = R_1 \supseteq R_2 \supseteq ... \supseteq R_{\lfloor \frac{n}{2} \rfloor} \supseteq \{*\}$ be the associated filtration. Let $\mathbb{K}$ be a field containing $\mathbb{Q}$. Then, for each k, and setting $r_p = n - 2p$ for each p, the* TL_n*-representation structure of homology is given by:*

$$H_k(Y, \mathbb{K}) = \bigoplus_{p=1}^{\lfloor \frac{n}{2} \rfloor} V_{n,p}^{\oplus \left[\dim(H_k(R_p)) + \sum_{p<q\leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\lambda \in \mathrm{Comp}(q-p)} (-1)^{\mathrm{row}(\lambda)} \cdot d_\lambda^{r_p} \cdot \dim(H_k(R_q)) \right) \right]}$$

Proof. Since $\mathbb{K} \supseteq \mathbb{Q}$, there is no torsion.

Observe that if $A_{i_1} \cap ... \cap A_{i_p}$ is any p intersection, $\mathrm{TL}_n \cdot H_k(A_{i_1} \cap ... \cap A_{i_p}) = \mathrm{TL}_n \cdot H_k(R_p)$, since there are isomorphisms given by elements of TL_n which take each one to the other (by Lemma 3.3.7). Therefore, we have that $H_k(X) = \bigcup_{p=1}^{\lfloor \frac{n}{2} \rfloor} \mathrm{TL}_n \cdot H_k(R_p)$. Of course, the terms in the above union have nontrivial redundancy. We must understand this redundancy, for which we may consider the following recursive procedure:

- The base case is when $p = \lfloor \frac{n}{2} \rfloor$. Any set $T \supsetneq \{1, 3, 5, ..., \lfloor \frac{n}{2} \rfloor\}$ must satisfy $\bigcap_{i \in T} A_i = Q = \{*\}$. As a consequence, every $\alpha \in H_k(R_{\lfloor \frac{n}{2} \rfloor}, \mathbb{K})$ satisfies the hypothesis of Theorem 3.4.12. Therefore, $R_{\lfloor \frac{n}{2} \rfloor}$ contributes a term $V_{n,\lfloor \frac{n}{2} \rfloor}^{\oplus \dim H_k R_{\lfloor \frac{n}{2} \rfloor}}$.
- For the recursion, we suppose that, for any $q = p+1, p+2, ..., \lfloor \frac{n}{2} \rfloor$, R_q contributes a term $V_{n,q}^{\oplus s_q}$. The set $\{1, 2, 3, ..., s_q\}$ corresponds to a linearly independent set of homology classes $\alpha_1, ..., \alpha_{s_q} \in H_k(R_q)$, but not all homology classes in $H_k(R_q)$ live in the TL_n-representation generated by these, because some classes belong to $V_{n,q'}$ for

$q' > q$. We assume for the recursion that

$H_k(R_q) = \text{Span}\{\alpha_1, ..., \alpha_{s_q}\} \oplus (\bigcup_{q'>q} \text{TL}_n \cdot H_k(R_{q'})) \cap H_k(R_q)$

- We now do the inductive step. Extend a basis for $\left(\bigcup_{q>p} \text{TL}_n \cdot H_k(R_q)\right) \cap H_k(R_p) \subseteq H_k(R_p)$ to a basis of $H_k(R_p)$, by appending a collection of linearly independent vectors $\{\alpha_1, ..., \alpha_{s_p}\}$. Observe that in our inductive step, we assumed that for any $q > p$, $H_k(R_q) = \text{Span}\{\alpha_1, ..., \alpha_{s_q}\} \oplus \left(\bigcup_{q'>q} \text{TL}_n \cdot H_k(R_{q'})\right) \cap H_k(R_q)$, and thus all homology classes in $H_k(R_q)$ for $q > p$ have already been accounted for. Thus, must have that each α_i satisfies the hypothesis of Theorem 3.4.12, that is, if $T \supsetneq \{1, 3, 5, ..., p\}$, $a \in \text{TL}_n$, and $a \cdot \alpha_i \in \bigcap_{j \in T} A_j$, then in fact $a \cdot \alpha_i = 0$. Thus, by Theorem 3.4.12, we see that $\text{TL}_n \cdot \alpha_i = V_{n,p}$. We deduce that $H_k(R_p)$ contributes a term of $V_{n,p}^{\oplus s_p}$ and moreover $H_k(R_p) = \text{Span}\{\alpha_1, ..., \alpha_{s_p}\} \oplus (\bigcup_{q>p} \text{TL}_n \cdot H_k(R_q)) \cap H_k(R_p)$, thereby proving the inductive step.

- Now, we notice that the "redundancy" comes from the fact that some of the homology classes in $H_k(R_p)$ belong to copies of $V_{n,q}$ for $q > p$. Take $\alpha \in H_k(R_q)$ for $q > p$. The elements in $\text{TL}_n \cdot \alpha$ which reside in $H_k(R_p)$ correspond to precisely those link states which have the first p cups fixed in their positions, and the rest is allowed to vary. The "rest" amounts to placing $q - p$ cups in $n - 2p$ locations, and so the number of link states with this property amounts choosing a link state of $V_{n-2p,q-p}$. Recall that $\dim V_{n-2p,q-p} = (\binom{n-2p}{q-p} - \binom{n-2p}{q-p-1})$, and we denote it by $d_{n-2p,q-p}$. We therefore conclude that $\dim(\text{TL}_n \cdot \alpha \cap H_k(R_p)) = d_{n-2p,q-p}$.

- Therefore, s_p, the dimension of the span of all homology classes which are not

obtained as part of some $V_{n,q}$ for $q > p$, is given by the recursion:

$$s_{\lfloor \frac{n}{2} \rfloor} = \dim H_k(R_{\lfloor \frac{n}{2} \rfloor})$$
$$s_p = \dim(H_k(R_p)) - \sum_{q=p+1}^{\lfloor \frac{n}{2} \rfloor} d_{n-2p,q-p} \cdot s_q$$

What remains to be shown is that the above recursive formula yields the closed-form combinatorial formula which is in the statement of the theorem. For $p = \lfloor \frac{n}{2} \rfloor$, observe that both formulae yield $\dim(H_k(R_{\lfloor \frac{n}{2} \rfloor}))$, since, in both cases, the sum over $q > p$ is void.

Our inductive hypothesis is that for any $q > p$,

$$s_q = \dim(H_k(R_q)) + \sum_{q < q' \leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\lambda \in \mathrm{Comp}(q'-q)} (-1)^{\mathrm{row}(\lambda)} \cdot d_\lambda^{r_q} \cdot \dim(H_k(R_{q'})) \right)$$

So, then:

$$\begin{aligned} s_p &= \dim(H_k(R_p)) - \sum_{q=p+1}^{\lfloor \frac{n}{2} \rfloor} d_{n-2p,q-p} \cdot s_q \\ &= \dim(H_k(R_p)) - \sum_{q=p+1}^{\lfloor \frac{n}{2} \rfloor} d_{n-2p,q-p} \cdot \left[\dim(H_k(R_q)) + \sum_{q < q' \leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\mu \in \mathrm{Comp}(q'-q)} (-1)^{\mathrm{row}(\mu)} \cdot d_\mu^{r_q} \cdot \dim(H_k(R_{q'})) \right) \right] \end{aligned}$$

Handling the first sum:

Now, for $\lambda = (q-p) \in \mathrm{Comp}(q-p)$, observe that:
(1) $d_\lambda^{r_p} = d_{r_p,q-p} = d_{n-2p,q-p}$
(2) $\mathrm{row}(\lambda) = 1$ and so $(-1)^{\mathrm{row}(\lambda)} = -1$

Thus, we may suggestively rewrite

$$-\sum_{q=p+1}^{\lfloor \frac{n}{2} \rfloor} d_{n-2p,q-p} \cdot \dim(H_k(R_q)) = \sum_{p<q\leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\lambda \in \{(q-p)\} \subset \mathrm{Comp}(q-p)} (-1)^{\mathrm{row}(\lambda)} d_\lambda^{r_p} \dim(H_k(R_q)) \right)$$

and since relabeling q by q' in the above expression is harmless (since q' does not appear), we have that:

$$-\sum_{p<q'\leq \lfloor \frac{n}{2} \rfloor} d_{n-2p,q-p} \cdot \dim(H_k(R_q)) = \sum_{p<q'\leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\lambda \in \{(q'-p)\} \subset \mathrm{Comp}(q'-p)} (-1)^{\mathrm{row}(\lambda)} d_\lambda^{r_p} \dim(H_k(R_{q'})) \right)$$

Handling the second sum:

Observe that given $q > p$ and $\mu \in \mathrm{Comp}(q'-q)$, $(q-p, \mu) \in \mathrm{Comp}(q'-p)$. Moreover,
(1) all such compositions are distinct, since the μs are distinct
(2) every composition in $\mathrm{Comp}(q'-p)$ is either of this form or is the single sum composition $(q'-p)$.

In other words, for each $q' > p$, $\mathrm{Comp}(q'-p) = \{(q'-p)\} \cup \bigcup_{p<q<q'} \mathrm{Comp}(q'-q)$.

Finally, observe that by Lemma 3.4.16, we have that $d_{(q-p,\mu)}^{r_p} = d_{r_p,q-p} \cdot d_\mu^{r_p-2(q-p)}$, and observe that $r_p - 2(q-p) = n - 2p - 2(q-p) = n - 2q = r_q$, and thus we conclude that

$$d_{(q-p,\mu)}^{r_p} = d_{r_p,q-p} \cdot d_\mu^{r_q}$$

Therefore, combining what we have observed and noting that $\mathrm{row}(q-p,\mu) = 1 + \mathrm{row}(\mu)$, we see that:

$$
\begin{aligned}
&- \sum_{q=p+1}^{\lfloor \frac{n}{2} \rfloor} d_{n-2p,q-p} \sum_{q<q'\leq \frac{n}{2}} \left(\sum_{\mu \in \mathrm{Comp}(q'-q)} (-1)^{\mathrm{row}(\mu)} \cdot d_{\mu}^{r_q} \cdot \dim(H_k(R_{q'})) \right) \\
&\qquad = - \sum_{p<q<q'\leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\mu \in \mathrm{Comp}(q'-q)} (-1)^{\mathrm{row}(\mu)} \cdot d_{n-2p,q-p} \cdot d_{\mu}^{r_q} \cdot \dim(H_k(R_{q'})) \right) \\
&\qquad = \sum_{p<q<q'\leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\mu \in \mathrm{Comp}(q'-q)} (-1)^{\mathrm{row}(\mu)+1} \cdot d_{(q-p,\mu)}^{r_p} \cdot \dim(H_k(R_{q'})) \right) \\
&\qquad = \sum_{p<q'\leq \lfloor \frac{n}{2} \rfloor} \left(\sum_{\lambda \in \mathrm{Comp}(q'-p)-\{(q'-p)\}} (-1)^{\mathrm{row}(\lambda)} \cdot d_{\lambda}^{r_p} \cdot \dim(H_k(R_{q'})) \right)
\end{aligned}
$$

Putting together the handling of the first and second sums:

We saw that the first sum produced all required summands for compositions in the singletons $\{(q'-p)\}$ for all $q' > p$. We saw that the second sum produced all required summands for compositions except singletons, i.e $\lambda \in \mathrm{Comp}(q'-p) - \{(q'-p)\}$ for all $q' > p$. Putting these two together, we see that:

$$
\begin{aligned}
s_p &= \dim(H_k(R_p)) + (\text{first sum}) + (\text{second sum}) \\
&= \dim(H_k(R_p)) + \sum_{p<q'\leq\lfloor\frac{n}{2}\rfloor} \left(\sum_{\lambda\in\{(q'-p)\}} (-1)^{\mathrm{row}(\lambda)} d_\lambda^{r_p} \dim(H_k(R_{q'})) \right) \\
&\quad + \sum_{p<q'\leq\lfloor\frac{n}{2}\rfloor} \left(\sum_{\lambda\in\mathrm{Comp}(q'-p)-\{(q'-p)\}} (-1)^{\mathrm{row}(\lambda)} \cdot d_\lambda^{r_p} \cdot \dim(H_k(R_{q'})) \right) \\
&= \dim(H_k(R_p)) + \sum_{p<q\leq\lfloor\frac{n}{2}\rfloor} \left(\sum_{\lambda\in\mathrm{Comp}(q-p)} (-1)^{\mathrm{row}(\lambda)} \cdot d_\lambda^{r_p} \cdot \dim(H_k(R_q)) \right)
\end{aligned}
$$

We have therefore proved the inductive step, and this concludes the proof of the theorem. □

3.5 Representation stability and Topological stability of the Temperley-Lieb monoid chain

In this Section, we first define a notion of representation stability for Temperley-Lieb algebras, and prove that sequences of standard representations are representation stable. It is conceievable that a competing notion could be obtained by considering representations of TL(∞) (representations of TL(∞) are studied, for instance, in [39](Moore)). The notion of representation stability we will introduce will make no reference to TL(∞), but rather will be analogous to the definition of FI-modules as defined in [46] (Church, Ellenberg, Farb). We will call our notion of a "stable module" as an "LS-module", analogous to the naming convention for "FI-modules". In Subsection 3.5.4, we will explain why some infinite-link-state representations of TL(∞) are not stable.

We then define a notion of topological stability of a chain of TL_n-spaces, and observe that if $\{X_n\}_{n\geq N}$ is a topologically stable chain of TL_n-spaces, then (an appropriate quotient of)

their homology groups form a finitely generated LS-module. This is philosophically interesting, because it is an analogue to a theorem in the foundational paper on representation stability (i.e [46] (Church, Ellenberg, Farb), Section 6), which says that the homology groups of configuration spaces are finitely generated FI-modules.

3.5.1 Defining representation stability

The definitions we provide assume that $\delta = 1$, and this is perhaps not a defect, but rather a feature of representation stability, at least from the viewpoint of actions on finite sets. With regard to topological actions, we are only interested in the $\delta = 1$ case and so we face no problems in this regard. One advantage of the notion of representation stability we provide is that it is naturally analogous to the definition of FI-modules, and hence our theorem that topological stability implies representation stability (Theorem 3.5.14) can be viewed as an analogue to the statement that the homology of configuration spaces is a finitely generated FI-module, as in [46] (Church, Ellenberg, Farb).

Let us think about the representation stability of symmetric groups as a motivation: there, one has natural sets upon which each S_n acts (namely $\{1, 2, ..., n\}$). One then considers the chain of these sets with the natural inclusions, and considers functors from the corresponding category to the category of vector spaces (or $\mathbb{Z}$-modules). We will do the analogous thing here. The natural set upon which TL_n acts is the set of all link states M_n (we follow the notation of [44] (Ridout, Saint-Aubin), Section 3). That is,

$$M_n = \bigcup_{p=1}^{\lfloor \frac{n}{2} \rfloor} \{(n, p) - \text{link states}\}$$

Adding loose strands gives inclusions $M_m \hookrightarrow M_n$ for $m < n$, and thus we form the chain:

$$M_1 \hookrightarrow M_2 \hookrightarrow M_3 ...$$

which we might compare (for analogy) with the FI-module chain

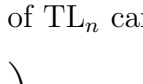
$$\{1\} \hookrightarrow \{1,2\} \hookrightarrow \{1,2,3\} \hookrightarrow ...$$

and by analogy, we arrive at the following definition:

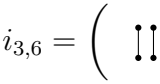
Definition 3.5.1 (LS-modules)**.** We define the category LS, which is a subcategory of ***Set***, to be the category such that:

Objects: The objects of LS are indexed by $\mathbb{N}$. They are: $\{M_n\}_{n\in\mathbb{N}}$.

Morphisms: The morphisms in LS are precisely the compositions of the following morphisms:

- For each n, each $a \in \mathrm{TL}_n$ gives rise to a morphism $M_n \to M_n$. Warning: different elements of TL_n can give rise to identical morphisms; for instance  and  give rise to the same morphism: $M_4 \to M_4$.
- For $m < n$, we have the morphism $i_{m,n} : M_m \hookrightarrow M_n$ which adds $n - m$ loose strands to the end of each link state of M_m. For example,

$$i_{5,7}\left(\quad \right) = \left(\quad \right)$$

Warning: Different compositions can lead to identical morphisms. For example,  $\circ\, i_{3,6} =$  $\circ\, i_{3,6}$.

An LS-module is a functor from LS to the category of vector spaces (over, say, a field $\mathbb{K}$).

To elucidate the above definition, note that an LS-module comprises of a chain $\{V_n\}_{n\in\mathbb{N}}$, where each V_n is a (left) representation (or module) of TL_n, and for every inclusion $i_{m,n} : M_m \hookrightarrow M_n$, there is a TL-equivariant map $(i_{m,n})_* : V_m \to V_n$. Of course, there are more properties which an LS-module will need to satisfy, and we will discuss that in future Subsections.

We will end this Subsection by defining finite generation: the key features of representation stability are obtained only when the stable modules are finitely generated. For example, in the world of FI-modules, the eventually-polynomial behavior of characters requires finite generation to hold.

Definition 3.5.2 (Finite generation of LS-modules)**.** Suppose that $\{V_n\}_{n\in\mathbb{N}}$ is an LS-module. For any collection $x_1, .., x_k \in V_{m_1}, ..., V_{m_k}$, we let $\mathrm{span}(x_1, .., x_k)$ denote the LS-submodule generated via TL_n actions on each V_n and inclusions $(i_{m,n})_*$ for each $m < n$. We define the rank:

$$\mathrm{rk}_{\mathrm{LS}}(\{V_n\}_{n\in\mathbb{N}}) = \min\{k \mid \text{ there exists } x_1, .., x_k \text{ such that } \mathrm{span}(x_1, .., x_k) = \{V_n\}_{n\in\mathbb{N}}\}$$

We say that $\{V_n\}_{n\in\mathbb{N}}$ is finitely generated if $\mathrm{rk}_{\mathrm{LS}}(\{V_n\}_{n\in\mathbb{N}}) < \infty$.

3.5.2 General form of a stable module criterion

It is useful in representation stability to have a criterion for determining whether a chain of representations is stable or not. For example, in the case of symmetric groups S_n, the

FI-module criterion says that (see for instance Exercise 9 of [60] (Wilson)):

Proposition 3.5.3 (The FI-module criterion)**.** *A sequence* $\{V_n\}_{n\in\mathbb{N}}$ *of symmetric group representations together with maps* $\{(i_{m,n})_* : V_m \to V_n\}_{m<n}$ *is an* FI*-module if and only if*

(a) *(Compatibility of inclusions) For any* $k < m < n$*,*

$$(i_{m,n})_* \circ (i_{k,m})_* = (i_{k,n})_*$$

(b) *(Equivariance of* $(i_{m,n})_*$*) For any* $\tau \in S_m \hookrightarrow S_n$*,*

$$\tau \circ (i_{m,n})_* = (i_{m,n})_* \circ \tau$$

(c) *(The* FI*-module criterion) For any* $\sigma \in S_{n-m}$*,*

$$\sigma\emptyset(i_{m,n})_* = (i_{m,n})_*$$

We now state the general form of a stable module criterion, which will be useful for us.

Proposition 3.5.4 (General form of a stable module criterion)**.** *Let* $\{\mathcal{A}_n\}_{n\in\mathbb{N}}$ *be a family of monoids which include into one another, and let* $\{M_n\}_{n\in\mathbb{N}}$ *be a collection of finite sets such that* M_n *carries an action of* $\mathcal{A}_n$*, and suppose that there are* $\mathcal{A}_m$*-equivariant maps* $i_{m,n} : M_m \hookrightarrow M_n$ *for* $m < n$*. Consider the category whose objects are* $\{M_n\}_{n\in\mathbb{N}}$ *and whose morphisms are generated by elements of* $\{\mathcal{A}_n\}_{n\in\mathbb{N}}$ *together with* $\{i_{m,n}\}_{m<n}$*. Suppose we define a stable module to mean a functor from this category to the category of vector spaces. Then,* $\{V_n\}_{n\in\mathbb{N}}$ *together with maps* $(i_{m,n})_* : V_m \to V_n$ *(the image of* $i_{m,n}$*) is a stable module if and only if:*

(a) *(Compatibility of inclusions) For any* $k < m < n$,

$$(i_{m,n})_* \circ (i_{k,m})_* = (i_{k,n})_*$$

(b) *(Equivariance of* $(i_{m,n})_*$*) For any* $\tau \in \mathcal{A}_m \hookrightarrow \mathcal{A}_n$,

$$\tau \circ (i_{m,n})_* = (i_{m,n})_* \circ \tau$$

(c) *(The stable-module criterion) If* $a, b \in \mathcal{A}_n$ *are such that* $a \circ i_{m,n} = b \circ i_{m,n}$*, then*

$$a \circ (i_{m,n})_* = b \circ (i_{m,n})_*$$

Proof. We need to show that any relation between the morphisms ($\{\mathcal{A}_n\}_{n\in\mathbb{N}}$ and $\{i_{m,n}\}_{m<n}$) can be reduced to relations of the above form.

Note first that (1) and (2) must hold since inclusions on $\{M_n\}_{n\in\mathbb{N}}$ are equivariant and compatible. Our task is therefore to show that the only other possible relation is (3).

By (1), and since $a, b \in \mathrm{TL}_k \implies ab \in \mathrm{TL}_k$, the relation must be of the form:

$$a_n i_{m_d,n} \ldots i_{m_2,m_3} a_{m_2} i_{m_1,m_2} a_{m_1} = a'_{n'} i_{m'_d,n} \ldots i_{m'_2,m'_3} a'_{m'_2} i_{m'_1,m'_2} a'_{m'_1}$$

By (2), we may move all the a_is to the left, and applying (1) again, we see that any remaining relation is of the form:

$$a i_{m,n} = b i_{m',n'}$$

Comparing domain and range, we see that $m = m'$ and $n = n'$. Therefore, any relation other than (1) and (2) must be of the form:

$$ai_{m,n} = bi_{m,n}$$

□

3.5.3 A chain of standard representations of TL_n is representation stable

The general form of a stable module criterion allows us to observe some general principles to construct stable modules. This will allow us to see that the chains of standard representations are LS-modules.

Proposition 3.5.5 (General principles for constructing stable modules)**.** *Let $\{\mathcal{A}_n\}_{n\in\mathbb{N}}$ be a family of monoids. Suppose the sequence $\{V_n\}_{n\in\mathbb{N}}$ together with maps $(i_{m,n})_* : V_m \to V_n$ is a stable sequence of $\mathcal{A}_n$ representations. Let $\{K_n\}_{n\in\mathbb{N}}$ be a sequence of subrepresentations ($K_n \leq V_n$) such that $(i_{m,n})_* K_m \leq K_n$. Then:*

(a) *$\{K_n\}_{n\in\mathbb{N}}$ is a stable sequence of representations.*

(b) *$\{V_n / K_n\}_{n\in\mathbb{N}}$ is a stable sequence of representations.*

Proof. For both (1) and (2), inclusions are well defined because $(i_{m,n})_* K_m \leq K_n$. Inclusions are obviously compatible in both cases. Moreover, since $(i_{m,n})_*$ is equivariant as a map from V_m to V_n, we see that this equivariance is preserved for submodules and quotient modules.

Finally, if $a \sim_m b$, then $a\phi(i_{m,n})_* = b\phi(i_{m,n})_*$ holds for $\{V_n\}_{n\in\mathbb{N}}$, and therefore, $a\phi(i_{m,n})_* \restriction_{K_m} = b\phi(i_{m,n})_* \restriction_{K_m}$, and thus (1) satisfies the stable module criterion. (2) satisfies

the stable module criterion because an equality which holds in a vector space must also hold in any quotient (an equality in a quotient is a weaker statement than equality). □

We next introduce a simple shorthand notation which will allow us to freely start at any $N \in \mathbb{N}$ rather than at 1, by which we mean:

Observation 3.5.6 (Starting from N)**.** Suppose that we are given a functor from the subcategory of LS whose objects are $\{M_n\}_{n \geq N}$ to the category of vector spaces, and let V_n be the image of M_n. Set $V_0 = V_1 = ... = V_{N-1} = 0$, and let the images of inclusions to and from V_k for $k \leq N$ to be zero maps. Then, $\{V_n\}_{n \in \mathbb{N}}$ is a stable sequence of representations.

Proof. This is true since inclusions of 0 modules are trivially compatible, trivially and the stable module criterion trivially holds - hence, all three requirements of Proposition 3.5.4 are satisfied. □

In light of the above observation, it will be convenient for us to refer to functors from the subcategory of LS whose objects are $\{M_n\}_{n \geq N}$ to the category of vector spaces also as LS-modules, and we will denote them by $\{V_n\}_{n \geq N}$.

For the representation stability of Temperley-Lieb algebras, the generalities above actually provide us useful information, because the representation theory of TL_n revolves around the standard representations, which are quotients of the $\mathbb{C}$-span of M_n (which we will denote by $\mathbb{C}M_n$). Following the notation of [44] (Ridout, Saint-Aubin), we will denote the standard representation generated by (n, p) link states by $V_{n,p}$.

Corollary 3.5.7 (Chains of standard representations are stable)**.** *For p fixed, consider the sequence $\{V_{n,p}\}_{n\geq N}$, a sequence of standard representations of (n,p) link states together with the inclusions induced by inclusions on $\{M_n\}_{n\in\mathbb{N}}$. Then, $\{V_{n,p}\}_{n\geq N}$ is an* LS*-module*

Proof. For each p, $V_{n,p}$ is a quotient module:

$$V_{n,p} = \mathbb{K}\left(\bigcup_{q\geq p}\{(n,q) - \text{link states}\}\right) \Big/ \mathbb{K}\left(\bigcup_{q>p}\{(n,q) - \text{link states}\}\right)$$

The inclusion of a (n,q) link state remains a (n,q) link state. Therefore, $V_{n,p}$ is a quotient of a submodule of $\mathbb{C}M_n$, and the hypotheses of Lemma 3.5.5 are satisfied for both the submodule and the sub-submodule in question. Therefore, we conclude by Lemma 3.5.5 that $\{V_{n,p}\}_{n\geq N}$ is an LS-module. □

Moreover, chains of standard representations have LS-rank 1 (in particular, they are finitely generated).

Proposition 3.5.8 (Chain of standard representations have LS-rank 1)**.**

$$\mathrm{rk}_{\mathrm{LS}}\{V_{n,p}\}_{n\geq N} = 1$$

Proof. Take any (N,p) link state v in $V_{N,p}$. For each $n \geq N$, $(i_{N,n})_* v$ is then a (n,p) link state of $V_{n,p}$. Every diagram element of $V_{n,p}$ which is not in the kernel of the usual bilinear form on $V_{n,p}$ is a cyclic generator of $V_{n,p}$ (see for example [44] (Ridout, Saint-Aubin), the proof of Proposition 3.3), and thus, when $\delta \neq 0$, every link state is a cyclic generator of $V_{n,p}$ - this is because for $\delta \neq 0$, the inner product of a link state with itself is some power of δ (and we are considering the case when $\delta = 1$). Therefore, by cyclicity we deduce that $\mathrm{span}(v) = \{V_{n,p}\}_{n\geq N}$. Hence, $\mathrm{rk}_{\mathrm{LS}}\{V_{n,p}\}_{n\geq N} = 1$. □

3.5.4 Example: an infinite-link-state representation of TL(∞) which is not stable

As a matter of curiosity and/or completeness, a reader who is interested in stability might ask for an example of a representation of TL(∞) which is not an LS-module. We will produce such an example in this Subsection. First, we need to learn how to translate between the notion of TL(∞)-representations and the notion of LS-modules. We may do that as follows:

Observation 3.5.9. Suppose that $\{V_n\}_{n\in\mathbb{N}}$ is an LS-module with the additional property that $V_m \subseteq V_n$ for $m \leq n$, and $(i_{m,n})_*$ is this inclusion. Then, $\bigcup_{n\in\mathbb{N}} V_n$ is a representation of TL(∞)

Proof. Given $a \in \mathrm{TL}(\infty)$ and $v \in \bigcup_{n\in\mathbb{N}} V_n$, define $a \cdot v$ as follows: we may choose N large enough such that $a \in \mathrm{TL}_N \leq \mathrm{TL}(\infty)$ and $v \in V_N$. Then define $a \cdot v$ to be via the action of TL_N on V_N. We must show that this is well defined (i.e does not depend on the choice of N). Suppose that $N_1 \leq N_2$ and consider $a \in \mathrm{TL}_{N_1}, \mathrm{TL}_{N_2}$ and $v \in V_{N_1}, i_{N_1,N_2}v \in V_{N_2}$. Then, by the equivariance of $(i_{N_1,N_2})_*$ (see Proposition, 3.5.4) $a(i_{N_1,N_2})_*v = (i_{N_1,N_2})_*av = av$, where the second equality followed from the hypothesis that $(i_{m,n})_*$ was the inclusion. This proves well definedness of the above action. □

Definition 3.5.10. Given a representation V of TL(∞), we say that
V corresponds to an LS-module if there is an LS-module $\{V_n\}_{n\in\mathbb{N}}$ such that: $V = \bigcup_{n\in\mathbb{N}} V_n$, as in the statement of the observation above.

