TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 11, Pages 329–395 (January 31, 2024)
https://doi.org/10.1090/btran/151

MONOIDAL CATEGORIES, REPRESENTATION GAP AND CRYPTOGRAPHY

MIKHAIL KHOVANOV, MAITHREYA SITARAMAN, AND DANIEL TUBBENHAUER

Abstract. The linear decomposition attack provides a serious obstacle to direct applications of noncommutative groups and monoids (or semigroups) in cryptography. To overcome this issue we propose to look at monoids with only big representations, in the sense made precise in the paper, and undertake a systematic study of such monoids. One of our main tools is Green's theory of cells (Green's relations).

A large supply of monoids is delivered by monoidal categories. We consider simple examples of monoidal categories of diagrammatic origin, including the Temperley–Lieb, the Brauer and partition categories, and discuss lower bounds for their representations.

Contents

1. Introduction 329
2. Representation gaps and faithfulness 336
3. Cell theory 348
4. Planar monoids 360
5. Symmetric monoids 380
Acknowledgments 390
References 390

1. Introduction

The main goal of this paper is to start connecting monoidal categories and cryptography.

1A. Protocols and platform groups.

1A. Protocols and platform groups. Some of the most important cryptographic protocols in use today are based on *commutative groups* and deliver a gold standard for cryptography (modulo the fear of quantum computers). On the other hand, *noncommutative group-based* and *monoid-based* (or *semigroup-based*, but we will stay with monoids in this paper) protocols seem to be less understood and in many cases admit efficient attacks.

Exceptionally successful Diffie–Hellman (DH), Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography algorithms, see e.g. [Ko98], [Wa08], are based on

Received by the editors January 8, 2022, and, in revised form, November 13, 2022, January 12, 2023, and January 23, 2023.

2020 *Mathematics Subject Classification.* Primary 18M05, 20M30; Secondary 94A60.

Key words and phrases. Monoidal categories, diagram categories, monoid/semigroup representations, representation gap, cryptography.

The first author was partially supported by NSF grant DMS-1807425 and the third author was supported by the Australian Research Council while working on the paper.

the commutative group $(\mathbb{Z}/n\mathbb{Z})^*$ of invertible residues modulo n and on the group of points on an elliptic curve E over a finite field $\mathbb{F}_q$, respectively. Here one usually wants these groups to contain a subgroup of large prime order and small index. For example, in the classical DH protocol the prime p as well as a generator $g \in (\mathbb{Z}/p\mathbb{Z})^*$ of the multiplicative group are public. Then party A chooses privately $a \in \mathbb{Z}$ and party B chooses privately $b \in \mathbb{Z}$. Party A communicates g^a, B sends g^b and the common secret is $(g^b)^a = g^{ab} = (g^a)^b$. A third party C has access to n, g, g^a and g^b, but finding g^{ab} from the known data is difficult as long as $p-1$ contains a large prime among its factors.

There has been many ideas and there is an extensive literature on constructing cryptographic protocols from noncommutative groups and monoids (monoids generalize groups and we switch to saying monoids from now on), see e.g. [MSU08], [MSU11] and references therein. Examples of such are Magyarik–Wagner public key protocol [WM85], Anshel–Anshel–Goldfeld key exchange [AAG99], Ko–Lee et al. key exchange protocol [KLC$^+$00] and Shpilrain–Zapata public key protocols [SZ06].

In the literature the monoid $\mathcal{S}$ used in protocols is often called the platform group/monoid. In [MR15, Section 4] there is a big list of various protocols and platform monoids, including but not limited to the ones named above. Sometimes these restrict to groups or matrix groups, sometimes general monoids can be used. A prototypical example for this paper is the Shpilrain–Ushakov (SU) key exchange protocol, see e.g. [MSU08, Section 4.2.1], which works as follows. The public data is a monoid $\mathcal{S}$, and two sets $A, B \subset \mathcal{S}$ of commuting elements and $g \in \mathcal{S}$. Party A chooses privately $a, a' \in A$ and party B chooses privately $b, b' \in A$. Party A communicates aga', B sends bgb' and the common secret is $abgb'a' = baga'b'$. Another example that does not use commuting elements is Stickel's secret key exchange (St) [St05]. Here $g, h \in \mathcal{S}$ with $gh \neq hg$ are public, party A picks $a, a' \in \mathbb{Z}_{\geq 0}$, party B picks $a, a' \in \mathbb{Z}_{\geq 0}$, A sends $g^a h^{a'}$, B sends $g^b h^{b'}$, and the common secret is $g^a g^b h^{b'} h^{a'} = g^b g^a h^{a'} h^{b'}$. Note that $\mathcal{S}$ can be an arbitrary monoid in these protocols. The complexity of $\mathcal{S}$ determines how difficult it is to find the common secret from the public data.

As shown by Myasnikov and Roman'kov [MR15] and also based on earlier work, the SU and St protocols and others in this spirit, the ones named two paragraphs above included, can be successfully attacked if $\mathcal{S}$ 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 $\mathcal{S}_n$ has $n!$ elements, but admits a faithful $(n-1)$-dimensional representation. The dimension of this representation is smaller than logarithmic in the size of the group, and the symmetric group would be a poor choice for various standard noncommutative group protocols. Likewise, finite simple groups of Lie type often admit representations of (exponentially) small dimension compared to their size. With few exceptions, including cyclic groups of prime order, which are related to the classical and well-understood protocols, the same is true for other finite simple groups. That is, these groups admit nontrivial representations of small dimension relative to their order. Since any finite group G surjects onto some finite simple group, reducing the problem of bounding representations of G from below to that of the simple quotient, linear attacks rule out many finite noncommutative groups.

Hence, it is not surprising that some platform groups proposed in the literature are infinite, e.g. Artin–Tits, Thompson or Grigorchuk groups, see [MSU08, Chapter 5].

This paper explores finite monoids (mostly coming from monoidal categories) instead of infinite groups. The questions we address are:

- What are (numerical) measures to determine whether a monoid can resist linear attacks?
- How to find a good supply of finite monoids for cryptographic use?

1B. **Linear attacks, representation gap and faithfulness.** The following observations regarding monoid-based cryptography are our starting points:

(a) As explained above, monoid-based protocols such as SU or St and many others often admit efficient attacks based on linear algebra [MR15].

(b) A natural solution to this problem is to restrict to monoids that have nontrivial representations only starting from a suitably big dimension. We call the smallest dimension of a nontrivial $\mathcal{S}$-representation the *representation gap* of $\mathcal{S}$. Alternatively and weaker, we also ask for the dimension of the smallest faithful $\mathcal{S}$-representation to be big, and we call this measure the *faithfulness* of $\mathcal{S}$. We elaborate on these in Section 2.

Remark 1B.1. Various monoid invariants similar to the representation gap and its companions have appeared in the literature and we give some references in the main body of the paper. However, the motivations to study these invariants in the literature are very different from ours, and it would be very interesting to make a connection to cryptography starting from these works.

It is thus essential to find monoids that have big representation gaps or with faithful representations of big dimension only. Suitably defined, a big representation gap or big faithfulness seems to be necessary, but not sufficient, condition for a monoid to be potentially useful in cryptography, however. Moreover, one problem not discussed here is potential information loss: multiplication by an element of a monoid may not be invertible.

1C. **Monoidal categories and monoids.** A category delivers a supply of monoids: any object X of a category $\mathbf{S}$ gives rise to the monoid $\mathcal{S} = \mathrm{End}_{\mathbf{S}}(X)$ of its endomorphisms. It is further natural to consider *monoidal categories*, where objects can be tensored $\otimes$ subject to suitable axioms, for the following reasons:

(c) It would be preferable to have a family of monoids $\mathcal{S}_n$, say one for each $n \in \mathbb{Z}_{\geq 0}$. This is where monoidal categories enter. A single object X of a monoidal category $\mathbf{S}$ produces a family of monoids $\{\mathcal{S}_n = \mathrm{End}_{\mathbf{S}}(X^{\otimes n}) | n \in \mathbb{Z}_{\geq 0}\}$.

(d) Commuting actions play a key role in cryptography, cf. the SU protocol recalled above. Such commuting actions exist naturally in the setting of categories and monoidal categories. For any pair of objects X, Y of a category $\mathbf{S}$, not necessarily monoidal, there is a commuting action of the monoids $\mathrm{End}_{\mathbf{S}}(X)^{op}$ (the opposite monoid) and $\mathrm{End}_{\mathbf{S}}(Y)$ on the set $\mathrm{Hom}_{\mathbf{S}}(X, Y)$. Thus, categories immediately produce a significant amount of commuting actions. Furthermore, monoidal categories provide an even richer supply of such actions: for any two objects X, Y the actions of the monoids $\mathrm{End}_{\mathbf{S}}(X)$ and $\mathrm{End}_{\mathbf{S}}(Y)$ on $X \otimes Y$ commute. It is easy to convert these to commuting actions on sets, for instance, on the set $\mathrm{Hom}_{\mathbf{S}}(Z, X \otimes Y)$ for $Z \in \mathrm{Ob}(\mathbf{S})$.

(e) Monoidal categories are naturally two-dimensional structures. They often can be described via generating objects, generating morphisms and defining relations. The latter can be understood as relations on planar diagrams or networks, see e.g. [Se11], [TV17]. A natural problem is to construct examples of diagrammatically defined monoidal categories that may be useful for cryptographic purposes. We start tackling this for planar diagrammatics in Section 4 and for diagrammatics involving permutation symmetries in Section 5.

These are our reasons to study (diagram) monoids coming from monoidal categories and we elaborate on their potential usefulness in cryptography in the main body of the text.

There are then three additional facts regarding this project that we stress and that we think makes our discussion interesting:

(f) The current literature on monoidal categories (see for example [EGNO15], [TV17] and references therein) mostly studies $\mathbb{K}$-linear categories or variations of such. This means hom-spaces between the objects are $\mathbb{K}$-vector spaces for some field $\mathbb{K}$. Such categories are not immediately useful from the cryptographic or any classical computation viewpoint, since it usually takes a prohibitive amount of data to record an element of the hom-space between two objects (those hom-spaces tend to have exponentially big dimensions). One the other hand, protocols in $\mathbb{K}$-linear categories with homs between objects having moderate dimensions can be dealt with via linear decomposition attacks, see [MR15].

It makes sense to develop *set-theoretic counterparts* of categories that appear in quantum algebra, quantum topology, mathematical physics, and TQFTs, and see whether related monoids have big representation gaps. We provide easy examples of such in the present paper and discuss their usefulness for cryptography, see parts of Section 4 and Section 5.

(g) It seems hard to build secure cryptographic protocols from noncommutative finite groups, due to finite simple groups having small representation gaps relative to their size. For example, among finite simple groups only the cyclic groups (of prime order) appear to be well-behaved for cryptographical purposes, cf. Example 2C.3 and Example 2E.13.

One of our points is that representation gaps and faithfulness *tend to be bigger for suitable monoids* than for groups when controlling for size. The abstract theory of monoid representations should be useful for some general statements in this direction, see Section 3 for some first steps.

(h) Finally, *lower bounds on dimensions* of representations of monoids or *growth rates* of such dimensions are not yet extensively studied in the literature, even not for group (representation theorists seem to prefer precise numbers).

Part of this project is also to get good bounds and growth rates for simple and faithful $\mathcal{S}$-representations, for finite monoids $\mathcal{S}$, see Theorem 4E.2 for an example.

1D. **Cell theory and cryptography.** Our main tool to study monoid representations are *Green's relations* a.k.a. *Green's theory of cells.* We explain the details in Section 2.

An example of how cell theory enters the paper is that a monoid $\mathcal{S}$ can be truncated by considering a large cell submonoid $\mathcal{S}^{\geq\mathcal{J}}$, see Section 2 for definition. Since simple $\mathcal{S}$-representations are ordered by cells, $\mathcal{S}^{\geq\mathcal{J}}$ will inherit precisely the simple $\mathcal{S}$-representations for large cells. The monoids of the form $\mathcal{S}^{\geq\mathcal{J}}$ sometimes have very few small representations. This truncation works actually in two ways, from above and from below, using Rees factors and cell truncations, and provides a good way to get rid of unwanted representations, cf. Section 3F.

Moreover, in Section 3 we will discuss so-called H-cells, how they control the representation theory of the monoids and how large cells resist against linear attacks.

Another way cells help to determine whether a given monoid could resist linear attacks is that they give rise to what we call the *semisimple representation gap*, which measures the normalized size of the cells. This numerical value is not as fine as the representation gap or the faithfulness, but easier to compute and agrees with the representation gap in the semisimple situation.

The representation gap, the semisimple representation gap and the faithfulness seem to be good first tests for determining whether a given monoid resists linear attacks. Throughout the text we list a few additional properties, partially motivated by cell theory, that may be useful for cryptographical applications.

1E. **Representation gap in some diagrammatic monoids.** Let us take the opportunity to recall some diagrammatic monoids which we will discuss in this paper. All of these will be very familiar to the reader with background in quantum algebra, quantum topology and alike, but they also are prominent examples in monoid theory.

We will be very brief and details and references will follow in the main text. We also indicate whether these monoids might be useful for cryptography in the sense of having substantial (semisimple) representation gaps or only big faithful representations.

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. [HR05] or [HJ20] for summaries):

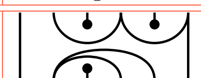
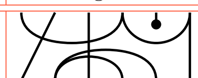
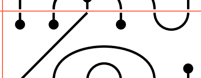
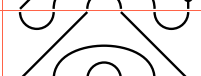
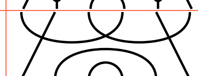
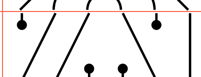
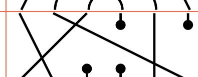
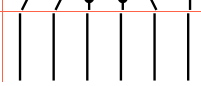
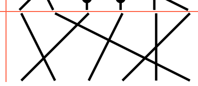
- The *partition monoid* $\mathcal{P}\mathrm{a}_n$ of all diagrams of partitions of a $2n$-element set.
- The *rook-Brauer monoid* $\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n$ consisting of all diagrams with components of sizes $1, 2$.
- The *Brauer monoid* $\mathcal{B}\mathrm{r}_n$ consisting of all diagrams with components of size 2.
- The *rook monoid* $\mathcal{R}\mathrm{o}_n$ consisting of all diagrams with components of sizes $1, 2$, and all partitions have at most one component at the bottom and at most one at the top.
- The *symmetric group* $\mathcal{S}_n$ consisting of all matchings with components of size 1.

- *Planar* versions of these: $\mathrm{p}\mathcal{P}\mathrm{a}_n$, $\mathrm{p}\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n = \mathcal{M}\mathrm{o}_n$, $\mathrm{p}\mathcal{B}\mathrm{r}_n = \mathcal{TL}_n$, $\mathrm{p}\mathcal{R}\mathrm{o}_n$ and $\mathrm{p}\mathcal{S}_n \cong \mathcal{S}_1$ (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.

Remark 1E.1. The above diagram monoids appear in many different fields of mathematics. This makes them on the one hand very appealing, but on the other hand tends to cause confusion from time to time. For example, as we already indicated above, these diagram monoids have different names that vary with the field, e.g. the Temperley–Lieb monoid is also known as the Jones monoid or the Kauffman monoid in monoid theory, but that name appears to be unheard-of in the representation theoretical literature on the algebra versions of these monoids.

(1E.2) summarizes our list, see also [HJ20, Section 2.3]. 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, and EX means excluded from the discussion due to triviality. This is explained in more details in Conclusion 4F.17 and Conclusion 5F.13.

(1E.2)

Symbol	Diagrams	Big reps	Symbol	Diagrams	Big reps
$\mathrm{p}\mathcal{P}\mathrm{a}_n$		YES*	$\mathcal{P}\mathrm{a}_n$		YES^*_c
$\mathcal{M}\mathrm{o}_n$		YES_c	$\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n$		YES^*_c
$\mathcal{TL}_n$		YES	$\mathcal{B}\mathrm{r}_n$		YES*
$\mathrm{p}\mathcal{R}\mathrm{o}_n$		YES*	$\mathcal{R}\mathrm{o}_n$		YES*
$\mathrm{p}\mathcal{S}_n$		EX	$\mathcal{S}_n$		NO

.

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, respectively faithfulness, in Section 4 (planar) and Section 5 (symmetric).

1F. **Further direction not discussed in this paper.** Although truncated versions of the monoids mentioned in Section 1E have big representation gaps, big semisimple representation gaps and are of high faithfulness, they might not be suitable for cryptographic purposes due to their other properties.

We list here several additional examples and ideas which might be interesting to study from the perspective of cryptography. For all of these making the setup set-theoretical is the first crucial (and nontrivial) step:

(a) Web categories in the sense of Kuperberg [Ku96]. These monoidal categories generalize the Temperley–Lieb category from the viewpoint of representation theory of Lie groups with Temperley–Lieb being the SL(2) case.

A naive lower bound for the semisimple representation gap of the associated endomorphism algebras can be easily obtained. This bound is bigger than for the Temperley–Lieb monoid itself, so this might be a fruitful direction.

Note that it is not clear how to make the appearing endomorphism algebras set-theoretical. For the Temperley–Lieb category what one effectively does to make its endomorphism algebras set-theoretical is to look at products of light ladders (in the sense of [El15]). The same might work for other web categories. Light ladder bases for these web categories were discussed for example in [AST18], [El15] or [Bo20].

Note that, if one can make these web categories set-theoretical, one would get new examples for monoid theory as well, which is interesting in its own right.

(b) Soergel bimodules or categorified quantum groups in various flavors.

Soergel bimodules [So92] form monoidal categories attached to a Coxeter system. These were diagrammatically reinterpreted in [EK10] and [EW16], see also [EMTW20] for a summary. For starters, one can look at the dihedral case [El16] and see whether its set-theoretic modifications can give interesting monoids. Looking at the analogs of light ladders, called light leaves in [Li08], might be crucial. Let us note that some set-theoretical variations of Soergel diagrammatics exist in the literature, see for example [CGGS20, Section 4], but their usefulness in cryptography has not been explored.

Categorified quantum groups originate in [La10], [KL09] and [Ro08], see also [KL11], [KL10]. These are also diagrammatic in nature and promising candidates, but may be harder to work with than Soergel bimodules.

As for web categories, set-theoretical versions of these would give novel examples in monoid theory.

(c) Foams are suitably decorated 2-dimensional CW-complexes, defined abstractly or embedded in $\mathbb{R}^3$. They originate and most prominently appear in the study of link homologies, see for example [Kh04], [EST17], [RW20] or [ETW18]. Using the universal construction from [BHMV95], they can be easily modified, see e.g. [EST16] or [KK20].

Similarly as in the previous points, if foams could be made set-theoretical, that would provide a big supply of potentially interesting monoids.

(d) The representation gap and the faithfulness of $\mathcal{S}$ depend on the underlying field. To get rid of the dependence of the field, it should be useful to consider integral representation of groups or monoids. This direction is widely open and not much appears to be known. However, their categorifications, called 2-representations, have been studied a lot in the recent years.

Potential directions are:

(i) 2-representations of tensor and fusion categories, see e.g. [EGNO15, Section 7] for a book chapter discussing these. Various diagrammatic fusion categories might be of interest to study here, see [MPS17] for a compelling list of examples. These diagrammatic fusion categories also generalize $\mathcal{TL}_n$, so it is expected that the list given in [MPS17] has suitable big ranks.

(ii) 2-representations of fiat 2-categories, see e.g. [Ma17] for a slightly outdated summary. For example, Soergel bimodules tend to have simple 2-representations of very big rank, see [MMM+19] for a classification. Other versions of 2-representations of Soergel bimodules might also be useful, see e.g. [MT19] or [MMMT20].
Another advantage of studying 2-representations of fiat 2-categories from the viewpoint of cryptography is that cell theory generalizes from monoids to these 2-categories, see e.g. [MMM+21], which served as a partial motivation for Section 3.

(e) Another approach is to use semirings for building cryptographic protocols, as proposed in [GS14], [GS19], [RS21], see also [Du20], which contains a detailed review of the literature.