In [39] (Moore), the author constructs representations of TL(∞) which are generated by infinite link states (one is allowed infinitely many cups if one desires). He denotes the link

state representation generated by a link state w by $\chi(w)$ - we will instead denote it by $V(w)$.

Example 3.5.11. (An infinite-link-state representation of TL(∞) which is not stable). Consider the infinite link state $w = \left(\cup\uparrow\uparrow\cup\uparrow\uparrow\cup\uparrow\uparrow \cdots \right)$. Suppose for contradiction that $V(w)$ corresponds to an LS-module. Then, there is an LS-module $\{V_n\}_{n\in\mathbb{N}}$ such that $V(w) = \bigcup_{n\in\mathbb{N}} V_n$. So, there is some $m \in \mathbb{N}$ such that $w \in V_m$. But then, there is some $m' > m$ such that on the strands $m', m'+1, m'+2, m'+3$, $V(w)$ has the pattern $\left(\cup\uparrow\uparrow \right)$. Let $a \in \mathrm{TL}_{m'+3}$ comprise of identity-map loose-strands at all positions less than m', and, from m' to $m'+3$ looks like: $\left(\right)$. Let $b \in \mathrm{TL}_{m'+3}$ comprise of identity-map loose-strands at all positions less than m', and, from m' to $m'+3$ looks like: $\left(\right)$. Observe that $a \circ i_{m,m'+3} = b \circ i_{m,m'+3}$ but $a \circ (i_{m,m'+3})_*(w) \neq b \circ (i_{m,m'+3})_*(w)$, since $a \circ (i_{m,m'+3})_*(w)$ has $\left(\cup\cup \right)$ at positions $m', m'+1, m'+2, m'+3$ whereas $b \circ (i_{m,m'+3})_*(w)$ has $\left(\cup\uparrow\uparrow \right)$ at positions $m', m'+1, m'+2, m'+3$. Therefore, $\{V_n\}_{n\in\mathbb{N}}$ does NOT satisfy the stable module criterion of 3.5.4, and hence is not an LS-module.

3.5.5 Defining topological stability

In the analogous story for symmetric groups, configuration spaces are natural candidates for a notion of topological stability. However, even there, it is not clear (at least to us), that there could not exist any other natural notion of topological stability of S_n-spaces, which has the property that chains of homology groups become finitely generated FI-modules. Similarly, we do not claim here that the notion of topological stability that we present here is somehow overarching - indeed, there could be families of topological stable spaces which we have entirely missed. However, we will define a notion which appears natural to us: In Subsection 3.3.4, we saw that associated to every topological action we may define an

intrinsic filtration $\mathcal{F}$; recall that $\mathcal{F}$ is intrinsic in the sense that all p-intersections are homeomorphic by Lemma 3.3.7. Since filtrations have a natural notion of stability, we may carry over this notion to define stability for a chain of TL_n-spaces, as follows:

Definition 3.5.12 (p-filtration stability)**.** Let $Y_N \subseteq Y_{N+1} \subseteq Y_{N+2} \subseteq ..$ be a chain of finite-CW surjective TL_n-spaces, such that:
(1) The inclusions $Y_n \subseteq Y_{n+1}$ are inclusions of TL_n-spaces (i.e TL_n-equivariant).
(2) $Q = \{*\}$ for each Y_n

Let

$$\mathcal{F}_n = R_1^{(n)} \supseteq R_2^{(n)} \supseteq ... \supseteq \{*\}$$

be the filtration associated to Y_n. $\{Y_n\}_{n \geq N}$ is said to be p-filtration stable if, for all $q \geq p$ and all $n \geq N$ $R_q^{(n)} = R_q^{(N)}$.

3.5.6 p-filtration stability results in representation stability of homology groups

We will show in this Subsection how p-filtration stability implies the representation stability of certain quotients of homology groups. These quotients will be quotients in the Grothendieck group, and thus we require some notation:

Definition 3.5.13 (Quotients in the Grothendieck group)**.** Suppose that $U_1, .., U_l$ are indecomposable representations of an algebra A with the property that representations in the split Grothendieck group generated by $U_1, .., U_l$ have unique direct sum decompositions in terms of $U_1, .., U_l$. Suppose that $V = \bigoplus_{i=1}^{l} U_i^{\oplus m_i}$. Then, we denote:

$$V \Big/ [U_{i_1}], ..., [U_{i_d}] = \bigoplus_{i \in \{1,...,l\} - \{i_1,...,i_d\}} U_i^{\oplus m_i}$$

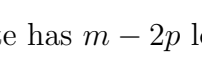
We call it a quotient in the Grothendieck group generated by $U_1, .., U_l$, since the Grothendieck bracket of the resulting representation is equal to $[V] \Big/ [U_{i_1}], ..., [U_{i_d}]$ in the quotient of the split Grothendieck group by $[U_{i_1}], ..., [U_{i_d}]$.

We can now state and prove the theorem of this Subsection, which is the second result stated in the introduction, and which can be viewed as a corollary of the work we did in Section 3.4:

Corollary 3.5.14. *Let $\{Y_n\}_{n \geq N}$ be a p-filtration stable chain of* TL*-spaces. Let $\mathbb{K}$ be a field containing $\mathbb{Q}$. Then, for each k, $\{H_k(Y_n, \mathbb{K}) \Big/ [V_{n,1}], ..., [V_{n,p-1}]\}_{n \geq N}$ is a finitely generated* LS*-module.*

Proof. Since $\{Y_n\}_{n \geq N}$ is p-filtration stable, we know that for any $n \geq N$ and $q \geq p$, $R_q^{(n)} = R_q^{(N)}$. Theorem 3.4.17gives us an explicit formula for $H_k(X, \mathbb{K})$ in terms of the filtration $\mathcal{F}$, and observe that since $R_q = R_p$ for $q \geq p$ for $n \geq N$, and since the contribution of $V_{n,p}$ in our formula only depends on R_q for $q \geq p$, we see that

$$\{H_k(Y_n, \mathbb{K}) \Big/ [V_{n,1}], ..., [V_{n,p-1}]\}_{n \geq N} = \{V_{n,p}^{\oplus s_1} \oplus .... \oplus V_{n,p_{max}}^{\oplus s_{p_{max}}}\}_{n \geq N}$$

where p_{max} is the largest q such that $R_q \neq \{*\}$, which is the same for all $n \geq N$ by filtration stability. Moreover, note that for $m, n \geq N$ the induced inclusion on homology takes, in the notation of the proof of Theorem 3.4.12, h  to h , where the first link state has $m - 2p$ loose strands while the second has $n - 2p$ loose strands. The rest of the map is determined by cyclicity, and thus if we restrict the map to any standard representation we see that the restriction $(i_{m,n})_* \restriction_{V_{m,q}} V_{m,q} \to V_{n,q}$ is just the

usual LS-module map associated with the chain of standard representations $\{V_{n,q}\}_{n\in\mathbb{N}}$, in the sense of Corollary 3.5.7. Thus, in light of Observation 3.5.6, we conclude that $\{H_k(Y_n,\mathbb{K})\Big/[V_{n,1}],...,[V_{n,p-1}]\}_{n\geq N}$ is a finitely generated LS-module. □

3.5.7 Examples of topological stability

The goal of this Subsection is to give a couple of examples of topological stability. This Section will likely not only be useful to a reader who is interested in topological stability, but will also be useful to a reader who wants to understand topological actions as in Section 3.3.

Example 3.5.15. Just as before, let $d_{n,p}=\dim V_{n,p}=\binom{n}{p}-\binom{n}{p-1}$. Let $n\geq 2p$. Let $Y_{n,p}$ be the wedge of $d_{n,p}$ copies of S^2. Let the filtration associated to TL_n-action on S^2 be

$$\mathcal{F}_{n,p}=\vee_{d_{n-2,p-1}}S^2\supseteq\vee_{d_{n-4,p-2}}S^2\supseteq...\supseteq\vee_{d_{n-2p,1}}S^2\supseteq S^2\supset\{*\}\supset...\supset\{*\}$$

In particular note that if $A_1,...,A_{n-1}$ are the retracts given by $u_1,...,u_{n-1}$, we have that $A_i\cong\vee_{d_{n-2,p-1}}S^2$ for each i. There is a well defined action of TL_n on $Y_{n,p}$ with this filtration. Before we spoil how to "cheat and define the action easily", the reader is encouraged to define this action for some small values of n and p, to appreciate the fact that a "naive approach" of writing down the actions from a topological perspective requires a little thought, since one needs to be careful that the retractions must be chosen to be compatible with one another. Nevertheless, one can do it. In this spirit, we have illustrated below an example for $n=5$ and $p=2$.

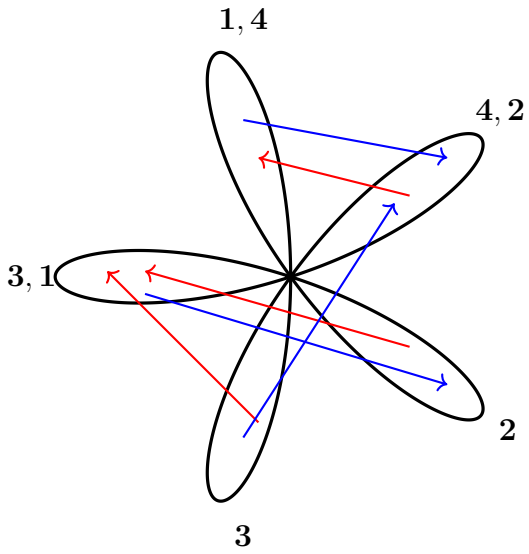


Figure 3.9: Above is a schematic of $Y_{5,2}$. This has a filtration $S^2 \vee S^2 \supseteq S^2 \supseteq \{*\}$. In particular, note that each $A_i \cong S^2 \vee S^2$. The numbers next to the copies of S^2 indicate the minimal intersection containing that copy. For example, $1, 4$ means that the minimal intersection containing that copy is $A_1 \cap A_4$. The action is as follows: each u_i preserves A_i, takes A_{i-1} and A_{i+1} isomorphically to A_i and retracts A_j to A_i for $|j-i| \geq 2$. However, these isomorphisms and retractions must be chosen carefully so as to not lead to any contradictions - this is really the heart of the matter. In red arrows above, we have drawn the action of u_1. In blue arrows above, we have drawn the action of u_2. The action of u_3 is similar to the action of u_2 and the action of u_4 is similar to the action of u_1

The spoiler is that the "backwards cheating way" to define this action is to assign one copy of S^2 for each (n, p) link state, TL_n action permutes the copies of S^2 via the actions on link states.

In any case, for p fixed, $\{Y_{n,p}\}_{n \in \mathbb{N}}$ is p-filtration stable since the filtration stabilizes after position $\geq p$, and therefore we know that $H_k(Y_{n,p}) \Big/ [V_{n,1}], ..., [V_{n,p-1}]$ is a finitely generated LS-module. Explicitly, we know that for $i \neq 2$, $H_i(Y_{n,p}) = 0$ for all n and p, and for $i = 2$,

as an LS-module:

$$\{H_2(Y_{n,p})\}_{n\geq 2p} = \{V_{n,p}\}_{n\geq 2p} =: V_{*,p}$$

At this point, we would like to emphasize the importance of Theorem 3.4.17. It guarantees us that every space which is a wedge of 2-spheres is a wedge of spaces of the above form. This justifies us to use the "backwards cheating trick" to construct actions. Without the theorem, a priori one might have believed that there are other actions possible which would give us other representations.

Example 3.5.16. Let $\{c_n\}_{n\geq 2}$ be a sequence of integers such that $c_n \geq \max\{d_{n,2}, n-1\}$ for each n. Given the c_n-torus $T^{c_n} = S^1 \times S^1 \times ... \times S^1$, we have a non-surjective action of TL_n on T^{c_n} by projecting onto the first $n-1$ coordinates. We will use this to construct a surjective action on a bigger space, and the sequence of such bigger spaces will be 2-filtration stable, with filtration:

$$T^{c_n} \supseteq S^1 \supseteq \{*\} \supseteq ... \supseteq \{*\}$$

Let us first, for concreteness, define the non-surjective action explicitly. We think of T^n as $(\mathbb{R}/\mathbb{Z})^n$. If we let p_j denote the projection onto the jth coordinate, we define, for $i \in \{1, 2, 3, ..., n-1\}$:

$$p_j r_i(x_1, ..., x_{c_n}) = \begin{cases} x_{i-1} + x_i + x_{i+1}\delta_{i+1\leq n-1} & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}$$

This is a well defined action since, if $|i_1 - i_2| \geq 2$ then $r_{i_1} r_{i_2} = 0 = r_{i_2} r_{i_1}$, and

$$p_j r_i r_{i\pm1} r_i(x_1, ..., x_{c_n}) = \begin{cases} x_{i-1} + x_i + x_{i+1}\delta_{i+1\leq n-1} & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases} = r_i(x_1, ..., x_{c_n})$$

Out of this non-surjective action we construct a surjective action on another space as follows by taking $n-1$ copies of T^{c_n} and glue them along the retracts. More precisely, let $(T^{c_n})_1, ..., (T^{c_n})_{n-1}$ be the $n-1$ copies of the tori, let $(T^{c_n})_{ij}$ denote the jth copy of S^1 in $(T^{c_n})_i$, that is: $0 \times 0 \times ... \times 0 \times (S^1)_j \times 0 \times ... \times 0_{c_n} \subset (T^{c_n})_i$. And we define

$$Y_n = \bigsqcup_{i=1}^{n-1} (T^{c_n})_i \Big/ (T^{c_n})_{kl} \sim (T^{c_n})_{lk} \text{ for } |k-l| \geq 2$$

Y_n admits an action of TL_n as follows: Modify Example 3.5.15 by replacing S^2 with S^1. This does not change any of the interesting properties of $Y_{n,2}$. Next, observe that since we have c_n components, and since our modified $Y_{n,2}$ is a wedge of $d_{n,2}$ circles, we should consider $Y_{n,2} \vee (\vee_{(c_n - d_{n,2})} Y_{n,1})$. For each $i \in \{1, 2, 3, ..., n-1\}$, let $\left[Y_{n,2} \vee (\vee_{(c_n-d_{n,2})} Y_{n,1})\right]_i$ denote the retract which we usually call A_i.

Intuitively: we construct the action on Y_n as follows: If $|j-i| \geq 2$, then u_j acts on the 1 skeleton of $T_i^{c_n}$ via the retraction on $\left[Y_{n,2} \vee (\vee_{(c_n-d_{n,2})} Y_{n,1})\right]_i$. The rest of the map is determined by linearity. Next, if $j = i \pm 1$, then u_j takes $T_i^{c_n}$ to $T_j^{c_n}$ via the isomorphism which is defined on the 1 skeleton by the isomorphism
$u_j : \left[Y_{n,2} \vee (\vee_{(c_n-d_{n,2})} Y_{n,1})\right]_i \to \left[Y_{n,2} \vee (\vee_{(c_n-d_{n,2})} Y_{n,1})\right]_j$, and the rest of the map is determined by linearity.

More formally: for each i, take the lengths of all loops in $\left[Y_{n,2} \vee (\vee_{(c_n-d_{n,2})} Y_{n,1})\right]_i$ to be 1, and likewise take the lengths of all loops in the 1-skeleton of $T_i^{c_n}$ to be 1. Then, for each i, fix an isometry:

$\phi_i : \left[Y_{n,2} \vee (\vee_{(c_n - d_{n,2})} Y_{n,1})\right]_i \cong$ 1-skeleton of $T_i^{c_n}$ which is given by considering components

with the property that for each i, j,

$$\phi_i(u_j \cdot \left[Y_{n,2} \vee (\vee_{(c_n - d_{n,2})} Y_{n,1})\right]_i) = T_{ij}^{c_n}$$

We then define the action of TL_n on Y_n by setting: For each i,

$$u_i(x_1, ..., x_{c_n}) = \begin{cases} \sum_{s=1}^{c_n} \phi_i \circ u_i \circ \phi_{i\pm1}^{-1} x_s \in T_i^{c_n} & \text{if } (x_1, ..., x_{c_n}) \in (T^{c_n})_{i\pm1} \\ \sum_{s=1}^{c_n} \phi_j \circ u_i \circ \phi_j^{-1} x_s \in T_{ji}^{c_n} & \text{if } (x_1, ..., x_{c_n}) \in (T^{c_n})_j \text{ where } |j-i| \geq 2 \end{cases}$$

$$= \begin{cases} \sum_{s=1}^{c_n} \phi_i \circ u_i \circ \phi_{i\pm1}^{-1} x_s \in T_i^{c_n} & \text{if } (x_1, ..., x_{c_n}) \in (T^{c_n})_{i\pm1} \\ r_i(x_1, ..., x_{c_n}) \in T_{ji}^{c_n} & \text{if } (x_1, ..., x_{c_n}) \in (T^{c_n})_{ji} \text{ where } |j-i| \geq 2 \end{cases}$$

Then, since the action of TL_n on $Y_{n,2} \vee (\vee_{(c_n - d_{n,2})} Y_{n,1})$ is well defined, the action of TL_n on Y_n is well defined, as is best seen by considering the first line in the above equation together with the reminder that $T_{ji}^{c_n} \sim T_{ij}^{c_n}$. Below is a schematic of Y_4.

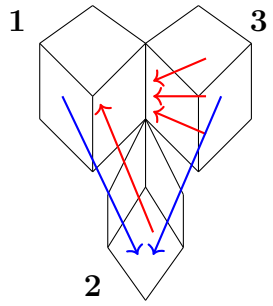


Figure 3.10: A schematic of Y_4. We have taken $c_4 = 3$. The cubes of course depict 3-tori. The numbers $1, 2, 3$ depict the retracts A_1, A_2, A_3 respectively - each of which is a 3-torus. The red arrows depict the action of u_1 - A_3 retracts to the copy of $S^1 \subset A_1 \cap A_3$ while A_2 is taken isomorphically to A_1. The blue arrows depict the action of u_2 - both A_1 and A_3 are taken isomorphically to A_2. The action of u_3 is similar to the action of u_1.

Now, since the filtrations $\{\mathcal{F}_n\}_{n\geq 2}$ stabilize at $p = 2$, we know from Theorem 3.5.14 that for each k, $H_k(Y_n) \Big/ [V_{n,1}]$ is a finitely generated LS-module. Moreover, by Theorem 3.4.17, we know that the generators of this LS module all lie in $R_2 = S^1$. It therefore follows that for $k > 1$, $H_k(Y_n) \Big/ [V_{n,1}] = 0$ and for $k = 1$, $H_k(Y_n) \Big/ [V_{n,1}] = V_{n,2}$. Therefore, as an LS-module,

$$H_k(Y_n) \Big/ [V_{n,1}] = \{V_{n,2}\}_{n\geq 2} =: V_{*,2}$$

Notice that while $H_k(Y_n) \Big/ [V_{n,1}] = \{V_{n,2}\}_{n\geq 2}$ is a finitely generated LS-module, $\{H_k(Y_n)\}_{n\geq 2}$ is NOT a finitely generated LS-module in general since, by Theorem 3.4.17, we may explicitly decompose $H_k(Y_n) = V_{n,2} \oplus V_{n,1}^{\oplus(c_n - d_{n,2})}$, and we may choose c_n to grow faster than quadratically, so that $H_k(Y_n)$ fails to be finitely generated. This demonstrates why we needed to take a quotient in the statement of Theorem 3.5.14. Lastly, notice that we constructed this family of TL_n-spaces by, to an extent, "working backwards". Theorem

3.4.17suggests to us that we ought to be able to work backwards to construct an arbitrary TL_n-space.

Chapter 4

On cryptographic efficacy and representation gap of diagrammatic monoid chains

This chapter is based on the paper [38], which is joint work with Mikhail Khovanov and Daniel Tubbenhauer.

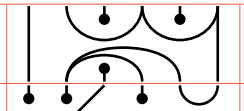
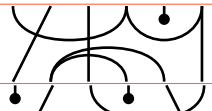
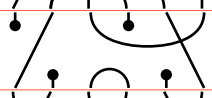
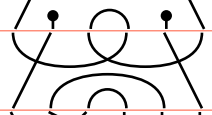
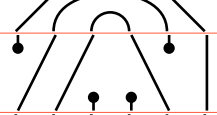
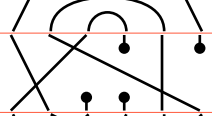
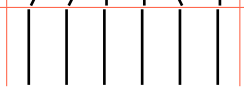
Consider a chain of diagrammatic monoids:

$$0 \hookrightarrow S_1 \hookrightarrow S_2 \hookrightarrow ...$$

We can consider cryptographic procedures (for example Diffie-Hellman) for each S_n and hope that as n becomes large, the cryptographic procedures become difficult to break. The most important cryptographic protocols in use today are based on *commutative groups* and deliver a gold standard for cryptography. On the other hand, *noncommutative group-based* and *monoid-based* protocols seem to be less understood and in many cases admit efficient attacks. One such kind of attack is a linear attack: As shown by Myasnikov and Roman'kov [40] (and also based on earlier work), cryptographic protocols on non-commutative monoids be successfully attacked if the monoid admits small nontrivial representations.

Therefore, the goal of this chapter is to explore families of diagrammatic monoids which resist these linear attacks, in the sense that they have what we call a "large representation gap". One of our main tools is Green's theory of cells (Green's relations). Another crucial idea is the idea of truncations - we may truncate monoids in order to remove small representations. We show that suitable truncations of several diagrammatic families on monoids have a large representation gap and therefore resist linear attacks.

The following table summarizes our list of diagrammatic monoids and results. In order to make components of size one visible we use loose dotted ends. We also indicate whether their nontrivial representations are reasonably big (the "Big reps" column), meaning after appropriate cell truncation. Hereby * means that they have such representations but still come with an aftertaste (such as being semisimple in some cases), $_c$ means conjectural (everything is proved except for results regarding potential nontrivial extensions of the trivial representations) and EX means excluded from the discussion due to triviality. This is explained in more details in Conclusion 4.4.11 and Conclusion 4.5.27.

Symbol	Diagrams	Big reps	Symbol	Diagrams	Big reps
pPa_n		YES*	Pa_n		YES$^*_c$
Mo_n		YES$_c$	RoBr_n		YES$^*_c$
TL_n		YES	Br_n		YES*
pRo_n		YES*	Ro_n		YES*
pS_n		EX	S_n		NO

. (4.0.0.1)

The left half of the table above contains *planar* monoids, the right half *symmetric* monoids. We discuss all of these monoids and their representation gaps

4.1 Representation gaps, faithfulness, and extensions

For background we refer the reader to standard textbooks such as [8], respectively [55], for the basic theory of finite-dimensional representations of finite-dimensional algebras (such as monoid algebras), respectively, finite monoids.

Notation 4.1.1. *We let* S *denote a finite monoid. If not stated otherwise, we work over*

an arbitrary field $\mathbb{K}$ *and consider only finite-dimensional (left)* S*-representation with ground field* $\mathbb{K}$*. The adjective* small *and* big *used for* S*-representations will mean dimension-wise, where dimension is measured with respect to* $\mathbb{K}$*.*

4.1.1 Representation gaps

We start with a subtle difference between groups and monoids: the latter may have two types of "trivial" representations.

Definition 4.1.2. Let $\mathrm{G} \subset \mathrm{S}$ be the subgroup of all invertible elements of S. Then we define *trivial representations*

$$\mathbb{1}_b \colon \mathrm{S} \to \mathbb{K}, \quad s \mapsto \begin{cases} 1 & \text{if } s \in \mathrm{G}, \\ 0 & \text{else}, \end{cases} \qquad \mathbb{1}_t \cong \mathbb{1} \colon \mathrm{S} \to \mathbb{K}, \quad s \mapsto 1.$$

A S-representation M is called *trivial* if $M \cong \mathbb{1}_b$ or $M \cong \mathbb{1}_t$.

The subscripts b and t are short for *bottom* and *top*, respectively. The top trivial representation $\mathbb{1}_t$ is also what is called the trivial representation $\mathbb{1}$ of S, the unit object of the monoidal category of representations of S with $\mathbb{1} \otimes M \cong M$ for any S-representation M.

Remark 4.1.3. The notation is justified as follows. The S-representation $\mathbb{1}_b$ is one of the simple S-representations associated with the bottom J-cell $\mathcal{J}_b = \mathrm{G}$, while the S-representation $\mathbb{1}_t$ is associated with the top J-cell $\mathcal{J}_t$, cf. Lemma 4.2.7 below.

Lemma 4.1.4. *Both,* $\mathbb{1}_b$ *and* $\mathbb{1}_t$ *are simple* S*-representations of dimension one. Moreover,* $\mathbb{1}_b \cong \mathbb{1}_t$ *if and only if* S *is a group.*

Proof. Immediate from the definitions. □

Notation 4.1.5. *We write* $\mathbb{1}_{bt}$ *short for either* $\mathbb{1}_b$ *or* $\mathbb{1}_t$*. In particular,* $\mathbb{1}_{bt}^{\oplus m}$ *means any of the* 2^m *possible direct sums of* $\mathbb{1}_b$ *and* $\mathbb{1}_t$ *with* m *symbols in total.*

For cryptographic purposes it should be interesting to collect examples of naturally occurring finite monoids S such that any representation of sufficiently small dimension relative to |S|, the size of S, is suitably trivial. Note that all elements of $S \setminus G$ act in the same way on any of the direct sums $\mathbb{1}_{bt}^{\oplus m}$ and these representations cannot distinguish any two elements of $S \setminus G$. Thus, suitably trivial could mean being isomorphic to $\mathbb{1}_{bt}^{\oplus m}$ which we take as the definition:

Definition 4.1.6. A pair $(S, \mathbb{K})$ of a monoid $S \ncong 1$ and a field $\mathbb{K}$ is called *m-trivial* if S-representations M with $\dim_{\mathbb{K}}(M) \leq m$ satisfy $M \cong \mathbb{1}_{bt}^{\oplus \dim_{\mathbb{K}}(M)}$. Moreover, by conventions, the trivial monoid is (-1)-trivial for all $\mathbb{K}$.
The maximal m such that $(S, \mathbb{K})$ is $(m-1)$-trivial is called the *representation gap* of $(S, \mathbb{K})$ and is denoted by $\mathrm{gap}_{\mathbb{K}}(S)$.

Note that the m-triviality is a lower bound on the dimension of the smallest nontrivial simple S-representation, assuming the absence of extensions between trivial representations $\mathbb{1}_t$ and $\mathbb{1}_b$, see also Lemma 4.1.12 and Lemma 4.1.14 below.

Definition 4.1.7. A monoid S is called *m-trivial* if $(S, \mathbb{K})$ is m-trivial for all $\mathbb{K}$.
The maximal m such that S is $(m-1)$-trivial is called the *representation gap* of S and is denoted by $\mathrm{gap}_*(S)$.

Notation 4.1.8. *Below we will meet several notions similar to* $\mathrm{gap}_{\mathbb{K}}(S)$ *and* $\mathrm{gap}_*(S)$. *For all of them it makes sense to vary the field which we indicated using* $*$. *Whenever the difference does not play a role we simply write* $\mathrm{gap}(S)$.

Remark 4.1.9 (***Main Task 1***). For cryptographic applications it should be useful to have a supply of monoids $\{S_n | n \in \mathbb{Z}_{\geq 0}\}$ with exponentially big $\mathrm{gap}(S_n)$ as $n \to \infty$.

Example 4.1.10. A pair $(S \ncong \mathbb{1}, \mathbb{K})$ is 0-trivial if and only if any there exists a one-dimensional S-representation which is nontrivial. In particular, if S has a nontrivial one-dimension representation, then $\mathrm{gap}_{\mathbb{K}}(S) = 1$.

Lemma 4.1.11. *The pair* $(\mathrm{S}, \mathbb{K})$ *is* m*-trivial if and only if* S*-representations* M *with* $\dim_{\mathbb{K}}(M) = m$ *satisfy* $M \cong \mathbb{1}_{bt}^{\oplus m}$.

Proof. By the unique decomposition property of finite-dimensional representations. □

Lemma 4.1.12. *We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{S}) \leq \min\{\dim_{\mathbb{K}}(L_K) | L_K \text{ is a nontrivial simple S-representation}\} \leq |\mathrm{S}|.$$

Moreover, when $\mathbb{K}$ *is algebraically closed, then* $|\mathrm{S}|$ *on the right can be replaced by* $\sqrt{|\mathrm{S}|}$.

Proof. The first inequality follows directly from the definitions. To see the second inequality observe that simple S-representation appear in the Jordan–Hölder filtration of $\mathbb{K}[\mathrm{S}]$, so their dimensions are bounded by $\dim_{\mathbb{K}}\big(\mathbb{K}[\mathrm{S}]\big) = |\mathrm{S}|$. When $\mathbb{K}$ is algebraically closed we have the inequality $\sum_L \dim_{\mathbb{K}}(L)^2 \leq |\mathrm{S}|$ where the sum runs over all simple S-representations. This implies the final claim. □

Example 4.1.13. Let $\mathrm{S}_n = \mathrm{Aut}(\{1, ..., n\})$ be the *symmetric group* on $\{1, ..., n\}$. For $\mathrm{char}(\mathbb{K}) \neq 2$ there is a 1-dimensional nontrivial simple S_n-representation, called the sign representation. Hence, $\mathrm{gap}_{\mathbb{K}}(\mathrm{S}_n) = 1$ unless $\mathrm{char}(\mathbb{K}) = 2$, which implies $\mathrm{gap}_*(\mathrm{S}_n) = 1$. Since $|\mathrm{S}_n| = n!$, the ratio between the representation gap and the size of S_n is thus very small. Even if one would argue that the sign representation is close to trivial, there is still the standard S_n-representation of dimension $n - 1$. So $\mathrm{gap}_{\mathbb{K}}(\mathrm{S}) \leq n - 1$ by Lemma 4.1.12, which is still small compared to $n!$.

4.1.2 Extensions and representation gaps

We now discuss extensions.

Lemma 4.1.14. *A pair* $(\mathrm{S}, \mathbb{K})$ *is* $(m > 1)$*-trivial if and only if any nontrivial simple* S*-representation has dimension at least* $m + 1$ *and all extensions*
$0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$ *split.*

Proof. Being m-trivial clearly implies the second statement. The converse follows by induction on m showing that any S-representation M with $\dim_{\mathbb{K}}(M) \leq m$ is a direct sum of $\mathbb{1}_{bt}$. □

Remark 4.1.15. If $\mathrm{S} = \mathrm{G}$ is a group so that $\mathbb{1}_b \cong \mathbb{1}_t$, then having no nontrivial extensions $0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$ is equivalent to $H^1(\mathrm{S}, \mathbb{K}) \cong 0$ (here S acts on $\mathbb{K}$ trivially: $s \mapsto 1$ for all $s \in \mathrm{S}$). Moreover, recall that $H^1(\mathrm{S}, \mathbb{K}) \cong 0$ if and only if the only homomorphism from S to $(\mathbb{K}, +)$ is the trivial one. We will use this below, in particular, maps from S are always to $(\mathbb{K}, +)$.

We consider now the four possible cases of extensions of $\mathbb{1}_{bt}$ by $\mathbb{1}_{bt}$. Precisely, let M be an S-representation. Suppose there is a short exact sequence

$$0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0.$$

Choosing a basis of M compatible with the corresponding filtration, the action of each $a \in \mathrm{S}$ in the basis will be given by an upper-triangular matrix, with either 0 or 1 in each diagonal entry (when the corresponding term is either $\mathbb{1}_b$ or $\mathbb{1}_t$, respectively). The remaining $(1, 2)$-entry is denoted by $f(a)$, so that the extension is described by a function $f \colon \mathrm{S} \to \mathbb{K}$. The condition $(ab)m = a(bm)$ for $m \in M$ translates into four possible relations on f depending on the types of the trivial representations involved:

Case (tt). This case is the same as for groups, cf. Remark 4.1.15.

Lemma 4.1.16. *If* $\mathrm{H}^1(\mathrm{S}, \mathbb{K}) \cong 0$*, then* S *has only the trivial extension of the form* $0 \longrightarrow \mathbb{1}_t \longrightarrow M \longrightarrow \mathbb{1}_t \longrightarrow 0$.

Proof. Extensions of the form $0 \longrightarrow \mathbb{1}_t \longrightarrow M \longrightarrow \mathbb{1}_t \longrightarrow 0$, viewed as elements of $\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_t)$, are classified by functions $f \colon \mathrm{S} \to \mathbb{K}$ such that $f(ab) = f(a) + f(b)$ for $a, b \in \mathrm{S}$. Any such extension is trivial if and only if $\mathrm{H}^1(\mathrm{S}, \mathbb{K}) \cong 0$. □

Case (bt). Recall that $\mathrm{G} \subset \mathrm{S}$ denotes the maximal subgroup of S.

Consider the symmetric and transitive closure of the relation $ba \approx_l a$ for $a, b \in \mathrm{S} \setminus \mathrm{G}$, and denote the closure by $\approx_l$ as well. We call S with a unique equivalence class in $\mathrm{S} \setminus \mathrm{G}$ under $\approx_l$ a *left-rounded monoid*, and, by convention, view groups as left-rounded monoids as well. We obtain a sufficient condition for the triviality of extensions:

Lemma 4.1.17. *If* S *is left-rounded and* $\mathrm{H}^1(\mathrm{G}, \mathbb{K}) \cong 0$*, then* S *has only the trivial extension of the form* $0 \longrightarrow \mathbb{1}_b \longrightarrow M \longrightarrow \mathbb{1}_t \longrightarrow 0$*.*

Proof. Extensions of the form $0 \longrightarrow \mathbb{1}_b \longrightarrow M \longrightarrow \mathbb{1}_t \longrightarrow 0$, viewed as elements of $\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_b)$, are classified by functions $f \colon \mathrm{S} \to \mathbb{K}$ such that

$$f(ba) = \begin{cases} f(a) & \text{if } a \in \mathrm{S} \setminus \mathrm{G}, \\ f(a) + f(b) & \text{if } a \in \mathrm{G}, \end{cases}$$

modulo the one-dimensional subspace of functions that are constant on $\mathrm{S} \setminus \mathrm{G}$ and zero on G. To see this, in a compatible basis $\{v_1, v_2\}$ of M the action of $a \in \mathrm{S} \setminus \mathrm{G}$ and $b \in \mathrm{G}$ is given by

$$a \mapsto \begin{pmatrix} 0 & f(a) \\ 0 & 1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & f(b) \\ 0 & 1 \end{pmatrix},$$

leading to the above equations. Moreover, the basis $\{v_1, v_2\}$ can be changed to $\{v_1, v_2 + \lambda v_1\}$ while preserving its compatibility with the sequence $0 \longrightarrow \mathbb{1}_b \longrightarrow M \longrightarrow \mathbb{1}_t \longrightarrow 0$, explaining why one needs to mod out by functions that are constant on $\mathrm{S} \setminus \mathrm{G}$ and zero on G.

Consequently,

$$|(\mathrm{S} \setminus \mathrm{G})/\approx_l| - 1 \leq \dim_{\mathbb{K}}\big(\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_b)\big) \leq |(\mathrm{S} \setminus \mathrm{G})/\approx_l| - 1 + \dim_{\mathbb{K}}\big(\mathrm{H}^1(\mathrm{G}, \mathbb{K})\big).$$

In particular, if $\dim_{\mathbb{K}}\big(\mathrm{H}^1(\mathrm{G},\mathbb{K})\big) = 0$, then

$$\dim_{\mathbb{K}}\big(\mathrm{Ext}^1(\mathbb{1}_t,\mathbb{1}_b)\big) = |(\mathrm{S}\setminus\mathrm{G})/\approx_l| - 1.$$

Thus, if S is left-rounded, then $\dim_{\mathbb{K}}\big(\mathrm{Ext}^1(\mathbb{1}_t,\mathbb{1}_b)\big) = 0$. □

Case (tb). A monoid S is called *right-rounded* if the opposite monoid S^{op} is left-rounded.

Lemma 4.1.18. *If* S *is right-rounded and* $\mathrm{H}^1(\mathrm{G},\mathbb{K}) \cong 0$*, then* S *has only the trivial extension of the form* $0 \longrightarrow \mathbb{1}_t \longrightarrow M \longrightarrow \mathbb{1}_b \longrightarrow 0$.

Proof. Dual to Lemma 4.1.17. □

Case (bb). Finally, we call a monoid S *null-rounded* if any noninvertible element of S can be written as a product of two noninvertible elements. That is, for $a \in \mathrm{S}\setminus\mathrm{G}$ we have $a = bc$ for some $b, c \in \mathrm{S}\setminus\mathrm{G}$.

Lemma 4.1.19. *If* S *is null-rounded and* $\mathrm{H}^1(\mathrm{G},\mathbb{K}) \cong 0$*, then* S *has only the trivial extension of the form* $0 \longrightarrow \mathbb{1}_b \longrightarrow M \longrightarrow \mathbb{1}_b \longrightarrow 0$.

Proof. The extensions as in the statement, when viewed as elements of $\mathrm{Ext}^1(\mathbb{1}_b,\mathbb{1}_b)$, are classified by functions $f\colon \mathrm{S}\to\mathbb{K}$ such that

$$f(ab) = \begin{cases} 0 & \text{if } a,b \in \mathrm{S}\setminus\mathrm{G}, \\ f(a)+f(b) & \text{if } a,b\in\mathrm{G}, \\ f(a) & \text{if } a\in\mathrm{S}\setminus\mathrm{G}, b\in\mathrm{G}, \\ f(b) & \text{if } a\in\mathrm{G}, b\in\mathrm{S}\setminus\mathrm{G}. \end{cases}$$

One can see this by writing the action on M in a compatible basis as

$$a \mapsto \begin{pmatrix} 0 & f(a) \\ 0 & 0 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 1 & f(b) \\ 0 & 1 \end{pmatrix},$$

where $a \in \mathrm{S} \setminus \mathrm{G}$ and $b \in \mathrm{G}$. The rest of the argument is similar to Lemma 4.1.17 and omitted. □

We say that a monoid S is *well-rounded* if it is null-rounded, left-rounded and right-rounded.

Theorem 4.1.1. *Assume* S *is well-rounded and* $\mathrm{H}^1(\mathrm{G}, \mathbb{K}) \cong 0$*, or* S *is semisimple (over* $\mathbb{K}$*). Then:*

(a) *Any short exact sequence*

$$0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$$

splits.

(b) *We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{S}) = \min\{\dim_{\mathbb{K}}(L_K) | L_K \ncong \mathbb{1}_{bt} \text{ is a simple S-representation}\}. \tag{4.1.2.1}$$

In particular, for groups it suffices to check whether $\mathrm{H}^1(\mathrm{G}, \mathbb{K}) \cong 0$ *to ensure that Equation 4.1.2.1 hold.*

Proof. Semisimple. In this case both claims are immediate.
Well-rounded and $\mathrm{H}^1(\mathrm{G}, \mathbb{K}) \cong 0$*, claim (a).* This claim follows from Remark 4.1.15, and the statements in Lemma 4.1.16, Lemma 4.1.18, Lemma 4.1.17 and Lemma 4.1.19.
Well-rounded and $\mathrm{H}^1(\mathrm{G}, \mathbb{K}) \cong 0$*, claim (b).* This follows from (a) and the definitions.
Finally, since groups are well-rounded then final claim also follows. □

Remark 4.1.20. Note that for upper bounds for gap(S) it suffices to find some nontrivial simple S-representation, but for lower bounds or the explicit value of gap(S) we will calculate $\mathrm{H}^1(\mathrm{S}, \mathbb{K})$ and $\mathrm{H}^1(\mathrm{G}, \mathbb{K})$.

4.1.3 Examples

The following is well-known. But since it is an important example for cryptography, see e.g. Example 4.1.22 below, we state and prove it here.

Proposition 4.1.21. *Let* $\mathrm{C}_n \cong \mathbb{Z}/n\mathbb{Z}$ *be the* cyclic group *of order* $n > 1$.

(a) *We have* $\mathrm{gap}_{\mathbb{Q}}(\mathrm{C}_n) = \min\{r-1 | r \text{ prime}, \ r \mid n\}$. *(In particular,* $\mathrm{gap}_{\mathbb{Q}}(\mathrm{C}_n) = n-1$ *if* n *is prime.)*

(b) *Let* $\mathbb{F}_q$ *denote a finite field with* $q = p^k$ *elements, where* p *is a prime.*

(i) *For* $\gcd(n, q-1) > 1$ *we have* $\mathrm{gap}_{\mathbb{F}_q}(\mathrm{C}_n) = 1$.

(ii) *For* $\gcd(n, q-1) = 1$ *and* $p \mid n$ *we have* $\mathrm{gap}_{\mathbb{F}_q}(\mathrm{C}_n) = 2$.

(iii) *For* $\gcd(n, q-1) = 1$ *and* $p \nmid n$ *we have*
$\mathrm{gap}_{\mathbb{F}_q}(\mathrm{C}_n) = \min\left\{d \in \mathbb{Z}_{\geq 0} | \gcd(n, q^d - 1) \neq 1\right\}$.

(c) *For any field* $\mathbb{K}$ *we have* $\mathrm{gap}_{\mathbb{K}}(\mathrm{C}_n) = \min_r(\mathrm{gap}_{\mathbb{K}}(\mathrm{C}_r))$, *where the minimum is taken over all prime divisors* r *of* n.

Proof. Case (a). First we have $\mathrm{H}^1(\mathrm{C}_n, \mathbb{Q}) \cong 0$, so by Theorem 4.1.1 it suffices to look at the dimensions of simple C_n-representations.
To this end, recall that representations of C_n are semisimple over $\mathbb{Q}$. The polynomial $X^n - 1$ has no repeated roots over $\mathbb{Q}$ and factors as $X^n - 1 = \prod_{d|n} \Phi_d$ for Φ_d the dth cyclotomic polynomial. The Chinese reminder theorem then gives $\mathbb{Q}[\mathrm{C}_n] \cong \bigoplus_{d|n} \mathbb{Q}[X]/(\Phi_d)$, and we see that there are simple C_n-representations for each Φ_d which are of the respective degrees $\deg \Phi_d = \varphi(d)$. This implies $\mathrm{gap}_{\mathbb{Q}}(\mathrm{C}_n) = \min\{\varphi(d) | d \text{ divides } n\}$. However, since $a \mid b$ implies $\varphi(a) \mid \varphi(b)$ we get the claimed formula from this expression.

Case (b). There is a nontrivial one-dimensional C_n-representation over $\mathbb{F}_q$ exactly when $\gcd(n, q-1) > 1$, implying (i). In case (ii), there exist a nontrivial homomorphism

$\mathrm{C}_n \to \mathbb{F}_q$, where the latter is considered an abelian group under addition, giving a nontrivial selfextension of the trivial representation of C_n.

In the remaining case (iii), when $\gcd(n, q-1) = 1$ and $p \nmid n$, the trivial representation has no selfextensions and it is the unique (up to isomorphism) representation of dimension one over $\mathbb{F}_p$. The representation gap $\mathrm{gap}_{\mathbb{F}_p}(\mathrm{C}_n)$ is then the dimension $d \geq 2$ of the smallest nontrivial simple representation. Such a representation corresponds to a nontrivial homomorphism $\mathrm{C}_n \to \mathrm{GL}(d, \mathbb{F}_q)$. Since $\gcd(n, q-1) = 1$ this homomorphism does not take C_n to multiples of the identity matrix. So d is the smallest number such that $\gcd(n, |\mathrm{GL}(d, \mathbb{F}_q)|) \neq 1$. The order of $\mathrm{GL}(d, \mathbb{F}_q)$, up to factors of $q-1$, which are coprime to n, is $(q^d-1)(q^d-q)...(q^d-q^{d-1})$. We see that the smallest d with $\gcd(n, |\mathrm{GL}(d, \mathbb{F}_q)|) \neq 1$ is the smallest d such that $gcd(n, q^d-1) \neq 1$.

Case (c). This follows from arguments very similar to those in (a) and (b) and is omitted. □

Example 4.1.22. For large primes $n+1$ the groups $\mathrm{C}_n \cong (\mathbb{Z}/(n+1)\mathbb{Z})^*$ lie at the heart of many standard cryptographic protocols, see e.g. [32, Section 1.4]. By Proposition 4.1.21 these groups have a big representation gap over $\mathbb{Q}$, which partially explains, from the viewpoint of this chapter, their usefulness in cryptography. However, the situation varies depending on the ground field.

Let n be a prime number. Over a characteristic zero field $\mathbb{K}$ that contains a primitive root of unity ξ of order r, all simple C_n-representations are one-dimensional, and $\mathrm{gap}_{\mathbb{K}}(\mathrm{C}_n) = 1$. Instead, as argued in the proof of Proposition 4.1.21, over the prime field $\mathbb{Q}$ there are two simple C_n-representations: the trivial $\mathbb{1}$ and an $(n-1)$-dimensional representation M, the complement of the trivial in the regular representation. The representation M over a larger field that contains ξ splits into the direct sum of one-dimensional C_n-representations, which are Galois conjugates of each other.

Thus, Proposition 4.1.21 and Example 4.1.22 imply that C_n has a substantial representation gap $n-1$ over $\mathbb{Q}$, close to its cardinality $n = |\mathrm{C}_n|$.

Example 4.1.23. Proposition 4.1.21 discusses the cyclic groups C_n. These are simple if n is a prime and the only commutative groups among the finite simple groups.
Let us briefly discuss other finite simple groups:

(a) The alternating groups $\mathrm{A}_n \subset \mathrm{S}_n$ of size $\frac{n!}{2}$ behave similarly to the symmetric groups, cf. Example 4.1.13. They are a bit better in the sense that they do not have a sign representation. However, over $\mathbb{Q}$ the standard representation of S_n restricts to a simple A_n-representations. Over other fields this representation might not be simple. But if its not, then it contains an even smaller nontrivial simple in its Jordan–Hölder filtration. Hence, $\mathrm{gap}_*(\mathrm{A}_n) \leq n-1$.

(b) The biggest part of the periodic table of simple groups are the finite groups of Lie type. (We consider the family of finite groups of Lie type in a very vague sense. In fact, the symmetric groups are secretly also part of this family, using the analogy that $\mathrm{S}_n \leftrightsquigarrow \mathrm{GL}_n(\mathbb{F}_1)$.) Most of these should have small representation gap over the defining field. To see this consider the group $\mathrm{PSL}_n(\mathbb{F}_q)$ for $q = p^k$ and p a prime. This is a finite simple group (unless $n = 2$ and $q \in \{2, 3\}$) with $\frac{q^{n(n-1)/2}}{\gcd(n,q-1)} \prod_{i=2}^{n}(q^i - 1)$ elements. (Thus, the number of elements growth exponentially in n.) However, $\mathrm{PSL}_n(\mathbb{F}_q)$ has a small nontrivial simple $\mathbb{F}_q$-representation of dimension $n^2 - 1$, namely $\big(\mathbb{F}_q^n \otimes (\mathbb{F}_q^n)^*\big)/\mathbb{F}_q$.

(c) Sporadic simple groups tend to have big representation gaps, see e.g. [28]. However, they do not come in $\mathbb{N}$-families and are all only moderately big. So they are probably not of immediate use for cryptography.

Let us discuss the monster group M as an example. Its smallest nontrivial and faithful representation over $\mathbb{C}$ has dimension 196883, see [28] under the entry $M = F_1$ therein (see also [26, Chapter 12] where this number+1 appears as the graded dimension of the moonshine module), and the smallest nontrivial and faithful representation over any field has dimension 196882, see [56]. With the minimal

representation of a sufficiently big dimension, there is a potential chance for cryptographic protocols built from the monster. However, the monster still is sporadic and does not come in an infinite family. We are not aware of any literature on the subject.

Thus, one could argue that noncommutative finite groups do not seem to be very useful for cryptography purposes by the above.

4.1.4 Field size and representation gap

In our definition of the representation gap we do not differentiate between a particular field used and our measure of complexity is the dimension of the smallest nontrivial representation over that field. More practically, we can keep track of the complexity of working over a specific field.

For the finite field $\mathbb{F}_q$ a natural measure of complexity is $\log_2(\mathbb{F}_q) = n\log_2(p)$, the log of the size of the field (or some related complexity that measures the difficulty of manipulating elements of the field). Given an S-representation M over $\mathbb{F}_q$, complexity of M can then be defined as

$$c(M) = \dim_{\mathbb{F}_q}(M)c(\mathbb{F}_q), \quad c(\mathbb{F}_q) = \log_2 |\mathbb{F}_q|.$$

Note that $c(M)$ is preserved when viewing M as an S-representation over any subfield of $\mathbb{F}_q$.

Definition 4.1.24. Define the *finite characteristic representation gap* $\text{gap}_f(\text{S})$ of S as the minimum of $c(M)$, over all nontrivial representations M over finite fields.

We can alternatively restrict to S-representations M over finite extensions $\mathbb{Q} \subset \mathbb{K}$ and define

$$c_0(M) = \dim_{\mathbb{K}}(M)[\mathbb{K} : \mathbb{Q}] = \dim_{\mathbb{Q}}(M).$$

Again, $c_0(M)$ does not change if M is viewed as an S-representation over a subfield $\mathbb{L} \subset \mathbb{K}$.

Definition 4.1.25. Define the *characteristic zero representation gap* $\mathrm{gap}_0(\mathrm{S})$ of S as the minimum of $c_0(M)$, over all nontrivial S-representations over finite extensions of $\mathbb{Q}$.

The pair $\big(\mathrm{gap}_0(\mathrm{S}), \mathrm{gap}_f(\mathrm{S})\big)$ is a measure of the representation complexity of S over both $\mathbb{Q}$ and finite fields.

Remark 4.1.26. Recall from above that the groups C_n have large (exponential) representation gap over $\mathbb{Q}$. The more refined notion of representation gap, introduced in this section, might be a better measure of the complexity of S from the linear attacks viewpoint.

4.1.5 Faithfulness

By a *faithful* S-representation we mean a representation on which any two elements of S act differently.

Remark 4.1.27. Since there is no $\mathbb{K}$-linear structure involved, this notion of faithfulness is slightly different from that of a faithful representation of the monoid algebra $\mathbb{K}[\mathrm{S}]$.

Besides the notion of the representation gap, we introduce a related (weaker) notion:

Definition 4.1.28. Let $\mathrm{faith}_{\mathbb{K}}(\mathrm{S})$ be the number

$$\mathrm{faith}_{\mathbb{K}}(\mathrm{S}) = \min\{\dim_{\mathbb{K}}(M) | M \text{ is a faithful S-representation}\}.$$

We call $\mathrm{faith}_{\mathbb{K}}(\mathrm{S})$ the *faithfulness* of $(\mathrm{S}, \mathbb{K})$.

In words, $\mathrm{faith}_{\mathbb{K}}(\mathrm{S})$ is the dimension of the smallest faithful S-representation.

Remark 4.1.29 (***Main Task 2***). Similarly as in Remark 4.1.9, for cryptographic applications it should be useful to have a supply of monoids with exponentially big $\mathrm{faith}_{\mathbb{K}}(\mathrm{S})$.

Remark 4.1.30. Faithfulness is only one measure of the complexity of S. As one example of a small size representation that is not faithful in general but still gives rise to efficient attacks is the Burau representation of the braid group Br_n on n strands. (The braid group is not a finite monoid, but that does not play a role for our discussions involving it.) The Burau representation has dimension n (or $n-1$ for the reduced Burau representation), and in the proposed protocols n is very small. Furthermore, the kernel of the Burau representation is also small, in an appropriate sense, and the action of an element of Br_n on the representation carries full information about the element for the protocol's purposes. Many of these protocols admit efficient attacks, as documented in the literature.

Example 4.1.31. The symmetric group S_n has its n-dimensional permutation representation, which is faithful. Hence, $\mathrm{faith}_*(\mathrm{S}_n) \leq n$.

Lemma 4.1.32. *We have* $\mathrm{gap}_{\mathbb{K}}(\mathrm{S}) \leq \mathrm{faith}_{\mathbb{K}}(\mathrm{S}) \leq |\mathrm{S}|$.

Over an algebraically closed field in the right inequality one can improve from $|\mathrm{S}|$ to $\sqrt{|\mathrm{S}|}$.

Proof. Every S-representation has a Jordan–Hölder filtration by simple representations, which therefore are of smaller (or equal) dimensions. The first claim follows from Lemma 4.1.12. The second inequality follows since every monoid admit a faithful representation on itself. □

Example 4.1.33. Let Br_n be the braid group on n strands. We already mentioned its Burau representation in Remark 4.1.30, but this representation is not faithful in general. However, a faithful Br_n-representation over $\mathbb{Q}(q,t)$ is the Laurence–Krammer–Bigelow representation, see [11] and [33], which is of dimension $\frac{n(n-1)}{2}$. Thus, $\mathrm{gap}_{\mathbb{Q}(q,t)}(\mathrm{Br}_n) \leq \mathrm{faith}_{\mathbb{Q}(q,t)}(\mathrm{Br}_n) \leq \frac{n(n-1)}{2}$, and Br_n does not seem suited for cryptography, see also [3].

The following is useful in examples:

Lemma 4.1.34. *Assume that there is a embedding of monoids* $\mathrm{S} \hookrightarrow \mathrm{T}$. *We have* $\mathrm{faith}_{\mathbb{K}}(\mathrm{S}) \leq \mathrm{faith}_{\mathbb{K}}(\mathrm{T})$.

Proof. This follows since a faithful T-representation restricts to a faithful S-representation. □

We come back to Example 4.1.22, but now from the viewpoint of faithfulness.

Proposition 4.1.35. *Let us consider the setting of Proposition 4.1.21.*

(a) *We have* $\mathrm{faith}_{\mathbb{Q}}(\mathrm{C}_n) = \sum_{i=1}^{k}(r_i^{d_i} - r_i^{d_i-1})$, *where* n *has the prime factor decomposition* $n = \prod_{i=1}^{k} r_i^{d_i}$. *(In particular,* $\mathrm{faith}_{\mathbb{Q}}(\mathrm{C}_n) = n - 1$ *if* n *is prime.)*

(b) *Let* n *be prime and* $\mathrm{char}(\mathbb{K}) \nmid n$. *Then* $\mathrm{faith}_{\mathbb{K}}(\mathrm{C}_n) = \mathrm{gap}_{\mathbb{K}}(\mathrm{C}_n)$ *for all the cases in Proposition 4.1.21.*

Proof. Case (a). Recall that $\mathbb{Q}[\mathrm{C}_n] \cong \bigoplus_{d|n} \mathbb{Q}[X]/(\Phi_d)$, see the proof of Proposition 4.1.21. The simple C_n-representations $\mathbb{Q}[X]/(\Phi_d)$ can be identified with $\mathbb{Q}(\zeta_d)$ for ζ_d a primitive dth root of unity. It is then easy to see that $\bigoplus_{i=1}^{k} \mathbb{Q}(\zeta_{r(i)})$ for $r(i) = r_i^{d_i}$ is a faithful C_n-representation. The dimensions of the summands are the degrees of the associated Φ_d. Hence, these summands are of dimensions $r_i^{d_i} - r_i^{d_i-1}$, which shows $\mathrm{faith}_{\mathbb{Q}}(\mathrm{C}_n) \leq \sum_{i=1}^{k}(r_i^{d_i} - r_i^{d_i-1})$. The decomposition of $\mathbb{Q}[\mathrm{C}_n]$ into $\mathbb{Q}(\zeta_d)$ also implies that one can not find a smaller faithful C_n-representation since Φ_d with $d = kr(i)$ and k coprime to r_i has bigger degree than $\Phi_{r(i)}$.

Case (b). This follows since C_n is a simple group when n is a prime, and because the representation theory of C_n is semisimple under the assumption $\mathrm{char}(\mathbb{K}) \nmid n$. □

The analog of Example 4.1.23 is:

Example 4.1.36. For finite simple groups faithfulness is not much different from Example 4.1.23. That is, Proposition 4.1.35 treats the cyclic groups and:

(a) The alternating groups A_n has a faithful representation of dimension n, which is the restriction of the permutation representation of S_n to A_n, see also Lemma 4.1.34. Thus, $\mathrm{faith}_*(\mathrm{A}_n) \leq n$.

(b) The $\mathrm{GL}_n(\mathbb{F}_q)$-representation $\mathbb{F}_q^n$ is faithful, giving an example of a group acting faithfully on a small representation. To pass to a simple group, one can take $\mathrm{PSL}_n(\mathbb{F}_q)$, which then acts faithfully on $\mathbb{F}_q^n \otimes (\mathbb{F}_q^n)^*$. Hence, $\mathrm{faith}_{\mathbb{F}_q}(\mathrm{PSL}_n(\mathbb{F}_q)) \leq n^2$.

(c) For sporadic groups the same remarks as in Example 4.1.23 apply. The smallest faithful representations for sporadic groups are listed in [27].

Example 4.1.23 and this example motivate to study monoids that are not groups.