A linear attack on a semiring-based protocol would require the semiring to act on a vector space or a module, and it is not even clear how a semiring can act linearly on anything. There is the notion of a semimodule over a semiring, which is much closer to set theory compared to that of a module over a ring, and the theory of semimodules over semirings is computationally difficult, even for semimodules over the Boolean semiring $\mathbb{B} = \{0, 1 | 1 + 1 = 1\}$, see for example [CC19]. A semiring can appear from a linear structure, as the Grothendieck semiring of an additive category. However, realizing even the Boolean semiring (or the tropical semiring) in this way appears rather nontrivial, due to impossibility of an isomorphism $\mathbb{1} \oplus \mathbb{1} \cong \mathbb{1}$ in a monoidal category, cf. [KT19] which discusses ways to resolve such problems in similar situations.

2. Representation gaps and faithfulness

For background we refer the reader to standard textbooks such as [Be98], respectively [St16], for the basic theory of finite-dimensional representations of finite-dimensional algebras (such as monoid algebras), respectively, finite monoids.

Notation 2.1. We let $\mathcal{S}$ denote a finite monoid. If not stated otherwise, we work over an arbitrary field $\mathbb{K}$ and consider only finite-dimensional (left) $\mathcal{S}$-representation with ground field $\mathbb{K}$. The adjective *small* and *big* used for $\mathcal{S}$-representations will mean dimension-wise, where dimension is measured with respect to $\mathbb{K}$.

2A. **Representation gaps.** We start with a subtle difference between groups and monoids: the latter may have two types of "trivial" representations.

Definition 2A.1. Let $\mathcal{G} \subset \mathcal{S}$ be the subgroup of all invertible elements of $\mathcal{S}$, i.e. $\mathcal{G}$ is the group of units. Then we define *trivial representations*

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

An $\mathcal{S}$-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 $\mathcal{S}$-representation M.

Remark 2A.2. The notation is justified as follows. The $\mathcal{S}$-representation $\mathbb{1}_b$ is one of the simple $\mathcal{S}$-representations associated with the bottom J-cell $\mathcal{J}_b = \mathcal{G}$, while the $\mathcal{S}$-representation $\mathbb{1}_t$ is associated with the top J-cell $\mathcal{J}_t$, cf. Lemma 3A.9.

Remark 2A.3. With respect to Remark 2A.2 and Section 3, we warn the reader familiar with monoid theory that the order we use for J-cells (a.k.a. Green's J-classes) is opposite of the one often used in monoid theory. Thus, what we call bottom/top is usually the top/bottom in monoid theory. In contrast, our convention matches most of the cellular algebra literature.

Lemma 2A.4. *Both, $\mathbb{1}_b$ and $\mathbb{1}_t$ are simple $\mathcal{S}$-representations of dimension one. Moreover, $\mathbb{1}_b \cong \mathbb{1}_t$ if and only if $\mathcal{S}$ is a group.*

Proof. Immediate from the definitions. □

Notation 2A.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 $\mathcal{S}$ such that any representation of sufficiently small dimension relative to $|\mathcal{S}|$, the size of $\mathcal{S}$, is suitably trivial. Note that all elements of $\mathcal{S} \setminus \mathcal{G}$ 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 $\mathcal{S} \setminus \mathcal{G}$. Thus, suitably trivial could mean being isomorphic to $\mathbb{1}_{bt}^{\oplus m}$ which we take as the definition. To state our definition let $\mathcal{S}_1$ be the trivial monoid with one element, and let $\mathcal{S}_{0;1}$ be the monoid on the set $\{a_0\} \cup \{1\}$ with unit 1 and multiplication $a_0 \cdot a_0 = a_0$ otherwise.

Definition 2A.6. A pair $(\mathcal{S}, \mathbb{K})$ of a monoid, with $\mathcal{S} \ncong \mathcal{S}_1$ and $\mathcal{S} \ncong \mathcal{S}_{0;1}$, and a field $\mathbb{K}$ is called *m-trivial* if $\mathcal{S}$-representations M with $\dim_{\mathbb{K}}(M) \leq m$ satisfy $M \cong \mathbb{1}_{bt}^{\oplus \dim_{\mathbb{K}}(M)}$. Moreover, by conventions, $\mathcal{S}_1$ and $\mathcal{S}_{0;1}$ are (-1)-trivial for all $\mathbb{K}$.

The maximal m such that $(\mathcal{S}, \mathbb{K})$ is $(m-1)$-trivial is called the *representation gap* of $(\mathcal{S}, \mathbb{K})$ and is denoted by $\mathrm{gap}_{\mathbb{K}}(\mathcal{S})$.

Remark 2A.7. The two monoids $\mathcal{S}_1$ and $\mathcal{S}_{0;1}$ are the only two monoids for which every representation is a direct sum of trivial representations. Hence, their representation gap would be infinity if we would use the same definition for m-triviality as for other monoids. Since we define $\mathcal{S}_1$ and $\mathcal{S}_{0;1}$ to be (-1)-trivial we have $\mathrm{gap}_{\mathbb{K}}(\mathcal{S}_1) = \mathrm{gap}_{\mathbb{K}}(\mathcal{S}_{0;1}) = 0$.

Note that the m-triviality is a lower bound on the dimension of the smallest nontrivial simple $\mathcal{S}$-representation, assuming the absence of extensions between trivial representations $\mathbb{1}_t$ and $\mathbb{1}_b$, see also Lemma 2A.14 and Lemma 2B.2.

Definition 2A.8. A monoid $\mathcal{S}$ is called *m-trivial* if $(\mathcal{S}, \mathbb{K})$ is m-trivial for all $\mathbb{K}$.

The maximal m such that $\mathcal{S}$ is $(m-1)$-trivial is called the *representation gap* of $\mathcal{S}$ and is denoted by $\mathrm{gap}_*(\mathcal{S})$.

Remark 2A.9. In group theory the representation gap and similar notions are well-known invariants studied by many people and with a number of applications, see [BG08] or [Go08] for examples. However, the motivations in those papers are different from the ones in this paper and it would be interesting to make a connection.

Notation 2A.10. Below we will meet several notions similar to $\mathrm{gap}_{\mathbb{K}}(\mathcal{S})$ and $\mathrm{gap}_*(\mathcal{S})$. 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 $\mathrm{gap}(\mathcal{S})$.

Remark 2A.11 (Main task 1). For cryptographic applications it should be useful to have a supply of monoids $\{\mathcal{S}_n | n \in \mathbb{Z}_{\geq 0}\}$ with exponentially big $\mathrm{gap}(\mathcal{S}_n)$ as $n \to \infty$.

Example 2A.12. A pair $(\mathcal{S} \ncong \mathcal{S}_1, \mathbb{K})$ or $(\mathcal{S} \ncong \mathcal{S}_{0,1}, \mathbb{K})$ is 0-trivial if and only if any there exists a one-dimensional $\mathcal{S}$-representation which is nontrivial. In particular, if $\mathcal{S}$ has a nontrivial one-dimension representation, then $\mathrm{gap}_{\mathbb{K}}(\mathcal{S}) = 1$.

Lemma 2A.13. *The pair* $(\mathcal{S}, \mathbb{K})$ *is* m*-trivial if and only if* $\mathcal{S}$*-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 2A.14. *Assume that* $\mathcal{S}$ *has at least one nontrivial simple representation. We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{S}) \leq \min\{\dim_{\mathbb{K}}(L_K) | L_K \textit{ is a nontrivial simple } \mathcal{S}\textit{-representation}\} \leq |\mathcal{S}| - 1.$$

Moreover, when $\mathbb{K}$ *is algebraically closed, then* $|\mathcal{S}| - 1$ *on the right can be replaced by* $\sqrt{|\mathcal{S}| - 1}$. *In all cases, when* $\mathcal{S}$ *is not a group, then every appearance of* $|\mathcal{S}| - 1$ *can be replaced by* $|\mathcal{S}| - 2$.

Proof. The first inequality follows directly from the definitions. To see the second inequality observe that simple $\mathcal{S}$-representations appear in the Jordan–Hölder filtration of $\mathbb{K}\mathcal{S}$, the monoid algebra, so their dimensions are bounded by $\dim_{\mathbb{K}}\big(\mathbb{K}\mathcal{S}\big) = |\mathcal{S}|$. Since the trivial representations $\mathbb{1}_{bt}$ must appear as composition factors we actually get $|\mathcal{S}| - 2$ or $|\mathcal{S}| - 1$ as an upper bound, depending on whether $\mathbb{1}_b \ncong \mathbb{1}_t$ or not. When $\mathbb{K}$ is algebraically closed we have the inequality $\sum_L \dim_{\mathbb{K}}(L)^2 \leq |\mathcal{S}|$ where the sum runs over all simple $\mathcal{S}$-representations. This implies the final claim after again taking into account that $\mathbb{1}_{bt}$ must appear as composition factors. □

Remark 2A.15. Note that we assume that $\mathcal{S}$ has at least one nontrivial simple representation in Lemma 2A.14. This restriction is necessary. For example, let $\mathcal{S}_{0,\dots,n-1;1}$ be the monoid on $\{a_0, \dots, a_{n-1}\} \cup \{1\}$ with unit 1 and multiplication $a_i a_j = a_i$ otherwise. Then the only simple $\mathcal{S}_{0,\dots,n-1;1}$-representations are $\mathbb{1}_{bt}$, as follows directly from Proposition 3B.5. Thus, the middle number in Lemma 2A.14 is ambiguous.

Example 2A.16. Let $\mathcal{S}_n = \mathrm{Aut}(\{1, \dots, n\})$ be the *symmetric group* on $\{1, \dots, n\}$. For $\mathrm{char}(\mathbb{K}) \neq 2$ there is a 1-dimensional nontrivial simple $\mathcal{S}_n$-representation, called the sign representation. Hence, $\mathrm{gap}_{\mathbb{K}}(\mathcal{S}_n) = 1$ unless $\mathrm{char}(\mathbb{K}) = 2$, which implies $\mathrm{gap}_*(\mathcal{S}_n) = 1$. Since $|\mathcal{S}_n| = n!$, the ratio between the representation gap and the size of $\mathcal{S}_n$ is thus very small. Even if one would argue that the sign representation is close to trivial, there is still the standard $\mathcal{S}_n$-representation of dimension $n - 1$. So $\mathrm{gap}_{\mathbb{K}}(\mathcal{S}) \leq n - 1$ by Lemma 2A.14, which is still small compared to $n!$.

Example 2A.17. For the monoid in Remark 2A.15 we have $\mathrm{gap}_*(\mathcal{S}_{0;1}) = 0$ for $n = 1$ and $\mathrm{gap}_*(\mathcal{S}_{0,\dots,n-1;1}) = 2$ otherwise. This is not hard to verify, see also Example 2B.1.

2B. **Extensions and representation gaps.** We now discuss extensions. These results are essentially in the literature, but we decided to keep the proofs for convenience of the reader. We elaborate on the literature in Remark 2B.13.

We start with an example showing that there can be arbitrary complicated extensions, even with only trivial composition factors:

Example 2B.1. Back to Example 2A.17. One can check that $\mathbb{K}\mathcal{S}_{0,\dots,n-1;1}$ is a split basic algebra whose quiver Γ is of the form

$$n=1\colon \Gamma = \bullet \quad \bullet, \quad n=2\colon \Gamma = \bullet \to \bullet, \quad n=3\colon \Gamma = \bullet \rightrightarrows \bullet,$$

and so on, i.e. one has two vertices and $n-1$ edges for $\mathbb{K}\mathcal{S}_{0,\dots,n-1;1}$.

Let us use the convention on path algebras where paths are composed from right to left. Then an isomorphism that realizes these descriptions sends a_0 to the initial vertex (on the left-hand side above), $1-a_0$ to the terminal vertex and, for $n \geq 2$, $a_i - a_0$ to the ith edge, counting e.g. from top to bottom in the illustration, for $i \in \{1,\dots,n-1\}$.

By usual quiver representation theory it follows that $\mathbb{K}\mathcal{S}_{0,\dots,n-1;1}$ is semisimple for $n=1$, has finite representation type for $n=2$, tame representation type for $n=3$ and is of wild representation type for $n \geq 4$.

However, as we have seen in Example 2A.17, $\mathcal{S}_{0,\dots,n-1;1}$ has only the trivial simple representations $\mathbb{1}_{bt}$ and is 1-trivial unless $n=1$. Thus, in general, $\mathcal{S}_{0,\dots,n-1;1}$ has many nontrivial extensions of the form $0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$ with only trivial composition factors for M.

Lemma 2B.2. *A pair $(\mathcal{S},\mathbb{K})$ is m-trivial if and only if any nontrivial simple $\mathcal{S}$-representation has dimension at least $m+1$ and all extensions $0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0$ for $\dim_{\mathbb{K}}(M) \leq m$ split.*

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

Remark 2B.3. If $\mathcal{S} = \mathcal{G}$ 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 $H^1(\mathcal{S},\mathbb{K}) \cong 0$, here $\mathcal{S}$ acts on $\mathbb{K}$ trivially: $s \mapsto 1$ for all $s \in \mathcal{S}$. Moreover, for any monoid $\mathcal{S}$, recall that $H^1(\mathcal{S},\mathbb{K})$ consists of all homomorphisms from $\mathcal{S}$ to $(\mathbb{K},+)$. In particular, $H^1(\mathcal{S},\mathbb{K}) \cong 0$ if and only if the only homomorphism from $\mathcal{S}$ to $(\mathbb{K},+)$ is the trivial one. We will use this below, in particular, maps from $\mathcal{S}$ 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 $\mathcal{S}$-representation. Suppose there is a short exact sequence

$$0 \longrightarrow \mathbb{1}_{bt} \longrightarrow M \longrightarrow \mathbb{1}_{bt} \longrightarrow 0, \quad \text{meaning all four possibilities.}$$

Choosing a basis of M compatible with the corresponding filtration, the action of each $a \in \mathcal{S}$ 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 $f\colon \mathcal{S} \to \mathbb{K}$. 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 2B.3, that is:

Lemma 2B.4. *We have $\mathrm{H}^1(\mathcal{S},\mathbb{K}) \cong 0$ if and only if $\mathcal{S}$ 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 $f\colon \mathcal{S} \to \mathbb{K}$ such that $f(ab) = f(a)+f(b)$ for $a,b \in \mathcal{S}$. Any such extension is trivial if and only if $\mathrm{H}^1(\mathcal{S},\mathbb{K}) \cong 0$. □

Case (bt). Recall that $\mathcal{G} \subset \mathcal{S}$ denotes the group of units of $\mathcal{S}$.

Consider the symmetric and transitive closure of the relation $ab \approx_r a$ for $a, b \in \mathcal{S} \setminus \mathcal{G}$, and denote the closure by $\approx_r$ as well. We call $\mathcal{S}$ with a unique equivalence class in $\mathcal{S} \setminus \mathcal{G}$ under $\approx_r$ a right-connected monoid.

Remark 2B.5. Note that groups $\mathcal{S} = \mathcal{G}$ are not right-connected since for groups we have $\mathcal{S} \setminus \mathcal{G} = \emptyset$, and the empty set has no equivalence classes under $\approx_r$.

We obtain a sufficient condition for the triviality of extensions:

Lemma 2B.6. *If $\mathcal{S}$ is right-connected, then $\mathcal{S}$ 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 $f\colon \mathcal{S} \to \mathbb{K}$ such that

$$f(ab) = \begin{cases} f(a) & \text{if } a \in \mathcal{S} \setminus \mathcal{G}, \\ f(a) + f(b) & \text{if } a \in \mathcal{G}, \end{cases} \tag{2B.7}$$

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

If f satisfies (2B.7), then the fact that $f(ab) = f(a)$ for $a \in \mathcal{S} \setminus \mathcal{G}$ and $b \in \mathcal{S}$, together with right-connectedness implies that f is constant on $\mathcal{S} \setminus \mathcal{G}$. Fix $b \in \mathcal{S} \setminus \mathcal{G}$ (the set $\mathcal{S} \setminus \mathcal{G}$ is nonempty by right-connectedness). Then, if $a \in \mathcal{G}$, we have $ab \in \mathcal{S} \setminus \mathcal{G}$ and so $f(b) = f(ab) = f(a) + f(b)$, whence $f(a) = 0$. Thus, f vanishes on $\mathcal{G}$. We deduce that $\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_b) \cong 0$ by the previous paragraph. ☐

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

Lemma 2B.8. *If $\mathcal{S}$ is left-connected, then $\mathcal{S}$ 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 2B.6. ☐

Case (bb). Finally, we call a monoid $\mathcal{S}$ *null-connected* if any noninvertible element of $\mathcal{S}$ can be written as a product of two noninvertible elements. That is, for $a \in \mathcal{S} \setminus \mathcal{G}$ we have $a = bc$ for some $b, c \in \mathcal{S} \setminus \mathcal{G}$. Note that groups are null-connected.

Lemma 2B.9. *If $\mathcal{S}$ is null-connected and $\mathrm{H}^1(\mathcal{G}, \mathbb{K}) \cong 0$, then $\mathcal{S}$ 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 $f\colon \mathcal{S}\to\mathbb{K}$ such that

$$f(ab)=\begin{cases}0 & \text{if } a,b\in\mathcal{S}\setminus\mathcal{G},\\ f(a)+f(b) & \text{if } a,b\in\mathcal{G},\\ f(a) & \text{if } a\in\mathcal{S}\setminus\mathcal{G}, b\in\mathcal{G},\\ f(b) & \text{if } a\in\mathcal{G}, b\in\mathcal{S}\setminus\mathcal{G}.\end{cases}$$

Similarly as before, 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 $a\in\mathcal{S}\setminus\mathcal{G}$ and $b\in\mathcal{G}$. The rest of the argument is similar to Lemma 2B.6 and omitted. □

We say that a monoid $\mathcal{S}$ is *well-connected* if it is either a group or right-connected, left-connected and null-connected.

Theorem 2B.10. *Assume $\mathcal{S}$ is well-connected and $\mathrm{H}^1(\mathcal{G},\mathbb{K})\cong 0$. Then:*

(a) *Any short exact sequence*

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

splits.

(b) *We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{S})=\min\{\dim_{\mathbb{K}}(L)\,|\,L\ncong\mathbb{1}_{bt} \text{ is a simple } \mathcal{S}\text{-representation}\}. \tag{2B.11}$$

In particular, for groups $\mathcal{S}=\mathcal{G}$ it suffices to check whether $\mathrm{H}^1(\mathcal{G},\mathbb{K})\cong 0$ to ensure that (2B.11) *holds.*

Moreover, if $\mathcal{S}$ is semisimple over $\mathbb{K}$, then $\mathcal{S}$ is well-connected and $\mathrm{H}^1(\mathcal{G},\mathbb{K})\cong 0$, so (a) *and* (b) *hold.*

Proof. Well-connected and $\mathrm{H}^1(\mathcal{G},\mathbb{K})\cong 0$ imply Claim (a)*.* This claim follows from Remark 2B.3, and the statements in Lemma 2B.4, Lemma 2B.8, Lemma 2B.6 and Lemma 2B.9.

Well-connected and $\mathrm{H}^1(\mathcal{G},\mathbb{K})\cong 0$ imply Claim (b)*.* This follows from (a) and the definitions.

Groups. Since $\mathbb{1}_b\cong\mathbb{1}_t$, Lemma 2B.4 handles this case. It hence suffices to check $\mathrm{H}^1(\mathcal{G},\mathbb{K})\cong 0$ for groups.

We now assume that $\mathcal{S}$ is semisimple over $\mathbb{K}$.

Left and right-connectivity. Assume that $\mathcal{S}$ is not a group. To see that $\mathcal{S}$ is right-connected note that the $\mathcal{S}$-representation $\mathbb{1}_t$ is projective. Thus, there exists $e\in\mathcal{S}$ with $e^2=e$ and $\mathbb{1}_t\cong\mathbb{K}\mathcal{S}e$. Let $a,b\in\mathcal{S}$ with a in the support of e and $b\in\mathcal{S}\setminus\mathcal{G}$. Then, since $be=e$, we get that there exists $c\in\mathcal{S}$ with $a=bc$ so $\mathcal{S}$ is right-connected. Finally, taking the opposite monoid preserves semisimplicity, so the same arguments as for right-connectivity imply left-connectivity.

Null-connectivity. Recall that ideals in semisimple algebras are (unital) semisimple algebras. Hence, $\mathbb{K}(\mathcal{S}\setminus\mathcal{G})/(\mathcal{S}\setminus\mathcal{G})^2$ is semisimple, so it cannot be nilpotent. This implies that $(\mathcal{S}\setminus\mathcal{G})=(\mathcal{S}\setminus\mathcal{G})^2$, and thus, $\mathcal{S}$ is well-connected.