4.1.6 Ratios

As argued earlier, for potential cryptographic purposes one wants to specialize to monoids with the representation gap of size comparable to $|\mathrm{S}|^\epsilon$, for some $\epsilon > 0$, as opposed to monoids where representation gap is exponentially smaller than the size of S. As a measure of complexity, we can define:

Definition 4.1.37. The *gap-ratio* and the *faithful-ratio* of S are

$$\mathrm{gapr}_{\mathbb{K}}(\mathrm{S}) = \frac{\mathrm{gap}_{\mathbb{K}}(\mathrm{S})}{\sqrt{|\mathrm{S}|}}, \quad \mathrm{faithr}_{\mathbb{K}}(\mathrm{S}) = \frac{\mathrm{faith}_{\mathbb{K}}(\mathrm{S})}{\sqrt{|\mathrm{S}|}}. \tag{4.1.6.1}$$

Remark 4.1.38 (***Additional Task 1***). For cryptographic applications it makes sense to search for naturally occurring families of monoids $\{\mathrm{S}_n | n \in \mathbb{Z}_{\geq 0}\}$ such that $\lim_{n\to\infty} \mathrm{gapr}_{\mathbb{K}}(\mathrm{S}_n)$ or $\lim_{n\to\infty} \mathrm{faithr}_{\mathbb{K}}(\mathrm{S}_n)$ do not approach 0 exponentially fast.
Note that these are rather crude: They are motivated by the search for families of monoids $\{\mathrm{S}_n | n \in \mathbb{Z}_{\geq 0}\}$ where representation gap grows exponentially while computations in the monoid grow polynomial, but oversimplify this problem.

Remark 4.1.39. The square root in Equation 4.1.6.1 comes from the observation that over an algebraically closed field a simple S-representation has dimension at most $\sqrt{|\mathrm{S}|}$.

Example 4.1.40. For the symmetric group S_n, cf. Example 4.1.13 and Example 4.1.31, we have $\mathrm{gapr}_*(\mathrm{S}_n) = \frac{1}{\sqrt{n!}}$ and $\mathrm{faithr}_*(\mathrm{S}_n) \leq \frac{n}{\sqrt{n!}}$, again indicating that S_n is not very useful for cryptography. The alternating group as in Example 4.1.23 and Example 4.1.36 has $\mathrm{gapr}_*(\mathrm{A}_n), \mathrm{faithr}_*(\mathrm{A}_n) \leq \frac{\sqrt{2}n}{\sqrt{n!}}$, which are still tiny.

4.2 Cell Theory

An important tool to study representations of monoids are *Green cells* or *Green's relations*. In this section we explain how these help to calculate $\mathrm{gap}(\mathrm{S})$ and $\mathrm{faith}(\mathrm{S})$, and also give us another numerical measure which we will call *semisimple representation gap*.

Remark 4.2.1. We will summarize the main constructions using the language of cells as in [19], which is more common in representation theory. The classical description using Green's relations can be found in many (older and newer) sources e.g. [20], [41] or [55]. The cell based discussion is not so easy to find in the literature, see however [21] or [57].

4.2.1 The basics

Recall that S denotes a finite monoid. (Cell theory also works for infinite monoids, but the theory is technically more involved. We will not discuss it here.)
We define a preorders on S, called *left, right and two-sided cell order*, by

$$(a \leq_l b) \Leftrightarrow \exists c : b = ca,$$

$$(a \leq_r b) \Leftrightarrow \exists c : b = ac,$$

$$(a \leq_{lr} b) \Leftrightarrow \exists c, d : b = cad.$$

In words, a is left lower than b if b can be obtained from a by left multiplication, and similarly for right ans two-sided. We define equivalence relations, the *left, right and*

two-sided equivalence, by

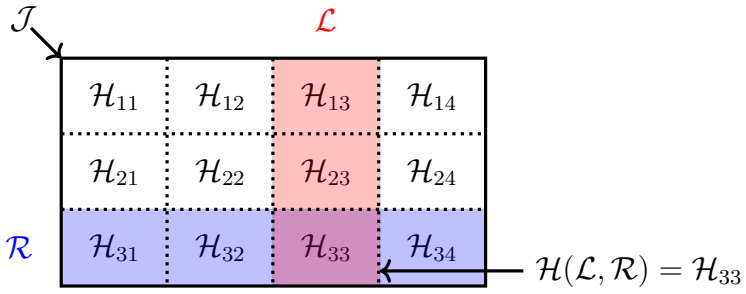
$$(a \sim_l b) \Leftrightarrow (a \leq_l b \text{ and } b \leq_l a),$$

$$(a \sim_r b) \Leftrightarrow (a \leq_r b \text{ and } b \leq_r a),$$

$$(a \sim_{lr} b) \Leftrightarrow (a \leq_{lr} b \text{ and } b \leq_{lr} a).$$

The respective equivalence classes are called left, right respectively two-sided *cells*. We denote all these by $\mathcal{L}$, $\mathcal{R}$ and $\mathcal{J}$ and call two-sided cells *J-cells*. Finally, an *H-cell* $\mathcal{H} = \mathcal{H}(\mathcal{L}, \mathcal{R}) = \mathcal{L} \cap \mathcal{R}$ is an intersection of a left $\mathcal{L}$ and a right cell $\mathcal{R}$.

The picture to keep in mind (stolen from [57, Section 2]) is



, (4.2.1.1)

where we use matrix notation for the twelve H-cells in $\mathcal{J}$. In this notation left cells are columns, right cells are rows, the J-cell is the whole block and H-cells are the small blocks. We will also write $<_l$ or $\geq_r$ etc., having the evident meanings. Note that the three preorders also give rise to preorders on the set of cells, as well as between elements of S and cells. For example, the notations $\mathcal{L} \geq_l a$ or $\mathcal{L} \leq_l \mathcal{L}'$ make sense. In particular, for a fixed left cell $\mathcal{L}$ we can define

$$\mathrm{S}_{\geq_l \mathcal{L}} = \{a \in \mathrm{S} | a \geq_l \mathcal{L}\},$$

as well as various versions which we will distinguish by the subscript.

Remark 4.2.2. The cell orders need not to be total orders. In all of our examples the

$\leq_{lr}$-order is a total order, but that is a coincidence.

Example 4.2.3. If S is a group, then it has only one cell, the whole group, which is a left, right, J- and H-cell at the same time.

Remark 4.2.4. Example 4.2.3 shows why the reader familiar with the theory of groups might have never heard about cell theory: for groups cell theory is trivial.

We write $\mathcal{H}(e)$ if $\mathcal{H}$ contains an idempotent $e \in S$. The H-cells of the form $\mathcal{H}(e)$ are called *idempotent H-cells*, and the J-cells $\mathcal{J}(e)$ containing these $\mathcal{H}(e) \subset \mathcal{J}(e)$ are called *idempotent J-cells*. H-cells are crucial as justified by:

Proposition 4.2.5. *For the monoid* S *we have:*

(a) *Every H-cell is contained in some J-cell, and every J-cell is a disjoint union of H-cells.*

(b) *$\mathcal{H}(e)$ is a group with identity e. In this case $\mathcal{H}(e) = \mathcal{J}(e) \cap (e\mathrm{S}e)$.*

Proof. Part (a) is clear, while (b) is classical, see [20, Theorem 7]. □

Notation 4.2.6. *One case will play a special role, namely the case where $\mathcal{H}(e)$ is the trivial group. In this case we say $\mathcal{H}(e)$ is* trivial *and write $\mathcal{H}(e) \cong 1$.*

We have minimal and maximal J-cells in the $\leq_{lr}$-order. In our illustrations the minimal cell will be at the bottom, so we call it the *bottom cell* $\mathcal{J}_b$, while the maximal cell will be at the top, so we call it the *top cell* $\mathcal{J}_t$.

Lemma 4.2.7. *Every monoid has a unique bottom and top J-cell which are minimal respectively maximal in the $\leq_{lr}$-order. Both are idempotent J-cells.*

Proof. The bottom J-cell is easy to find: Let G ⊂ S be the maximal subgroup of S, i.e. the set of invertible elements of S. Then G forms a left, a right and a J-cell at the same time, and is the smallest in all cell orders. To see this note that $1 \leq_l a$ for all $a \in$ S since we can

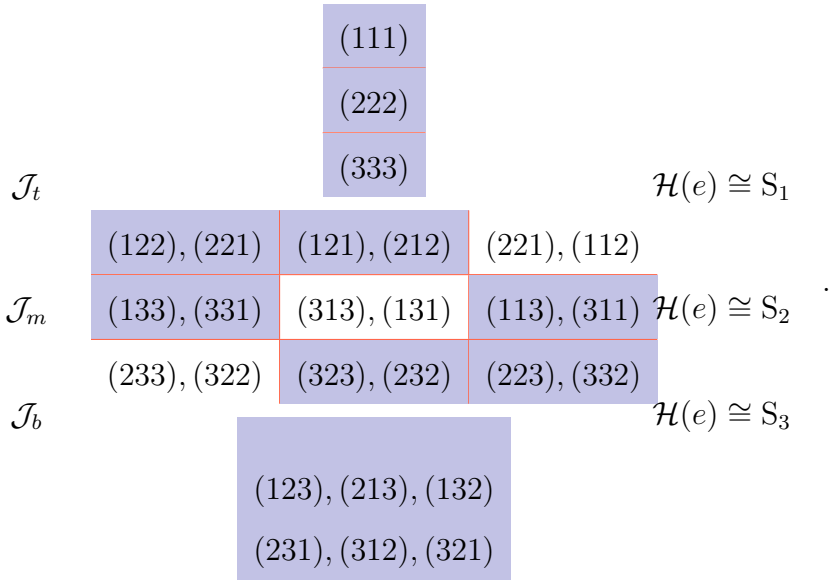
choose $c = a$. But every invertible element $b \in \mathrm{S}$ satisfies $1 = b^{-1}b$, which implies $b \leq_l 1$, thus $b \sim_l 1$. Similarly for $\sim_r$ and $\sim_{lr}$. The converse also holds, i.e. every element in a minimal J-cell is invertible, so G is the unique bottom cell $\mathcal{J}_b$.

The unit is an idempotent in $\mathcal{J}_b$.

If $\mathcal{J}$ and $\mathcal{J}'$ are maximal J-cells, then $\mathcal{J} = \mathcal{J}\mathcal{J}' = \mathcal{J}'$ by maximality. Existence of a maximal J-cell follows from the finiteness of S.

The J-cell $\mathcal{J}_t$ contains an idempotent since $\mathcal{J}_t\mathcal{J}_t = \mathcal{J}_t$ by maximality. This ensures the existence of an idempotent, see [55, Proposition 1.23]. □

Example 4.2.8. The *transformation monoid* T_n on the set $\{1, ..., n\}$ is $\mathrm{End}(\{1, ..., n\})$. The cells of T_3, whose elements are written in one-line notation, with (ijk) denoting the map $1 \mapsto i, 2 \mapsto j, 3 \mapsto k$, are as follows. Using the illustration conventions as in Equation 4.2.1.1 we have



That is, $a \sim_l b$ if and only if $a(x) = a(y) \Leftrightarrow b(x) = b(y)$ (as functions), and $a \sim_r b$ if and only if they have the same image. All idempotent H-cells are symmetric groups S_k of

varying sizes. Note that not all H-cells contain idempotents: we have colored/shaded the H-cells containing idempotents.

Let $|\mathcal{L}|$, $|\mathcal{R}|$ and $|\mathcal{H}|$ denote the sizes of fixed left, right and H-cells in a J-cell $\mathcal{J}$ of size $|\mathcal{J}|$.

Lemma 4.2.9. *Within one J-cell we have $|\mathcal{L}| = |\mathcal{L}'|$, $|\mathcal{R}| = |\mathcal{R}'|$ and $|\mathcal{H}| = |\mathcal{H}'|$, and we have $|\mathcal{L}| \cdot |\mathcal{R}| = |\mathcal{J}|$. Moreover, $|\mathcal{H}|$ divides both, $|\mathcal{L}|$ and $|\mathcal{R}|$.*

Proof. The first three equalities follow from [20, Theorem 1], the final two statements can then be shown from the previous three. □

Note that $|\mathcal{L}|, |\mathcal{R}|, |\mathcal{J}|, |\mathcal{H}| \in \mathbb{Z}_{\geq 0}$, and Lemma 4.2.9 gives us additionally $|\mathcal{L}|/|\mathcal{H}|, |\mathcal{R}|/|\mathcal{H}| \in \mathbb{Z}_{\geq 0}$. These are important measures of the complexity of S.

Example 4.2.10. The middle J-cell in Example 4.2.8 has $\mathcal{J} = 36 = 6 \cdot 6 = |\mathcal{L}| \cdot |\mathcal{R}|$, $|\mathcal{H}| = 2$ and $|\mathcal{L}|/|\mathcal{H}| = |\mathcal{R}|/|\mathcal{H}| = 3$.

A *left ideal* $I \subset S$ is a set such that $aI \subset I$. Right and two-sided ideals are defined similarly. The following lemma explains the matrix notation:

Lemma 4.2.11. *For fixed left cell $\mathcal{L}$ the set $\mathrm{S}_{\geq_l \mathcal{L}}$ is a left ideal in* S. *Similarly, $\mathrm{S}_{\geq_r \mathcal{R}}$ is a right and $\mathrm{S}_{\geq_{lr} \mathcal{J}}$ is a two-sided ideal. The same works when replacing $\geq$ by $>$.*

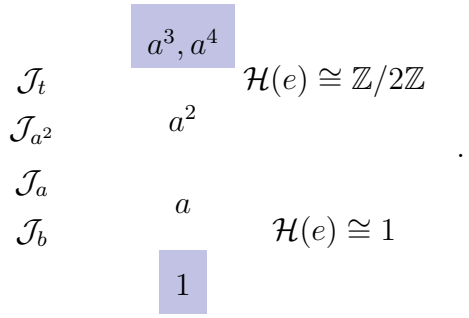
Proof. Directly from the definitions: given $b \in \mathrm{S}_{\geq_l \mathcal{L}}$, the element ab is still left greater or equal to $l \in \mathcal{L}$ since $b = cl$ for some c. □

Let us state how cell theory helps to understand periods of elements, which in turn are of importance in cryptography. To this end, for $a \in \mathrm{S}$ recall that the *index* $i(a) \in \mathbb{Z}_{\geq 0}$ is the smallest number such that $a^{i(a)} = a^{i(a)+d}$ for some $d \in \mathbb{Z}_{>0}$. The smallest possible d is then in turn called the *period* of a and we denote it by $p(a)$.

Theorem 4.2.1. *There exists an H-cell $\mathcal{H}(e)$ such that $\mathrm{C}_{p(a)} \cong \{a^s \mid s \geq i(a)\} \subset \mathcal{H}(e)$ is a subgroup. In particular, $p(a) \mid |\mathcal{H}(e)|$.*

Proof. As a consequence of [20, Theorem 7], the H-cells of the form $\mathcal{H}(e)$ are the maximal subgroups of S, so no other subgroup will be contained in some $\mathcal{H}(e)$. □

Example 4.2.12. Given $i \in \mathbb{Z}_{\geq 0}$, $p \in \mathbb{Z}_{\geq 1}$ form the finite cyclic monoid $\mathrm{C}_{i,p} = \langle a | a^{i+p} = a^i \rangle$ of cardinality $i + p$. The element a has index $i(a) = i$ and period $p(a) = p$. Moreover, the monoid $\mathrm{C}_{i,p}$ is commutative, so left, right and J-sided cells coincide. The elements $1, a, ..., a^{i-1}$ each constitute a single J-cell, in total $i - 1$ such J-cells. All the remaining elements $\mathcal{J}_t = \{a^i, a^{i+1}, ..., a^{i+p-1}\}$ constitute one J-cell (the top cell) which is a cyclic group of order p under multiplication. The element $e = a^{pj}$ where j is such that $i \leq pj < i + p$ is the idempotent for $\mathcal{J}_t = \mathcal{H}(e)$ and the identity of that group. Out of the $i + 1$ cells in $\mathrm{C}_{i,p}$ two cells are idempotent: $\mathcal{J}_b = \{1\}$ and $\mathcal{J}_t$.
To be completely explicit, let us consider $\mathrm{C}_{3,2}$, which is the monoid be generated by one element a of index 3 and period 2. Then $\mathrm{C}_{3,2} = \{1, a, a^2, a^3, a^4\}$ and its cell structure is



Note that S_a is commutative, so left, right, J- and H-cells agree.

Remark 4.2.13 (***Additional Task 2***). Using the DH protocol in a finite monoid S other than a group, it would be important to find elements $g \in \mathrm{S}$ of big period that has a large prime factor, see e.g. the original DH key exchange [32], [**?** , Section 1.2]. So, by Theorem 4.2.1, it would be preferable to have a monoid S with H-cells whose orders have large prime divisors since the period of $a \in \mathrm{S}$ divides the order of the idempotent H-cell of S

that contains the top cell of $\mathrm{C}_{i,p}$.

4.2.2 Classification of simple modules

We consider now S-representations defined over $\mathbb{K}$. Cells can be considered S-representations, called *cell representations* or Schützenberger representations, up to higher order terms:

Lemma 4.2.14. *Each left cell $\mathcal{L}$ of* S *gives rise to a left* S*-representation $\Delta_{\mathcal{L}} = \mathbb{K}\mathcal{L}$ by*

$$a \cdot l \in \Delta_{\mathcal{L}} = \begin{cases} al & \text{if } al \in \mathcal{L}, \\ 0 & \text{else.} \end{cases}$$

Similarly, right cells give right representations ${}_{\mathcal{R}}\Delta$ and J-cells give birepresentations (often called bimodules). We have $\dim_{\mathbb{K}}(\Delta_{\mathcal{L}}) = |\mathcal{L}|$ *and* $\dim_{\mathbb{K}}({}_{\mathcal{R}}\Delta) = |\mathcal{R}|$.

Proof. Directly from the definitions. □

The annihilator $\mathrm{Ann}_{\mathrm{S}}(M) = \{s \in \mathrm{S} | s \cdot M = 0\}$ of an S-representation M is a left ideal of S. An *apex* of M is a J-cell $\mathcal{J}$ such that $\mathcal{J} \cap \mathrm{Ann}_{\mathrm{S}}(M) = \emptyset$ and all J-sided cells $\mathcal{J}'$ with $\mathcal{J}' \cap \mathrm{Ann}_{\mathrm{S}}(M) = \emptyset$ satisfy $\mathcal{J}' \leq_{lr} \mathcal{J}$. In other words, an apex is the $\leq_{lr}$-maximal J-cell not annihilating M. The following justifies the terminology of the *apex of a simple* S*-representation*:

Lemma 4.2.15. *Every simple* S*-representation has a unique apex.*

Proof. This is classical, see e.g. [41, Theorem 5]. □

Example 4.2.16. The apex of $\mathbb{1}_b$ is always $\mathcal{J}_b = \mathrm{G}$. On the other hand, the apex of $\mathbb{1}_t$ is $\mathcal{J}_t$ since every $s \in \mathrm{S}$ acts as 1.

Recall that the nonunital way to induce is $\mathrm{Ind}(M) = M \otimes_{\mathbb{K}[e\mathrm{S}e]} \mathbb{K}[e\mathrm{S}]$ for some idempotent $e \in \mathrm{S}$, see e.g. [55, Section 4.1] (inducing from the submonoid $e\mathrm{S}e$ to S, or rather using

their monoid rings). Since $\mathcal{H}(e) = \mathcal{J}(e) \cap (e\mathrm{S}e)$ is a subgroup of S, we can then define an induction functor

$$\mathrm{Ind}_{\mathcal{H}(e)}^{\mathrm{S}} M = \Delta_{\mathcal{L}} \otimes_{\mathcal{H}(e)} M,$$

where M is a $\mathcal{H}(e)$-representation and $\mathcal{H}(e) = (\mathcal{L} \cap \mathcal{R}) \subset \mathcal{J}$ for some right cell $\mathcal{R}$.

Example 4.2.17. Let $\mathbb{K}[\mathcal{H}(e)]$ denote the regular $\mathcal{H}(e)$-representation. We have $\mathrm{Ind}_{\mathcal{H}(e)}^{\mathrm{S}} \mathbb{K}[\mathcal{H}(e)] \cong \Delta_{\mathcal{L}}$ as left S-representations.

Recall also that the *head* $\mathrm{Hd}(M)$ of an S-representation M is the maximal semisimple quotient of M. It is well-defined, up to isomorphism, for any module over a finite monoid and is isomorphic to the quotient $M/\mathrm{Rad}(M)$. Here $\mathrm{Rad}(M)$ denotes the radical, which is the intersection of all maximal submodules of M.
We get the *Clifford–Munn–Ponizovskiĭ theorem*:

Proposition 4.2.18. *For a monoid* S*:*

$$\{\textit{simple } \mathrm{S}\textit{-representations of apex } \mathcal{J}\}/\cong \overset{1:1}{\longleftrightarrow} \{\textit{simple } \mathcal{H}(e)\textit{-representations}\}/\cong,$$

where $\mathcal{H}(e) \subset \mathcal{J}$ is any idempotent H-cell in an idempotent J-cell $\mathcal{J}$. Moreover, an explicit bijection (from right to left) is given by

$$K \mapsto L_K \cong \mathrm{Hd}(\mathrm{Ind}_{\mathcal{H}(e)}^{\mathrm{S}} K).$$

Proof. The above is an easy reformulation of [41, Theorem 7] or [55, Theorem 5.5]. □

Note that only idempotent J-cells contribute to the classification. We usually omit to write e.g. "simples up to isomorphism" in the rest of the chapter.

Remark 4.2.19. The 1:1 correspondence in Proposition 4.2.18 always exists regardless of $\mathbb{K}$. However, the classification still depends on $\mathbb{K}$ since the number of simple

$\mathcal{H}(e)$-representation does.

Example 4.2.20. Let $\mathrm{char}(\mathbb{K})$ be such that $\mathrm{char}(\mathbb{K}) \nmid 3! = 6$, e.g. $\mathrm{char}(\mathbb{K}) = 0$. The cell structure from Example 4.2.8 shows that T_3 has three simple T_3-representations of apex $\mathcal{J}_b$, two of apex $\mathcal{J}_m$ and one of apex $\mathcal{J}_t$ since the associated $\mathcal{H}(e)$ are the symmetric groups S_3, S_2 and S_1 (and the number of simple S_n-representations is given by the number of partitions of n).

Note that if $\mathcal{H}(e)$ is trivial, then Proposition 4.2.18 implies that one can say that the simples or *indexed by a poset*, namely the poset of apexes with the partial order given by $\leq_{lr}$. If $\mathcal{H}(e)$ is nontrivial, then we will still use this terminology keeping in mind that simple S-representations associated to the same apex are incomparable.

4.2.3 Cells and (semisimple) representation gaps

Note that Proposition 4.2.18 makes it easy to classify simple S-representations but does not give much information about their dimensions.

Theorem 4.2.2. *The dimension of the simple* S*-representation L_K associated to the simple $\mathcal{H}(e)$-module K via Proposition 4.2.18 can be bounded by*

$$\dim_{\mathbb{K}}(L_K) \leq |\mathcal{L}|/|\mathcal{H}| \cdot \dim_{\mathbb{K}}(K).$$

Proof. This follows from the explicit bijection in Proposition 4.2.18. □

Note that dimension of $\mathrm{Hd}(\mathrm{Ind}^{\mathrm{S}}_{\mathcal{H}(e)}K)$ depends on the field, in general, and can be hard to compute. The quantity $|\mathcal{L}|/|\mathcal{H}| \cdot \dim_{\mathbb{K}}(K)$ is often easy to compute in practice so we define:

Definition 4.2.21. We call $\mathrm{ssdim}_{\mathbb{K}}(L_K) = |\mathcal{L}|/|\mathcal{H}| \cdot \dim_{\mathbb{K}}(K)$ the *semisimple dimension* of L_K. The minimal m such that there is a nontrivial simple S-representation with $\mathrm{ssdim}_{\mathbb{K}}(L_K) = m$ is called the *semisimple representation gap* $\mathrm{ssgap}_{\mathbb{K}}(\mathrm{S})$ of S.
We also call $\mathrm{ssgapr}_{\mathbb{K}}(\mathrm{S}) = \frac{\mathrm{ssgap}_{\mathbb{K}}(\mathrm{S})}{\sqrt{|\mathrm{S}|}}$ the *semisimple-gap-ratio*.

Theorem 4.2.3. *We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{S}) \leq \min\{\dim_{\mathbb{K}}(L_K) | L_K \ncong \mathbb{1}_{bt} \text{ is a simple S-representation}\} \leq \mathrm{ssgap}_{\mathbb{K}}(\mathrm{S}) \leq |\mathrm{S}|.$$

Proof. Clear by definition and Lemma 4.1.12. □

Remark 4.2.22 (***Additional Task 3***). As before, it is important for potential cryptographic applications to find monoids with $\mathrm{ssgap}_{\mathbb{K}}(\mathrm{S})$ exponentially big.

Example 4.2.23. In the setting of Examples 4.2.8 and 4.2.20 (in particular, $\mathrm{char}(\mathbb{K}) \nmid 6$) we have the following.
The three simple T_3-representations of apex $\mathcal{J}_b$ are the simple S_3-representations inflated to T_3, so they are of dimensions 1, 2 and 1 (one of these is $\mathbb{1}_b$). These are also their semisimple dimensions.
The simple S_3-representation of apex $\mathcal{J}_t$ can be identified with $\mathbb{1}_t$, so is of dimension one, which is also its semisimple dimension.
The two simple S_3-representations of apex $\mathcal{J}_m$ are induced from the respective S_2-representations, and are of semisimple dimension 3. One can check that they are of dimensions 3 respectively 2.

The name semisimple representation gap is justified by the following.

Proposition 4.2.24. *The following are equivalent.*

(a) *The monoid* S *is semisimple.*

(b) *All J-cells are idempotent, all* $\mathcal{H}(e)$ *are semisimple and* $\dim_{\mathbb{K}}(L_K) = \mathrm{ssdim}_{\mathbb{K}}(L_K)$ *for all simple* S*-representations* L_K*.*

Proof. This follows from [55, Theorem 5.19] and the paragraph below that theorem. □

4.2.4 Cells and Gram matrices

Recall the following construction of Gram matrices, see e.g. [55, Section 5.4]. Fix an idempotent H-cell $\mathcal{H}(e) = \mathcal{L} \cap \mathcal{R}$ in some idempotent J-cell $\mathcal{J}$. Then $\mathcal{L}$ is a free right $\mathcal{H}(e)$-set and $\mathcal{R}$ is a free left $\mathcal{H}(e)$-set, so we can let $\{l_1, ..., l_R\}$ and $\{r_1, ..., r_L\}$ complete sets of representatives for $\mathcal{L}/\mathcal{H}(e)$ respectively for $\mathcal{H}(e)\backslash\mathcal{R}$. Here R is the number of right cells and L is the number of left cells in $\mathcal{J}$.

The *Gram matrix* $P^{\mathcal{J}} = (P^{\mathcal{J}}_{i,j})_{i,j}$ is the matrix with values in $\mathbb{K}[\mathcal{H}(e)]$ defined by

$$P^{\mathcal{J}}_{i,j} = \begin{cases} r_i l_j & \text{if } r_i l_j \in \mathcal{H}(e), \\ 0 & \text{else.} \end{cases}$$

Note that $P^{\mathcal{J}}$ depends on choices, but one can show that its important properties do not depend on these choices.

Gram matrices are in particularly useful for $\mathcal{H}(e) \cong 1$ and $L = R$ as justified by the following (which the reader familiar with [19] might recognize):

Proposition 4.2.25. *Fix and idempotent J-cell $\mathcal{J}$ with $L = R$ and $\mathcal{H}(e) \subset \mathcal{J}$ satisfying $\mathcal{H}(e) \cong 1$. Assume further that $P^{\mathcal{J}}$ is symmetric. Let $L_{\mathcal{J}}$ denote the associated simple* S*-representation, see Proposition 4.2.18. Then:*

$$\dim_{\mathbb{K}}(L_{\mathcal{J}}) = \mathrm{rk}(P^{\mathcal{J}}).$$

Proof. Let $\mathrm{Rad}_{\mathcal{J}}$ denote the radical of the symmetric bilinear form associated to $P^{\mathcal{J}}$. We claim that $\mathrm{Rad}_{\mathcal{J}}$ is a S-submodule of the corresponding cell representation $\Delta_{\mathcal{L}}$. To see this note that $r_i l_j \notin \mathcal{H}(e)$ can only occur if they end up in $\mathcal{J}_{>_{lr}\mathcal{J}}$, and multiplying by elements from S preserves this property.

We further claim that any element in $\Delta_{\mathcal{L}} \setminus \mathrm{Rad}_{\mathcal{J}}$ generates $\Delta_{\mathcal{L}}$. This can be proven as in [14, Lemma 3.4].