The cohomology vanishes. The surjection $\mathbb{K}\mathcal{S} \twoheadrightarrow \mathbb{K}\mathcal{G}$ given by $a \mapsto a$ for $a \in \mathcal{G}$ and $a \mapsto 0$ for $a \in \mathcal{S} \setminus \mathcal{G}$ implies that $\mathcal{G}$ is semisimple over $\mathbb{K}$ if $\mathcal{S}$ is. Thus, we get $\mathrm{H}^1(\mathcal{G}, \mathbb{K}) \cong 0$. $\square$

Remark 2B.12. Note that for upper bounds for $\mathrm{gap}(\mathcal{S})$ it suffices to find some nontrivial simple $\mathcal{S}$-representation, but for lower bounds or the explicit value of $\mathrm{gap}(\mathcal{S})$ we will calculate $\mathrm{H}^1(\mathcal{S}, \mathbb{K})$ and $\mathrm{H}^1(\mathcal{G}, \mathbb{K})$.

Remark 2B.13. The paper [MS12a] computes certain quivers for monoid algebras with the computation of a generalization of $\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_b)$ being a main point. The above lemmas are deducible from their computations, more precisely from [MS12a, Section 7]. In fact, [MS12a, Section 7] work in much greater generality and the setting with $\mathbb{1}_t$ and $\mathbb{1}_b$ is a very special case.

Remark 2B.14. Using ideas in [MS12a], one can get a description of $\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_b)$ as in the proof of Lemma 2B.6. That is, one can prove that $\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_b) \cong \widetilde{\mathrm{H}}^0(\Delta(P_r), \mathbb{K})^{\mathcal{G}}$ (reduced cohomology) where P_r is the poset of proper principal right ideals of $\mathcal{S}$ and $\Delta(P_r)$ is its order complex. There is, of course, the dual version for $\mathrm{Ext}^1(\mathbb{1}_b, \mathbb{1}_t)$ using proper principal left ideals of $\mathcal{S}$. Let us also mention that the special case of this result where $\mathcal{G}$ is trivial was explicitly proved in [MSS15] and a different proof was given in [MSS21] for left regular bands.

Similarly, following the ideas in [MS12a], one can show that $\mathrm{Ext}^1(\mathbb{1}_t, \mathbb{1}_t) \cong \mathrm{H}^1(\mathcal{G}, \mathbb{K}) \oplus \mathbb{K}^{|\mathcal{G}/A\backslash\mathcal{G}|}$ where $A = (\mathcal{S} \setminus \mathcal{G})/(\mathcal{S} \setminus \mathcal{G})^2$.

Recall for monoid theory that $a \in \mathcal{S}$ is called *von Neumann regular* if it can be written as $a = aba$ for some $b \in \mathcal{S}$, and $\mathcal{S}$ is *von Neumann regular* if all of its elements are. Examples of von Neumann regular monoids are the diagram monoids in (1E.2). As a final statement in this section we add:

Lemma 2B.15. *If $\mathcal{S}$ is von Neumann regular, then $\mathcal{S}$ is null-connected.*

Proof. Any $a \in \mathcal{S} \setminus \mathcal{G}$ satisfies $a = aba$ for some $b \in \mathcal{S}$. Since $ba \in \mathcal{S} \setminus \mathcal{G}$ whenever $a \in \mathcal{S} \setminus \mathcal{G}$, null-connectivity follows. $\square$

2C. **Examples.** The following is well-known. But since it is an important example for cryptography, see e.g. Example 2C.2, we state and prove it here.

Proposition 2C.1. *Let $\mathcal{C}_n \cong \mathbb{Z}/n\mathbb{Z}$ be the* cyclic group *of order $n > 1$.*

(a) *We have $\mathrm{gap}_{\mathbb{Q}}(\mathcal{C}_n) = \min\{r-1 | r \text{ prime}, \ r \mid n\}$. (In particular, $\mathrm{gap}_{\mathbb{Q}}(\mathcal{C}_n) = n-1$ 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 $\mathrm{gap}_{\mathbb{F}_q}(\mathcal{C}_n) = 1$.*
   (ii) *For $\gcd(n, q-1) = 1$ and $p \mid n$ we have $\mathrm{gap}_{\mathbb{F}_q}(\mathcal{C}_n) = 2$.*
   (iii) *For $\gcd(n, q-1) = 1$ and $p \nmid n$ we have $\mathrm{gap}_{\mathbb{F}_q}(\mathcal{C}_n) = \min\{d \in \mathbb{Z}_{\geq 0} | \gcd(n, q^d - 1) \neq 1\}$.*

(c) *For any field $\mathbb{K}$ we have $\mathrm{gap}_{\mathbb{K}}(\mathcal{C}_n) = \min_r(\mathrm{gap}_{\mathbb{K}}(\mathcal{C}_r))$, where the minimum is taken over all prime divisors r of n.*

Proof.

Case (a). First we have $\mathrm{H}^1(\mathcal{C}_n, \mathbb{Q}) \cong 0$, so by Theorem 2B.10 it suffices to look at the dimensions of simple $\mathcal{C}_n$-representations.

To this end, recall that representations of $\mathcal{C}_n$ 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 $\mathbb{Q}[\mathcal{C}_n] \cong \bigoplus_{d|n} \mathbb{Q}[X]/(\Phi_d)$, and we see that there are simple $\mathcal{C}_n$-representations for each Φ_d which are of the respective degrees $\deg \Phi_d = \varphi(d)$. This implies $\mathrm{gap}_{\mathbb{Q}}(\mathcal{C}_n) = \min\{\varphi(d) | d \text{ divides } n\}$. 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 $\mathcal{C}_n$-representation over $\mathbb{F}_q$ exactly when $\gcd(n, q-1) > 1$, implying (i). In case (ii), there exists a nontrivial homomorphism $\mathcal{C}_n \to \mathbb{F}_q$, where the latter is considered an abelian group under addition, giving a nontrivial selfextension of the trivial representation of $\mathcal{C}_n$.

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 $\mathrm{gap}_{\mathbb{F}_p}(\mathcal{C}_n)$ is then the dimension $d \geq 2$ of the smallest nontrivial simple representation. Such a representation corresponds to a nontrivial homomorphism $\mathcal{C}_n \to \mathrm{GL}(d, \mathbb{F}_q)$. Since $\gcd(n, q-1) = 1$ this homomorphism does not take $\mathcal{C}_n$ to multiples of the identity matrix. So d is the smallest number such that $\gcd\big(n, |\mathrm{GL}(d, \mathbb{F}_q)|\big) \neq 1$. The order of $\mathrm{GL}(d, \mathbb{F}_q)$, up to factors of $q-1$, which are coprime to n, is $(q^d - 1)(q^d - q) \dots (q^d - q^{d-1})$. We see that the smallest d with $\gcd\big(n, |\mathrm{GL}(d, \mathbb{F}_q)|\big) \neq 1$ is the smallest d such that $gcd(n, q^d - 1) \neq 1$.

Case (c). This follows from (a) and (b). □

Example 2C.2. The groups $\mathcal{C}_n$ lie at the heart of many standard cryptographic protocols, see e.g. [Ko98, Section 1.4]. By Proposition 2C.1 these groups have a quite big representation gap over $\mathbb{Q}$. However, the situation varies depending on the ground field, and over $\mathbb{C}$ the representation gap is small. In particular, for cryptographical purposes the point is that protocols are broken as soon as $\mathcal{C}_n$ is identified explicitly. For $n + 1 = p$ with p a large prime the classical protocols "disguise" $\mathcal{C}_n$ since finding a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, meaning finding an explicit isomorphism of groups $(\mathbb{Z}/p\mathbb{Z})^* \cong \mathcal{C}_n$, is difficult.

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 $\mathcal{C}_n$-representations are one-dimensional, and $\mathrm{gap}_{\mathbb{K}}(\mathcal{C}_n) = 1$. Instead, as argued in the proof of Proposition 2C.1, over the prime field $\mathbb{Q}$ there are two simple $\mathcal{C}_n$-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 $\mathcal{C}_n$-representations, which are Galois conjugates of each other.

Thus, for n prime Proposition 2C.1 and Example 2C.2 imply that $\mathcal{C}_n$ has a substantial representation gap $n-1$ over $\mathbb{Q}$, close to its cardinality $n = |\mathcal{C}_n|$.

Example 2C.3. Proposition 2C.1 discusses the cyclic groups $\mathcal{C}_n$. 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 $\mathcal{A}_n \subset \mathcal{S}_n$ of size $\frac{n!}{2}$ behave similarly to the symmetric groups, cf. Example 2A.16. They are a bit better in the sense that they do not have a sign representation. However, over $\mathbb{Q}$ the standard representation of $\mathcal{S}_n$ restricts to a simple $\mathcal{A}_n$-representation. Over other fields this representation might not be simple. But if it is not, then it contains an even smaller nontrivial simple in its Jordan–Hölder filtration. Hence, $\mathrm{gap}_*(\mathcal{A}_n) \leq n-1$.

(b) The biggest part of the periodic table of simple groups is 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 $\mathcal{S}_n \leftrightsquigarrow \mathcal{GL}_n(\mathbb{F}_1)$.) Most of these should have small representation gap over the defining field. To see this consider the group $\mathcal{PSL}_n(\mathbb{F}_q)$ 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 grows exponentially in n.) However, $\mathcal{PSL}_n(\mathbb{F}_q)$ 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. [CCN+85]. However, they do not come in $\mathbb{Z}_{\geq 0}$-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 [CCN+85] under the entry $M = F_1$ therein (see also [FLM88, Chapter 12] where this number+1 appears as the graded dimension of the moonshine representation), and the smallest nontrivial and faithful representation over any field has dimension 196882, see [LPWW98]. 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.

Example 2C.4. Finite groups that often have a big representation gap are p-groups for a prime p. Under the name minimal character degree, there is a big literature on the representation gap of these groups, see for example [Hu92] or [JZM02], often aiming for an upper bound and not a lower bound as we would need it. Having a large representation gap might make them useful in cryptography, see e.g. [Ro18, Section 3].

2D. **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 $\mathcal{S}$-representation M over $\mathbb{F}_q$, the *complexity* of M over $\mathbb{F}_q$ can then be defined as

$$c(M) = \dim_{\mathbb{F}_q}(M)c(\mathbb{F}_q), \quad \text{where } c(\mathbb{F}_q) = \log_2 |\mathbb{F}_q|.$$

Note that $c(M)$ is preserved when viewing M as an $\mathcal{S}$-representation over any subfield of $\mathbb{F}_q$.

Definition 2D.1. Define the *finite characteristic representation gap* $\mathrm{gap}_f(\mathcal{S})$ of $\mathcal{S}$ as the minimum of $c(M)$, over all nontrivial representations M over finite fields.

We can alternatively restrict to $\mathcal{S}$-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 $\mathcal{S}$-representation over a subfield $\mathbb{L} \subset \mathbb{K}$.

Definition 2D.2. Define the *characteristic zero representation gap* $\mathrm{gap}_0(\mathcal{S})$ of $\mathcal{S}$ as the minimum of $c_0(M)$, over all nontrivial $\mathcal{S}$-representations over finite extensions of $\mathbb{Q}$.

The pair $\big(\mathrm{gap}_0(\mathcal{S}), \mathrm{gap}_f(\mathcal{S})\big)$ is a measure of the representation complexity of $\mathcal{S}$ over both $\mathbb{Q}$ and finite fields.

Remark 2D.3. Recall from above that the groups $\mathcal{C}_n$ 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 $\mathcal{S}$ from the linear attacks viewpoint.

2E. **Faithfulness.** By a *faithful* $\mathcal{S}$-representation we mean a representation on which any two elements of $\mathcal{S}$ act differently.

Remark 2E.1. 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 $\mathbb{K}\mathcal{S}$.

Besides the notion of the representation gap, we introduce a related (weaker) notion:

Definition 2E.2. Let $\mathrm{faith}_{\mathbb{K}}(\mathcal{S})$ be the number

$$\mathrm{faith}_{\mathbb{K}}(\mathcal{S}) = \min\{\dim_{\mathbb{K}}(M) | M \text{ is a faithful } \mathcal{S}\text{-representation}\}.$$

We call $\mathrm{faith}_{\mathbb{K}}(\mathcal{S})$ the *faithfulness* of $(\mathcal{S}, \mathbb{K})$. We also define $\mathrm{faith}_*(\mathcal{S})$ to be the minimum of $\mathrm{faith}_{\mathbb{K}}(\mathcal{S})$ over all fields.

In words, $\mathrm{faith}(\mathcal{S})$ is the dimension of the smallest faithful $\mathcal{S}$-representation.

Remark 2E.3 (Main task 2). Similarly as in Remark 2A.11, for cryptographic applications it should be useful to have a supply of monoids with exponentially big $\mathrm{faith}_{\mathbb{K}}(\mathcal{S})$.

Remark 2E.4. For finite groups $\mathrm{faith}(\mathcal{S})$ is a well-known invariant studied since the early days of representation theory. It is sometimes called representation dimension, and has attracted recent attention, see [Mo21] and the references therein, including [CKR11] or [BMKS16]. Various versions of faithfulness have been studied in monoid theory as well, see for example [MS12b] who call the faithfulness the effective dimension.

Remark 2E.5. Faithfulness is only one measure of the complexity of $\mathcal{S}$. 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 $\mathcal{B}\mathrm{r}_n$ 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 $\mathcal{B}\mathrm{r}_n$ 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 2E.6. The symmetric group $\mathcal{S}_n$ has its n-dimensional permutation representation, which is faithful. Hence, $\mathrm{faith}_*(\mathcal{S}_n) \leq n$.

In fact, one can do better. If the characteristic of $\mathbb{K}$ does not divide n, then $\mathrm{faith}_{\mathbb{K}}(\mathcal{S}_n) = n-1$. The corresponding $\mathcal{S}_n$-representation is the standard representation. Otherwise and if $n \geq 5$ one has $\mathrm{faith}_{\mathbb{K}}(\mathcal{S}_n) = n-2$, and hence, still assuming $n \geq 5$, we have $\mathrm{faith}_*(\mathcal{S}_n) = n-2$. This is a fact from the early days of representation theory, see e.g. [MS12b, Section 9.3] for a modern formulation.

Example 2E.7. We have $\mathrm{faith}_{\mathbb{C}}(\mathcal{C}_{i,p}) = i+1$ for the cyclic monoid that we will meet in Example 3A.15, see e.g. [MS12b, Section 10] where the authors list $\mathrm{faith}_{\mathbb{C}}(\mathcal{S})$ for various monoids, including the cyclic ones.

Lemma 2E.8. *Assume that $\mathcal{S}$ has at least one nontrivial simple representation. Then we have*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{S}) \leq \mathrm{faith}_{\mathbb{K}}(\mathcal{S}) \leq |\mathcal{S}|.$$

Proof. Every S-representation has a Jordan–Hölder filtration by simple representations, which therefore are of smaller (or equal) dimensions. The first claim then follows from Lemma 2A.14. The second inequality follows since every monoid admits a faithful representation on itself. □

Remark 2E.9. The assumption in Lemma 2E.8 is necessary for the same reasons as in Remark 2A.15.

Example 2E.10. Let $\mathcal{B}\mathrm{r}_n$ be the braid group on n strands. We already mentioned its Burau representation in Remark 2E.5, but this representation is not faithful in general. However, a faithful $\mathcal{B}\mathrm{r}_n$-representation over $\mathbb{Q}(q,t)$ is the Laurence–Krammer–Bigelow representation, see [Bi01] and [Kr02], which is of dimension $\frac{n(n-1)}{2}$. Thus, $\mathrm{gap}_{\mathbb{Q}(q,t)}(\mathcal{B}\mathrm{r}_n) \leq \mathrm{faith}_{\mathbb{Q}(q,t)}(\mathcal{B}\mathrm{r}_n) \leq \frac{n(n-1)}{2}$, which creates obstacles of applications of $\mathcal{B}\mathrm{r}_n$ to cryptography, see also [MSU05].

The following is useful in examples:

Lemma 2E.11. *Assume that there is an embedding of monoids $\mathcal{S} \hookrightarrow \mathcal{T}$.*

$$\mathrm{faith}(\mathcal{S}) \leq \mathrm{faith}(\mathcal{T}).$$

Proof. This follows since a faithful $\mathcal{T}$-representation restricts to a faithful $\mathcal{S}$-representation. □

We come back to Example 2C.2, but now from the viewpoint of faithfulness.

Proposition 2E.12. *Let us consider the setting of Proposition* 2C.1.

(a) *We have* $\mathrm{faith}_{\mathbb{Q}}(\mathcal{C}_n)=\sum_{i=1}^{k}(r_i^{d_i}-r_i^{d_i-1})$*, where n has the prime factor decomposition* $n=\prod_{i=1}^{k}r_i^{d_i}$*. (In particular,* $\mathrm{faith}_{\mathbb{Q}}(\mathcal{C}_n)=n-1$ *if n is prime.)*

(b) *Let n be prime and* $\mathrm{char}(\mathbb{K})\nmid n$*. Then* $\mathrm{faith}_{\mathbb{K}}(\mathcal{C}_n)=\mathrm{gap}_{\mathbb{K}}(\mathcal{C}_n)$ *for all the cases in Proposition* 2C.1.

Proof.

Case (a). Recall that $\mathbb{Q}[\mathcal{C}_n]\cong\bigoplus_{d|n}\mathbb{Q}[X]/(\Phi_d)$, see the proof of Proposition 2C.1. The simple $\mathcal{C}_n$-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 $\mathcal{C}_n$-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 $\mathrm{faith}_{\mathbb{Q}}(\mathcal{C}_n)\leq\sum_{i=1}^{k}(r_i^{d_i}-r_i^{d_i-1})$. The decomposition of $\mathbb{Q}[\mathcal{C}_n]$ into $\mathbb{Q}(\zeta_d)$ also implies that one cannot find a smaller faithful $\mathcal{C}_n$-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 $\mathcal{C}_n$ is a simple group when n is a prime, and because the representation theory of $\mathcal{C}_n$ is semisimple under the assumption $\mathrm{char}(\mathbb{K})\nmid n$. □

The analog of Example 2C.3 is:

Example 2E.13. For finite simple groups faithfulness is not much different from Example 2C.3. That is, Proposition 2E.12 treats the cyclic groups and:

(a) The alternating group $\mathcal{A}_n$ has a faithful representation of dimension n, which is the restriction of the permutation representation of $\mathcal{S}_n$ to $\mathcal{A}_n$, see also Lemma 2E.11. Thus, $\mathrm{faith}_*(\mathcal{A}_n)\leq n$.

(b) The $\mathcal{GL}_n(\mathbb{F}_q)$-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 $\mathcal{PSL}_n(\mathbb{F}_q)$, which then acts faithfully on $\mathbb{F}_q^n\otimes(\mathbb{F}_q^n)^*$. Hence, $\mathrm{faith}_{\mathbb{F}_q}\big(\mathcal{PSL}_n(\mathbb{F}_q)\big)\leq n^2$.

(c) For sporadic groups the same remarks as in Example 2C.3 apply. The smallest faithful representations for sporadic groups are listed in [Ja05].

Example 2C.3 and this example motivate to study monoids that are not groups.

Example 2E.14. Similarly as in Example 2C.4, p-groups tend to have a large faithfulness and this is well-studied, see e.g. [Ja70] for some early results and [Mo21] for a more recent treatment.

2F. **Ratios.** As argued earlier, for potential cryptographic purposes one wants to specialize to monoids with the representation gap of size comparable to $|\mathcal{S}|^{\epsilon}$, for some $\epsilon>0$, as opposed to monoids where representation gap is exponentially smaller than the size of $\mathcal{S}$. As a measure of complexity, we can define:

Definition 2F.1. The *gap-ratio* and the *faithful-ratio* of $\mathcal{S}$ are

$$\mathrm{gapr}_{\mathbb{K}}(\mathcal{S})=\frac{\mathrm{gap}_{\mathbb{K}}(\mathcal{S})}{\sqrt{|\mathcal{S}|}},\quad \mathrm{faithr}_{\mathbb{K}}(\mathcal{S})=\frac{\mathrm{faith}_{\mathbb{K}}(\mathcal{S})}{|\mathcal{S}|}. \tag{2F.2}$$

Remark 2F.3 (Additional task 1). For cryptographic applications it makes sense to search for naturally occurring families of monoids $\{\mathcal{S}_n|n\in\mathbb{Z}_{\geq 0}\}$ with

$\lim_{n\to\infty} \mathrm{gapr}_{\mathbb{K}}(\mathcal{S}_n)$ or $\lim_{n\to\infty} \mathrm{faithr}_{\mathbb{K}}(\mathcal{S}_n)$ that do not approach 0 exponentially fast.