It follows that $\Delta_{\mathcal{L}}/\mathrm{Rad}_{\mathcal{J}}$ is a simple S-representation since any proper submodule of it must be contained in $\mathrm{Rad}_{\mathcal{J}}$. Since the apex of $\Delta_{\mathcal{L}}/\mathrm{Rad}_{\mathcal{J}}$ is $\mathcal{J}$, by construction, it follows that $\Delta_{\mathcal{L}}/\mathrm{Rad}_{\mathcal{J}} \cong L_{\mathcal{J}}$. The proof completes. □

Theorem 4.2.4. *Let* $\mathrm{R} \subset \mathrm{S}$ *be a submonoid. Under the assumptions in Proposition 4.2.25, for any idempotent* J*-cell* $\mathcal{J}$ *of* S *that restricts to an idempotent* J*-cell of* R *we have*

$$\dim_{\mathbb{K}}(L^{\mathrm{S}}_{\mathcal{J}}) \geq \dim_{\mathbb{K}}(L^{\mathrm{R}}_{\mathcal{J}}),$$

for the associated simple R*- and* S*-representations.*

Proof. Note that under the assumptions we have that $P^{\mathcal{J}}_{\mathrm{R}}$ is a submatrix of $P^{\mathcal{J}}$. The rank of a matrix is always greater or equal to the rank of a submatrix, so the statement follows by Proposition 4.2.25. □

4.2.5 Cells, Burnside–Brauer and faithfulness

Let $cl_{\mathcal{H}(e)}$ denote the number of conjugacy classes of the group $\mathcal{H}(e)$. Let $\{e_1, ..., e_r\}$ be a choice of one idempotent per idempotent J-cell, and define

$$cl(\mathrm{S}) = cl_{\mathcal{H}(e_1)} + ... + cl_{\mathcal{H}(e_r)}.$$

Lemma 4.2.26. *The number* $cl(\mathrm{S}) \in \mathbb{Z}_{\geq 0}$ *is independent of the choice of* $\{e_1, ..., e_r\}$.

Proof. This is a consequence of [55, Section 7.1]. □

Hence, $cl(\mathrm{S})$ is a constant depending on S only. One can use $cl(\mathrm{S})$ for the *Burnside–Brauer theorem*:

Proposition 4.2.27. *Let* $\mathrm{char}(\mathbb{K}) = 0$. *If* F *is a faithful* S*-representation, then every simple* S*-representation appears as a composition factor of* $F^{\otimes k}$ *for some* $0 \leq k \leq cl(\mathrm{S}) - 1$.

Proof. See [54] or [55, Section 7.4] and the observation that the r in that theorem satisfies $r \leq cl(\mathrm{S})$ by the discussion in [55, Section 7.1]. □

Example 4.2.28. The bound given in Proposition 4.2.27 is often not optimal but cannot be improved uniformly. For example, for C_n we have $cl(\mathrm{C}_n) = n$. Assume n is prime. Over $\mathbb{C}$ the nth primitive root of unity $\exp(\frac{2\pi i}{n})$ gives rise to a 1-dimensional faithful C_n-representation, and only the $(n-1)$th power of it will contain the simple C_n-representation associated to $\exp(\frac{2\pi i(n-1)}{n})$.

The Burnside–Brauer theorem gives a bound for the dimension of faithful S-representations:

Theorem 4.2.5. *Let* $\mathrm{char}(\mathbb{K}) = 0$*, and let* L_{max} *be a simple* S*-representation of the biggest dimension. If* F *is a faithful* S*-representation, then* $\dim_{\mathbb{K}}(F) \geq \sqrt[cl(\mathrm{S})-1]{\dim_{\mathbb{K}}(L_{max})}$*. Hence,*

$$\mathrm{faith}_{\mathbb{K}}(\mathrm{S}) \geq \sqrt[cl(\mathrm{S})-1]{\dim_{\mathbb{K}}(L_{max})}.$$

Proof. This follows from Proposition 4.2.27. □

Note that one can use Theorem 4.2.5 often in combination with Lemma 4.1.34.

Remark 4.2.29 (***Additional Task 4***). Thus, by Theorem 4.2.5 it is preferable for cryptographical applications to find a monoid S with $c(\mathrm{S})$ being small.

Example 4.2.30. Applying Theorem 4.2.5 for T_3 gives $\sqrt[6]{3}$ as a lower bound, which rounds to 2. The smallest faithful T_3-representation is $\mathbb{K}\{1,2,3\}$ (with the defining action), so of dimension three.

With respect to extensions as discussed in Section 4.1.1 we get:

Proposition 4.2.31. *Let* $\mathrm{char}(\mathbb{K}) = 0$*. There is a faithful* S*-representation containing only* $\mathbb{1}_{bt}$ *as composition factors if and only if* S *has at most two idempotent* J*-cells and all idempotent* H*-cells are trivial, i.e.* $\mathcal{H}(e) \cong 1$*.*

Proof. $\Rightarrow$. If F is a faithful S-representations only containing $\mathbb{1}_{bt}$ as composition factors, then Proposition 4.2.27 implies that there can be no simple S-representations except $\mathbb{1}_{bt}$. Thus, the result follows by Proposition 4.2.18.

$\Leftarrow$. In this case Proposition 4.2.18 implies that $\mathbb{1}_{bt}$ are the only simple S-representations. □

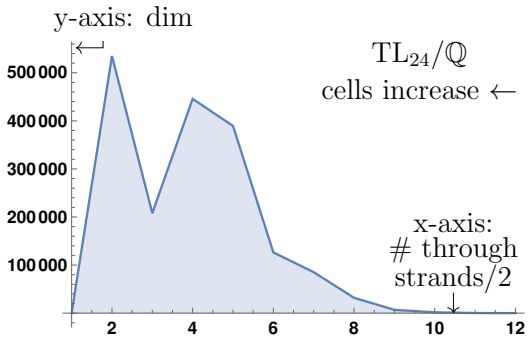
Example 4.2.32. Let $\mathrm{char}(\mathbb{K}) = 0$. When S is a group Proposition 4.2.31 implies that only the trivial group has faithful representations entirely made of trivial representations. (Note that this is clear because of a different reason: the assumption is $\mathrm{char}(\mathbb{K}) = 0$ so the representation theory of groups is semisimple.)

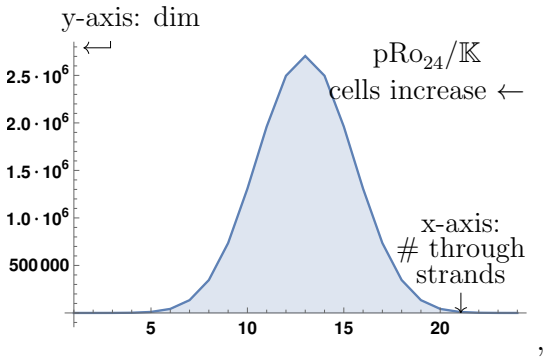
Example 4.2.33. It follows from the discussion in Equation 4.3.1.1 that the Temperley–Lieb monoid on three strands TL_3 is an example of a nontrivial monoid that has a faithful representation entirely made of $\mathbb{1}_{bt}$. This works in arbitrary characteristic.

4.2.6 Cell submonoids and subquotients

Recall that simple S-representations arrange themselves according to the cells, see Proposition 4.2.18. Let us for simplicity assume that $\mathcal{H}(e) \cong 1$ for all idempotent H-cells and that all J-cells are idempotent. Then the dimensions of the simple S-representations very often have the following form, which is roughly as expected from combinatorial

numbers:



,


, (4.2.6.1)

TL dim: $(1, 534888, 208011, 445741, 389367, 126292, 85216, 31878, 6876, 1726, 252, 22, 1)$,

pRo dim: $\begin{pmatrix} 1, 24, 276, 2024, 10626, 42504, 134596, 346104, 735471, 1307504, 1961256, 2496144, \\ 2704156, 2496144, 1961256, 1307504, 735471, 346104, 134596, 42504, 10626, 2024, 276, 24, 1 \end{pmatrix}$.

These illustrations show the dimensions of the simple TL_{24}-representation (left) over $\mathbb{Q}$ (or any field of characteristic zero) and the simple pRo_{24}-representations for general $\mathbb{K}$, respectively. (Note the two trivial TL_{24}- respectively pRo_{24}-representations for the bottom and top cell.) Thus, it seems preferable to cut-off the representations for small cells, and get rid of the fluctuations for very big cells.

The key to do the first is are *cell submonoids* as follows.

Definition 4.2.34. For a J-cell $\mathcal{J}$ with $1 \notin \mathcal{J}$ define the *$\mathcal{J}$-submonoid*

$$\mathrm{S}_{\geq \mathcal{J}} = \mathrm{S}_{\geq_{lr} \mathcal{J}} \cup \{1\}.$$

In words, we artificially adjoint a unit 1 (strictly speaking we should write $1'$) to the two-sided ideal $\mathrm{S}_{\geq_{lr} \mathcal{J}}$ from Lemma 4.2.11.

Lemma 4.2.35. *For any J-cell $\mathcal{J}$ with $1 \notin \mathcal{J}$, $\mathrm{S}_{\geq \mathcal{J}}$ is a submonoid of* S.

Proof. By Lemma 4.2.11. □

Remark 4.2.36. There are minor, but not essential, differences between representations of monoids and semigroups. Adjoining a unit is for convenience only so that we do not need

to leave the world of monoids.

Annihilating the bigger cells can be done using the *Rees factor* S/I of a monoid S by a two-sided ideal I. The construction works as follows. As a set $\mathrm{S}/I = (\mathrm{S} \setminus I) \cup \{0\}$, where one artificially adjoints an element 0. The multiplication is $s \bullet t = st$ if $s, t, st \in \mathrm{S} \setminus I$, and $s \bullet t = 0$ otherwise.

Lemma 4.2.37. *For any two-sided ideal, the Rees factor* S/I *is a well-defined monoid.*

Proof. An easy exercise, see also [55, Exercise 1.6]. □

We can thus define *cell subquotients*:

Definition 4.2.38. For two J-cells $\mathcal{J} \leq_{lr} \mathcal{K}$ with $1 \notin \mathcal{J}$ define the $\mathcal{J}$-$\mathcal{K}$-*subquotient* as the Rees factor

$$\mathrm{S}_{\mathcal{J}}^{\mathcal{K}} = \mathrm{S}_{\geq \mathcal{J}}/\mathcal{K}.$$

Here we additionally allow the following extremal cases:

$$\mathrm{S}_{\mathcal{J}}^{none} = \mathrm{S}_{\geq \mathcal{J}}, \quad \mathrm{S}_{none}^{\mathcal{K}} = \mathrm{S}/\mathcal{K}, \quad \mathrm{S}_{none}^{none} = \mathrm{S}.$$

We also call all of the above *cell subquotients* for short.

By Lemma 4.2.35 and Lemma 4.2.37, $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$ is a subquotient of S. Unless we are in one of the extreme cases, $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$ has $\mathcal{J}_b = \{1\}$ and $\mathcal{J}_t = \{0\}$. Both are left, right, J- and H-cells at the same time.

Definition 4.2.39. We call S *left-admissible* if, for all left cells $\mathcal{L}$:

$$\forall a, b \in \mathcal{L}\ \exists c \in \mathcal{J} \supset \mathcal{L} \text{ such that } a = cb.$$

Right- and J-admissible are defined similarly, using right or two-sided multiplication. We say S is *admissible* if it is left-, right- and J-admissible.

The admissibility condition is to ensure that the cells are not affected when taking cell subquotients.

Lemma 4.2.40. *Let* S *be J-admissible. In the nonextremal cases the J-cells of* $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$ *are given by*

$$\{\mathcal{J}_b\} \cup \{\mathcal{M} | \mathcal{M} \text{ is a } J\text{-cell of } \mathrm{S} \text{ with } \mathcal{J} \leq_{lr} \mathcal{M} <_{lr} \mathcal{K}\} \cup \{\mathcal{J}_t\}.$$

Similarly for left, and right cells, assuming the respective admissibility condition, and H-cells.
An analog statement holds in the extremal cases.

Proof. By the admissibility assumption, the remaining elements of $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$ arrange themselves into cells precisely as in S. □

We require that S is admissible for the remainder of this section.
Assume that we are in the nonextremal cases. Then $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$ has trivial representations $\mathbb{1}_b$ and $\mathbb{1}_t$ associated to the apexes $\mathcal{J}_b$ and $\mathcal{J}_t$, and these are the only $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$-representations of these apexes. The other simple $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$-representations and their dimensions are given by the following statement. Note hereby that any $\mathrm{S}_{\mathcal{J}}$-representation with apex $\mathcal{M}$ can be *inflated* to a S-representation by letting all elements in $\mathrm{S}_{<_{lr}\mathcal{J}}$ act by zero.

Proposition 4.2.41. *Assume that we are in the nonextremal cases. Let $\mathcal{M} \notin \{\mathcal{J}_b, \mathcal{J}_t\}$ be an apex of* $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$ *which is also an apex of* S*. Then we have:*

$$\{\text{simple } \mathrm{S}_{\mathcal{J}}^{\mathcal{K}}\text{-representations of apex } \mathcal{M}\}/\cong \overset{1:1}{\longleftrightarrow} \{\text{simple S-representations of apex } \mathcal{M}\}/\cong .$$

Moreover, an explicit bijection (from left to right) is given by inflating simple $\mathrm{S}_{\mathcal{J}}^{\mathcal{K}}$*-representations to simple* S*-representations. The dimensions of the simples is preserved under this bijection.*
An analog statement holds in the extremal cases.

Proof. The first part follows from Proposition 4.2.18. For the final part note that inflation clearly does not change property of being simple nor the dimension. □

Theorem 4.2.6. *For any two J-cells $\mathcal{J} \leq_{lr} \mathcal{K}$ we have*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{S}^{\mathcal{K}}_{\mathcal{J}}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{S}).$$

Proof. By Proposition 4.2.41. □

Remark 4.2.42 (***Additional Task 5***). By Theorem 4.2.6, a strategy is to find a monoid S with big representations for a slice of the cells. Then taking an appropriate cell subquotient the resulting monoid will have a suitable representation gap.

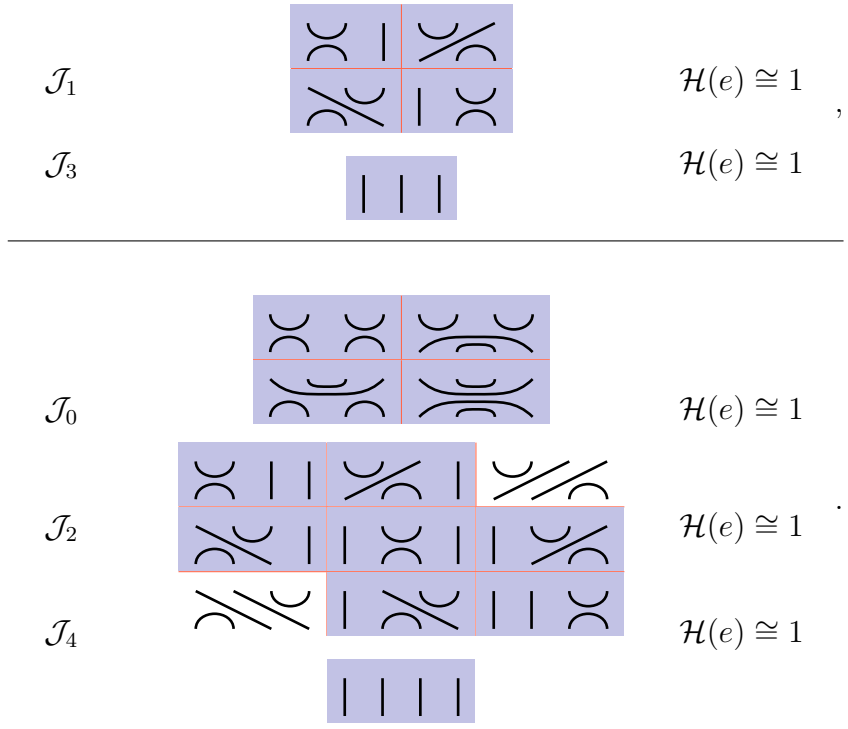
4.3 The Temperley-Lieb monoid chain, worked out in detail

4.3.1 Cells of the Temperley–Lieb monoid

We now discuss the cell structure of TL_n.

Remark 4.3.1. The cell structure of the Temperley–Lieb monoid TL_n is very nice and easy to compute. It is well-known and was (re)discovered in many papers, see e.g. [44], or [31] or [50], although not always in the language of cells. So we decided to repeat it here in that language.

The main pictures to keep in mind (which we will explain momentarily) are:



(4.3.1.1)

These are the cells of TL_3 and TL_4, which should be read as in Equation 4.2.1.1. We have also colored/shaded the idempotent H-cells. Note that $\mathcal{J}_k$ is the set of crossingless matchings with k through strands, and k and n have the same parity. These diagrams have $c(k) = \frac{n-k}{2}$ caps respectively cups.

Proposition 4.3.2. *We have the following.*

(a) *The left and right cells of* TL_n *are given by crossingless matchings where one fixes the bottom respectively top half of the diagram. The* $\leq_l$*- and the* $\leq_r$*-order increases as the number of through strands decreases. Within* $\mathcal{J}_k$ *we have*

$$|\mathcal{L}| = |\mathcal{R}| = \tfrac{n-2c(k)+1}{n-c(k)+1}\binom{n}{c(k)}.$$

(b) *The* J*-cells* $\mathcal{J}_k$ *of* TL_n *are given by crossingless matchings with a fixed number of through strands* k*. The* $\leq_{lr}$*-order is a total order and increases as the number of*

through strands decreases. For any $\mathcal{L} \subset \mathcal{J}_k$ *we have*

$$|\mathcal{J}_k| = |\mathcal{L}|^2.$$

(c) *Each* J*-cell of* TL_n *is idempotent, and* $\mathcal{H}(e) \cong 1$ *for all idempotent* H*-cells. We have*

$$|\mathcal{H}| = 1.$$

Proof. (a)+(b). For (a) and (b) we recall that the $\mathbb{K}$-linear version of this theorem can be found in e.g. [19, Example 1.4] or [44, Section 2]. (Note that [44, Section 2] gives $|\mathcal{L}| = |\mathcal{R}| = \binom{n}{c(k)} - \binom{n}{c(k)-1}$, which we rewrite into the claimed expression via algebra autopilot.) The arguments given in these papers do not depend on $\mathbb{K}$ nor on the parameter δ and go through in the set-theoretical case without change as well.

(c). This is then immediate from (a) and (b). □

Proposition 4.3.3. *The set of apexes for simple* TL_n*-representations can be indexed* 1:1 *by the poset* $\Lambda = (\{n, n-2, ...\}, >)$ *(ending on either* 0 *or* 1*, depending on the parity of* n*), and there is precisely one simple* TL_n*-representation of a fixed apex up to* $\cong$*.*

Proof. By Proposition 4.3.2, this is a direct application of Proposition 4.2.18. □

By Proposition 4.3.3 there is a poset Λ indexing the J-cells and the simple TL_n-representations. We can thus enumerate the J-cells by $\mathcal{J}_k$ for $k \in \Lambda$. We do the same for the simple TL_n-representations and we write L_k for these. (Here we mean any choice of representatives of the isomorphism classes. Similarly below, and we stop stressing this.)

Lemma 4.3.4. *Within one* J*-cell, all left cell modules* $\Delta_{\mathcal{L}}$ *and all right cell modules* ${}_{\mathcal{R}}\Delta$ *are isomorphic. We write* Δ_k *respectively* ${}_k\Delta$ *for those in* $\mathcal{J}_k$*.*
We have $\Delta_k \cong {}_k\Delta$ *as* $\mathbb{K}$*-vector spaces and* $\dim_{\mathbb{K}}(\Delta_k) = \dim_{\mathbb{K}}({}_k\Delta) = \frac{n-2c(k)+1}{n-c(k)+1}\binom{n}{c(k)}$.

Proof. The diagrammatic antiinvolution $\_^*$ is compatible with the cells structure and shows $\Delta_k \cong {}_k\Delta$. The dimension formula then follows from Proposition 4.3.2 and Lemma 4.2.14. □

Proposition 4.3.5. *The semisimple dimensions are* $\mathrm{ssdim}_{\mathbb{K}}(L_k) = \frac{n-2c(k)+1}{n-c(k)+1}\binom{n}{c(k)}$.

Proof. The equation follows immediately from Proposition 4.3.2 and Proposition 4.3.3. □

The numbers $\dim_{\mathbb{K}}(L_k)$ are as follows. These were computed in many papers, e.g. in [4] and [50] which compute them for general $\mathbb{K}$ and $\delta \in \mathbb{K}$. (Strictly speaking [4] needs $\delta = -q - q^{-1}$ because Andersen uses the connection to tilting modules.) To state them we need some preliminary definitions.

Remark 4.3.6. The definitions below are fairly standard for Temperley–Lieb calculi over arbitrary fields, see e.g. [50], [51] or [35]. The reader only interested in $\mathrm{char}(\mathbb{K}) = 0$ (which is $\mathrm{char}(\mathbb{K}) = \infty$ below) can ignore all definitions involving p-adic combinatorics. We elaborate on the $\mathrm{char}(\mathbb{K}) = 0$ case in Example 4.3.7 below.

Let $\mathrm{char}(\mathbb{K}) = p$, allowing $p = \infty$ which is the case $\mathrm{char}(\mathbb{K}) = 0$. Let ν_p denote the *p-adic valuation*. Let $\nu_{3,p}(x) = 0$ if $x \not\equiv 0 \bmod 3$, and $\nu_{3,p}(x) = \nu_p(\frac{x}{3})$ otherwise. Let further $x = [..., x_1, x_0]$ denote the $(3,p)$-*adic expansion* of x given by

$$[..., x_1, x_0] = \sum_{i=1}^{\infty} 3p^{i-1}x_i + x_0 = x, \quad x_{i>0} \in \{0, ..., p-1\}, x_0 \in \{0, 1, 2\}.$$

The numbers x_j are the digits of x, and most of these x_j are zero. Let now $x \lhd y$ if $[..., x_1, x_0]$ is digit-wise smaller or equal to $[..., y_1, y_0]$. We also write $x \lhd' y$ if $x \lhd y$, $\nu_{3,p}(x) = \nu_{3,p}(y)$ and the $\nu_{3,p}(x)$th digit of x and y agree. Finally, set

$$e_{n,k} = \begin{cases} 1 & \text{if } n \equiv k \bmod 2,\ \nu_{3,p}(k) = \nu_{3,p}(\frac{n+k}{2}),\ k \lhd' \frac{n+k}{2}, \\ -1 & \text{if } n \equiv k \bmod 2,\ \nu_{3,p}(k) < \nu_{3,p}(\frac{n+k}{2}), k \lhd \frac{n+k}{2} - 1, \\ 0 & \text{else.} \end{cases} \tag{4.3.1.2}$$

Example 4.3.7. For $\mathrm{char}(\mathbb{K}) = 0$ the above simplifies quite a bit. First, the only two relevant numbers $x_1 \in \mathbb{Z}_{\geq 0}, x_0 \in \{0, 1, 2\}$ are given by $x = 3x_1 + x_0$, so x_0 is the reminder of x upon division by 3. The equation Equation 4.3.1.2 simplifies to the following matrix whose entries are $e_{n,k}$:

n\k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1		1															
2	-1		1														
3				1													
4					1												
5				-1		1											
6	1		-1				1										
7								1									
8	-1		1				-1		1 ← $e_{8,8}$								
9				1		-1				1							
10											1						
11				-1		1				-1		1					
12	1		-1				1		-1				1				
13														1			
14	-1		1				-1		1				-1		1		
15				1		-1				1		-1				1	
16																	1

$e_{15,11}$

Here we have illustrated the case $n = 16$. The pattern is that every third row has only one nonzero entry. Otherwise, the pattern $(-1, 0, 1)$ respectively $(1, 0, -1)$ is shifted along rows with a distance of three zeros.

We have the following alternating sum of $\dim_{\mathbb{K}}(\Delta_{\mathcal{L}}) = \frac{n-2c(k)+1}{n-c(k)+1}\binom{n}{c(k)}$. (Recall that $c(k)$ denotes the number of caps respectively cups for diagrams in the J-cell $\mathcal{J}_k$.) That a dimension formula is of this form is expected from the cell structure, and the precise coefficients $e_{n,k}$ are the main point:

Proposition 4.3.8. *We have* $\dim_{\mathbb{K}}(L_k) = \sum_{r=0}^{c(k)} e_{n-2r+1,k+1}\left(\frac{n-2c(k)+1}{n-c(k)+1}\binom{n}{c(k)}\right)$. *In particular, for* $k \in \{0, 1, n\}$ *we have* $\dim_{\mathbb{K}}(L_k) = 1$.

Proof. For the Temperley–Lieb algebra $\mathrm{TL}_n^{lin}(1)$ these dimensions were computed in [50, Corollary 9.3]. These computations use the $\mathbb{K}$-linear cell structure of $\mathrm{TL}_n^{lin}(1)$ given by it being a cellular algebra. These turn out to be the same calculations as for the cell structure of the Temperley–Lieb monoid TL_n discussed in Theorem 4.2.2 and the results in [50, Corollary 9.3] work thus for TL_n without change. □

Example 4.3.9. It is easy to feed the above into a machine. Below we list the first few dimensions of the simple TL_n-representations L_k for $\mathrm{char}(\mathbb{K}) = 0$ (first table), and $\mathrm{char}(\mathbb{K}) = 2$ (second table). Here $0 \leq n \leq 16$ is indexing the rows and $0 \leq k \leq 16$ the columns.

n\k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1		1															
2	1		1														
3		1		1													
4	1		3		1												
5		1		4		1											
6	1		9		4		1										
7		1		13		6		1									
8	1		28		13		7		1								
9		1		41		27		7		1							
10	1		90		41		34		9		1						
11		1		131		110		34		10		1					
12	1		297		131		144		54		10		1				
13		1		428		429		144		64		12		1			
14	1		1001		428		573		273		64		13		1		
15		1		1429		1638		573		337		90		13		1	
16	1		3432		1429		2211		1260		337		103		15		1

Order of cells ←

$\mathrm{char}(\mathbb{K}) = 0$

← $\dim_{\mathbb{K}}(L_8)$ for TL_8

$\dim_{\mathbb{K}}(L_{11})$ for TL_{15}

n\k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1		1															
2	1		1														
3		1		1													
4	1		3		1												
5		1		4		1											
6	1		9		4		1										
7		1		13		6		1									
8	1		27		13		7		1								
9		1		40		27		7		1							
10	1		81		40		34		9		1						
11		1		121		110		34		10		1					
12	1		243		121		144		54		10		1				
13		1		364		429		144		64		12		1			
14	1		729		364		573		272		64		13		1		
15		1		1093		1638		573		336		90		13		1	
16	1		2187		1093		2211		1245		336		103		15		1

Order of cells ←

$\mathrm{char}(\mathbb{K}) = 2$

← $\dim_{\mathbb{K}}(L_8)$ for TL_8

$\dim_{\mathbb{K}}(L_{11})$ for TL_{15}

These tables also appear in [4]. Note that the representation L_0 for even n and L_1 for odd n, separated by a dotted line, are always of dimension one. This is a special coincidence of the involved combinatorics and was observed from a very different direction in [35, Proposition 4.5].

Recall that $c(k)$ denotes the number of caps respectively cups in $\mathcal{J}_k$. The following lower bound for the dimensions ($k \notin \{0, 1\}$ in covered in Proposition 4.3.8):

Proposition 4.3.10. *Let* $\mathrm{char}(\mathbb{K}) = 0$. *For* $k \notin \{0, 1\}$ *we have*

$$\dim_{\mathbb{K}}(L_k) \geq \frac{1}{(n - c(k) + 1)(n - c(k) + 2)} \binom{n}{c(k)}.$$

Proof. See [50, In preparation]. □

Example 4.3.11. The dimensions of the simple TL_{24}-representations over $\mathbb{Q}$ and their lower bounds are given by the tuples

$$\begin{aligned} \dim\colon\ & (1, 534888, 208011, 445741, 389367, 126292, 85216, 31878, 6876, 1726, 252, 22, 1), \\ \text{lower bound}\colon\ & \left(14858, 11886, 8171, 4807, 2403, 1012, 354, 101, 23, 4, 0.5, 0.04, \tfrac{1}{650}\right). \end{aligned}$$

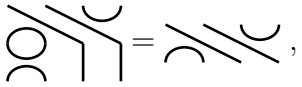
Here L_0 correspond to the leftmost entry and then k increases in steps of two from left to right. Note that the lower bound does not work for $k = 0$.

4.3.2 Truncating the Temperley–Lieb monoid

Recall that we need an admissibility condition to ensure that taking cell subquotients works as expected, cf. Definition 4.2.39. We first establish:

Lemma 4.3.12. *The monoid* TL_n *is admissible.*

Proof. We check that TL_n is left-admissible. Take a and b with k through strands, both in the same left cell within $\mathcal{J}_k$. Thus, a and b have the same bottom half $\beta_a = \beta_b$ but the top halves $\gamma_a \neq \gamma_b$ can be different. We can now use $c = \gamma_a \circ (\gamma_b)^*$ which implies that $a = cb$, as required. The picture is:



which is a calculation in $\mathcal{J}_2$ as in Equation 4.3.1.1. Right- and J-admissibility can be check verbatim. □

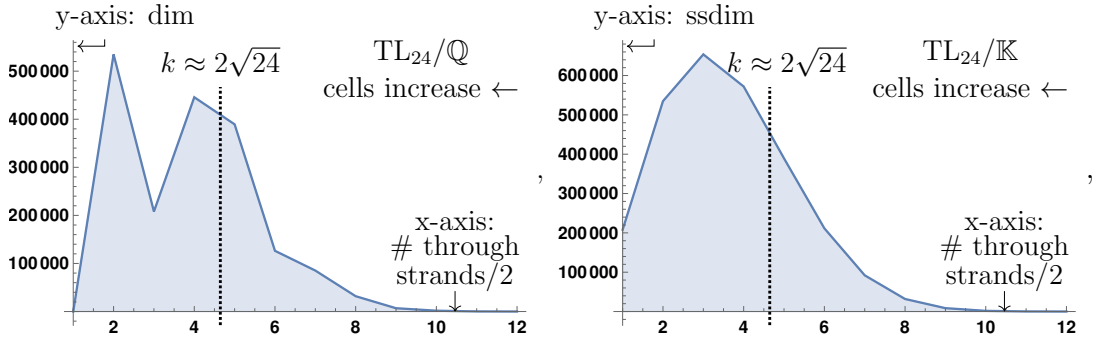
Motivated by Example 4.3.14 below we define:

Definition 4.3.13. Define the *kth truncated Temperley–Lieb monoid* by

$$\mathrm{TL}_n^{\leq k} = (\mathrm{TL}_n)_{\geq \mathcal{J}_k}.$$

This is the cell submonoid, see Section 4.2.6. In words, $\mathrm{TL}_n^{\leq k}$ consist of all crossingless matchings with fewer than k through strands, together with an identity element.

Example 4.3.14. Let us come back to Equation 4.2.6.1. Looking at the graphs of the dimensions and the semisimple dimensions of the simple TL_{24}-representations



$$\text{dim}: (1, 534888, 208011, 445741, 389367|126292, 85216, 31878, 6876, 1726, 252, 22, 1),$$

$$\text{ssdim}: (208012, 534888, 653752, 572033, 389367|211508, 92092, 31878, 8602, 1748, 252, 23, 1), \tag{4.3.2.1}$$

it seems preferable to cut these graphs roughly at $k \approx 2\sqrt{24}$ or at even lower values, as illustrated above. The submonoid $\mathrm{TL}_{24}^{\leq k}$ for this specific value of k now does not have too small representations anymore and is still rich enough as a monoid. (The one-dimensional simple $\mathrm{TL}_{24}^{\leq k}$-representation for $\mathcal{J}_0$ is $\mathbb{1}_b$, so we do not need to get rid of it.)

Our main statement about the Temperley–Lieb case is a bound for the representation gap of $\mathrm{TL}_n^{\leq k}$, but before we can prove it we need to discuss extensions.

4.3.3 Trivial extensions in Temperley–Lieb monoids

Our next goal is to show that TL_n and $\mathrm{TL}_n^{\leq k}$ have no extensions between $\mathbb{1}_{bt}$ (under some minor restrictions on n and k). Let X be either TL_n or $\mathrm{TL}_n^{\leq k}$, and recall the notions of left-rounded, right-rounded, null-rounded and well-rounded from Section 4.1.1.

Lemma 4.3.15. *The monoid* X *is null-rounded.*

Proof. Note first that for each of these monoids the group G of invertible elements is trivial. For $a \in \mathrm{X} \setminus \mathrm{G}$ the decomposition $a = a_1 a_2^*$ (see Definition 3.4.11), we have that these monoids are null-rounded since $a_2^* = a_2^* a_2 a_2^*$ and $a = a a_2 a_2^*$ is then a product of a and $a_2^* a_2 \in \mathrm{X} \setminus \mathrm{G}$. □

Before we can prove the main statement of this section we need some terminology.

Remark 4.3.16. The reader might recognize the definitions below from the theory of Temperley–Lieb cells (or the many other occasions where this theory has appeared in disguise). That is no coincidence as the notions of being left- or right-rounded are closely related to left and right cells.

Recall that a diagram $a \in \mathrm{B}_m^n$ consists of m through strands and $\frac{n-m}{2}$ cups. The through strands connect top and bottom endpoints in a, while cups connects top endpoints in pairs. For the following notion we naively compose diagrams, meaning that we do not remove internal circles. We say that $a, b \in \mathrm{B}_m^n$ are in a *vertical position* if the diagram $b^* a$ is isotopic to id_m, the identity diagram on m strands. Elements $a, b \in \mathrm{B}_m^n$ are said to be in a *weakly vertical position* if $b^* a$ is isotopic to id_m together with potential internal circles.

Example 4.3.17. Consider $a, b \in \mathrm{B}_2^6$ given by

Then a and b are in vertical position, as illustrated above. But neither a and a nor b and b are. The latter are only in weakly vertical position.

Denote by $\mathrm{Vert}_n^m \subset \mathrm{B}_m^n \times \mathrm{B}_m^n$ the set of pairs of diagrams in a vertical position, and write $(a, b) \in \mathrm{Vert}_n^m$. This relation on diagrams is symmetric.

Denote by $\mathrm{WVert}_m^n \subset \mathrm{B}_m^n \times \mathrm{B}_m^n$ the set of pairs of diagrams in weakly vertical position, and write $(a, b) \in \mathrm{WVert}_m^n$. Note that $(a, a) \in \mathrm{WVert}_m^n$ for any $a \in \mathrm{B}_m^n$. Again, this relation on diagrams is symmetric.

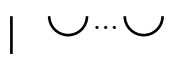
If $(a_2, b_1) \in \mathrm{WVert}_m^n$, then $a_1 a_2^* b_1 b_2^* = a_1 (a_2^* b_1) b_2^* = a_1 b_2^*$. That is, inserting $a_2^* b_1$ in the middle of $a_1 b_2^*$ does not change the latter.

Definition 4.3.18. Let Γ_m^n denote the unoriented graph with vertex set B_m^n and edges between a and b for all $(a, b) \in \mathrm{Vert}_m^n$.

Note that Γ_m^n is nonempty if and only if $n \geq m$ and $n + m$ is even.

Lemma 4.3.19. *The graph Γ_m^n is connected if $m > 0$.*

Proof. Case $m = 1$. In this case the lemma can be proved by induction on n, by showing that any diagram $a \in \mathrm{B}_1^n$ is connected by a path in Γ_1^n to the diagram



with the through strand on the far left and $\frac{n-1}{2}$ unnested cups.

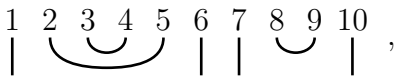
General case. Consider a diagram $a \in \mathrm{B}_m^n$. Each through strand c of a may be surrounded by a cluster of cups on either side. The first case allows to bring each such cluster together with c to a standard form as above (through strands followed by a sequence of unnested cups) via paths in suitable graphs Γ_1^k, utilizing only one through strand c. Doing this transformation with each through strands in a and moving all through strands all the way to the left transforms a to a standard form of m parallel vertical strands on the left followed by unnested $\frac{n-m}{2}$ cups. This shows that Γ_m^n is connected. □

A cup is called *outer* if it is not separated from the bottom of the diagram by any cup. A pair $(a, b) \in \mathrm{B}_m^n \times \mathrm{B}_m^n$ is called a *flip pair* if b is obtained from a by converting an outer cup

c into a pair of through strands while simultaneously closing up a pair p of adjacent through strands in a into a cup. Note that c must not be located between the two strands in p, and that the flip pair relation is symmetric.

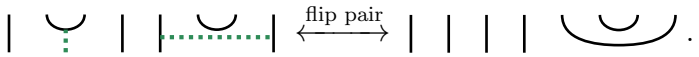
Example 4.3.20.

(a) In the element of B_3^{10}



the cups $(2,5)$ and $(8,9)$ are outer. The cups $(2,5)$ and $(3,4)$ are nested, with $(2,5)$ an outer nested cup.

(b) The following is a flip pair:



We have indicated where we apply operations on the left-hand diagram.

The reader might want to think of a flip pair as two diagrams related by opposite saddles moves.

Definition 4.3.21. Let Δ_m^n denote the unoriented graph with vertex set B_m^n and edges between a and b for all flipped pairs (a, b).

Note that the graph Δ_2^n is not connected for even $n \geq 4$, since a diagram with one through strand on the far left and one on the far right is not in any flip pair.

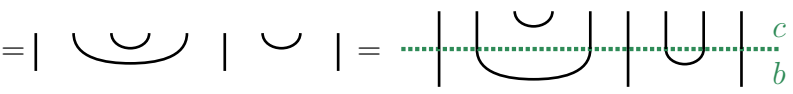
Lemma 4.3.22. *The graph Δ_3^n is connected.*

Proof. We view the empty graph (with no vertices) as connected, which is the case when n is even. For odd $n = 3 + 2k$ the proof is by induction on k.

Case $k = 1$. In this case the graph has the form

thus is connected.

Case $k > 1$. Represent $a \in \mathrm{B}_3^{3+2k}$ as a composition $a = cb$ of a diagram $c \in \mathrm{B}_{1+2k}^{3+2k}$ with a single cup and $b \in \mathrm{B}_3^{1+2k}$, e.g.:

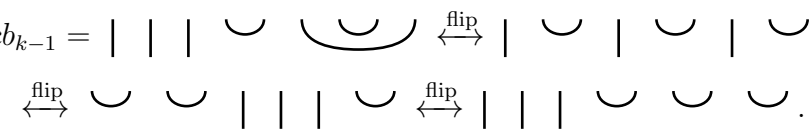
$a =$  .

By induction on k, the diagram b is connected in the graph Δ_3^{2k+1} to the diagram b_{k-1}, called standard, of three through strands on the far left and by $k-1$ unnested cups on the right. For example

$b =$  .

(4.3.3.1)

Consequently, in Δ_3^{2k+3} the diagrams a and cb_{k-1} are connected. If the extra cup in cb_{k-1} coming from c is not nested inside the rightmost cup of b_{k-1}, as shown in Equation 4.3.3.2, then cb_{k-1} can be represented as a diagram in B_3^{2k+1} union a cup on the far right, $cb_{k-1} = d \otimes \cup$, with d in very specific form, see Equation 4.3.3.1. By induction, d is connected to the standard diagram b_{k-1} in Δ_3^{2k+1}. The union of the latter with a cup on the far right gives the standard diagram in Δ_3^{2k+3}, implying that a is connected to the standard diagram $b_k \in \Delta_3^{2k+3}$.

$cb_{k-1} =$  .

(4.3.3.2)

The remaining case is when the cup from c is nested inside the rightmost cup of b_{k-1}, see

Equation 4.3.3.2. Then a series of transformations along paths in the graph Δ_3^{2k+3}, possible by induction, show that a is in the same connected component as the diagram b_k, concluding the induction step. □

Lemma 4.3.23. *The graph Δ_m^n is connected for any $m \geq 3$.*

Proof. The proof is by induction on m. Case $m = 3$ has already been established. Denote by $b_{n,m}$ the diagram with m through strands on the far left followed by $\frac{n-m}{2}$ unnested cups to the right. If the leftmost strand of a is a through strand, then the diagram a can be written as a union $a = | \otimes a'$ of a through strand and a diagram a' in B_{m-1}^{n-1}. By induction, a' is connected to the standard diagram $b_{n-1,m-1}$ implying that a is connected to $b_{n,m}$.
If the leftmost strand of a is a cup, consider the three leftmost through strands of a and form the subdiagram a_1 that consists of these strands and all cups to the left and in between of these through strands. We can write $a = a_1 \otimes a_2$, with a_2 the complement a_2 of a_1 in a. By Lemma 4.3.22, a_1 is connected to some diagram b_r with r through strands to the left. Hence, $a = a_1 \otimes a_2$ is connected to $b_r \otimes a_2$. In the latter diagram the leftmost strand is through, and the previous case allows to use the induction step. □

Recall the relation $\approx_l$ given by the closure of the relation $ba \approx_l a$, where $a, b \in \mathrm{S} \setminus \mathrm{G}$.

Lemma 4.3.24. (a) *Suppose $(a, b) \in \mathrm{B}_m^n$ is a flip pair, and $m \leq k$. Then $aa^* \approx_l bb^*$ in $\mathrm{TL}_n^{\leq k}$. Moreover, for $a, b \in \mathrm{B}_m^n$, $m \leq k$ we have $aa^* \approx_l bb^*$ in $\mathrm{TL}_n^{\leq k}$.*

(b) *For $a, b, c \in \mathrm{B}_k^n$ we have $ac^* \approx_l bc^*$ in $\mathrm{TL}_n^{\leq k}$, for $k \geq 3$.*

Proof. (a). Suppose the flip is described via an outer cup c and a pair p of adjacent through strands in a, as in the definition of a flip. Let $d \in \mathrm{B}_{m-2}^n$ is obtained from a by closing up the pair p into a strand. It is straightforward to check that $dd^*aa^* = dd^* = dd^*bb^*$, which implies that $aa^* \approx_l bb^*$. The second claim follows then from the first.

(b). Since Δ_k^n is connected, we can choose a path $a = a_1, a_2, ..., a_r = b$ in it, with each (a_i, a_{i+1}) an edge. Then $a_{i+1}^* a_i = id_k$, and $a_{i+1}c = a_{i+1}a_{i+1}^* a_i c \approx_l a_i c$, and $ac = a_0 c \approx_l a_r c = bc$. □

We are ready to prove that the Temperley–Lieb monoids are left-rounded.

Lemma 4.3.25. *We have the following.*

(a) *The monoid* TL_n *is left-rounded if* $n \geq 5$.

(b) *The monoid* $\mathrm{TL}_n^{\leq k}$ *is left-rounded if* $n \geq 5$ *and* $k \geq 3$.

Proof. Recall the classical generator-relation presentation of TL_n.

(a). It is easy to see that TL_3 has two equivalence classes $\{u_1, u_2u_1\}$ and $\{u_2, u_1u_2\}$ under $\approx_l$, which are the top left cells in Equation 4.3.1.1. The monoid TL_4 also has two $\approx_l$ equivalence classes, represented by u_1 and u_2. In general, since the u_i generate TL_n, any $\approx_l$ equivalence class is represented by some u_i. For $n > 4$, each u_i is in the same equivalence class as either u_1 or u_{n-1}. For instance, if $i > 2$, u_i and u_1 commute and $u_i \approx_l u_1u_i = u_iu_1 \approx_l u_1$. Finally, $u_1 \approx_l u_{n-1}u_1 = u_1u_{n-1} \approx_l u_{n-1}$.

(b). We need to show that there is a unique equivalence class under $\approx_l$ in $\mathrm{TL}_n^{\leq k} \setminus \{1\}$. First, any element u in the latter set is equivalent under $\approx_l$ to an element of width k. To see this, write a minimal length presentation $u = u_{i_r}u_{i_{r-1}}...u_{i_1}$ of u as a product of generators. The element u has width $m \leq k$. Pick the smallest p such that the suffix $v = u_{i_p}u_{i_{p-1}}...u_{i_1}$ of the presentation has width k (this is possible since multiplication of an element by a generator u_i either preserves the width or reduces it by one). Then $u = v'v$ where v' is the product of the remaining terms. Note that $v = vv^*v$ and $u = v'v = (v'vv^*)v$. Widths $\omega(v'vv^*) \leq k$, $\omega(v) = k$, so that both of these elements are in $\mathrm{TL}_n^{\leq k} \setminus \{1\}$, and $u = v'vv^*v \approx_l v$. We see that u is equivalent to an element of width k.

Consequently, it is enough to show that $a \approx_l b$ for any two a, b of width k. Factorize $a = a_1a_2^*, b = b_1b_2^*$ with $a_1, a_2, b_1, b_2 \in \mathrm{B}_k^n$. From Lemma 4.3.25 we have $a_1a_2^* \approx_l a_2a_2^*$ and $b_1b_2^* \approx_l b_2b_2^*$. From the same lemma, $a_2a_2^* \approx_l b_2b_2^*$, so that $a \approx_l b$. □

Note that the statement of part (b) of the lemma essentially contains part (a) by taking $k = n$. We have included both parts for clarity.

Lemma 4.3.26. *The monoid* TL_n *is well-rounded if* $n \geq 5$*, and the monoid* $\mathrm{TL}_n^{\leq k}$ *is well-rounded if* $n \geq 5$ *and* $k \geq 3$*.*

Proof. This is just the combination of the previous lemmas. Note hereby that the diagrammatic antiinvolution $\_^*$ implies that the monoids TL_n and $\mathrm{TL}_n^{\leq k}$ are left-rounded if and only if they are right-rounded. □

Let X be either TL_n or $\mathrm{TL}_n^{\leq k}$ for $k \geq 3$.

Lemma 4.3.27. *We have* $\mathrm{H}^1(\mathrm{X}, \mathbb{K}) \cong 0$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

Proof. Case $\mathrm{X} = \mathrm{TL}_n$*.* A homomorphism $f\colon \mathrm{TL}_n \to \mathbb{K}$ takes each idempotent $e \in \mathrm{TL}_n$ to 0. From the classical generators-relation presentation of TL_n, it is clear that every nonidentity element is a product of idempotents, so we get $\mathrm{H}^1(\mathrm{TL}_n, \mathbb{K}) \cong 0$.

Case $\mathrm{X} = \mathrm{TL}_n^{\leq k}$*.* We now need a different argument. Suppose give a homomorphism $f\colon \mathrm{TL}_n \to \mathbb{K}$. Consider all diagrams of width k in X. They have the form ab^*, $a, b \in \mathrm{B}_k^n$. Necessarily $f(aa^*) = 0$. If (b, c) is an edge in Γ_k^n and $d \in \mathrm{B}_k^n$, then $ab^*cd^* = ad^*$ and there is a relation

$$f(ad^*) = f(ab^*) + f(cd^*).$$

Choosing a path from a to d in Γ_k^n allows to write $f(ad^*)$ as a sum over $f(bc^*)$ where (b, c) is an edge in Γ_k^n. The relation $bc^*bb^* = bb^*$ implies

$$f(bb^*) = f(bc^*) + f(bb^*),$$

so that $f(bc^*) = 0$ for an edge (b, c). Consequently, $f(ad^*) = 0$ for a, d as above, and $f(x) = 0$ for any x of width k in X. The elements y of X of smaller width are products of elements of width k, showing that $f(y) = 0$ as well. Thus, f is identically 0 on X. □

Proposition 4.3.28. *Let M be an* X*-representation. Assume that $n \geq 5$ and in the truncated case $k \geq 3$. Then any short exact sequence*

$$0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$$

splits.

Proof. Note that the group of units G of X is trivial, so $\mathrm{H}^1(\mathrm{G}, \mathbb{K}) \cong 0$. Combine this with Lemma 4.3.26 and Theorem 4.1.1. □

4.3.4 Representation gap and faithfulness of the Temperley–Lieb monoid

We are ready to state and prove the main statements about the Temperley–Lieb monoid. Let X be either TL_n or $\mathrm{TL}_n^{\leq k}$.

Theorem 4.3.1. *Let $n > 4$, and let $m(l)$ be the dimension of the simple* X*-representation L_l as in Proposition 4.3.8. Then:*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{TL}_n) = \min\big\{m(l) | l \notin \{0, 1, n\}\big\},$$
$$\mathrm{gap}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}) = \min\big\{m(l) | l \notin \{0, 1, k+1, k+2, ..., n\}\big\}.$$

Proof. By Theorem 4.1.1 and Proposition 4.3.28. □

Recall that k denotes the number of through strands, and crossingless matchings with k through strands have $\frac{n-k}{2}$ caps and cups. In particular, $\mathrm{TL}_n^{\leq k}$ for $0 \leq k \leq 2\sqrt{n}$ has crossingless matchings with at most $2\sqrt{n}$ through strands and at least $\frac{n-2\sqrt{n}}{2}$ (this number is bigger than $\sqrt{n}$ for $n > 16$) caps and cups. Also recall the Bachmann–Landau notation $f \in \Theta(g)$, meaning that f is bounded both above and below by g asymptotically.

Theorem 4.3.2. *Let $n \geq 5$ and fix $0 \leq k \leq 2\sqrt{n}$. Let* $\mathrm{char}(\mathbb{K}) = 0$*, and let $\mathbb{L}$ be an*

arbitrary field. We have the following lower bounds:

$$\begin{aligned}
\operatorname{gap}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}) &\geq \frac{4}{(n+2\sqrt{n}+2)(n+2\sqrt{n}+4)}\binom{n}{\frac{n}{2}-\sqrt{n}} \in \Theta\big(2^n n^{-5/2}\big),\\
\operatorname{ssgap}_{\mathbb{L}}(\mathrm{TL}_n^{\leq k}) &\geq \frac{2}{2n}\binom{n}{\lfloor\frac{n}{2}\rfloor} \in \Theta\big(2^n n^{-3/2}\big),\\
\operatorname{faith}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}) &\geq \frac{6}{n+4}\binom{n}{\frac{n'}{2}-1} \in \Theta\big(2^n n^{-3/2}\big).
\end{aligned}$$

where in the final bound $n' = n$, if n is even, and $n' = n-1$, if n is odd.

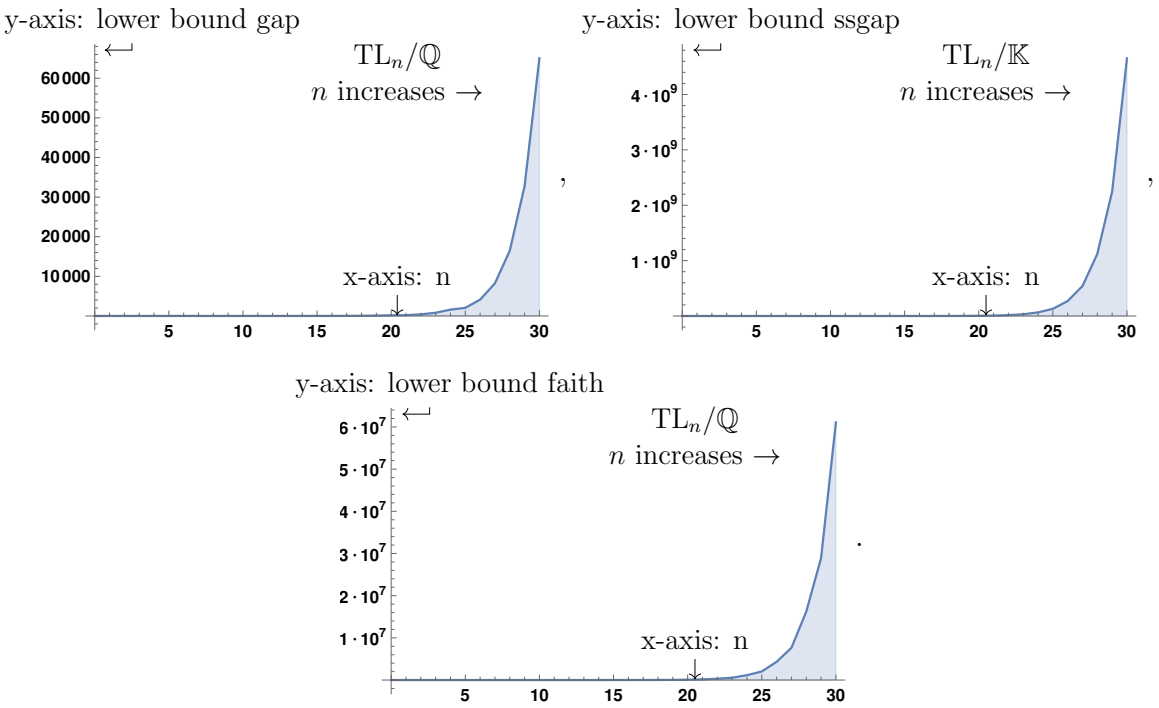
Proof. Representation gap. We will make use of Proposition 4.3.28. By Theorem 4.1.1, this statement ensures that we only need to compute dimension bounds for simple $\mathrm{TL}_n^{\leq k}$-representations. The first bound then follows from Proposition 4.3.10. The formula $\frac{1}{(n-c(k)+1)(n-c(k)+2)}\binom{n}{c(k)}$ has its minimum for $k = \lfloor 2\sqrt{n}\rfloor$. Plotting this k into the formula and a bit of algebra autopilot gives the claimed lower bound. The asymptotic formula then follows by using that $\frac{4}{(n+2\sqrt{n}+2)(n+2\sqrt{n}+4)}$ is in $\Theta(\frac{1}{n^2})$, and using Stirling's approximation for $n!$ to get that the binomial is in $\Theta(2^n n^{-1/2})$.

Semisimple representation gap. The second bound can be seen as follows. We need to minimize the formula in Proposition 4.3.5 for $0 \leq k \leq 2\sqrt{n}$. Observe that the function $\frac{n-2c(k)+1}{n-c(k)+1}\binom{n}{c(k)}$ in k has precisely one peak between $k=0$ and $k = \lfloor 2\sqrt{n}\rfloor$, and is monotone increasing respectively decreasing otherwise. So we only need to compare the two values for $k = 0, 1$ and $k = \lfloor 2\sqrt{n}\rfloor$, and it is then easy to see that the $k = 0, 1$ value is smaller. Since $c(0) = \frac{n-0}{2}$ and $c(1) = \lfloor\frac{n}{2}\rfloor$, the result follows. The asymptotic formula follows also from Stirling's approximation for $n!$.

Faithfulness. For the final bound we use Lemma 4.1.34. This lemma says that it suffices to find a lower bound for $\mathrm{TL}_n^{\leq 2}$: If n is even, then $\mathrm{TL}_n^{\leq 2} \hookrightarrow \mathrm{TL}_n^{\leq k}$. If n is odd, then we can still use $\mathrm{TL}_n^{\leq 2}$ after adding another strand. Note that a faithful $\mathrm{TL}_n^{\leq 2}$-representation can not be a nontrivial extension of $\mathbb{1}_{bt}$ by Proposition 4.4.10 and also not a direct sum of $\mathbb{1}_{bt}$. Hence, any faithful $\mathrm{TL}_n^{\leq 2}$-representation must contain L_2. The combinatorics from Example 4.3.7

implies that $\dim_{\mathbb{K}}(L_2) = \mathrm{ssdim}_{\mathbb{K}}(L_2)$, so the claimed formula follows from Proposition 4.3.5. The asymptotic formula can be verified in the same way as for (a) and (b).
Let us note that alternatively to direct computations for the asymptotic formulas, the reader can also input the above bounds into a computer algebra system such as Mathematica and ask the computer to algebraically manipulate the symbols. □

Example 4.3.29. The lower bounds in Theorem 4.3.2 are far from being optimal. But they still grow very fast. Here are their plots:



In these plots n increases form 0 to 30 when going left to right.

Note that the bound $0 \leq k \leq 2\sqrt{n}$ in Theorem 4.3.2 means that the monoid $\mathrm{TL}_n^{\leq k}$ has few through strands. This has the advantage that the dimensions of simple $\mathrm{TL}_n^{\leq k}$-representations peak, but it also means that the information loss during multiplication is big. Alternatively one might want to keep k close to n, so we also state:

Theorem 4.3.3. *Let $n \geq 8$ and fix $2\sqrt{n} \leq k \leq n - \sqrt{n}$. Let $\mathrm{char}(\mathbb{K}) = 0$, and let $\mathbb{L}$ be an*

arbitrary field. We have the following lower bounds:

$$\begin{aligned}
\mathrm{gap}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}) &\geq \frac{1}{(n-\frac{\sqrt{n}}{2}+1)(n-\frac{\sqrt{n}}{2}+2)}\binom{n}{\frac{\sqrt{n}}{2}} \in \Theta\big(n^{\sqrt{n}/4}n^{-9/4}(2e)^{\sqrt{n}/2}\big),\\
\mathrm{ssgap}_{\mathbb{L}}(\mathrm{TL}_n^{\leq k}) &\geq \frac{n-\sqrt{n}+1}{n-\sqrt{n}/2+1}\binom{n}{\frac{\sqrt{n}}{2}} \in \Theta\big(n^{\sqrt{n}/4}n^{-3/4}(2e)^{\sqrt{n}/2}\big),\\
\mathrm{faith}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}) &\geq \frac{6}{n+4}\binom{n}{\frac{n'}{2}-1} \in \Theta\big(2^n n^{-3/2}\big).
\end{aligned}$$

where in the final bound $n' = n$, if n is even, and $n' = n-1$, if n is odd.

Proof. Similar to the proof of Theorem 4.3.2 and omitted. (The assumption $n \geq 8$ ensures that $k \geq 3$, so we can use Lemma 4.3.26.) □

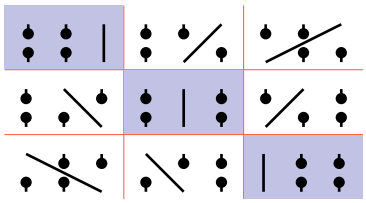
4.4 Other planar monoid chains

Let us now discuss cells, simples and bounds for the other planar monoids from Equation 4.0.0.1 in ascending order (of complexity). The constructions and statements are very similar to the Temperley–Lieb case, so we will be brief. The reader can find more details about the basics about the diagram monoids, and also references, in e.g. [22].