Note that these are rather crude: They are motivated by the search for families of monoids $\{\mathcal{S}_n | n \in \mathbb{Z}_{\geq 0}\}$ where representation gap grows exponentially while computations in the monoid grow polynomial, but oversimplify this problem.

Remark 2F.4. The square root in (2F.2) comes from the observation that over an algebraically closed field a simple $\mathcal{S}$-representation has dimension at most $\sqrt{|\mathcal{S}|}$. We stress that we have a slightly better bound of $\sqrt{|\mathcal{S}|-1}$ or $\sqrt{|\mathcal{S}|-2}$ in (2F.2), but the differences to $\sqrt{|\mathcal{S}|}$ do not play significant roles so we ignored these bounds in (2F.2) for the sake of simplicity.

Example 2F.5. For the symmetric group $\mathcal{S}_n$, cf. Example 2A.16 and Example 2E.6, we have $\mathrm{gapr}_*(\mathcal{S}_n) = \big(\sqrt{n!}\big)^{-1}$ and $\mathrm{faithr}_*(\mathcal{S}_n) = \big((n-3)!(n-1)n\big)^{-1}$, again indicating that $\mathcal{S}_n$ is not very useful for cryptography. The alternating group as in Example 2C.3 and Example 2E.13 has $\mathrm{gapr}_*(\mathcal{A}_n) \leq \sqrt{2}(n-1)\big(\sqrt{n!}\big)^{-1}$ and $\mathrm{faithr}_*(\mathcal{A}_n) \leq 2\big((n-1)!\big)^{-1}$, which are still tiny.

Example 2F.6. For monoids it is not hard to find examples with $\mathrm{faithr}_*(\mathcal{S}) = 1$, see [MS12b, Proposition 28] for an explicit example. Moreover, the main monoids under study in this paper have also large $\mathrm{gapr}_*(\mathcal{S})$, see e.g. Theorem 4E.2.

3. Cell theory

An important tool to study representations of monoids is *Green cells* or *Green's relations*. In this section we explain how these help to calculate $\mathrm{gap}(\mathcal{S})$ and $\mathrm{faith}(\mathcal{S})$, and also give us another numerical measure which we will call *semisimple representation gap*.

Remark 3.1. We will summarize the main constructions using the language of cells as in [GL96], which is more common in representation theory. The classical description using Green's relations from monoid theory can be found in many (older and newer) papers e.g. [Gr51] or [GMS09], and also in books such as [CP61], [CP67] or [St16]. The cell based discussion is not so easy to find in the literature, see however [GW15], [TV21] or [Tu22].

3A. **The basics.**

Recall that $\mathcal{S}$ 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 preorders on $\mathcal{S}$, 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 and two-sided.

Remark 3A.1. As in Remark 2A.3, these orders are in-line with the most common convention used in the theory of cellular algebras but the opposite of the one usually used in monoid theory.

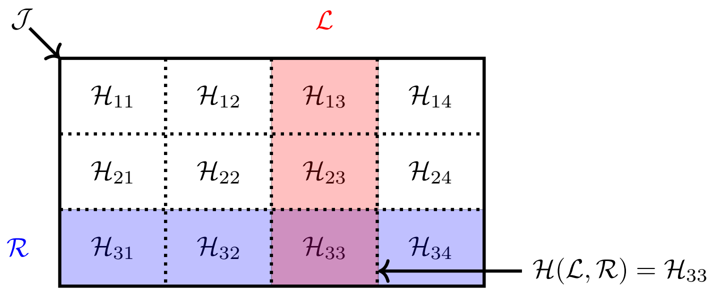
We define equivalence relations, the *left, right and two-sided equivalence*, by

$$(a \sim_l b) \Leftrightarrow (a \leq_l b \text{ and } b \leq_l a),$$
$$(a \sim_r b) \Leftrightarrow (a \leq_r b \text{ and } b \leq_r a),$$
$$(a \sim_{lr} b) \Leftrightarrow (a \leq_{lr} b \text{ and } b \leq_{lr} a).$$

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 [TV21, Section 2]) is

(3A.2)



,

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 $\mathcal{S}$ 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

$$\mathcal{S}_{\geq_l \mathcal{L}} = \{a \in \mathcal{S} | a \geq_l \mathcal{L}\},$$

as well as various versions which we will distinguish by the subscript.

Remark 3A.3. The cell orders need not be total orders. In all of our examples the $\leq_{lr}$-order is a total order, but that is a coincidence.

Example 3A.4. If $\mathcal{S}$ 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 3A.5. Example 3A.4 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*.

Remark 3A.6. In monoid theory idempotent H and J-cells are called regular to avoid confusion with the property that e.g. $\mathcal{J}\mathcal{J} = \mathcal{J}$ and because it is equivalent to each element of the cell being von Neumann regular in the sense of the definition before Lemma 2B.15. However, for us the existence of an idempotent is crucial, so we use the above nomenclature.

H-cells are crucial as justified by:

Proposition 3A.7. *For the monoid $\mathcal{S}$ 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 $\mathcal{H}(e) = \mathcal{J}(e) \cap (e\mathcal{S}e)$.*

Proof. Part (a) is clear, while (b) is classical, see [Gr51, Theorem 7]. □

Notation 3A.8. 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 $\mathcal{H}(e) \cong \mathcal{S}_1$.

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 3A.9. *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.*

This is classical, e.g. [CP67, Chapter 6] discusses ordering relations on J-cells, but we will give a short proof for completeness.

Proof. The bottom J-cell is easy to find: Let $\mathcal{G} \subset \mathcal{S}$ be the group of units of $\mathcal{S}$, i.e. the set of invertible elements of $\mathcal{S}$. Then $\mathcal{G}$ 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 $a \in \mathcal{S}$ since we can choose $c = a$. But every invertible element $b \in \mathcal{S}$ 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 $\mathcal{G}$ is the unique bottom cell $\mathcal{J}_b$. Moreover, the unit is an idempotent in $\mathcal{J}_b$.

The top J-cell is not much harder to find: 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 $\mathcal{S}$. Furthermore, 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 [St16, Proposition 1.23]. □

Example 3A.10. The *transformation monoid* $\mathcal{T}_n$ on the set $\{1, \dots, n\}$ is $\mathrm{End}(\{1, \dots, n\})$. The cells of $\mathcal{T}_3$, 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 (3A.2) we have

$$\mathcal{J}_t \qquad \begin{array}{|c|}\hline (111)\\ \hline (222)\\ \hline (333)\\ \hline \end{array} \qquad \mathcal{H}(e) \cong \mathcal{S}_1$$

$$\mathcal{J}_m \qquad \begin{array}{c|c|c} (122),(211) & (121),(212) & (221),(112)\\ \hline (133),(311) & (313),(131) & (113),(331)\\ \hline (233),(322) & (323),(232) & (223),(332) \end{array} \qquad \mathcal{H}(e) \cong \mathcal{S}_2 \quad .$$

$$\mathcal{J}_b \qquad \begin{array}{c} (123),(213),(132)\\ (231),(312),(321) \end{array} \qquad \mathcal{H}(e) \cong \mathcal{S}_3$$

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 $\mathcal{S}_k$ 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 3A.11. *Within one J-cell we have $|\mathcal{L}| = |\mathcal{L}'|$, $|\mathcal{R}| = |\mathcal{R}'|$ and $|\mathcal{H}| = |\mathcal{H}'|$, and we have $|\mathcal{L}| \cdot |\mathcal{R}|/|\mathcal{H}| = |\mathcal{J}|$. Moreover, $|\mathcal{H}|$ divides both, $|\mathcal{L}|$ and $|\mathcal{R}|$.*

Proof. The first three equalities follow from [Gr51, 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 3A.11 gives us additionally

$$|\mathcal{L}|/|\mathcal{H}|, |\mathcal{R}|/|\mathcal{H}| \in \mathbb{Z}_{\geq 0}.$$

These are important measures of the complexity of $\mathcal{S}$.

Example 3A.12. The middle J-cell in Example 3A.10 has $|\mathcal{H}| = 2$, $\mathcal{J}_m = 18 = 6 \cdot 6/2 = |\mathcal{L}| \cdot |\mathcal{R}|/|\mathcal{H}|$ 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. Lemma 3A.13 explains the matrix notation:

Lemma 3A.13. *For fixed left cell $\mathcal{L}$ the set $\mathcal{S}_{\geq_l \mathcal{L}}$ is a left ideal in $\mathcal{S}$. Similarly, $\mathcal{S}_{\geq_r \mathcal{R}}$ is a right and $\mathcal{S}_{\geq_{lr} \mathcal{J}}$ is a two-sided ideal. The same works when replacing $\geq$ by $>$.*

Proof. Directly from the definitions: given $b \in \mathcal{S}_{\geq_l \mathcal{L}}$, the element ab is still left greater than 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, recall that the *index* $i(a) \in \mathbb{Z}_{\geq 0}$ for $a \in \mathcal{S}$ 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 3A.14. *There exists an H-cell $\mathcal{H}(e)$ such that $\mathcal{C}_{p(a)} \cong \{a^s \mid s \geq i(a)\} \subset \mathcal{H}(e)$ is a subgroup. In particular, $p(a) \mid |\mathcal{H}(e)|$.*

Proof. As a consequence of [Gr51, Theorem 7], the H-cells of the form $\mathcal{H}(e)$ are the maximal subgroups of $\mathcal{S}$, so no other subgroup will be contained in some $\mathcal{H}(e)$. □

Example 3A.15. Given $i \in \mathbb{Z}_{\geq 0}$, $p \in \mathbb{Z}_{\geq 1}$ form the finite cyclic monoid $\mathcal{C}_{i,p} = \langle a | a^{i+p} = a^i \rangle$ of cardinality $i + p$. The element a has index $i(a) = i$ and period $p(a) = p$. Moreover, the monoid $\mathcal{C}_{i,p}$ is commutative, so left, right and J-cells coincide. The elements $1, a, \dots, a^{i-1}$ each constitute a single J-cell, in total $i - 1$ such J-cells. All the remaining elements $\mathcal{J}_t = \{a^i, a^{i+1}, \dots, a^{i+p-1}\}$ 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 $\mathcal{C}_{i,p}$ two cells are idempotent: $\mathcal{J}_b = \{1\}$ and $\mathcal{J}_t$.

To be completely explicit, let us consider $\mathcal{C}_{3,2}$, which is the monoid be generated by one element a of index 3 and period 2. Then $\mathcal{C}_{3,2} = \{1, a, a^2, a^3, a^4\}$ and its cell structure is

$$\begin{array}{lcl} \mathcal{J}_t & \boxed{a^3, a^4} & \mathcal{H}(e) \cong \mathcal{C}_2 \cong \mathbb{Z}/2\mathbb{Z} \\ \mathcal{J}_{a^2} & a^2 & \\ \mathcal{J}_a & a & \\ \mathcal{J}_b & \boxed{1} & \mathcal{H}(e) \cong \mathcal{S}_1 \end{array}.$$

Note that $\mathcal{S}_a$ is commutative, so left, right, J- and H-cells agree.

Remark 3A.16 (Additional task 2). Using the DH protocol with protocol monoid $\mathcal{S}$ other than a group, it would be important to find elements $g \in \mathcal{S}$ of big period that has a large prime factor, see e.g. the original DH key exchange [Ko98], [MSU08, Section 1.2]. So, by Theorem 3A.14, it would be preferable to have a monoid $\mathcal{S}$ with H-cells whose orders have large prime divisors since the period of $a \in \mathcal{S}$ divides the order of the idempotent H-cell of $\mathcal{S}$ that contains the top cell of $\mathcal{C}_{i,p}$.

3B. **Classification of simple representations.** Recall that we consider $\mathcal{S}$-representations defined over $\mathbb{K}$.

Cells can be considered $\mathcal{S}$-representations, called *cell representations* or *Schützenberger representations*, up to higher order terms:

Lemma 3B.1. *Each left cell $\mathcal{L}$ of $\mathcal{S}$ gives rise to a left $\mathcal{S}$-representation $\Delta_{\mathcal{L}} = \mathbb{K}\mathcal{L}$ by*

$$a \centerdot l \in \Delta_{\mathcal{L}} = \begin{cases} al & \text{if } al \in \mathcal{L}, \\ 0 & \text{else.} \end{cases}$$

Similarly, right cells give right $\mathcal{S}$-representations ${}_{\mathcal{R}}\Delta$ and J-cells give $\mathcal{S}$-birepresentations (often called $\mathcal{S}$-birepresentations). 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 $\mathrm{Ann}_{\mathcal{S}}(M) = \{s \in \mathcal{S} | s \centerdot M = 0\}$ of an $\mathcal{S}$-representation M is a two-sided ideal of $\mathcal{S}$. An *apex* of M is a J-cell $\mathcal{J}$ such that, firstly, $\mathcal{J} \cap \mathrm{Ann}_{\mathcal{S}}(M) = \emptyset$, and secondly, all J-cells $\mathcal{J}'$ with $\mathcal{J}' \cap \mathrm{Ann}_{\mathcal{S}}(M) = \emptyset$ 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 $\mathcal{S}$-representation*:

Lemma 3B.2. *Every simple $\mathcal{S}$-representation has a unique apex.*

Proof. This is classical, see e.g. [GMS09, Theorem 5]. □

Example 3B.3. The apex of $\mathbb{1}_b$ is always $\mathcal{J}_b = \mathcal{G}$. On the other hand, the apex of $\mathbb{1}_t$ is $\mathcal{J}_t$ since every $s \in \mathcal{S}$ acts as 1.

Recall that the nonunital way to induce is $\mathrm{Ind}(M) = \mathbb{K}\mathcal{S}e \otimes_{\mathbb{K}e\mathcal{S}e} M$ for some idempotent $e \in \mathcal{S}$, see e.g. [St16, Section 4.1] (inducing from the submonoid $e\mathcal{S}e$ to $\mathcal{S}$, or rather using their monoid algebras). It follows from [Gr51] that $\Delta_{\mathcal{L}}$ is a free right $\mathcal{H}(e)$-representation, and this action commutes with the left $\mathcal{S}$-action. Thus, $\Delta_{\mathcal{L}}$ is an $\mathcal{S}$-$\mathcal{H}(e)$-birepresentation. We can then define an induction functor

$$\mathrm{Ind}_{\mathcal{H}(e)}^{\mathcal{S}} M = \Delta_{\mathcal{L}} \otimes_{\mathcal{H}(e)} M,$$

where M is a left M-representation.

Example 3B.4. Let $\mathbb{K}[\mathcal{H}(e)]$ denote the regular $\mathcal{H}(e)$-representation, which as a $\mathbb{K}$-vector space is just $\mathbb{K}\mathcal{H}(e)$ and the $\mathcal{H}(e)$-action is the multiplication action. We have $\mathrm{Ind}_{\mathcal{H}(e)}^{\mathcal{S}}\mathbb{K}[\mathcal{H}(e)] \cong \Delta_{\mathcal{L}}$ as left $\mathcal{S}$-representations.

Recall also that the *head* $\mathrm{Hd}(M)$ of an $\mathcal{S}$-representation M is the maximal semisimple quotient of M. It is well-defined, up to isomorphism, for any representation 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 subrepresentations of M.

We get the *Clifford–Munn–Ponizovskiĭ theorem* or *H-reduction*:

Proposition 3B.5. *For a monoid $\mathcal{S}$:*

$$\{\textit{simple } \mathcal{S}\textit{-representations of apex } \mathcal{J}\}/\cong \xleftrightarrow{1:1} \{\textit{simple } \mathcal{H}(e)\textit{-representations}\}/\cong,$$

where $\mathcal{H}(e) \subset \mathcal{J}$ is any arbitrarily chosen idempotent H-cell in an idempotent J-cell $\mathcal{J}$. Moreover, an explicit bijection (from right to left) is given by

$$K \mapsto L_K \cong \mathrm{Hd}(\mathrm{Ind}_{\mathcal{H}(e)}^{\mathcal{S}}K).$$

Proof. The above is an easy reformulation of [GMS09, Theorem 7] or [St16, 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 paper.

Remark 3B.6. The 1:1 correspondence in Proposition 3B.5 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 3B.7. 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 3A.10 shows that $\mathcal{T}_3$ has three simple $\mathcal{T}_3$-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 $\mathcal{S}_3$, $\mathcal{S}_2$ and $\mathcal{S}_1$ (and the number of simple $\mathcal{S}_n$-representations is given by the number of partitions of n).

For $\mathrm{char}(\mathbb{K}) = 3$ one gets only two simple $\mathcal{T}_3$-representations of apex $\mathcal{J}_b$ since $\mathcal{S}_3$ has only two simple representations in this characteristic; the rest remains the same as for $\mathrm{char}(\mathbb{K}) = 0$. Similarly, for $\mathrm{char}(\mathbb{K}) = 2$ both apexes $\mathcal{J}_b$ and $\mathcal{J}_m$ have one fewer associated simple $\mathcal{T}_3$-representation than for $\mathrm{char}(\mathbb{K}) = 0$, but $\mathcal{J}_t$ still has the same count.

We can thus define a partial order, also denoted by $\leq_{lr}$, on the set of simple $\mathcal{S}$-representations by saying that one simple is strictly smaller than another if its apex is strictly smaller. Note that simples of the same apex are incomparable.

Example 3B.8. Note that if $\mathcal{H}(e)$ is trivial, then Proposition 3B.5 implies that one can say that the simples are indexed by the poset of apexes.

Remark 3B.9. When working over $\mathbb{C}$ and when all J-cells are idempotent, it is shown in [Pu98, Theorem 2.1] that $\leq_{lr}$ makes the representation category of $\mathcal{S}$ into a highest weight category in the sense of [CPS88]. In fact, for the reader familiar with cellular algebras as in [GL96], [TV21] or [Tu22] we point out that [Pu98, Theorem 2.1] shows that, if all J-cells are idempotent, then the monoid algebra $\mathbb{C}\mathcal{S}$ is a quasi-hereditary sandwich cellular algebra.

As a historical remark, the fact that the monoid algebra $\mathbb{C}\mathcal{S}$ of a regular monoid (a regular monoid satisfies any of the conditions in Lemma 3F.6) in characteristic zero is a quasi-hereditary sandwich cellular algebra was first proven in [Ni71] in the early 1970s. Of course the result was phrased in a different language since [Ni71] appeared before quasi-hereditary or (sandwich) cellular algebras were defined.

3C. **Cells and (semisimple) representation gaps.** Note that Proposition 3B.5 makes it easy to classify simple $\mathcal{S}$-representations but does not give much information about their dimensions.

Theorem 3C.1. *The dimension of the simple $\mathcal{S}$-representation L_K associated to the simple $\mathcal{H}(e)$-representation K via Proposition* 3B.5 *can be bounded by*

$$\dim_{\mathbb{K}}(L_K) \leq |\mathcal{L}|/|\mathcal{H}| \cdot \dim_{\mathbb{K}}(K).$$

Proof. First, recall from Lemma 3A.11 that all left and H-cells within one J-cell are of the same size, so for the bound we can and will omit writing $\mathcal{L}(e)$ and $\mathcal{H}(e)$. Then this follows from the explicit bijection in Proposition 3B.5 and the fact that $\Delta_{\mathcal{L}}$ is a free $\mathcal{H}(e)$-representation of rank $|\mathcal{L}|/|\mathcal{H}|$. □

Note that dimension of $\mathrm{Hd}(\mathrm{Ind}_{\mathcal{H}(e)}^{\mathcal{S}} K)$ 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 3C.2. 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 $\mathcal{S}$-representation with $\mathrm{ssdim}_{\mathbb{K}}(L_K) = m$ is called the *semisimple representation gap* $\mathrm{ssgap}_{\mathbb{K}}(\mathcal{S})$ of $\mathcal{S}$.

We also call $\mathrm{ssgapr}_{\mathbb{K}}(\mathcal{S}) = \frac{\mathrm{ssgap}_{\mathbb{K}}(\mathcal{S})}{\sqrt{|\mathcal{S}|}}$ the *semisimple-gap-ratio.*

The square root in the definition of $\mathrm{ssgapr}_{\mathbb{K}}(\mathcal{S})$ is used for the same reasons as in Remark 2F.4. With the same assumptions as in e.g. Lemma 2A.14 we have:

Theorem 3C.3. *Assume that $\mathcal{S}$ has at least one nontrivial simple representation. We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{S}) \leq \min\{\dim_{\mathbb{K}}(L_K) \mid L_K \not\cong \mathbb{1}_{bt} \textit{ is a simple } \mathcal{S}\textit{-representation}\} \leq \mathrm{ssgap}_{\mathbb{K}}(\mathcal{S}) \leq |\mathcal{S}|.$$

Proof. Clear by definition and Lemma 2A.14. □

Remark 3C.4 (Additional task 3). As before, it is important for potential cryptographic applications to find monoids with $\mathrm{ssgap}_{\mathbb{K}}(\mathcal{S})$ exponentially big.

Example 3C.5. In the setting of Example 3A.10 and Example 3B.7 (in particular, $\mathrm{char}(\mathbb{K}) \nmid 6$) we have the following.

The three simple $\mathcal{T}_3$-representations of apex $\mathcal{J}_b$ are the simple $\mathcal{S}_3$-representations inflated to $\mathcal{T}_3$, so they are of dimensions 1, 2 and 1 (one of these is $\mathbb{1}_b$). These are also their semisimple dimensions.

The simple $\mathcal{S}_3$-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 $\mathcal{S}_3$-representations of apex $\mathcal{J}_m$ are induced from the respective $\mathcal{S}_2$-representations, and are of semisimple dimension 3. One can check that they are of dimension 3 respectively 2.

In general, for the representation theory of $\mathcal{T}_n$ see [Pu98, Section 4] or [St16, Section 5.3].

The name semisimple representation gap is justified by the following.

Proposition 3C.6. *The following are equivalent.*

(a) *The monoid $\mathcal{S}$ is semisimple over $\mathbb{K}$.*

(b) *All J-cells are idempotent, all $\mathcal{H}(e)$ are semisimple over $\mathbb{K}$ and $\dim_{\mathbb{K}}(L_K) = \mathrm{ssdim}_{\mathbb{K}}(L_K)$ for all simple $\mathcal{S}$-representations L_K.*

Proof. This follows from [St16, Theorem 5.19] and the paragraph below that theorem. □

3D. **Cells and Gram matrices.** Recall the following construction of Gram matrices, also called sandwich matrices in monoid theory, see e.g. [CP61, Section 5.2] or [St16, 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 $\{l_1, \dots, l_R\}$ and $\{r_1, \dots, r_L\}$ 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, see the references above.

Gram matrices are in particularly useful for $\mathcal{H}(e) \cong \mathcal{S}_1$ and $L = R$ as justified by part (a) of the following (which the reader familiar with [GL96] might recognize):

Proposition 3D.1. *Fix an idempotent J-cell $\mathcal{J}$. All cells in the statement are within $\mathcal{J}$.*

(a) *Assume $\mathcal{H}(e) \subset \mathcal{J}$ satisfies $\mathcal{H}(e) \cong \mathcal{S}_1$. Assume further that $P^{\mathcal{J}}$ is square and symmetric. Let $L_{\mathcal{J}}$ denote the associated simple $\mathcal{S}$-representation, see Proposition 3B.5. Then:*

$$\dim_{\mathbb{K}}(L_{\mathcal{J}}) = \mathrm{rank}(P^{\mathcal{J}}).$$

(b) *More generally, let K be a simple $\mathcal{H}(e)$-representation and let L_K be the associated simple $\mathcal{S}$-representation. Let $P^{\mathcal{J}}_K$ denote the matrix one gets by applying K to each entry of $P^{\mathcal{J}}$. Then:*

$$\dim_{\mathbb{K}}(L_K) = \mathrm{rank}(P^{\mathcal{J}}_K).$$

Proof. (a) 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 an $\mathcal{S}$-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 $\mathcal{S}$ 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 [ET21, Lemma 3.4].

It follows that $\Delta_{\mathcal{L}}/\mathrm{Rad}_{\mathcal{J}}$ is a simple $\mathcal{S}$-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.

(b) Adjusting the arguments in (a), see e.g. [St16, Corollary 5.30] for details. □

Theorem 3D.2. *Let $\mathcal{R} \subset \mathcal{S}$ be a submonoid. Under the assumptions in Proposition* 3D.1*, if $\mathcal{J}$ restricts to an idempotent J-cell of $\mathcal{R}$, then*

$$\dim_{\mathbb{K}}(L_{\mathcal{J}}^{\mathcal{S}}) \geq \dim_{\mathbb{K}}(L_{\mathcal{J}}^{\mathcal{R}}),$$

for the associated simple $\mathcal{R}$ and $\mathcal{S}$-representations.

Proof. Note that under the assumptions we have that the Gram matrix for $\mathcal{R}$ is a submatrix of $P^{\mathcal{J}}$. The rank of a matrix is always greater than or equal to the rank of a submatrix, so the statement follows by Proposition 3D.1. □

We stress that it is not generally true that $\mathcal{J}$ restricts to a(n idempotent) J-cell of $\mathcal{R}$, so the assumption in Theorem 3D.2 is necessary.

3E. **Cells, Burnside–Brauer–Steinberg and faithfulness.** Let $cl_{\mathcal{H}(e)}$ denote the number of conjugacy classes of the group $\mathcal{H}(e)$. Let $\{e_1, \dots, e_r\}$ be a choice of one idempotent per idempotent J-cell, and define

$$cl(\mathcal{S}) = cl_{\mathcal{H}(e_1)} + \cdots + cl_{\mathcal{H}(e_r)}.$$

Lemma 3E.1. *The number $cl(\mathcal{S}) \in \mathbb{Z}_{\geq 0}$ is independent of the choice of $\{e_1, \dots, e_r\}$.*

Proof. This is a consequence of [St16, Section 7.1]. □

Hence, $cl(\mathcal{S})$ is a constant depending on $\mathcal{S}$ only. One can use $cl(\mathcal{S})$ for the *Burnside–Brauer theorem* (characteristic zero) and the *Steinberg theorem* (arbitrary characteristic):

Proposition 3E.2. *If F is a faithful $\mathcal{S}$-representation, then every simple $\mathcal{S}$-representation appears as a composition factor of $F^{\otimes k}$ for some $0 \leq k \leq cl(\mathcal{S}) - 1$. Moreover, if F is a faithful $\mathcal{S}$-representation whose composition factors are one-dimensional, then the composition factors of $F^{\otimes k}$ are also one-dimensional.*

Proof. For characteristic zero see [St14] or [St16, Section 7.4] and the observation that the r in that theorem satisfies $r \leq cl(\mathcal{S})$ by the discussion in [St16, Section 7.1]. For the characteristic free version see [St16, Corollary 10.7], using the same observation. □

Example 3E.3. The bound given in Proposition 3E.2 is often not optimal but cannot be improved uniformly. For example, for $\mathcal{C}_n$ we have $cl(\mathcal{C}_n) = n$. 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 $\mathcal{C}_n$-representation, and only the $(n-1)$th power of it will contain the simple $\mathcal{C}_n$-representation associated to $\exp(\frac{2\pi i(n-1)}{n})$.

The Burnside–Brauer–Steinberg theorem Proposition 3E.2 gives a bound for the dimension of faithful $\mathcal{S}$-representations:

Theorem 3E.4. *Let $\mathrm{char}(\mathbb{K}) = 0$, and let L_{max} be a simple $\mathcal{S}$-representation of the biggest dimension. If F is a faithful $\mathcal{S}$-representation, then $\dim_{\mathbb{K}}(F) \geq \sqrt[cl(\mathcal{S})-1]{\dim_{\mathbb{K}}(L_{max})}$. Hence,*

$$\mathrm{faith}_{\mathbb{K}}(\mathcal{S}) \geq \sqrt[cl(\mathcal{S})-1]{\dim_{\mathbb{K}}(L_{max})}.$$

Proof. This follows from Proposition 3E.2. □

Note that one can use Theorem 3E.4 often in combination with Lemma 2E.11.

Remark 3E.5 (Additional task 4). Thus, by Theorem 3E.4 it is preferable for cryptographical applications to find a monoid $\mathcal{S}$ with $c(\mathcal{S})$ being small.

Example 3E.6. Applying Theorem 3E.4 for $\mathcal{T}_3$ gives $\sqrt[6]{3}$ as a lower bound, which rounds to 2. The smallest faithful $\mathcal{T}_3$-representation is $\mathbb{K}\{1,2,3\}$ (with the defining action), so of dimension three.

With respect to extensions as discussed in Section 2A we get:

Proposition 3E.7. *There is a faithful $\mathcal{S}$-representation containing only $\mathbb{1}_{bt}$ as composition factors if and only if $\mathcal{S}$ has at most two idempotent J-cells and all idempotent H-cells are trivial, i.e. $\mathcal{H}(e) \cong \mathcal{S}_1$.*

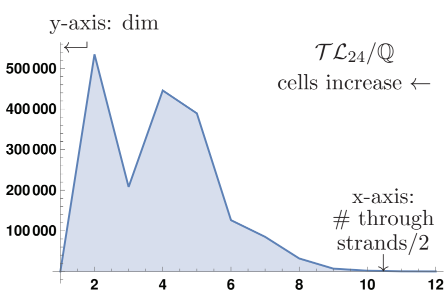
Proof. $\Rightarrow$. If F is a faithful $\mathcal{S}$-representation only containing $\mathbb{1}_{bt}$ as composition factors, then Proposition 3E.2 implies that there can be no simple $\mathcal{S}$-representations except $\mathbb{1}_{bt}$. Thus, the result follows by Proposition 3B.5.

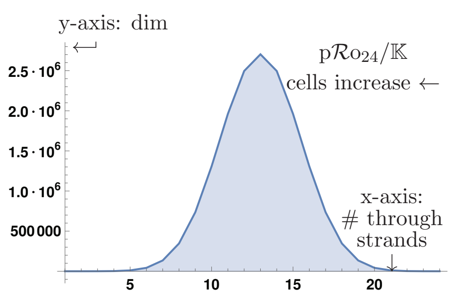
$\Leftarrow$. In this case Proposition 3B.5 implies that $\mathbb{1}_{bt}$ are the only simple $\mathcal{S}$-representations. $\square$

Example 3E.8. Let $\mathrm{char}(\mathbb{K}) = 0$. When $\mathcal{S}$ is a group Proposition 3E.7 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 3E.9. It follows from the discussion in (4B.2) that the Temperley–Lieb monoid on three strands $\mathcal{TL}_3$ is an example of a nontrivial monoid that has a faithful representation entirely made of $\mathbb{1}_{bt}$. This works in arbitrary characteristic.

3F. **Cell submonoids and subquotients.** Recall that simple $\mathcal{S}$-representations arrange themselves according to the cells, see Proposition 3B.5. Let us in this motivational paragraph for simplicity assume that $\mathcal{H}(e) \cong \mathcal{S}_1$ for all idempotent H-cells and that all J-cells are idempotent. Then the dimensions of the simple $\mathcal{S}$-representations very often have the following form, which is roughly as expected from combinatorial numbers:



,


,

$$\text{TL dim}\colon \begin{pmatrix} 1, 534888, 208011, 445741, 389367, \\ 126292, 85216, 31878, 6876, 1726, 252, 22, 1 \end{pmatrix},$$

$$\text{pRo dim}\colon \begin{pmatrix} 1, 24, 276, 2024, 10626, 42504, 134596, 346104, 735471, \\ 1307504, 1961256, 2496144, 2704156, 2496144, 1961256, \\ 1307504, 735471, 346104, 134596, 42504, 10626, 2024, 276, 24, 1 \end{pmatrix}.$$

These illustrations show the dimensions of the simple $\mathcal{TL}_{24}$-representation (left) over $\mathbb{Q}$ (or any field of characteristic zero) and the simple $\mathrm{p}\mathcal{R}\mathrm{o}_{24}$-representations for general $\mathbb{K}$, respectively. See Section 4 for details. (Note the two trivial $\mathcal{TL}_{24}$-respectively p$\mathcal{R}$o$_{24}$-representations of dimension one for the bottom and top cells.) 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 *cell submonoids* as follows.

Definition 3F.1. For a J-cell $\mathcal{J}$ with $1 \notin \mathcal{J}$ define the *$\mathcal{J}$-submonoid*

$$\mathcal{S}_{\geq \mathcal{J}} = \mathcal{S}_{\geq_{lr} \mathcal{J}} \cup \{1\}.$$

In words, we artificially adjoint a unit 1 (strictly speaking we should write $1'$) to the two-sided ideal $\mathcal{S}_{\geq_{lr} \mathcal{J}}$ from Lemma 3A.13.

Lemma 3F.2. *For any J-cell $\mathcal{J}$ with $1 \notin \mathcal{J}$, $\mathcal{S}_{\geq \mathcal{J}}$ is a submonoid of $\mathcal{S}$.*

Proof. By Lemma 3A.13. □

Remark 3F.3. 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* $\mathcal{S}/I$ of a monoid $\mathcal{S}$ by a two-sided ideal I. The construction works as follows. As a set $\mathcal{S}/I = (\mathcal{S} \setminus I) \cup \{0\}$, where one artificially adjoints an element 0. The multiplication is $s \bullet t = st$ if $s, t, st \in \mathcal{S} \setminus I$, and $s \bullet t = 0$ otherwise.

Lemma 3F.4. *For any two-sided ideal, the Rees factor $\mathcal{S}/I$ is a well-defined monoid.*

Proof. An easy exercise, see also [St16, Exercise 1.6]. □

We can thus define *cell subquotients*:

Definition 3F.5. 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

$$\mathcal{S}_{\mathcal{J}}^{\mathcal{K}} = \mathcal{S}_{\geq \mathcal{J}} / \mathcal{S}_{\geq \mathcal{K}}.$$

Here we additionally allow the following extremal cases:

$$\mathcal{S}_{\mathcal{J}}^{none} = \mathcal{S}_{\geq \mathcal{J}}, \quad \mathcal{S}_{none}^{\mathcal{K}} = \mathcal{S}/\mathcal{S}_{\geq \mathcal{K}}, \quad \mathcal{S}_{none}^{none} = \mathcal{S}.$$

We also call all of the above *cell subquotients* for short.

By Lemma 3F.2 and Lemma 3F.4, $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$ is a subquotient of $\mathcal{S}$. Unless we are in one of the extreme cases, $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$ has $\mathcal{J}_b = \{1\}$ and $\mathcal{J}_t = \{0\}$. Both are left, right, J- and H-cells at the same time.

Lemma 3F.6. *The following conditions are equivalent:*

(a) *For all left cells $\mathcal{L}$:*

$$\forall a, b \in \mathcal{L}\ \exists c \in \mathcal{J} \supset \mathcal{L} \text{ such that } a = cb.$$

(b) *For all right cells $\mathcal{R}$:*

$$\forall a, b \in \mathcal{R}\ \exists c \in \mathcal{J} \supset \mathcal{R} \text{ such that } a = bc.$$

(c) *For all J-cells $\mathcal{J}$:*

$$\forall a, b \in \mathcal{J}\ \exists c, d \in \mathcal{J} \text{ such that } a = cbd.$$

(d) *All J-cells are idempotent.*

(e) *For all $a \in \mathcal{S}$ we have $a \in a\mathcal{S}a$.*

Proof. Well-known, see e.g. [RS09, Theorem A.3.7]. $\square$

We say $\mathcal{S}$ is *regular* (this is also sometimes called von Neumann regular) if any of the equivalent conditions in Lemma 3F.6 hold.

The regularity condition ensures that the cells are not affected when taking cell subquotients.

Lemma 3F.7. *Let $\mathcal{S}$ be regular. In the nonextremal cases the J-cells of $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$ are given by*

$$\{\mathcal{J}_b\} \cup \{\mathcal{M} | \mathcal{M} \text{ is a } J\text{-cell of } \mathcal{S} \text{ with } \mathcal{J} \leq_{lr} \mathcal{M} <_{lr} \mathcal{K}\} \cup \{\mathcal{J}_t\}.$$

Similarly for left, and right cells, assuming the respective regularity condition, and H-cells.

An analog statement holds in the extremal cases.

Proof. By the regularity assumption, the remaining elements of $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$ arrange themselves into cells precisely as in $\mathcal{S}$. $\square$

We require that $\mathcal{S}$ is regular for the remainder of this section.

Assume that we are in the nonextremal cases. Then $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$ 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 $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$-representations of these apexes. The other simple $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$-representations and their dimensions are given by the following statement. Note hereby that any $\mathcal{S}_{\mathcal{J}}$-representation with apex $\mathcal{M}$ can be *inflated* to an $\mathcal{S}$-representation by letting all elements in $\mathcal{S}_{<_{lr}\mathcal{J}}$ act by zero.

Proposition 3F.8. *Assume that we are in the nonextremal cases. Let $\mathcal{M} \notin \{\mathcal{J}_b, \mathcal{J}_t\}$ be an apex of $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$ which is also an apex of $\mathcal{S}$. Then we have:*

$$\{\textit{simple } \mathcal{S}_{\mathcal{J}}^{\mathcal{K}}\textit{-representations of apex } \mathcal{M}\}/\cong \xleftrightarrow{1:1} \{\textit{simple } \mathcal{S}\textit{-representations of apex } \mathcal{M}\}/\cong .$$

Moreover, an explicit bijection (from left to right) is given by inflating simple $\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}$-representations to simple $\mathcal{S}$-representations. The dimensions of the simples are preserved under this bijection.

An analog statement holds in the extremal cases.

Proof. The first part follows from Proposition 3B.5. For the final part note that inflation clearly does not change property of being simple nor the dimension. $\square$

Theorem 3F.9. *For any two J-cells $\mathcal{J} \leq_{lr} \mathcal{K}$ we have*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{S}_{\mathcal{J}}^{\mathcal{K}}) \geq \mathrm{gap}_{\mathbb{K}}(\mathcal{S}).$$

Proof. By Proposition 3F.8. □

Remark 3F.10 (Additional task 5). By Theorem 3F.9, a strategy is to find a monoid $\mathcal{S}$ with big representations for a slice of the cells. Then taking an appropriate cell subquotient the resulting monoid will have a suitable representation gap.

We will see examples of the task in Remark 3F.10 in the next two sections.

4. Planar monoids

We work over an arbitrary field $\mathbb{K}$.

4A. **Temperley–Lieb categories and monoids.**

We now recall the *Temperley–Lieb category* $\mathbf{TL}^{lin}(\delta)$. This category is a $\mathbb{K}$-linear monoidal category which depends on a parameter $\delta \in \mathbb{K}$. There are many references (the Temperley–Lieb calculus has been rediscovered many times, and there are too many papers to be cited here) for $\mathbf{TL}^{lin}(\delta)$ where more details can be found, see for example [KL94]. The endomorphism spaces in the Temperley–Lieb category form $\mathbb{K}$-algebras, called *Temperley–Lieb algebras*. By appropriate reformulation we obtain set-theoretical versions of both of these.

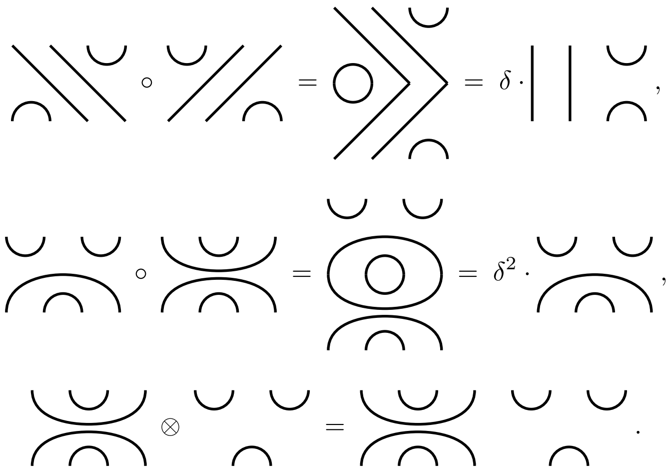
Remark 4A.1. It may be convenient to represent $\delta = -q - q^{-1}$ where q is either in $\mathbb{K}$ or its quadratic extension. For our main application we need $\delta = 1$, so q in this case is a primitive third root of unity. This is for example important when one wants to connect $\mathbf{TL}^{lin}(\delta)$ to the category of tilting representations for quantum SL_2, see e.g. [TW21, Proposition 2.28] or [STWZ21, Proposition 2.20] for a precise statement. This perspective is sometimes useful, see for example [An19], [Sp20] or [TW22] for nontrivial results about the set-theoretical Temperley–Lieb algebras using tilting representations.