Remark 4.4.1. As we will see, the common theoretical feature of planar monoids is that their H-cells are all of size one.

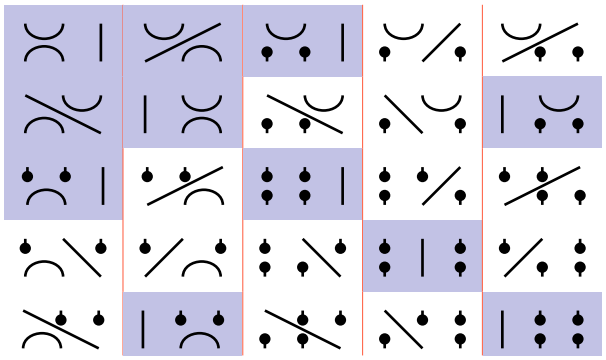
We leave the case of the *planar symmetric group* to the reader and start with the *planar rook monoid* pRo_n. (This monoid was rediscovered several times, see e.g. [30], and the reader might know it under a different name.) The construction of pRo_n is almost the same as for TL_n, but instead of caps and cups we have end and start dots, and all internal components are removed whenever they appear during composition. The monoid pRo_n has

$\binom{2n}{n}$ elements and a typical cell is of the form

$\mathcal{J}_1$  $\mathcal{H}(e) \cong 1$. (4.4.0.1)

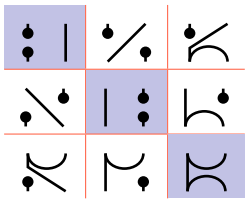
This illustrates $\mathcal{J}_1$ of pRo_3, which has one through strand.

The monoid containing both, TL_n and pRo_n, as submonoids is the *Motzkin monoid* Mo_n. The definition of this monoid works mutatis mutandis as for TL_n and pRo_n, now with caps and cups as well as start and end dots, and all internal components are removed whenever they appear during composition. The Motzkin monoid has $\sum_{k=0}^{n} \frac{1}{k+1}\binom{2n}{2k}\binom{2k}{k}$ elements. The J-cells $\mathcal{J}_i$ are still given by through strands k, and a prototypical example is

$\mathcal{J}_1$  $\mathcal{H}(e) \cong 1$.

This illustrates $\mathcal{J}_1$ and Mo_3.

Finally, the *planar partition monoid* pPa_n has all of the above mentioned planar monoids as submonoids, as it allows now arbitrary partitions, and has $Ca(n/2)$ elements. (Recall that $Ca(k)$ was the kth Catalan number) As before, internal components are removed and cells look very familiar to the cells of the other planar monoids. For example $\mathcal{J}_1$ for pPa_2 is:

$\mathcal{J}_1$  $\mathcal{H}(e) \cong 1$.

In the following we will focus on pRo_n and Mo_n as justified by:

Lemma 4.4.2. *There is an isomorphism of monoids* $\mathrm{pPa}_n \cong \mathrm{TL}_{2n}$.

Proof. See [23, (1.5)]. □

Not surprisingly, the analogs of Proposition 4.3.2 and Proposition 4.4.4 read almost the same. Below, if not stated otherwise, let X be either pRo_n or Mo_n.

Proposition 4.4.3. *We have the following.*

(a) *The left and right cells of* X *are given by the respective type of diagrams where one fixes the bottom respectively top half of the diagram. The* $\leq_l$*- and the* $\leq_r$*-order increases as the number of through strands decreases. Within* $\mathcal{J}_k$ *we have*

$$\mathrm{pRo}_n\colon |\mathcal{L}| = |\mathcal{R}| = \binom{n}{k},$$
$$\mathrm{Mo}_n\colon |\mathcal{L}| = |\mathcal{R}| = \sum_{t=0}^{n} \frac{k+1}{k+t+1}\binom{n}{k+2t}\binom{k+2t}{t}.$$

(b) *The* J*-cells* $\mathcal{J}_k$ *of* X *are given by the respective type of diagrams with a fixed number of through strands* k*. The* $\leq_{lr}$*-order is a total order and increases as the number of through strands decreases. For any* $\mathcal{L} \subset \mathcal{J}$ *we have*

$$\mathrm{X}\colon |\mathcal{J}_k| = |\mathcal{L}|^2.$$

(c) *Each* J*-cell of* X *is idempotent, and* $\mathcal{H}(e) \cong 1$ *for all idempotent* H*-cells. We have*

$$\mathrm{X}\colon |\mathcal{H}| = 1.$$

Proof. Omitted. See also [22, Section 3.3]. Note that the reference gives the dimensions of the simple pRo_n- and Mo_n-representations in the semisimple case, which are thus the sizes of the corresponding cells, see Proposition 4.2.24. □

Proposition 4.4.4. *The set of apexes for simple* X*-representations can be indexed* 1:1 *by the poset* $\Lambda = (\{n, n-1, ...\}, >)$*, and there is precisely one simple* X*-representation of a fixed apex up to* $\cong$*.*

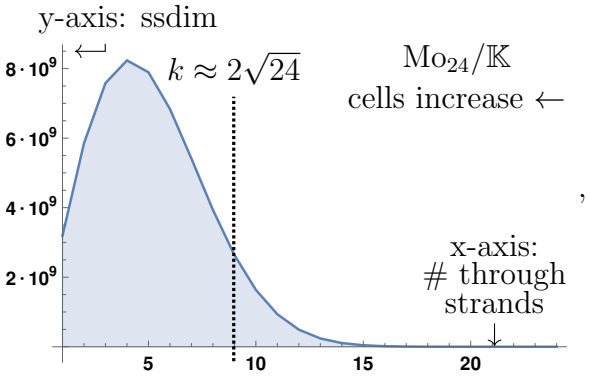
Proof. Clear by Proposition 4.4.3. □

We can number the simple X-representations by L_k for $k \in \Lambda$.

Proposition 4.4.5. *The semisimple dimensions for* pRo_n *and* Mo_n *are* $\mathrm{ssdim}_{\mathbb{K}}(L_k) = \binom{n}{k}$ *and* $\mathrm{ssdim}_{\mathbb{K}}(L_k) = \sum_{t=0}^{n} \frac{k+1}{k+t+1} \binom{n}{k+2t} \binom{k+2t}{t}$*, respectively.*

Proof. Directly from Proposition 4.4.3 and Proposition 4.4.4. □

The semisimple dimensions of pRo_n are given in Equation 4.3.2.1. (Note that Equation 4.3.2.1 shows the dimensions of the simple pRo_n-representations, but we will see in Proposition 4.4.6 below that $\dim_{\mathbb{K}}(L_k) = \mathrm{ssdim}_{\mathbb{K}}(L_k)$ holds for pRo_n.) The semisimple dimensions of Mo_n behave similarly as the semisimple dimensions of TL_n, cf. Equation 4.3.2.1:



$$\mathrm{ssdim}: \left(\begin{array}{c} 3192727797, 5850674704, 7583013474, 8234447672, 7895719634, 6839057544, \\ 5412710842, 3938013264, 2641866894, 1636117512, 935163394, 492652824, \\ 238637282, 105922544, 42884259, 15742672, 5199909, 1530144, 395922, 88504, 16674, 2552, 299, 24, 1 \end{array} \right).$$

The dimensions of simple pRo_n-modules are easy to obtain:

Proposition 4.4.6. *We have* $\dim_{\mathbb{K}}(L_k) = \mathrm{ssdim}_{\mathbb{K}}(L_k) = \binom{n}{k}$ *for* pRo_n*, and* pRo_n *is semisimple.*

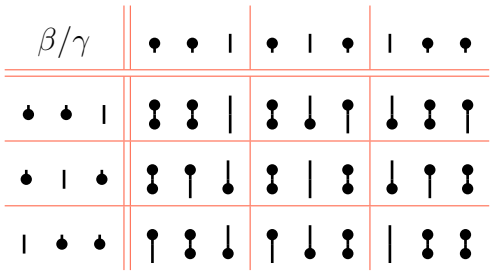
Proof. We only need to prove that pRo_n is semisimple, which implies the other results by Proposition 4.2.24 and Proposition 4.4.5.

To show semisimplicity we use [55, Theorem 5.21] which says that a finite monoid is semisimple if and only if all J-cells are idempotent, all idempotent H-cells are semisimple and the Gram matrices $P(e)$, see Section 4.2.4, for all idempotent H-cell $\mathcal{H}(e)$ are invertible.

By Proposition 4.4.3 we only need to compute the Gram matrices. Since $\mathcal{H}(e) \cong 1$, the reader familiar with the theory of cellular algebras will recognize the following calculation. The Gram matrix for any of the planar monoids discussed in this chapter can be computed using analogs of Definition 3.4.11. Precisely, for each J-cell there are bottom diagrams $\beta_1, ..., \beta_L$ and top diagrams $\gamma_1, ..., \gamma_L$ indexing the rows and columns of the J-cell in question. The Gram matrix is then

$$P(e)_{ij} = \begin{cases} 1 & \text{if } \beta_j \gamma_i = 1, \\ 0 & \text{else,} \end{cases}$$

where 1 is the element of $\mathcal{H}(e) \cong 1$. For example, the Gram matrix of $\mathcal{J}_1$ of pRo_3, see Equation 4.4.0.1, takes the form



$$\leftrightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

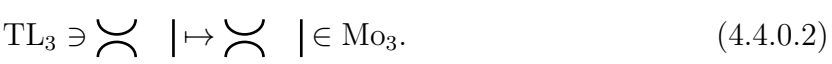
This is the identity matrix. In fact, $P(e)$ is always a permutation matrix: any end dot needs to hit a start dot in order for $\beta_j \gamma_i$ to keep the same number of through strands, and there is precisely one β_j for a fixed γ_i for this to happen. The proof completes. □

The behavior of the dimensions of the simple pRo_n-representations is sketched in Equation

4.2.6.1. Sadly, we do not know the dimensions of the simple Mo_n-representations, but we have the following.

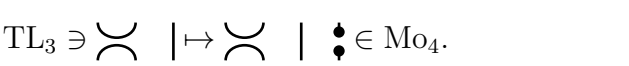
Proposition 4.4.7. *Let $L_l^{\mathrm{TL}_n}$ denote the lth simple TL_n-representation, cf. Section 4.3.1. We have $\dim_{\Bbbk}(L_k) \geq \dim_{\Bbbk}(L_k^{\mathrm{TL}_n})$, if $n-k$ is even, and $\dim_{\Bbbk}(L_k) \geq \dim_{\Bbbk}(L_k^{\mathrm{TL}_{n-1}})$, if $n-k$ is odd, both for Mo_n.*

Proof. Note that TL_n embeds into Mo_n by sending every element to the element with the same description in Mo_n, e.g.:



(4.4.0.2)

Thus, TL_n is a submonoid of Mo_n and Theorem 4.2.4 applies whenever $n-k$ is even since in this case $\mathcal{J}_k$ restricts to an idempotent J-cell of TL_n.
For the odd case we can use the same argument and the embedding of semigroups given by adding a pair of an end and a start dot to the right, e.g.



Theorem 4.2.4 can be easily extended to cover this case as well. □

Lemma 4.4.8. *The monoid* X *is admissible.*

Proof. Easy and omitted. □

This suggests again that we use truncations. Note that $\mathrm{pRo}_n^{\leq k,<l}$ below is constructed using an honest Rees factor, cf. Definition 4.2.38, while $\mathrm{Mo}_n^{\leq k}$ is a submonoid of Mo_n.

Definition 4.4.9. Define the *k-l truncated planar rook monoid* for $k \leq l$ and the *kth truncated Motzkin monoid* by

$$\mathrm{pRo}_n^{\leq k,<l} = (\mathrm{pRo}_n)_{\geq \mathcal{J}_k}/(> \mathcal{J}_l), \quad \mathrm{Mo}_n^{\leq k} = (\mathrm{Mo}_n)_{\geq \mathcal{J}_k}.$$

Let X be either pRo_n or $\mathrm{pRo}_n^{\leq k,<l}$.

Proposition 4.4.10. *Let M be an* X*-representation. Then any short exact sequence*

$$0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$$

splits.

Proof. The monoid pRo_n is semisimple, see Proposition 4.4.6, so Theorem 4.1.1 applies. The case of $\mathrm{pRo}_n^{\leq k,<l}$ follows verbatim as the monoid is also semisimple by the analog of Proposition 4.4.6. □

The following statement is only about pRo_n, since we do not know the dimensions of the simple Mo_n-representations.

Theorem 4.4.1. *We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{pRo}_n) = n, \quad \mathrm{gap}_{\mathbb{K}}(\mathrm{pRo}_n^{\leq k,<l}) = \min\left\{\binom{n}{k}, \binom{n}{l-1}\right\}.$$

Proof. By Theorem 4.1.1, Proposition 4.4.10 and Proposition 4.4.6. □

Theorem 4.4.2. *Let k be arbitrary and $l = \lfloor 2\sqrt{n} \rfloor$. We have the following lower bounds:*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{pRo}_n^{\leq l,<n-l}) = \mathrm{ssgap}_{\mathbb{K}}(\mathrm{pRo}_n^{\leq l,<n-l}) \geq \binom{n}{\lfloor 2\sqrt{n} \rfloor},$$

$$\mathrm{faith}_{\mathbb{K}}(\mathrm{pRo}_n^{\leq l,<n-l}) \geq \sqrt[2\lfloor\sqrt{n}\rfloor+1]{\binom{n}{\lfloor \frac{n}{2} \rfloor}},$$

$$\mathrm{ssgap}_{\mathbb{K}}(\mathrm{Mo}_n^{\leq k}) \geq \mathrm{ssgap}_{\mathbb{L}}(\mathrm{TL}_{n-1}^{\leq k}), \quad \mathrm{faith}_{\mathbb{K}}(\mathrm{Mo}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{K}}(\mathrm{TL}_{n-1}^{\leq k}).$$

Because of Proposition 4.4.7, we also think that $\mathrm{gap}_{\mathbb{K}}(\mathrm{Mo}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{TL}_{n-1}^{\leq k})$. We can not prove this since we would need the analog of Proposition 4.4.10 for the Motzkin monoid.

Proof. Planar rook. We start with pRo_n. The first inequality is immediate from Proposition 4.4.6 and the behavior of binomial coefficients. For the second claim we apply

Theorem 4.2.5. Note that $\mathrm{TL}_n^{\leq l,n-l}$ has $4\lfloor\sqrt{n}\rfloor+1$ cells, but we can restrict to the submonoid with only $2\lfloor\sqrt{n}\rfloor+1$ as in the proof of Theorem 4.3.2.

Motzkin. The first claim follows also from Theorem 4.3.2 by identifying the smallest cell of Temperley–Lieb as a subcell of the smallest cell of $\mathrm{Mo}_n^{\leq k}$. The final inequality follows then from Proposition 4.4.7, Theorem 4.2.5 and Theorem 4.3.2. (Note that using $n-1$ is for convenience so that state a closed formula independent of even and odd issues.) □

Conclusion 4.4.11. *From the viewpoint of linear attacks using small representations, all of the planar monoids* pRo_n, TL_n, Mo_n *and* pPa_n, *or actually their truncations, have only big nontrivial representations. However,* TL_n *is our main example:* pRo_n *appears to be a bit too simple as a monoid to be of use and is semisimple, and* pPa_n *is just* TL_{2n}. *The discussion about* Mo_n *is unfinished and deserves more study.*

4.5 Symmetric monoid chains

We still have a fixed field $\mathbb{K}$.

4.5.1 Brauer categories and monoids

We will now recall the definitions of the *Brauer category* $\mathbf{Br}^{lin}(\delta)$, the *Brauer algebra* $\mathrm{Br}_n^{lin}(\delta)$ and explain how to construct set-based versions of these. Brauer categories and algebras are classical topics in representation theory, see e.g. [12] for the original reference. Moreover, the discussion is quite similar to the analogue for Temperley-Lieb monoids, so we will be brief.

The crucial difference between $\mathbf{Br}^{lin}(\delta)$ and $\mathbf{TL}^{lin}(\delta)$ is that the former is additionally a symmetric category. The morphisms are then called *perfect matchings*. Prototypical examples of these perfect matchings are crossingless matchings but also e.g.:

The relations on these diagrams are build such that they are the same if and only if they represent the same perfect matching. Otherwise the definition of $\mathbf{Br}^{lin}(\delta)$ is the same as for $\mathbf{TL}^{lin}(\delta)$.

Perfect matchings can be numbered by $b(k) = (2k-1)!!$. Letting P_m^n denote the set of perfect matching with m bottom and n top boundary points, we have the following:

Lemma 4.5.1. *The set P_m^n is a $\mathbb{K}$-linear basis of $\mathrm{Hom}_{\mathbf{Br}^{lin}(\delta)}(m,n)$. Hence, the dimension of this space is either zero if $m \not\equiv n \bmod 2$, and otherwise given by $\dim_{\mathbb{K}}\mathrm{Hom}_{\mathbf{Br}^{lin}(\delta)}(m,n) = b(\frac{m+n}{2})$.*

Proof. Well-known, see e.g. [19, Lemma 4.4]. □

The Brauer algebra on n-strands is then $\mathrm{Br}_n^{lin}(\delta) = \mathrm{End}_{\mathbf{Br}^{lin}(\delta)}(n)$.

Remark 4.5.2. Similar as $\mathrm{TL}_n^{lin}(\delta)$, the algebra $\mathrm{Br}_n^{lin}(\delta)$ originates in Schur–Weyl–Brauer duality [12]. See e.g. [24, Section 3.4] for a summary of these dualities.

We then get the *set-theoretic Brauer category* **Br** and the *Brauer monoid* on n-strands is defined by $\mathrm{Br}_n = \mathrm{End}_{\mathbf{Br}}(n)$. This monoid has $(2n-1)!!$ elements.

Lemma 4.5.3. *Sending the natural $\mathbb{K}$-linear basis of TL_n to crossingless matchings in P_m^n from Lemma 4.5.1 defines an embedding of monoids $\mathrm{TL}_n \hookrightarrow \mathrm{Br}_n$.*

Proof. Clear by the respective lemmas. □

Note that the symmetric group S_n on n-strands is isomorphic to the group of units G of Br_n. An isomorphism is given by the map

$$\mathrm{S}_n \hookrightarrow \mathrm{Br}_n, \quad (i, i+1) \mapsto \times,$$

where the crossing crosses the ith and the $(i+1)$th strand when read from left to right. We will use this to identify S_n with the respective subgroup of Br_n and with the corresponding set of morphisms in **Br**.

The analog of Definition 3.4.11 now is:

Lemma 4.5.4. *For $a \in \mathrm{Hom}_{\mathbf{Br}}(m,n)$ there is unique factorization of the form $a = \gamma \circ \sigma_k \circ \beta$ for minimal k, and $\beta \in \mathrm{Hom}_{\mathbf{Br}}(m,k)$, $\sigma_k \in \mathrm{S}_n$ and $\gamma \in \mathrm{Hom}_{\mathbf{Br}}(k,n)$.*

Proof. Very similar to the argument provided surrounding Definition 3.4.11. The picture now is

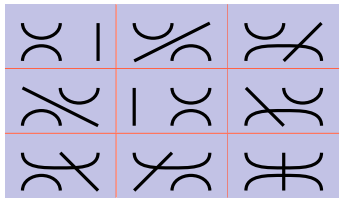
$a =$  .

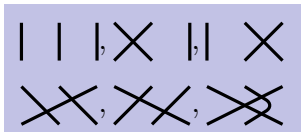
which one easily generalizes to prove the lemma. (Note that one can always push crossing in the middle unless they have to cross a cap or cup.) □

We apply the same terminology as for Br_n regarding through strands, bottom half and top half. As before for TL_n, this notion will give us the cell structure of Br_n.

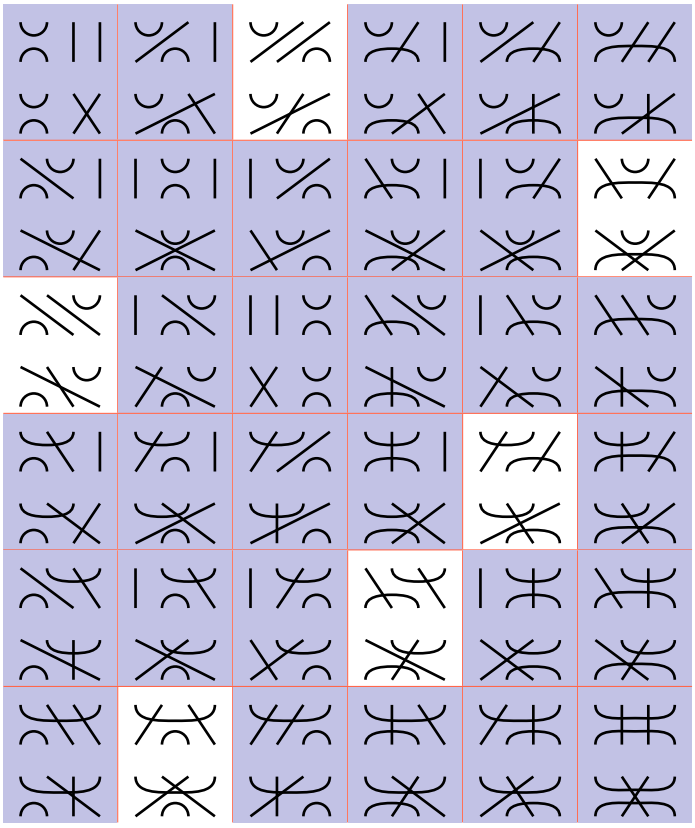
4.5.2 Cells of the Brauer monoid

The picture for the cell structure of Br_n is now:

$\mathcal{J}_1$  $\mathcal{H}(e) \cong \mathrm{S}_1$

$\mathcal{J}_3$  $\mathcal{H}(e) \cong \mathrm{S}_3$.

These are the cells of Br_3. Here is another example, where $\mathcal{H}(e) \cong \mathrm{S}_2$:

$\mathcal{J}_2$  $\mathcal{H}(e) \cong \mathrm{S}_2$.

This illustrated the cell $\mathcal{J}_2$ in Br_4.

Formally and with contrast to Proposition 4.3.2, we have now nontrivial H-cells:

Proposition 4.5.5. *We have the following.*

(a) *The left and right cells of* Br_n *are given by perfect matchings where one fixes the bottom respectively top half of the diagram. The* $\leq_l$*- and the* $\leq_r$*-order increases as the number of through strands decreases. Within* $\mathcal{J}_k$ *we have*

$$|\mathcal{L}| = |\mathcal{R}| = k! \binom{n}{k} (n-k-1)!!.$$

Here $(n-k-1)!!$ *denotes the double factorial.*

(b) *The J-cells* $\mathcal{J}_k$ *of* Br_n *are given by perfect matchings with a fixed number of through strands* k*. The* $\leq_{lr}$*-order is a total order and increases as the number of through*

strands decreases. For any $\mathcal{L} \subset \mathcal{J}$ we have

$$|\mathcal{J}_k| = \tfrac{1}{k!}|\mathcal{L}|^2.$$

(c) *Each J-cell of Br_n is idempotent, and $\mathcal{H}(e) \cong \mathrm{S}_k$ for all idempotent H-cells in $\mathcal{J}_k$. Within $\mathcal{J}_k$ have*

$$|\mathcal{H}| = k!.$$

Proof. All of these are known statements. However, the cells of Br_n do not correspond to the cells coming from the cellular structure of $\mathrm{Br}_n^{lin}(\delta)$, but rather from the sandwich cellular structure, cf. [16] or [57, Section 2D]. □

Let $L_{\mathrm{S}_n}/\cong$ denote the set of simple S_n-representations. For $\mathrm{char}(\mathbb{K}) = 0$ it is well-known that $L_{\mathrm{S}_n}/\cong$ can be identified with partitions of n. For $\mathrm{char}(\mathbb{K}) > 0$ there is a slightly more involved statement of the same kind, see e.g. [36, Section 3.4] for an even more general statement.

Proposition 4.5.6. *The set of apexes for simple Br_n-representations can be indexed 1:1 by the poset $\Lambda = (\{n, n-2, ...\}, >)$, and*

$$\{\textit{simple } \mathrm{Br}_n\textit{-representations of apex } k\}/\cong \overset{1:1}{\longleftrightarrow} L_{\mathrm{S}_k}/\cong .$$

Proof. As before by using Proposition 4.2.18 and the cell structure in Proposition 4.5.5. □

By Proposition 4.5.6, we use the same number scheme and poset as for the Temperley–Lieb but also keeping track of $L_K \in L_{\mathrm{S}_k}/\cong$.

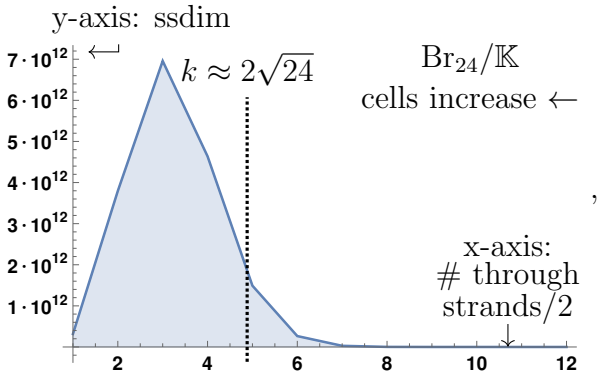
Lemma 4.5.7. *Within one J-cell all left cell modules $\Delta_{\mathcal{L}}$ and all right cell modules ${}_{\mathcal{R}}\Delta$ are isomorphic. We write Δ_k respectively ${}_k\Delta$ for those in $\mathcal{J}_k$.*
We have $\Delta_k \cong {}_k\Delta$ as $\mathbb{K}$-vector spaces and $\dim_{\mathbb{K}}(\Delta_k) = \dim_{\mathbb{K}}({}_k\Delta) = \binom{n}{k}(n-k-1)!!$.

Proof. Using Proposition 4.5.5, the proof is similar to the Temperley–Lieb case. □

Proposition 4.5.8. *Let K a simple S_k-representation, and let L_K denote its associated simple Br_n-representation of apex $\mathcal{J}_k$. The semisimple dimensions are* $\mathrm{ssdim}_{\mathbb{K}}(L_K) \geq \binom{n}{k}(n-k-1)!!$.

Proof. As for the Temperley–Lieb case with the extra observation that a smallest semisimple dimension is associated to the trivial S_k-representation. □

Example 4.5.9. The lower bound for the semisimple dimensions of Br_{24} can be illustrated by



$\log_{10}(\mathrm{ssdim})$: $(11.5, 12.5792, 12.8424, 12.6663, 12.1734, 11.4233, 10.4489, 9.26797, 7.88775, 6.30512, 4.50349, 2.44091, 0)$.

For readability, we took the base 10 log of the actual numbers. This picture again motivates truncation, and we will do this in Section 4.5.3 below.

Let us discuss the dimensions of simple Br_n-representations. To the best of our knowledge, the dimensions of simple Br_n-representations are not known. The best we get is:

Proposition 4.5.10. *Let $L_k^{\mathrm{TL}_n}$ denote the kth simple TL_n-representation, cf. Section 4.3.1. Let K be a simple S_k-representation and let L_K denote its associated simple Br_n-representation of apex $\mathcal{J}_k$. We have* $\dim_{\mathbb{K}}(L_K) \geq \dim_{\mathbb{K}}(L_k^{\mathrm{TL}_n})$.

Proof. The Temperley–Lieb monoid TL_n embeds into Br_n by the evident map that diagrammatically is as the one in Equation 4.4.0.2. See also Lemma 4.5.3. The proof is

thus essentially the same as for Mo_n, see Proposition 4.4.7. The difference is that we can not use Theorem 4.2.4 directly, but we instead need to argue slightly differently: First, we use the Brauer algebra $\mathrm{Br}_n^{lin}(1)$ for circle parameter 1. The monoid algebra of Br_n is $\mathrm{Br}_n^{lin}(1)$, hence, finding dimension bounds for Br_n or $\mathrm{Br}_n^{lin}(1)$ is the same problem. Working with $\mathrm{Br}_n^{lin}(1)$ has the advantage that we can use the cellular structure to split the J-cells $\mathcal{J}_k$ further until H-cells are of size one, see [19, Section 4]. This can be achieved by using e.g. the Kazhdan–Lusztig bases of the S_k. The sign representation of S_k in its cell structure correspond to the bottom cell where there are only through strands. This cell for $\mathrm{Br}_n^{lin}(1)$ has then $\mathrm{TL}_n^{lin}(1)$ inside and the pairing argument applies. All other simple $\mathrm{Br}_n^{lin}(1)$-representations associated to $\mathcal{J}_k$ have bigger dimensions, so the proof completes. □

4.5.3 Truncating the Brauer monoid

We continue with truncation, which is almost identical as for the Temperley–Lieb monoid in Section 4.3.2.

Lemma 4.5.11. *The monoid* Br_n *is admissible.*

Proof. The same arguments as in Lemma 4.5.11 work. □

Definition 4.5.12. Define the *kth truncated Brauer monoid* by

$$\mathrm{Br}_n^{\leq k} = (\mathrm{Br}_n)_{\geq \mathcal{J}_k}.$$

Again, let us stress that diagrams in $\mathrm{Br}_n^{\leq k}$ have at most k through strands. We are almost ready to state our main results, but before we need to discuss extensions.

4.5.4 Trivial extensions in Brauer monoids

The following is the same as for TL_n.

Lemma 4.5.13. *The monoid* Br_n *is well-rounded if* $n \geq 5$*, and the monoid* $\mathrm{Br}_n^{\leq k}$ *is well-rounded if* $n \geq 5$ *and* $k \leq 3$*.*

Proof. This follows from Lemma 4.5.4 and the respective statement about the Temperley–Lieb monoid in Lemma 4.3.26. To see this note that the left-rounded condition $ba \approx_l a$ implies that within on $\approx_l$ equivalence class we can focus on the part where $\sigma_k = 1$ since for $a = \gamma \circ \sigma_k \circ \beta$ we can chose $b = \gamma \circ \sigma_k^{-1} \circ \beta^*$ and get $\gamma \circ id_k \circ \beta \approx_l \gamma \circ \sigma_k \circ \beta$. The same works for right-rounded and null-rounded. □

We now restrict to a field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) \neq 2$.

Lemma 4.5.14. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$*. We have* $\mathrm{H}^1(\mathrm{S}_n, \mathbb{K}) \cong 0$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

Proof. The cases $n = 0, 1$ are clear, so let $n \geq 2$. Recall from Remark 4.1.15 that $\mathrm{H}^1(\mathrm{S}_n, \mathbb{K}) \cong 0$ is trivial if and only if the only homomorphism $\mathrm{S}_n \to \mathbb{K}$ is trivial. To see that this is the case, note that any such homomorphism must send the transposition $(i, i+1)$ of $\mathrm{S}_n = \mathrm{Aut}(\{1, ..., n\})$ to $k \in \mathbb{K}$ with $2k = 0$, which implies $k = 0$. The claim follows since S_n is generated by transpositions. □

Let X be either Br_n or $\mathrm{Br}_n^{\leq k}$ for $k \geq 3$.

Lemma 4.5.15. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$*. We have* $\mathrm{H}^1(\mathrm{X}, \mathbb{K}) \cong 0$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

Proof. We will use Lemma 4.5.14.

Case $\mathrm{X} = \mathrm{Br}_n$. Similar to the proof of Lemma 4.3.27 with the difference that elements in $\mathcal{J}_b$ are not generated by idempotents, but rather by idempotents and symmetric group generators. Idempotents are send to zero, as for the Temperley–Lieb monoid, and the symmetric group generators are also send to zero. These taken together show the claim.

Case $\mathrm{X} = \mathrm{Br}_n^{\leq k}$. The argument is also similar to the proof of Lemma 4.3.27. In this case diagrams of width k are of the form $a\sigma_k b^*$ where $\sigma_k \in \mathrm{S}_n$. Keeping this in mind as well as $\mathrm{H}^1(\mathrm{S}_k, \mathbb{K}) \cong 0$, the argument given in the proof of Lemma 4.3.27 works mutatis mutandis. □

Proposition 4.5.16. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$. *Let* M *be an* X*-representation. Then any short exact sequence*

$$0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$$

splits.

Proof. The proposition follows as for the Temperley–Lieb monoid by the above lemmas. The only difference to Proposition 4.3.28 is that the group of units is $\mathrm{G} \cong \mathrm{S}_n$, but that is taken care of in Lemma 4.5.14. □

4.5.5 Representation gap and faithfulness of the Brauer monoid

The analog of Section 4.3.4 is (the weaker statement):

Theorem 4.5.1. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$. *We have the following lower bounds:*

$$\begin{aligned}
&\mathrm{gap}_{\mathbb{K}}(\mathrm{Br}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}),\\
&\mathrm{ssgap}_{\mathbb{K}}(\mathrm{Br}_n^{\leq k}) \geq \begin{cases} \mathrm{ssgap}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}) & \text{always,} \\ (n-1)!! \in \Theta(n^{n/2}e^{n/2}) & \text{if } n \gg 0, 0 \leq k \leq 2\sqrt{n}, \end{cases}\\
&\mathrm{faith}_{\mathbb{K}}(\mathrm{Br}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{K}}(\mathrm{TL}_n^{\leq k}).
\end{aligned}$$

Note that the lower bound $(n-1)!!$ is bigger than the one using TL_n from Theorem 4.3.2.

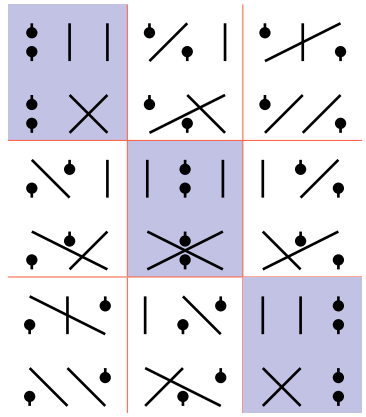
Proof. Since TL_n embeds into Br_n (see the proof of Proposition 4.5.10 or Lemma 4.5.3), Proposition 4.5.16 and using the arguments from the proof of Proposition 4.5.10, most of this theorem follows from the ones for TL_n or $\mathrm{TL}_n^{\leq k}$. The exception is the lower bound given by $(n-1)!!$. To see that this lower bound holds under the given assumptions, we observe that $\binom{n}{k}(n-k-1)!!$ has its minimum at either $k = 0$ or $k = \lfloor 2\sqrt{n} \rfloor$. Evaluating at these values for $n \gg 0$ (as there are some fluctuations for small n) shows that the lower bound is achieved at $k = 0$. □

4.5.6 Other symmetric monoids

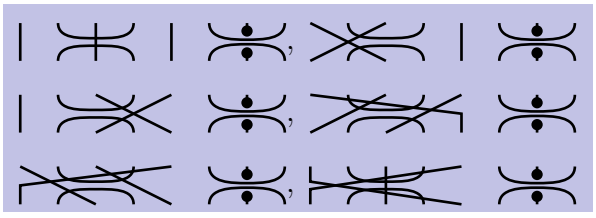
We now discuss the remaining symmetric monoids from Equation 4.0.0.1 in ascending order (of complexity). We will be brief since almost everything follows mutatis mutandis as before. The basics can be found e.g. in [22].

Remark 4.5.17. Symmetric monoids have the symmetric groups as H-cells, as we will explain below.

The *symmetric group* was discussed in Example 4.1.13, so let us start with the *rook monoid* Ro_n. The rook monoid is the nonplanar version of pRo_n and has $\sum_{k=0}^{n} k!\binom{n}{k}$ elements. Its J-cells are again given by through strands. A typical cell is $\mathcal{J}_2$ for Ro_3:

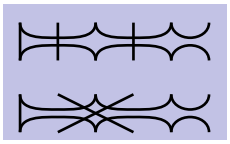
$\mathcal{J}_2$  $\mathcal{H}(e) \cong \mathrm{S}_2$.

The *rook-Brauer monoid* RoBr_n is a symmetric version of the Motzkin monoid. The rook-Brauer monoid has $\sum_{k=0}^{n}(2k)!!\binom{2n}{2k}$ elements. The J-cells are, as usual, indexed by through strands. They get huge very fast, so let us just illustrate a typing idempotent (and symmetric) H-cell:

Part of $\mathcal{J}_3$  $\mathcal{H}(e) \cong \mathrm{S}_3$.

The *partition monoid* Pa_n contains all the other planar and symmetric monoids as

submonoid. It has $Be(2n)$ elements, where Be denotes the Bell number. The J-cells are still given by through strands. As for RoBr_n, the sizes of the cells are very large, so we only illustrate an idempotent (and symmetric) H-cell:

Part of $\mathcal{J}_2$  $\mathcal{H}(e) \cong \mathrm{S}_2$.

Below, if not stated otherwise, let X be either Ro_n, RoBr_n or Pa_n.

Proposition 4.5.18. *We have the following.*

(a) *The left and right cells of* X *are given by the respective type of diagrams where one fixes the bottom respectively top half of the diagram. The $\leq_l$- and the $\leq_r$-order increases as the number of through strands decreases. Within $\mathcal{J}_k$ we have*

$$\mathrm{Ro}_n\colon |\mathcal{L}| = |\mathcal{R}| = k!\binom{n}{k},$$
$$\mathrm{RoBr}_n\colon |\mathcal{L}| = |\mathcal{R}| = k!\sum_{t=0}^{n}\binom{n}{k}\binom{n-k}{2t}(2t-1)!!,$$
$$\mathrm{Pa}_n\colon |\mathcal{L}| = |\mathcal{R}| = k!\sum_{t=0}^{n}\left\{ {n \atop t} \right\}\binom{t}{k}.$$

Here $\left\{ {n \atop t} \right\}$ denotes the Stirling number of the second kind.

(b) *The J-cells $\mathcal{J}_k$ of* X *are given by the respective type of diagrams with a fixed number of through strands k. The $\leq_{lr}$-order is a total order and increases as the number of through strands decreases. For any $\mathcal{L} \subset \mathcal{J}$ we have*

$$\mathrm{X}\colon |\mathcal{J}_k| = \tfrac{1}{k!}|\mathcal{L}|^2.$$

(c) *Each J-cell of* X *is idempotent, and $\mathcal{H}(e) \cong \mathrm{S}_k$ for all idempotent H-cells in $\mathcal{J}_k$.*

Within $\mathcal{J}_k$ have

$$\mathrm{X}\colon |\mathcal{H}| = k!.$$

Proof. Easy and omitted, see also [22, Section 3.3]. □

Proposition 4.5.19. *The set of apexes for simple* X*-representations can be indexed* 1:1 *by the poset* $\Lambda = (\{n, n-1, ...\}, >)$*, and*

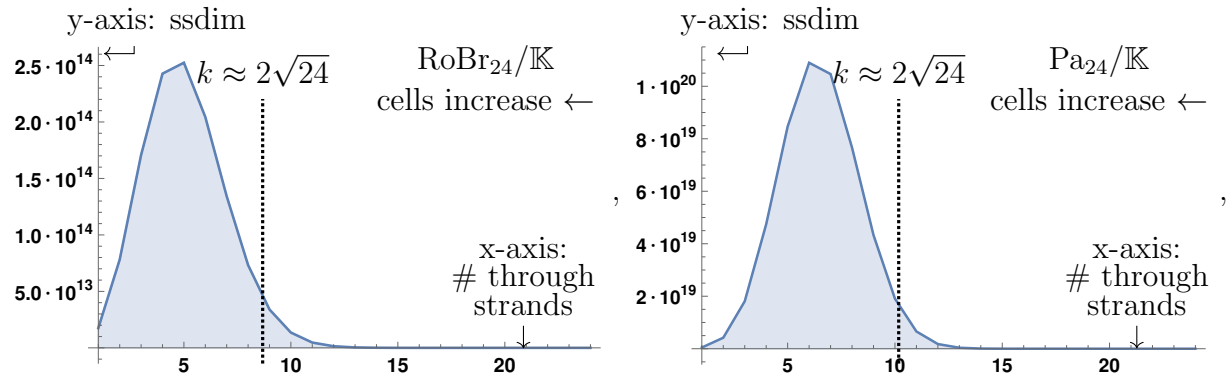
$$\{\textit{simple X-representations of apex } k\}/\cong \overset{1:1}{\longleftrightarrow} L_{\mathrm{S}_k}/\cong \ .$$

Proof. By Proposition 4.5.18. □

Proposition 4.5.20. *Let K a simple S_k-representation, and let L_K denote its associated simple* X*-representation of apex $\mathcal{J}_k$. The semisimple dimensions are* $\mathrm{ssdim}_{\mathbb{K}}(L_K) \geq \binom{n}{k}$, $\mathrm{ssdim}_{\mathbb{K}}(L_K) \geq \sum_{t=0}^{n} \binom{n}{k}\binom{n-k}{2t}(2t-1)!!$ *respectively* $\mathrm{ssdim}_{\mathbb{K}}(L_K) \geq \sum_{t=0}^{n} \left\{ {n \atop t} \right\}\binom{t}{k}$.

Proof. This follows verbatim as Proposition 4.5.8. □

Example 4.5.21. As before, let us illustrate the lower bound for the semisimple dimensions:



$$\text{RoBr } \log_{10}(\text{ssdim})\colon \left(\begin{matrix} 13.2428, 13.8931, 14.2325, 14.3852, 14.4022, 14.3105, 14.1279, 13.8651, 13.5313, 13.1314, 12.671, 12.152, \\ 11.5786, 10.9499, 10.2701, 9.53474, 8.74966, 7.90469, 7.00985, 6.0434, 5.02637, 3.90827, 2.74194, 1.38021, 0 \end{matrix}\right),$$

$$\text{Pa } \log_{10}(\text{ssdim})\colon \left(\begin{matrix} 17.6493, 18.6225, 19.2572, 19.6761, 19.9277, 20.0373, 20.0198, 19.8843, 19.6367, 19.2804, 18.8176, 18.2495, \\ 17.5764, 16.7982, 15.9143, 14.9234, 13.8234, 12.6115, 11.2832, 9.83189, 8.24761, 6.51485, 4.60773, 2.47712, 0 \end{matrix}\right),$$

where we again took the base 10 log. We have not illustrated the situation for Ro_n as it is the same as for pRo_n with semisimple dimensions given by binomial coefficients, cf. Equation 4.2.6.1.

Let Y denote either pRo_n, Mo_n and pPa_n associated to their respective X.

Lemma 4.5.22. *The monoid* X *contains* Y *as a submonoid, by the analog of Equation 4.4.0.2.*

Proof. Clear, see also Lemma 4.5.3. □

Proposition 4.5.23. *Let* L_k^{Y} *denote the* k*th simple* Y*-representation. Let* K *denote a simple* S_k*-representation and let* L_K *denote its associated simple* X*-representation of apex* $\mathcal{J}_k$*. We have* $\dim_{\mathbb{K}}(L_K^{\mathrm{X}}) \geq \dim_{\mathbb{K}}(L_k^{\mathrm{Y}})$.

Proof. This follows again by observing that the planar version embed into their nonplanar counterparts, see Lemma 4.5.22. □

Proposition 4.5.24. *Let* $\mathrm{char}(\mathbb{K}) \nmid n!$*, including* $\mathrm{char}(\mathbb{K}) = 0$*. We have* $\dim_{\mathbb{K}}(L_k) = \mathrm{ssdim}_{\mathbb{K}}(L_k) = \binom{n}{k}$ *for* Ro_n*, and* Ro_n *is semisimple.*

Proof. The argument is the same as in Proposition 4.4.6 with the additional caveat of the symmetric groups S_k for $0 \leq k \leq n$ appearing as idempotent H-cells which forces the condition $\mathrm{char}(\mathbb{K}) \nmid n!$. □

Lemma 4.5.25. *The monoid* X *is admissible.*

Proof. Omitted. □

Definition 4.5.26. Define the *k-l truncated rook monoid* for $k \leq l$ and the *kth truncated rook-Brauer monoid* respectively *k truncated partition monoid* by

$$\mathrm{Ro}_n^{\leq k,<l} = (\mathrm{Ro}_n)_{\geq \mathcal{J}_k}/(> \mathcal{J}_l), \quad \mathrm{RoBr}_n^{\leq k} = (\mathrm{RoBr}_n)_{\geq \mathcal{J}_k}, \quad \mathrm{Pa}_n^{\leq k} = (\mathrm{Pa}_n)_{\geq \mathcal{J}_k}.$$

Let X be either of the above monoids or their truncations. For the following theorem, note that the *kth truncated planar partition monoid* $\mathrm{pPa}_n^{\leq k}$ can be defined in the evident way.

Theorem 4.5.2. *Let* $\mathrm{char}(\mathbb{K}) \nmid n!$*, including* $\mathrm{char}(\mathbb{K}) = 0$*, and let* $\mathbb{L}$ *be an arbitrary field. We have the following lower bounds:*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{Ro}_n^{\leq k,<l}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{pRo}_n^{\leq k,<l})$$

$$\mathrm{ssgap}_{\mathbb{L}}(\mathrm{Ro}_n^{\leq k,<l}) = \mathrm{ssgap}_{\mathbb{L}}(\mathrm{pRo}_n^{\leq k,<l}), \quad \mathrm{faith}_{\mathbb{L}}(\mathrm{Ro}_n^{\leq k,<l}) \geq \mathrm{faith}_{\mathbb{L}}(\mathrm{pRo}_n^{\leq k,<l}),$$

$$\mathrm{ssgap}_{\mathbb{L}}(\mathrm{RoBr}_n^{\leq k}) \geq \begin{cases} \mathrm{ssgap}_{\mathbb{L}}(\mathrm{Mo}_n^{\leq k}) & \textit{always,} \\ \sum_{t=0}^{n} \binom{n}{2t}(2t-1)!! & \textit{if } n \gg 0, 0 \leq k \leq 2\sqrt{n}, \end{cases},$$

$$\mathrm{faith}_{\mathbb{L}}(\mathrm{RoBr}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{L}}(\mathrm{Mo}_n^{\leq k})$$

$$\mathrm{ssgap}_{\mathbb{L}}(\mathrm{Pa}_n^{\leq k}) \geq \begin{cases} \mathrm{ssgap}_{\mathbb{L}}(\mathrm{pPa}_n^{\leq k}) & \textit{always,} \\ \sum_{t=0}^{n} \left\{ {n \atop t} \right\} & \textit{if } n \gg 0, 0 \leq k \leq 2\sqrt{n}, \end{cases},$$

$$\mathrm{faith}_{\mathbb{L}}(\mathrm{Pa}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{L}}(\mathrm{pPa}_n^{\leq k}).$$

Note that the above lower bounds in the cases $n \gg 0, 0 \leq k \leq 2\sqrt{n}$ are bigger than the ones coming from the embeddings. We also expect that

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{RoBr}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{Mo}_n^{\leq k}), \quad \mathrm{gap}_{\mathbb{K}}(\mathrm{Pa}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{pPa}_n^{\leq k}),$$

but we were not able to prove this since there might be extensions.

Proof. All lower bounds except the first follow directly by using the embedding in Lemma 4.5.22. The first uses additionally Proposition 4.5.24 which also holds for the truncation. The equality $\mathrm{ssgap}_{\mathbb{K}}(\mathrm{Ro}_n^{\leq k,<l}) = \mathrm{ssgap}_{\mathbb{K}}(\mathrm{pRo}_n^{\leq k,<l})$ is clear by Proposition 4.5.18. For the semisimple gaps of RoBr_n and $\mathrm{Pa}_n^{\leq k}$ one can use the same arguments as in Theorem 4.5.1. □

Conclusion 4.5.27. *As with the planar monoids, all of the symmetric monoids* Ro_n*,* Br_n*,*

RoBr_n *and* Pa_n *appear to have big nontrivial representations. However, it is not clear why they should be preferable over their planar counterparts since they are, roughly speaking, their planar version inflated by the symmetric group* S_k*. In fact most of our arguments above use the planar versions to derive bounds.*

Bibliography

[1] V. Shpilrain A. Myasnikov and A. Ushakov. *Non-commutative cryptography and complexity of group-theoretic problems*, volume 177 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2011.

[2] Ayush Agarwal and Christian Gaetz. Differential posets and restriction in critical groups. *Algebraic Combinatorics*, 2(6):1311–1327, 2019.

[3] Vladimir Shpilrain Alexei Myasnikov and Alexander Ushakov. *A practical attack on a braid group based cryptographic protocol*, volume 3621 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2005.

[4] Henning Haahr Andersen. Simple modules for Temperley–Lieb algebras and related algebras. *J. Algebra*, 520:276–308, 2019.

[5] Krishnan Balasubramanian. Generators of the character tables of generalized wreath product groups. *Theoretica chimica acta*, 78(1):31–43, 1990.

[6] Daniel Barter, Inna Entova-Aizenbud, and Thorsten Heidersdorf. Deligne categories and representations of the infinite symmetric group. *To appear in Advances in Mathematics*, 2019.

[7] Jonathan Belletete, David Ridout, and Yvan Saint-Aubin. Restriction and induction of indecomposable modules over the Temperley-Lieb algebras. *Journal of Physics A: Mathematical and Theoretical*, 51(4), 2017.

[8] David J. Benson. *Representations and cohomology. I.* Basic representation theory of finite groups and associative algebras. volume 30 of Cambridge University Press, Cambridge, second edition, 1998.

[9] Nantel Bergeron, Thomas Lam, and Huilan Li. Combinatorial Hopf algebras and towers of algebras - dimension, quantization and functorality. *Algebras and Representation Theory*, 15(4):675–696, 2012.

[10] Nantel Bergeron and Huilan Li. Algebraic structures on Grothendieck groups of a tower of algebras. *Journal of Algebra*, 321:2068–2084, 2009.

[11] Stephen J. Bigelow. Braid groups are linear. *J. Amer. Math. Soc*, 14(2):471–486, 2001.

[12] Richard Brauer. On algebras which are connected with the semisimple continuous groups. *Ann. of Math. (2)*, 38(4):857–872, 1937.

[13] Thomas Church, Jordan S. Ellenberg, and Benson Farb. FI-modules and stability for representations of symmetric groups. *Duke Math. J.*, 164(9):1833–1910, 2015.

[14] Michael Ehrig and Daniel Tubbenhauer. Relative cellular algebras. *Transform. Groups*, 26(1):229–277, 2021.

[15] Steve Ferry and Andrew Ranicki. A survey of Wall's finiteness obstruction. *"Surveys on Surgery Theory", Annals of Mathematics Studies*, 2(149):63–80, 2001.

[16] Simon Fishel and Ian Grojnowski. Canonical bases for the Brauer centralizer algebra. *Math. Res. Lett.*, 2(1):15–26, 1995.

[17] Sergey Fomin. Duality of graded graphs. *Journal of Algebraic Combinatorics*, 3:357–404, 1994.

[18] Christian Gaetz. Dual graded graphs and Bratteli diagrams of towers of groups. *Electronic Journal of Combinatorics*, 26(1):25, 2019.

[19] J.J. Graham and G.I. Lehrer. Cellular algebras. *Invent. Math.*, 123(1):1–34, 1996.

[20] J.A. Green. On the structure of semigroups. *Ann. of Math. (2)*, 54:163–172, 1951.

[21] Nicolas Guay and Stewart Wilcox. Almost cellular algebras. *J. Pure Appl. Algebra*, 219(9):4105–4116, 2015.

[22] Tom Halverson and Theodore Jacobson. Set-partition tableaux and representations of diagram algebras. *Algebr. Comb.*, 3(2):509–538, 2020.

[23] Tom Halverson and Arun Ram. Partition algebras. *European J. Combin.*, 26(6):869–921, 2005.

[24] Catharina Stroppel Henning Haahr Andersen and Daniel Tubbenhauer. Semisimplicity of Hecke and (walled) Brauer algebras. *J. Aust. Math. Soc*, 103(1):1–44, 2017.

[25] M. Anshel I. Anshel and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6(3-4):287–291, 1999.

[26] James Lepowsky Igor Frenkel and Arne Meurman. Vertex operator algebras and the Monster, volume 134 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA, 1988.

[27] Christoph Jansen. The minimal degrees of faithful representations of the sporadic simple groups and their covering groups. *LMS J. Comput. Math.*, 8:122–144, 2005.

[28] S.P. Norton R.A. Parker J.H. Conway, R.T. Curtis and R.A. Wilson. $\mathbb{ATLAS}$ *of finite groups*. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J.G. Thackray. Oxford University Press, Eynsham, 1985.

[29] J.H. Cheon J.W. Han J. Kang K.H. Ko, S.J. Lee and C. Park. *New public-key cryptosystem using braid groups*, volume 1880 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 2000.

[30] Mikhail Khovanov and Radmila Sazdanovic. Categorifications of the polynomial ring. *Fund. Math.*, 230(3):251–280, 2015.

[31] Mikhail Khovanov and Radmila Sazdanovic. Diagrammatic categorification of the Chebyshev polynomials of the second kind. *J. Pure Appl. Algebra*, 225(6), 2021.

[32] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998.

[33] Daan Krammer. Braid groups are linear. *Ann. of Math. (2)*, 155(1):131–156, 2002.

[34] Xiaoyu Liu and Krishnan Balasubramanian. Computer generation of character tables of generalized wreath product groups. *Journal of Computational Chemistry*, 1(5):589–602, 1990.

[35] Paul Wedrich Louise Sutton, Daniel Tubbenhauer and Jieru Zhu. SL2 tilting modules in the mixed case. *preprint*, 2021.

[36] Andrew Mathas. Iwahori-Hecke algebras and Schur algebras of the symmetric group, volume 15 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1999.

[37] Sandro Mattarei. On character tables of wreath products. *Journal of Algebra*, 175(1):157–178, 1995.

[38] Representation Gap Monoidal Categories and Cryptography. Mikhail Khovanov, Maithreya Sitaraman, and Daniel Tubbenhauer. *preprint*, 2022.

[39] Stephen T. Moore. On the representation theory of the infinite Temperley-Lieb algebra. *To appear in Journal of Algebra and Its Applications*, August 2020.

[40] Alexei Myasnikov and Vitaly Roman'kov. A linear decomposition attack. *Groups Complex. Cryptol.*, 7(1):81–94, 2015.

[41] Volodymyr Mazorchuk Olexandr Ganyushkin and Benjamin Steinberg. On the irreducible representations of a finite semigroup. *Proc. Amer. Math. Soc.*, 137(11):3585–3592, 2009.

[42] Sun Woo Park and Maithreya Sitaraman. Polynomial relations between operators on chains of representation rings. *Communications in Algebra*, 0(0):1–28, 2022.

[43] Peter Patzt. Representation stability for diagram algebras. *preprint*, 2020.

[44] David Ridout and Yvan Saint-Aubin. Standard modules, induction and the Temperley-Lieb algebra. *Adv. Theor. Math. Phys.*, 18:957–1041, 2014.

[45] Daniele Rosso and Alistair Savage. A general approach to Heisenberg categorification via wreath product algebras. *Mathematische Zeitschrift*, 286(1-2):603–655, 2017.

[46] Steven V. Sam and Andrew Snowden. Stability patterns in representation theory. *Forum of Mathematics, Sigma*, 3(11), 2015.

[47] Alistair Savage. Affine wreath product algebras. *International Mathematics Research Notices*, 00(0):1–65, 2018.

[48] V. Shpilrain and G. Zapata. Combinatorial group theory and public key cryptography. *Appl. Algebra Engrg. Comm. Comput.*, 17(3-4):291–302, 2006.

[49] Maithreya Sitaraman. Topological actions of temperley-lieb monoids and representation stability. *preprint*, 2021.

[50] Robert A. Spencer. The modular Temperley–Lieb algebra. *preprint*, 2020.

[51] Robert A. Spencer. Modular valenced Temperley–Lieb algebras. *preprint*, 2021.

[52] Richard Stanley. Differential posets. *Journal of the American Mathematical Society*, 1(4):919–961, 1988.

[53] Itamar Stein. The Littlewood-Richardson rule for wreath products with symmetric groups and the quiver of the category $F \wr FI_n$. *Communications in Algebra*, 45(5):2105–2126, 2016.

[54] Benjamin Steinberg. On the Burnside–Brauer–Steinberg theorem. *preprint*, 2014.

[55] Benjamin Steinberg. *Representation theory of finite monoids*. Universitext. Springer, Cham, 2016.

[56] Peter Walsh Steve Linton, Richard Parker and Robert Wilson. Computer construction of the Monster. *J. Group Theory*, 1(4):307–337, 1998.

[57] Daniel Tubbenhauer and Pedro Vaz. Handlebody diagram algebras. *preprint*, 2021.

[58] N.R. Wagner and M.R. Magyarik. A public-key cryptosystem based on the word problem. In *Advances in cryptology (Santa Barbara, Calif., 1984)*, Lecture Notes in Comput. Sci., pages 19–36, Springer, Berlin, 1985.

[59] C. T. C. Wall. Finiteness conditions for cw-complexes finiteness conditions for cw-complexes finiteness conditions for CW-complexes. *Annals of Mathematics*, Second Series, Vol. 81(1):56–69, 1965.

[60] Jennifer C.H. Wilson. An introduction to FI–modules and their generalizations. Michigan Representation Stability Week 2018.

[61] Andrey Zelevinsky. *Representations of finite classical groups: a Hopf algebra approach*. Number 869 in Lecture Notes in Mathematics book series. Springer Verlag, 1981.