The Temperley–Lieb category $\mathbf{TL}^{lin}(\delta)$ has objects $n \in \mathbb{Z}_{\geq 0}$. The morphisms from m to n are $\mathbb{K}$-linear combinations of isotopy classes of diagrams of matchings of $m + n$ points in the strip $\mathbb{R} \times [0, 1]$, with m points at the bottom and n points at the top line of the strip. These morphisms are known as *crossingless matchings*. The relations on them are such that two diagrams represent the same morphism if and only if they represent the same crossingless matching.

Composition $\circ$ of crossingless matchings is given by *vertical* gluing (and rescaling), using the convention to glue $a\colon m \to n$ on top of $b\colon k \to m$, which is denoted using the operator notation $a \circ b$. This will give another crossingless matching, but with potentially internal circles. To get rid of this ambiguity, we remove such internal circles, say we have k of these, and the resulting crossingless matching is multiplied by δ^k.

The monoidal structure $\otimes$ is given by $m \otimes n = m + n$ on objects and *horizontal* juxtaposition on morphisms, extended bilinearly to $\mathbb{K}$-linear combinations.

Notation 4A.2. The following pictures summarize the main points from above, and also fix the reading conventions that we will use for diagrammatics throughout.



Let C_m^n denote the set of crossingless matching with m bottom and n top boundary points. Let $Ca(k) = \frac{1}{k+1}\binom{2k}{k}$ be the kth Catalan number. Note that Lemma 4A.3 is independent of $\mathbb{K}$ and $\delta \in \mathbb{K}$.

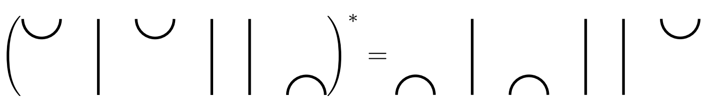
Lemma 4A.3. *The set C_m^n is a $\mathbb{K}$-linear basis of $\mathrm{Hom}_{\mathbf{TL}^{lin}(\delta)}(m,n)$. Hence, the dimension of this space is either zero if $m \not\equiv n \bmod 2$, and otherwise given by $\dim_{\mathbb{K}}\big(\mathrm{Hom}_{\mathbf{TL}^{lin}(\delta)}(m,n)\big) = Ca(\frac{m+n}{2})$.*

Proof. This is well-known, see e.g. [RTW32] for the version with $\delta = -2$. □

Lemma 4A.4. *The category $\mathbf{TL}^{lin}(\delta)$ has an antiinvolution $\_^*$, i.e. is a $*$-monoid, given by reflecting diagrams in a horizontal axis.*

Proof. Easy and omitted. □

The picture to keep in mind is



Remark 4A.5. It is easy to see (and we will use this silently) that $\_^*$ works for all the diagrammatic categories, algebras and monoids we use in this and the next section. We call $\_^*$ the *diagrammatic antiinvolution.*

The Temperley–Lieb algebra on n-strands is then $\mathcal{TL}_n^{lin}(\delta) = \mathrm{End}_{\mathbf{TL}^{lin}(\delta)}(n)$. This is the algebra of crossingless matchings with n strands and only vertical composition.

Remark 4A.6. The algebra $\mathcal{TL}_n^{lin}(\delta)$ was introduced in the context of Schur–Weyl duality, see [RTW32]. Sometimes it is useful to use this perspective as e.g. the reference [An19] does (using the connection to tilting representations, cf. Remark 4A.1) which we will use below.

Now comes the main definition of this section.

Definition 4A.7. The *set-theoretic Temperley–Lieb category* **TL** is defined in almost the same way as $\mathbf{TL}^{lin}(\delta)$ above with two crucial differences:

(a) The hom-spaces are $\mathrm{Hom}_{\mathbf{TL}}(m,n) = C_m^n$, and,

(b) the vertical composition $\circ$ is still given by vertical gluing, but all internal circles are just removed from the diagram, that is, without any factor.

The *Temperley–Lieb monoid* on n-strands is defined by $\mathcal{TL}_n = \mathrm{End}_{\mathbf{TL}}(n)$.

Remark 4A.8. The Temperley–Lieb monoid appears in many works, way too many to be cited here, see however e.g. [HR05], [HJ20] or [Si20]. In most papers coming from representation theory, quantum algebra and quantum topology it is however studied as an algebra. Note hereby that Definition 4A.7 is not quite the same as $\mathbf{TL}^{lin}(1)$ where the circle evaluates to 1. The difference is that $\mathbf{TL}^{lin}(1)$ is $\mathbb{K}$-linear, but $\mathbf{TL}$ is not $\mathbb{K}$-linear. But the monoid algebra $\mathbb{K}[\mathcal{TL}_n]$ is isomorphic to $\mathcal{TL}_n^{lin}(1)$. Let us stress that the Temperley–Lieb monoid is also called the Jones monoid in monoid theory, or sometimes even the Kauffman monoid, see e.g. [LFG06].

The monoid $\mathcal{TL}_n$ has $Ca(n)$ elements. By [KL94, Section 2.2] (or [Ea21] for a new proof of the presentation), the monoid $\mathcal{TL}_n$ can be abstractly defined by the generators $\{u_1, \dots, u_{n-1}\}$ and the defining relations

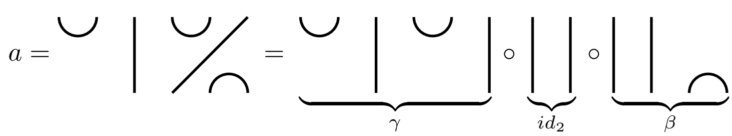
$$u_i^2 = u_i, \quad u_i u_{i\pm 1} u_i = u_i, \quad u_i u_j = u_j u_i, \ |i-j| > 1. \tag{4A.9}$$

Denote by id_k the identity on $k \in \mathbb{Z}_{\geq 0}$. The following determines the cell structure:

Lemma 4A.10. *For $a \in \mathrm{Hom}_{\mathbf{TL}}(m,n)$ there is a unique factorization of the form $a = \gamma \circ id_k \circ \beta$ for minimal k, and $\beta \in \mathrm{Hom}_{\mathbf{TL}}(m,k)$ and $\gamma \in \mathrm{Hom}_{\mathbf{TL}}(k,n)$.*

Proof. The following picture

(4A.11)



generalizes without much work. ☐

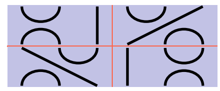
We call k the number of *through strands* of α, also known as the *width*. Necessarily k has the same parity as m and n and $k \leq m, n$. The diagram a has $\frac{m-k}{2}$ caps and $\frac{n-k}{2}$ cups. The diagrams β and γ have no cups, respectively no caps, but the same number of caps, respectively cups, as α. We call β as in Lemma 4A.10 the *bottom half* and γ the *top half* of a.

Denote by $\mathrm{B}_m^n \subset \mathrm{Hom}_{\mathbf{TL}}(m,n)$ the set of diagrams without caps. An example for $m = 2$ and $n = 6$ is given by γ in (4A.11). In other words, B_m^n consists of m *through strands* and $\frac{n-m}{2}$ cups. Necessarily $m \leq n$ and $m+n$ is even. In the above factorization, in general, $\gamma, \beta^* \in \mathrm{B}_m^n$. We may also write this factorization of a as $a = a_1 a_2^*$, $a_1, a_2 \in \mathrm{B}_m^n$.

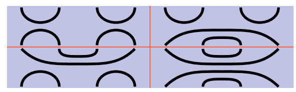
4B. **Cells of the Temperley–Lieb monoid.** We now discuss the cell structure of $\mathcal{TL}_n$.

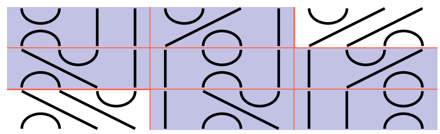
Remark 4B.1. The cell structure of the Temperley–Lieb monoid $\mathcal{TL}_n$ is very nice and easy to compute. It is well-known, see e.g. [GL96, Example 1.4], and was rediscovered in many papers, see e.g. [RSA14], or [KS21] or [Sp20], although not always in the language of cells. The cell structure has also been rediscovered in monoid theory, see e.g. [LFG06]. In any case, the description of the cells is prototypical for diagram monoids and algebras so we decided to repeat it here in that language.

The main pictures to keep in mind (which we will explain momentarily) are:

$\mathcal{J}_1$  $\mathcal{H}(e) \cong \mathcal{S}_1$,

$\mathcal{J}_3$  $\mathcal{H}(e) \cong \mathcal{S}_1$

(4B.2) $\mathcal{J}_0$  $\mathcal{H}(e) \cong \mathcal{S}_1$

$\mathcal{J}_2$  $\mathcal{H}(e) \cong \mathcal{S}_1$.

$\mathcal{J}_4$  $\mathcal{H}(e) \cong \mathcal{S}_1$

These are the cells of $\mathcal{TL}_3$ and $\mathcal{TL}_4$, which should be read as in (3A.2). 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 4B.3. *We have the following.*

(a) *The left and right cells of $\mathcal{TL}_n$ 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 $\mathcal{TL}_n$ 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 $\mathcal{TL}_n$ is idempotent, and $\mathcal{H}(e) \cong \mathcal{S}_1$ 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 proposition can be found in e.g. [GL96, Example 1.4] or [RSA14, Section 2]. (Note that [RSA14, 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. In monoid theory this appears again in many works, e.g. in [LFG06].

(c) Observing that every crossingless matching that is symmetric under horizontal mirroring is an idempotent, this is then immediate from (a) and (b). $\square$

Proposition 4B.4. *The set of apexes for simple $\mathcal{TL}_n$-representations can be indexed* 1:1 *by the poset $\Lambda = (\{n, n-2, \dots\}, >)$ (ending on either* 0 *or* 1*, depending on the parity of* n*), and there is precisely one simple $\mathcal{TL}_n$-representation of a fixed apex up to $\cong$.*

Proof. By Proposition 4B.3, this is a direct application of Proposition 3B.5. □

By Proposition 4B.4 there is a poset Λ indexing the J-cells and the simple $\mathcal{TL}_n$-representations. We can thus enumerate the J-cells by $\mathcal{J}_k$ for $k \in \Lambda$. We do the same for the simple $\mathcal{TL}_n$-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 4B.5. *Within one J-cell, all left cell representations $\Delta_{\mathcal{L}}$ and all right cell representations ${}_{\mathcal{R}}\Delta$ 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 cell structure and shows $\Delta_k \cong {}_k\Delta$. The dimension formula then follows from Proposition 4B.3 and Lemma 3B.1. □

Proposition 4B.6. *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 Propositions 4B.3 and 4B.4. □

The numbers $\dim_{\mathbb{K}}(L_k)$ are as follows. These were computed in many papers, e.g. in [An19] and [Sp20] which compute them for general $\mathbb{K}$ and $\delta \in \mathbb{K}$. (Strictly speaking [An19] needs $\delta = -q - q^{-1}$ because Andersen uses the connection to tilting representations as recalled in Remark 4A.1.) To state them we need some preliminary definitions.

Remark 4B.7. The definitions below are fairly standard for Temperley–Lieb calculi over arbitrary fields, see e.g. [Sp20], [Sp21] or [STWZ21]. 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 4B.9.

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 $x = [\dots, x_1, x_0]$ denote the *$(3,p)$-adic expansion* of x given by

$$[\dots, x_1, x_0] = \sum_{i=1}^{\infty} 3p^{i-1}x_i + x_0 = x, \quad x_{i>0} \in \{0, \dots, p-1\}, x_0 \in \{0,1,2\}.$$

The numbers x_j are the digits of x, and most of these x_j are zero. Let now $x \lhd y$ if $[\dots, x_1, x_0]$ is digit-wise smaller than or equal to $[\dots, y_1, y_0]$. 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

$$e_{n,k} = \begin{cases} 1 & \text{if } n \equiv k \bmod 2,\ \nu_{3,p}(k) = \nu_{3,p}(\frac{n+k}{2}),\ k \lhd' \frac{n+k}{2}, \\ -1 & \text{if } n \equiv k \bmod 2,\ \nu_{3,p}(k) < \nu_{3,p}(\frac{n+k}{2}), k \lhd \frac{n+k}{2} - 1, \\ 0 & \text{else.} \end{cases} \tag{4B.8}$$

Example 4B.9. 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. Equation (4B.8) 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 $\longleftarrow e_{8,8}$								
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 $\swarrow e_{15,11}$				1	
16																	1

.

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 4B.10. *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 $\mathcal{TL}_n^{lin}(1)$ these dimensions were computed in [Sp20, Corollary 9.3]. These computations use the $\mathbb{K}$-linear cell structure of $\mathcal{TL}_n^{lin}(1)$ 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 $\mathcal{TL}_n$ discussed in Theorem 3C.1 and the results in [Sp20, Corollary 9.3] work thus for $\mathcal{TL}_n$ without change. □

Example 4B.11. It is easy to feed the above into a machine. Below we list the first few dimensions of the simple $\mathcal{TL}_n$-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

$0 \le k \le 16$ the columns.

$\mathrm{char}(\mathbb{K}) = 0$; Order of cells ←; $\mathrm{dim}_{\mathbb{K}}(L_8)$ for $\mathcal{TL}_8$; $\mathrm{dim}_{\mathbb{K}}(L_{11})$ for $\mathcal{TL}_{15}$

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		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

$\mathrm{char}(\mathbb{K}) = 2$; Order of cells ←; $\mathrm{dim}_{\mathbb{K}}(L_8)$ for $\mathcal{TL}_8$; $\mathrm{dim}_{\mathbb{K}}(L_{11})$ for $\mathcal{TL}_{15}$

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

These tables also appear in [An19]. Note that the representations 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 [STWZ21, 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 ($k \notin \{0,1\}$ is covered in Proposition 4B.10):

Proposition 4B.12. *Let* $\mathrm{char}(\mathbb{K}) = 0$. *For* $k \notin \{0,1\}$ *we have*

$$\mathrm{dim}_{\mathbb{K}}(L_k) \ge \frac{1}{(n-c(k)+1)(n-c(k)+2)} \binom{n}{c(k)}.$$

Proof. See [Sp20, Propositions 9.4 and 9.5]. □

Example 4B.13. The dimensions of the simple $\mathcal{TL}_{24}$-representations over $\mathbb{Q}$ and their lower bounds are given by the tuples

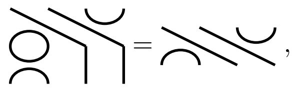
$$\mathrm{dim}\colon\ (1, 534888, 208011, 445741, 389367, 126292, 85216, 31878, 6876, 1726, 252, 22, 1),$$
$$\text{lower bound}\colon\ \big(14858, 11886, 8171, 4807, 2403, 1012, 354, 101, 23, 4, 0.5, 0.04, \tfrac{1}{650}\big).$$

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 $k = 0$.

4C. **Truncating the Temperley–Lieb monoid.** Recall that we need a regularity condition to ensure that taking cell subquotients works as expected, cf. Lemma 3F.6. We first establish:

Lemma 4C.1. *The monoid $\mathcal{TL}_n$ is regular.*

Proof. We check that $\mathcal{TL}_n$ satisfies condition (a) in Lemma 3F.6. 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 (4B.2).

Alternatively, from Lemma 3F.6 we get that this lemma follows from Neumann regularity in monoid theory, and of course this is well-known for the Temperley–Lieb monoid, see e.g. [LFG06]. □

Motivated by Example 4C.3 we define:

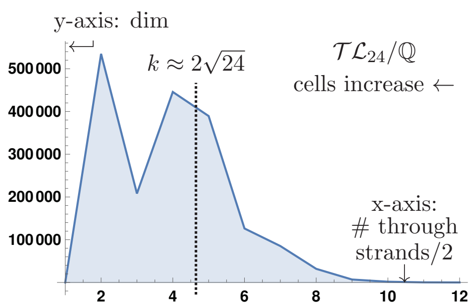
Definition 4C.2. Define the *kth truncated Temperley–Lieb monoid* by

$$\mathcal{TL}_n^{\leq k} = (\mathcal{TL}_n)_{\geq \mathcal{J}_k}.$$

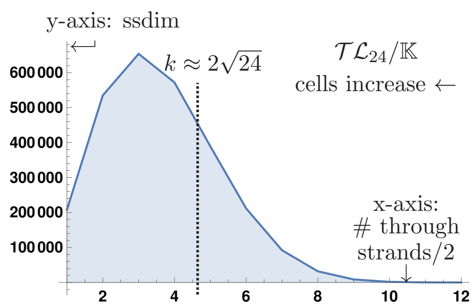
This is the cell submonoid, see Section 3F. In words, $\mathcal{TL}_n^{\leq k}$ consist of all crossingless matchings with fewer than k through strands, together with an identity element. Recall that, by Proposition 3F.8 and the discussion in Section 4A, we know the simple $\mathcal{TL}_n^{\leq k}$-representations and their dimensions.

Example 4C.3. Let us come back to (3F). Looking at the graphs of the dimensions and the semisimple dimensions of the simple $\mathcal{TL}_{24}$-representations

(4C.4)



,



$$\text{dim}\colon\ (1, 534888, 208011, 445741, 389367|126292, 85216, 31878, 6876, 1726, 252, 22, 1),$$

$$\text{ssdim}\colon\ (208012, 534888, 653752, 572033, 389367|211508, 92092, 31878, 8602, 1748, 252, 23, 1),$$

it seems preferable to cut these graphs roughly at $k \approx 2\sqrt{24}$ or at even lower values, as illustrated above. The submonoid $\mathcal{TL}_{24}^{\leq k}$ for this specific value of k now does not have too small representations anymore and is still rich enough as a monoid. Note that the one-dimensional simple $\mathcal{TL}_{24}^{\leq k}$-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 $\mathcal{TL}_n^{\leq k}$, but before we can prove it we need to discuss extensions.

4D. **Trivial extensions in Temperley–Lieb monoids.** Our next goal is to show that $\mathcal{TL}_n$ and $\mathcal{TL}_n^{\leq k}$ have no extensions between $\mathbb{1}_{bt}$ (under some minor restrictions on n and k). Let $\mathcal{X}$ be either $\mathcal{TL}_n$ or $\mathcal{TL}_n^{\leq k}$, and recall the notions of left-connected, right-connected, null-connected and well-connected from Section 2A.

Lemma 4D.1. *The monoid $\mathcal{X}$ is null-connected.*

Proof. Note first that for each of these monoids the group $\mathcal{G}$ of invertible elements is trivial. For $a \in \mathcal{X} \setminus \mathcal{G}$ the decomposition $a = \gamma \circ id_m \circ \beta = a_1 a_2^*$ from Lemma 4A.10 then implies that these monoids are null-connected since $a_2^* = a_2^* a_2 a_2^*$ and $a = a a_2 a_2^*$ is then a product of a and $a_2^* a_2 \in \mathcal{X} \setminus \mathcal{G}$. $\square$

Before we can prove the main statement of this section we need some terminology.

Remark 4D.2. 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-connected 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 4D.3. Consider $a, b \in \mathrm{B}_2^6$ given by

$a =$  , $b =$  , $b^* a =$  .

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 4D.4. 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 4D.5. *The graph Γ_m^n is connected if $m > 0$.*

Proof.

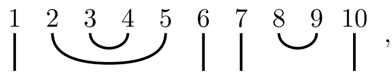
Case $(m = 1)$. In this case the lemma can be proved by induction on n, by showing that any diagram $a \in \mathrm{B}_1^n$ is connected by a path in Γ_1^n to the diagram with the through strand on the far left and $\frac{n-1}{2}$ unnested cups.

General case. Consider a diagram $a \in \mathrm{B}^n_m$. 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^k_1, utilizing only one through strand c. Doing this transformation with each through strand 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^n_m is connected. $\square$

A cup is called *outer* if it is not separated from the bottom of the diagram by any cup. A pair $(a, b) \in \mathrm{B}^n_m \times \mathrm{B}^n_m$ 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.

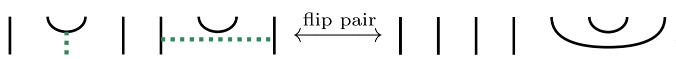
Example 4D.6.

(a) In the element of B^{10}_3



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.

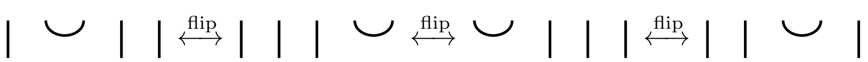
Definition 4D.7. Let Δ^n_m denote the unoriented graph with vertex set B^n_m and edges between a and b for all flipped pairs (a, b).

Note that the graph Δ^n_2 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 4D.8. *The graph Δ^n_3 is connected.*

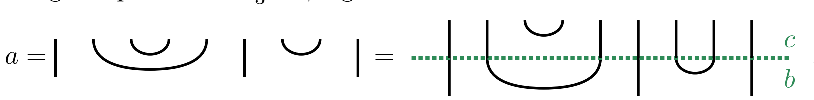
Proof. We view the empty graph (with no vertices) as connected, which is the case when n is even. For odd $n = 3 + 2k$ the proof is by induction on k.

Case $(k = 1)$. In this case the graph has the form

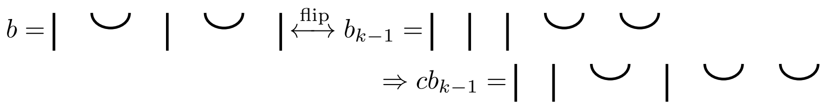


thus is connected.

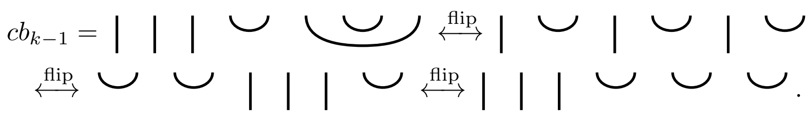
Case $(k > 1)$. Represent $a \in \mathrm{B}^{3+2k}_3$ as a composition $a = cb$ of a diagram $c \in \mathrm{B}^{3+2k}_{1+2k}$ with a single cup and $b \in \mathrm{B}^{1+2k}_3$, e.g. :



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

(4D.9)


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 (4D.10), 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 (4D.9). 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 $b_k \in \Delta_3^{2k+3}$.

(4D.10)


The remaining case is when the cup from c is nested inside the rightmost cup of b_{k-1}, see (4D.10). 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. $\square$

Lemma 4D.11. *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 4D.8, 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. $\square$

Recall the relation $\approx_l$ given by the closure of the relation $ba \approx_l a$, where $a, b \in \mathcal{S} \setminus \mathcal{G}$.

Lemma 4D.12.

(a) *Suppose $(a, b) \in \mathrm{B}_m^n$ is a flip pair, and $m \leq k$. Then $aa^* \approx_l bb^*$ in $\mathcal{TL}_n^{\leq k}$. Moreover, for $a, b \in \mathrm{B}_m^n$, $m \leq k$ we have $aa^* \approx_l bb^*$ in $\mathcal{TL}_n^{\leq k}$.*

(b) *For $a, b, c \in \mathrm{B}_k^n$ we have $ac^* \approx_l bc^*$ in $\mathcal{TL}_n^{\leq k}$, 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 $a = a_1, a_2, \ldots, a_r = b$ 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-connected.

Lemma 4D.13. *We have the following.*

(a) *The monoid $\mathcal{TL}_n$ is left-connected if $n \geq 5$.*

(b) *The monoid $\mathcal{TL}_n^{\leq k}$ is left-connected if $n \geq 5$ and $k \geq 3$.*

Proof. Recall the generator-relation presentation from (4A.9).

(a) It is easy to see that $\mathcal{TL}_3$ 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 (4B.2). The monoid $\mathcal{TL}_4$ also has two $\approx_l$ equivalence classes, represented by u_1 and u_2. In general, since the u_i generate $\mathcal{TL}_n$, 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 $u_i \approx_l u_1 u_i = u_i u_1 \approx_l u_1$. Finally, $u_1 \approx_l u_{n-1}u_1 = u_1 u_{n-1} \approx_l u_{n-1}$.

(b) We need to show that there is a unique equivalence class under $\approx_l$ in $\mathcal{TL}_n^{\leq k} \setminus \{1\}$. 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 $u = u_{i_r} u_{i_{r-1}} \ldots u_{i_1}$ of u as a product of generators. The element u has width $m \leq k$. Pick the smallest p such that the suffix $v = u_{i_p} u_{i_{p-1}} \ldots u_{i_1}$ 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 $\mathcal{TL}_n^{\leq k} \setminus \{1\}$, 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 $a = a_1 a_2^*, b = b_1 b_2^*$ with $a_1, a_2, b_1, b_2 \in \mathrm{B}_k^n$. From Lemma 4D.13 we have $a_1 a_2^* \approx_l a_2 a_2^*$ and $b_1 b_2^* \approx_l b_2 b_2^*$. From the same lemma, $a_2 a_2^* \approx_l b_2 b_2^*$, so that $a \approx_l b$. □

Note that the statement of part (b) of Lemma 4D.13 essentially contains part (a) by taking $k = n$. We have included both parts for clarity.

Lemma 4D.14. *The monoid $\mathcal{TL}_n$ is well-connected if $n \geq 5$, and the monoid $\mathcal{TL}_n^{\leq k}$ is well-connected 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 $\mathcal{TL}_n$ and $\mathcal{TL}_n^{\leq k}$ are left-connected if and only if they are right-connected. □

Let $\mathcal{X}$ be either $\mathcal{TL}_n$ or $\mathcal{TL}_n^{\leq k}$ for $k \geq 3$.

Lemma 4D.15. *We have $\mathrm{H}^1(\mathcal{X}, \mathbb{K}) \cong 0$ for all $n \in \mathbb{Z}_{\geq 0}$.*

Proof.

Case ($\mathcal{X} = \mathcal{TL}_n$). A homomorphism $f\colon \mathcal{TL}_n \to \mathbb{K}$ takes each idempotent $e \in \mathcal{TL}_n$ to 0. From the classical generators-relation presentation of $\mathcal{TL}_n$, see (4A.9), it is clear that every nonidentity element is a product of idempotents, so we get $\mathrm{H}^1(\mathcal{TL}_n, \mathbb{K}) \cong 0$.

Case ($\mathcal{X} = \mathcal{TL}_n^{\leq k}$). We now need a different argument. Suppose give a homomorphism $f\colon \mathcal{TL}_n \to \mathbb{K}$. Consider all diagrams of width k in $\mathcal{X}$. 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 $\mathcal{X}$. The elements y of $\mathcal{X}$ of smaller width are products of elements of width k, showing that $f(y) = 0$ as well. Thus, f is identically 0 on $\mathcal{X}$.

General approach. If $\mathcal{S}$ is any finite monoid with trivial H-cells, then $\mathrm{H}^1(\mathcal{X}, \mathbb{K}) \cong 0$, and even $\mathrm{H}^1(\mathcal{X}, A) \cong 0$ for any abelian group A. To see this note that Theorem 3A.14 and $\mathcal{H}(e) \cong \mathcal{S}_1$ imply that $\exists M \in \mathbb{Z}_{\geq 0}$ with $x^M = x^{M+1}$ for all $x \in \mathcal{S}$. Therefore each element has trivial image under any $f\colon \mathcal{S} \to A$ since A is a group. □

Proposition 4D.16. *Let M be an $\mathcal{X}$-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 $\mathcal{G}$ of $\mathcal{X}$ is trivial, so we get $\mathrm{H}^1(\mathcal{G}, \mathbb{K}) \cong 0$. Combine this with Lemma 4D.14 and Theorem 2B.10. □

4E. **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 $\mathcal{X}$ be either $\mathcal{TL}_n$ or $\mathcal{TL}_n^{\leq k}$ for $k \geq 3$.

Theorem 4E.1. *Let $n \geq 5$, and let $m(l)$ be the dimension of the simple $\mathcal{X}$-representation L_l as in Proposition* 4B.10*. Then:*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{TL}_n) = \min\big\{m(l) | l \notin \{0, 1, n\}\big\},$$
$$\mathrm{gap}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}) = \min\big\{m(l) | l \notin \{0, 1, k+1, k+2, \dots, n\}\big\}.$$

Proof. By Theorem 2B.10 and Proposition 4D.16. □

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, $\mathcal{TL}_n^{\leq k}$ 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 4E.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:*

$$\begin{aligned}
\mathrm{gap}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}) &\geq \frac{4}{(n+2\sqrt{n}+2)(n+2\sqrt{n}+4)} \binom{n}{\frac{n}{2}-\sqrt{n}} \in \Theta\big(2^n n^{-5/2}\big), \\
\mathrm{ssgap}_{\mathbb{L}}(\mathcal{TL}_n^{\leq k}) &\geq \frac{2}{2n} \binom{n}{\lfloor \frac{n}{2} \rfloor} \in \Theta\big(2^n n^{-3/2}\big), \\
\mathrm{faith}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}) &\geq \frac{6}{n+4} \binom{n}{\frac{n'}{2}-1} \in \Theta\big(2^n n^{-3/2}\big),
\end{aligned}$$

where in the final bound $n' = n$, if n is even, and $n' = n-1$, if n is odd.

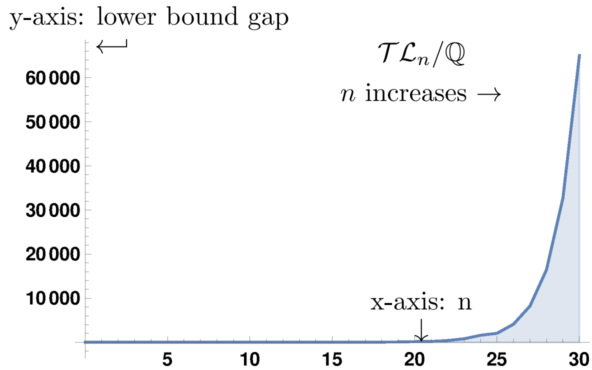
Proof. Representation gap. We will make use of Proposition 4D.16. By Theorem 2B.10, this statement ensures that we only need to compute dimension bounds for simple $\mathcal{TL}_n^{\leq k}$-representations. The first bound then follows from Proposition 4B.12. The formula $\frac{1}{(n-c(k)+1)(n-c(k)+2)}\binom{n}{c(k)}$ 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 4B.6 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 $n!$.

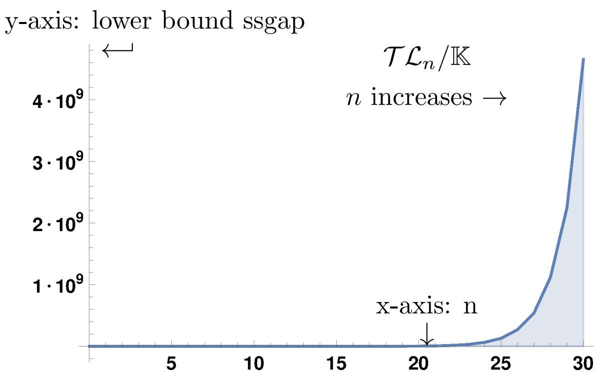
Faithfulness. For the final bound we use Lemma 2E.11. This lemma says that it suffices to find a lower bound for $\mathcal{TL}_n^{\leq 2}$: If n is even, then $\mathcal{TL}_n^{\leq 2} \hookrightarrow \mathcal{TL}_n^{\leq k}$. If n is odd, then we can still use $\mathcal{TL}_n^{\leq 2}$ after adding another strand. Note that a faithful $\mathcal{TL}_n^{\leq 2}$-representation cannot be a nontrivial extension of $\mathbb{1}_{bt}$ by Proposition 4D.16 and also not a direct sum of $\mathbb{1}_{bt}$. Hence, any faithful $\mathcal{TL}_n^{\leq 2}$-representation must contain L_2. The combinatorics from Example 4B.9 implies that $\dim_{\mathbb{K}}(L_2) = \mathrm{ssdim}_{\mathbb{K}}(L_2)$, so the claimed formula follows from Proposition 4B.6. 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. □

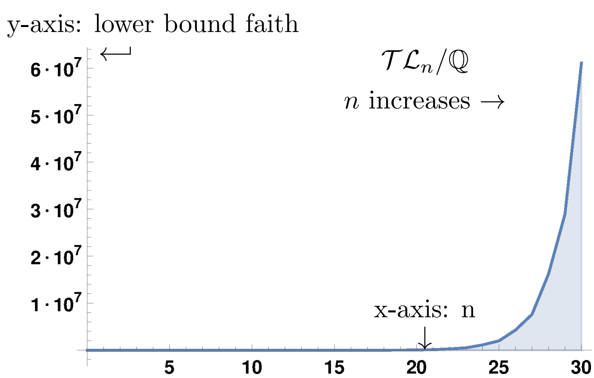
Example 4E.3. The lower bounds in Theorem 4E.2 are far from being optimal. But they still grow very fast. Here are their plots:



,



,



.

In these plots n increases from 0 to 30 when going left to right.

Note that the bound $0 \leq k \leq 2\sqrt{n}$ in Theorem 4E.2 means that the monoid $\mathcal{TL}_n^{\leq k}$ has few through strands. This has the advantage that the dimensions of simple $\mathcal{TL}_n^{\leq k}$-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 4E.4. *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:*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}) \geq \frac{1}{(n-\frac{\sqrt{n}}{2}+1)(n-\frac{\sqrt{n}}{2}+2)}\binom{n}{\frac{\sqrt{n}}{2}} \in \Theta\big(n^{\sqrt{n}/4}n^{-9/4}(2e)^{\sqrt{n}/2}\big),$$

$$\mathrm{ssgap}_{\mathbb{L}}(\mathcal{TL}_n^{\leq k}) \geq \frac{n-\sqrt{n}+1}{n-\sqrt{n}/2+1}\binom{n}{\frac{\sqrt{n}}{2}} \in \Theta\big(n^{\sqrt{n}/4}n^{-3/4}(2e)^{\sqrt{n}/2}\big),$$

$$\mathrm{faith}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}) \geq \frac{6}{n+4}\binom{n}{\frac{n'}{2}-1} \in \Theta\big(2^n n^{-3/2}\big),$$

where in the final bound $n' = n$, if n is even, and $n' = n-1$, if n is odd.

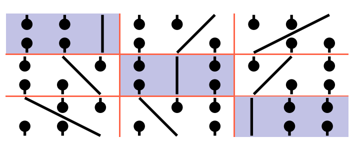
Proof. Similar to the proof of Theorem 4E.2 and omitted. (The assumption $n \geq 8$ ensures that $k \geq 3$, so we can use Lemma 4D.14.) □

Example 4E.5. The various ratios from Section 2F are easy to compute using Proposition 4B.3, which gives $|\mathcal{TL}_{16}^{\leq 8}| = \sum_{l\in\Lambda,l\geq k}|\mathcal{J}_l|$, and either of the theorems above. Explicitly, for $n = 16$, $k = 2\sqrt{16} = 8$ and using $\mathbb{K} = \mathbb{Q}$, which is the setting from Theorem 4E.2, we get $\mathrm{gapr}_{\mathbb{Q}}(\mathcal{TL}_{16}^{\leq 8}) \geq 1.686 \cdot 10^{-3}$. For comparison, the symmetric group $\mathcal{S}_{16}$ has $\mathrm{gapr}_{\mathbb{Q}}(\mathcal{S}_{16}) \approx 2.186 \cdot 10^{-7}$.

4F. **Other planar monoids.** Let us now discuss cells, simples and bounds for the other planar monoids from (1E.2) 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. [HJ20].

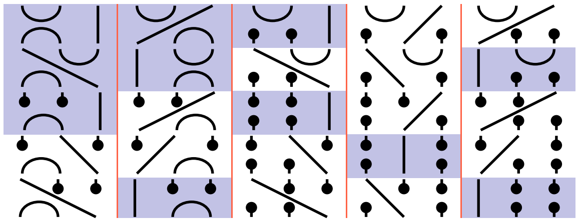
Remark 4F.1. As we will see, the common theoretical feature of planar monoids is that their H-cells are all of size one. As for the Temperley–Lieb monoid, the diagrammatically firm readers can deduce the cell structure of the planar diagram monoids in this section themselves. There are also many references in the literature and the cells of these diagram monoids have been rediscovered many times. For example, [DEG17] computes the cells of $\mathrm{p}\mathcal{R}\mathrm{o}_n$, and [BH14] computes the cells of $\mathcal{M}\mathrm{o}_n$.

We leave the case of the *planar symmetric group* to the reader and start with the *planar rook monoid* $\mathrm{p}\mathcal{R}\mathrm{o}_n$. This monoid was rediscovered several times, see e.g. [KS15], and the reader might know it under a different name. The construction of $\mathrm{p}\mathcal{R}\mathrm{o}_n$ is almost the same as for $\mathcal{TL}_n$, 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 $\mathrm{p}\mathcal{R}\mathrm{o}_n$ has $\binom{2n}{n}$ elements and a typical cell is of the form

(4F.2) $\mathcal{J}_1$  $\mathcal{H}(e) \cong \mathcal{S}_1$.

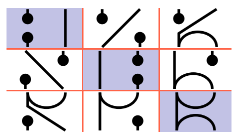
This illustrates $\mathcal{J}_1$ of $\mathrm{p}\mathcal{R}\mathrm{o}_3$, which has one through strand.

The monoid containing both $\mathcal{TL}_n$ and $\mathrm{p}\mathcal{R}\mathrm{o}_n$ as submonoids is the *Motzkin monoid* $\mathcal{M}\mathrm{o}_n$. The definition of this monoid works mutatis mutandis as for $\mathcal{TL}_n$ and $\mathrm{p}\mathcal{R}\mathrm{o}_n$, 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

$\mathcal{J}_1$  $\mathcal{H}(e) \cong \mathcal{S}_1$.

This illustrates $\mathcal{J}_1$ and $\mathcal{M}\mathrm{o}_3$.

Finally, the *planar partition monoid* $\mathrm{p}\mathcal{P}\mathrm{a}_n$ has all of the above mentioned planar monoids as submonoids, as it allows now arbitrary partitions, and has $Ca(2n)$ 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 $\mathrm{p}\mathcal{P}\mathrm{a}_2$ is:

$\mathcal{J}_1$  $\mathcal{H}(e) \cong \mathcal{S}_1$.

In the following we will focus on $\mathrm{p}\mathcal{R}\mathrm{o}_n$ and $\mathcal{M}\mathrm{o}_n$ as justified by our discussion of the Temperley–Lieb monoid and:

Lemma 4F.3. *There is an isomorphism of monoids* $\mathrm{p}\mathcal{P}\mathrm{a}_n \cong \mathcal{TL}_{2n}$.

Proof. See [HR05, (1.5)]. □

Not surprisingly, the analogs of Proposition 4B.3 and Proposition 4F.5 read almost the same. Below, if not stated otherwise, let $\mathcal{X}$ be either $\mathrm{p}\mathcal{R}\mathrm{o}_n$ or $\mathcal{M}\mathrm{o}_n$.

Proposition 4F.4. *We have the following.*

(a) *The left and right cells of* $\mathcal{X}$ *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*

$$\mathrm{p}\mathcal{R}\mathrm{o}_n\colon |\mathcal{L}| = |\mathcal{R}| = \binom{n}{k},$$
$$\mathcal{M}\mathrm{o}_n\colon |\mathcal{L}| = |\mathcal{R}| = \sum_{t=0}^{n}\frac{k+1}{k+t+1}\binom{n}{k+2t}\binom{k+2t}{t}.$$

(b) *The* J*-cells* $\mathcal{J}_k$ *of* $\mathcal{X}$ *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* $\mathcal{L}\subset\mathcal{J}_k$ *we have*

$$\mathcal{X}\colon |\mathcal{J}_k| = |\mathcal{L}|^2.$$

(c) *Each* J*-cell of* $\mathcal{X}$ *is idempotent, and* $\mathcal{H}(e)\cong 1$ *for all idempotent* H*-cells. We have*

$$\mathcal{X}\colon |\mathcal{H}| = 1.$$

Proof. Omitted. See also [HJ20, Section 3.3]. Note that the reference gives the dimensions of the simple p$\mathcal{R}$o$_n$- and $\mathcal{M}$o$_n$-representations in the semisimple case, which are thus the sizes of the corresponding cells, see Proposition 3C.6. □

Proposition 4F.5. *The set of apexes for simple $\mathcal{X}$-representations can be indexed* 1:1 *by the poset* $\Lambda = (\{n, n-1, \dots\}, >)$*, and there is precisely one simple $\mathcal{X}$-representation of a fixed apex up to* $\cong$.

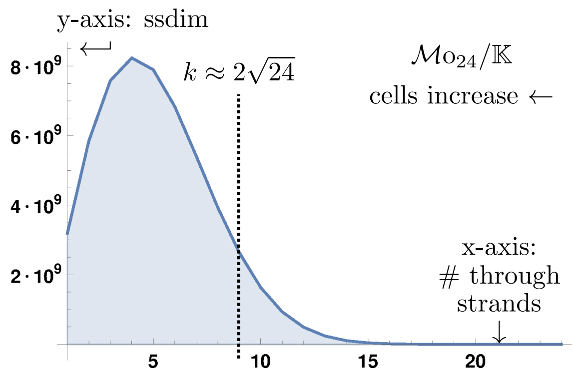
Proof. Clear by Proposition 4F.4. □

We can number the simple $\mathcal{X}$-representations by L_k for $k \in \Lambda$.

Proposition 4F.6. *The semisimple dimensions for* p$\mathcal{R}$o$_n$ *and* $\mathcal{M}$o$_n$ *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 4F.4 and Proposition 4F.5. □

The semisimple dimensions of p$\mathcal{R}$o$_n$ are given in (4C.4). (Note that (4C.4) shows the dimensions of the simple p$\mathcal{R}$o$_n$-representations, but we will see in Proposition 4F.7 that $\dim_{\mathbb{K}}(L_k) = \mathrm{ssdim}_{\mathbb{K}}(L_k)$ holds for p$\mathcal{R}$o$_n$.) The semisimple dimensions of $\mathcal{M}$o$_n$ behave similarly as the semisimple dimensions of $\mathcal{TL}_n$, cf. (4C.4):



,

$$\mathrm{ssdim}\colon \begin{pmatrix} 3192727797, 5850674704, 7583013474, 8234447672, 7895719634, \\ 6839057544, 5412710842, 3938013264, 2641866894, 1636117512, \\ 935163394, 492652824, 238637282, 105922544, 42884259, 15742672, \\ 5199909, 1530144, 395922, 88504, 16674, 2552, 299, 24, 1 \end{pmatrix}.$$

The dimensions of simple p$\mathcal{R}$o$_n$-representations are easy to obtain:

Proposition 4F.7. *We have* $\dim_{\mathbb{K}}(L_k) = \mathrm{ssdim}_{\mathbb{K}}(L_k) = \binom{n}{k}$ *for* p$\mathcal{R}$o$_n$*, and* p$\mathcal{R}$o$_n$ *is semisimple.*

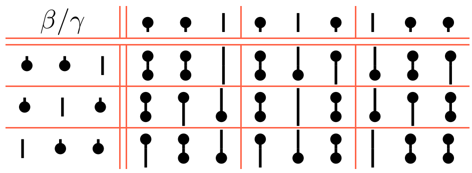
Proof. We only need to prove that p$\mathcal{R}$o$_n$ is semisimple, which implies the other results by Proposition 3C.6 and Proposition 4F.6.

To show semisimplicity we use [St16, 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 3D, for all idempotent H-cell $\mathcal{H}(e)$ are invertible.

By Proposition 4F.4 we only need to compute the Gram matrices. Since $\mathcal{H}(e) \cong \mathcal{S}_1$, 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 paper can be computed using analogs of Lemma 4A.10. Precisely, for each J-cell there are bottom diagrams $\beta_1, \dots, \beta_L$ and top diagrams $\gamma_1, \dots, \gamma_L$ 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 $\mathcal{H}(e) \cong \mathcal{S}_1$. For example, the Gram matrix of $\mathcal{J}_1$ of $\mathrm{p}\mathcal{R}\mathrm{o}_3$, see (4F.2), takes the form



$$\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

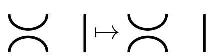
This is the identity matrix. In fact, $P(e)$ is always a permutation matrix: any end dot needs to hit a start dot in order for $\beta_j\gamma_i$ to keep the same number of through strands, and there is precisely one β_j for a fixed γ_i for this to happen. The proof completes.

Alternatively, using an argument from monoid theory, $\mathrm{p}\mathcal{R}\mathrm{o}_n$ is an inverse monoid, namely a submonoid of the symmetric inverse monoid that we will meet in Section 5F. Moreover, by Proposition 4F.4 we have $|\mathcal{H}| = 1$. Thus, [St16, Corollary 9.4] implies that $\mathrm{p}\mathcal{R}\mathrm{o}_n$ is semisimple. □

The behavior of the dimensions of the simple $\mathrm{p}\mathcal{R}\mathrm{o}_n$-representations is sketched in (3F). Sadly, we do not know the dimensions of the simple $\mathcal{M}\mathrm{o}_n$-representations, but we have the following.

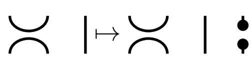
Proposition 4F.8. *Let $L_l^{\mathcal{TL}_n}$ denote the lth simple $\mathcal{TL}_n$-representation, cf. Section 4B. We have $\dim_{\mathbb{K}}(L_k) \geq \dim_{\mathbb{K}}(L_k^{\mathcal{TL}_n})$, if $n-k$ is even, and $\dim_{\mathbb{K}}(L_k) \geq \dim_{\mathbb{K}}(L_k^{\mathcal{TL}_{n-1}})$, if $n-k$ is odd, both for $\mathcal{M}\mathrm{o}_n$.*

Proof. Note that $\mathcal{TL}_n$ embeds into $\mathcal{M}\mathrm{o}_n$ by sending every element to the element with the same description in $\mathcal{M}\mathrm{o}_n$, e.g. :

(4F.9) $\mathcal{TL}_3 \ni$  $\in \mathcal{M}\mathrm{o}_3$.

Thus, $\mathcal{TL}_n$ is a submonoid of $\mathcal{M}\mathrm{o}_n$ and Theorem 3D.2 applies whenever $n-k$ is even since in this case $\mathcal{J}_k$ restricts to an idempotent J-cell of $\mathcal{TL}_n$.

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.

$\mathcal{TL}_3 \ni$  $\in \mathcal{M}\mathrm{o}_4$.

Theorem 3D.2 can be easily extended to cover this case as well. □

Lemma 4F.10. *The monoid $\mathcal{X}$ is regular.*

Proof. Using Lemma 3F.6 the claim is easy to verify: for $\mathrm{p}\mathcal{R}\mathrm{o}_n$ and $\mathcal{M}\mathrm{o}_n$ symmetric diagrams with k end and start dots give an idempotent in $\mathcal{J}_k$. See also [DEG17, Section 2] for a proof using regularity. □

This suggests again that we use truncations. Note that $\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l}$ below is constructed using an honest Rees factor, cf. Definition 3F.5, while $\mathcal{M}\mathrm{o}_n^{\leq k}$ is a submonoid of $\mathcal{M}\mathrm{o}_n$.

Definition 4F.11. Define the *k-l truncated planar rook monoid* for $k \leq l$ and the *kth truncated Motzkin monoid* by

$$\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l} = (\mathrm{p}\mathcal{R}\mathrm{o}_n)_{\geq \mathcal{J}_k}/(> \mathcal{J}_l), \quad \mathcal{M}\mathrm{o}_n^{\leq k} = (\mathcal{M}\mathrm{o}_n)_{\geq \mathcal{J}_k}.$$

Let $\mathcal{X}$ be either $\mathrm{p}\mathcal{R}\mathrm{o}_n$ or $\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l}$.

Proposition 4F.12. *Let M be an $\mathcal{X}$-representation. Then any short exact sequence*

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

splits.

Proof. The monoid $\mathrm{p}\mathcal{R}\mathrm{o}_n$ is semisimple, see Proposition 4F.7, so Theorem 2B.10 applies. The case of $\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l}$ follows verbatim as the monoid is also semisimple by the analog of Proposition 4F.7. □

Remark 4F.13. To prove Proposition 4F.12 for the Motzkin monoid and its truncation it suffices to show that they are left-connected: that they are right-connected follows by applying the diagrammatic antiinvolution $\_^*$, that they are null-connected follows from the fact that their J-cells are idempotent, the group of units $\mathcal{G}$ is trivial which implies $\mathrm{H}^1(\mathcal{G}, \mathbb{K}) \cong 0$, and $\mathrm{H}^1(\mathcal{M}\mathrm{o}_n, \mathbb{K}) \cong 0$ as well as its counterpart for $\mathcal{M}\mathrm{o}_n^{\leq k}$ follow from the same arguments as in the proof of Lemma 4D.15.

The following statement is only about $\mathrm{p}\mathcal{R}\mathrm{o}_n$, since we do not know the dimensions of the simple $\mathcal{M}\mathrm{o}_n$-representations.

Theorem 4F.14. *We have*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_n) = n, \quad \mathrm{gap}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l}) = \min\left\{\binom{n}{k}, \binom{n}{l-1}\right\}.$$

Proof. By Theorem 2B.10, Proposition 4F.12 and Proposition 4F.7. □

Theorem 4F.15. *Let k be arbitrary and $l = \lfloor 2\sqrt{n} \rfloor$. We have the following lower bounds:*

$$\mathrm{gap}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq l,<n-l}) = \mathrm{ssgap}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq l,<n-l}) \geq \binom{n}{\lfloor 2\sqrt{n} \rfloor},$$

$$\mathrm{faith}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq l,<n-l}) \geq \sqrt[2\lfloor\sqrt{n}\rfloor+1]{\binom{n}{\lfloor \frac{n}{2} \rfloor}},$$

$$\mathrm{ssgap}_{\mathbb{K}}(\mathcal{M}\mathrm{o}_n^{\leq k}) \geq \mathrm{ssgap}_{\mathbb{L}}(\mathcal{TL}_{n-1}^{\leq k}), \quad \mathrm{faith}_{\mathbb{K}}(\mathcal{M}\mathrm{o}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{K}}(\mathcal{TL}_{n-1}^{\leq k}).$$

Because of Proposition 4F.8, we also think that $\mathrm{gap}_{\mathbb{K}}(\mathcal{M}\mathrm{o}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathcal{TL}_{n-1}^{\leq k})$. We cannot prove this since we would need the analog of Proposition 4F.12 for the Motzkin monoid.

Proof. Planar rook. We start with $\mathrm{p}\mathcal{R}\mathrm{o}_n$. The first inequality is immediate from Proposition 4F.7 and the behavior of binomial coefficients. For the second claim we apply Theorem 3E.4. Note that $\mathcal{TL}_n^{\leq l,n-l}$ 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 4E.2.

Motzkin. The first claim follows also from Theorem 4E.2 by identifying the smallest cell of Temperley–Lieb as a subcell of the smallest cell of $\mathcal{M}\mathrm{o}_n^{\leq k}$. The final inequality follows then from Proposition 4F.8, Theorem 3E.4 and Theorem 4E.2. (Note that using $n-1$ is for convenience so that state a closed formula independent of even and odd issues.) □

Example 4F.16. As before for the Temperley–Lieb monoid, the various ratios are easy to get from the above. For example, $\mathrm{gap}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_{16}^{\leq 6,<10}) \approx 0.34$.

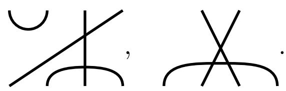
Conclusion 4F.17. From the viewpoint of linear attacks using small representations, all of the planar monoids $\mathrm{p}\mathcal{R}\mathrm{o}_n$, $\mathcal{TL}_n$, $\mathcal{M}\mathrm{o}_n$ and $\mathrm{p}\mathcal{P}\mathrm{a}_n$, or actually their truncations, have only big nontrivial representations. However, $\mathcal{TL}_n$ is our main example: $\mathrm{p}\mathcal{R}\mathrm{o}_n$ appears to be a bit too simple as a monoid to be of use and is semisimple, and $\mathrm{p}\mathcal{P}\mathrm{a}_n$ is just $\mathcal{TL}_{2n}$. The discussion about $\mathcal{M}\mathrm{o}_n$ is unfinished and deserves more study.

5. Symmetric monoids

We still have a fixed field $\mathbb{K}$.

5A. **Brauer categories and monoids.** We will now recall the definitions of the *Brauer category* $\mathbf{Br}^{lin}(\delta)$, the *Brauer algebra* $\mathcal{B}\mathrm{r}_n^{lin}(\delta)$ and explain how to construct set-based versions of these. Brauer categories and algebras are classical topics in representation theory, see e.g. [Br37] for the original reference. Moreover, the discussion is quite similar to the one in Section 4, 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 built 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 $b(k) = (2k-1)!!$ (the double factorial). Letting P_m^n denote the set of perfect matching with m bottom and n top boundary points, we have the following analog of Lemma 4A.3:

Lemma 5A.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 $m \not\equiv n \bmod 2$, or 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. [GL96, Lemma 4.4]. □

The Brauer algebra on n-strands is then $\mathcal{B}\mathrm{r}_n^{lin}(\delta) = \mathrm{End}_{\mathbf{Br}^{lin}(\delta)}(n)$.

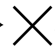
Remark 5A.2. Similar as $\mathcal{TL}_n^{lin}(\delta)$, the algebra $\mathcal{B}\mathrm{r}_n^{lin}(\delta)$ originates in Schur–Weyl–Brauer duality [Br37]. See e.g. [AST17, Section 3.4] for a summary of these dualities.

The definition of the set theoretical version of these works verbatim as in Definition 4A.7. We then get the *set-theoretic Brauer category* $\mathbf{Br}$ and the *Brauer monoid* on n-strands is defined by $\mathcal{B}\mathrm{r}_n = \mathrm{End}_{\mathbf{Br}}(n)$. This monoid has $(2n-1)!!$ elements.

Lemma 5A.3. *Sending the $\mathbb{K}$-linear basis from Lemma* 4A.3 *to crossingless matching in P_m^n from Lemma* 5A.1 *defines an embedding of monoids $\mathcal{TL}_n \hookrightarrow \mathcal{B}\mathrm{r}_n$.*

Proof. Clear by the respective lemmas. □

Note that the symmetric group $\mathcal{S}_n$ on n-strands is isomorphic to the group of units $\mathcal{G}$ of $\mathcal{B}\mathrm{r}_n$. An isomorphism is given by the map

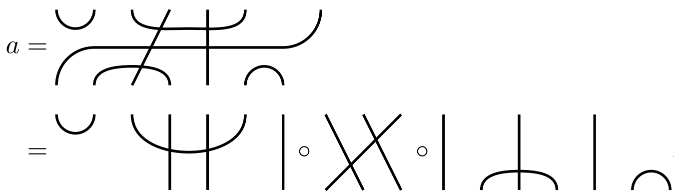
$$\mathcal{S}_n \hookrightarrow \mathcal{B}\mathrm{r}_n, \quad (i, i+1) \mapsto$$  ,

where the crossing crosses the ith and the $(i+1)$th strand when read from left to right. We will use this to identify $\mathcal{S}_n$ with the respective subgroup of $\mathcal{B}\mathrm{r}_n$ and with the corresponding set of morphisms in **Br**.

The analog of Lemma 4A.10 now is:

Lemma 5A.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 $\beta \in \mathrm{Hom}_{\mathbf{Br}}(m,k)$, $\sigma_k \in \mathcal{S}_n$ and $\gamma \in \mathrm{Hom}_{\mathbf{Br}}(k,n)$.*

Proof. Very similar to the proof of Lemma 4A.10. The picture now is



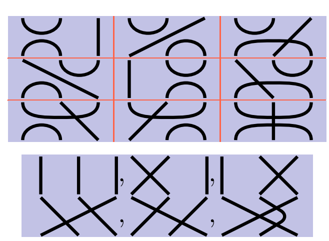
which one easily generalizes to prove the lemma. Note that one can always push crossing in the middle unless they have to cross a cap or cup. ☐

We apply the same terminology as for $\mathcal{B}\mathrm{r}_n$ regarding through strands, bottom half and top half. As before for $\mathcal{TL}_n$, this notion will give us the cell structure of $\mathcal{B}\mathrm{r}_n$.

5B. **Cells of the Brauer monoid.** The cell structure of the Brauer monoid is as follows.

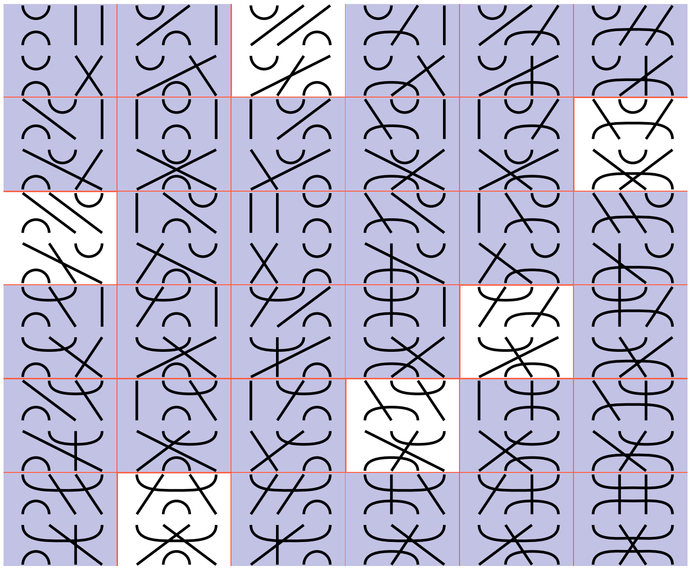
Remark 5B.1. As for all the other monoids we have seen, the computation of the cells of $\mathcal{B}\mathrm{r}_n$ is easy and a pleasant exercise. And, as before, there are plenty of references on the cell structure, see [Br55] for an early reference, [FG95] for a reference from quantum algebra and [KMM06] for a reference from monoid theory.

The picture for the cell structure of $\mathcal{B}\mathrm{r}_n$ is now:

$\mathcal{J}_1$  $\mathcal{H}(e) \cong \mathcal{S}_1$

$\mathcal{J}_3$ $\mathcal{H}(e) \cong \mathcal{S}_3$.

These are the cells of $\mathcal{B}\mathrm{r}_3$. Here is another example, where $\mathcal{H}(e) \cong \mathcal{S}_2$:

$\mathcal{J}_2$  $\mathcal{H}(e) \cong \mathcal{S}_2$.

This illustrated the cell $\mathcal{J}_2$ in $\mathcal{B}\mathrm{r}_4$.

Formally and with contrast to Proposition 4B.3, we have now nontrivial H-cells:

Proposition 5B.2. *We have the following.*

(a) *The left and right cells of $\mathcal{B}\mathrm{r}_n$ 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 $\mathcal{B}\mathrm{r}_n$ 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 $\mathcal{L} \subset \mathcal{J}_k$ we have*

$$|\mathcal{J}_k| = \tfrac{1}{k!}|\mathcal{L}|^2.$$

(c) *Each J-cell of $\mathcal{B}\mathrm{r}_n$ is idempotent, and $\mathcal{H}(e) \cong \mathcal{S}_k$ 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 $\mathcal{B}\mathrm{r}_n$ do not correspond to the cells coming from the cellular structure of $\mathcal{B}\mathrm{r}_n^{lin}(\delta)$, but rather from the sandwich cellular structure, cf. [FG95] or [TV21, Section 2D]. ∎

Let $L_{\mathcal{S}_n}/\cong$ denote the set of simple $\mathcal{S}_n$-representations. For $\mathrm{char}(\mathbb{K}) = 0$ it is well-known that $L_{\mathcal{S}_n}/\cong$ 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. [Ma99, Section 3.4] for an even more general statement.

Proposition 5B.3. *The set of apexes for simple $\mathcal{B}\mathrm{r}_n$-representations can be indexed* 1:1 *by the poset* $\Lambda = (\{n, n-2, \dots\}, >)$*, and*

$$\{\textit{simple } \mathcal{B}\mathrm{r}_n\textit{-representations of apex } k\}/\cong \xleftrightarrow{1:1} L_{\mathcal{S}_k}/\cong .$$

Proof. As before by using Proposition 3B.5 and the cell structure in Proposition 5B.2. ☐

By Proposition 5B.3, we use the same number scheme and poset as for the Temperley–Lieb monoid but also keeping track of $L_K \in L_{\mathcal{S}_k}/\cong$.

Lemma 5B.4. *Within one J-cell all left cell representations $\Delta_{\mathcal{L}}$ and all right cell representations ${}_{\mathcal{R}}\Delta$ are isomorphic. We write Δ_k respectively ${}_k\Delta$ for those in $\mathcal{J}_k$.*

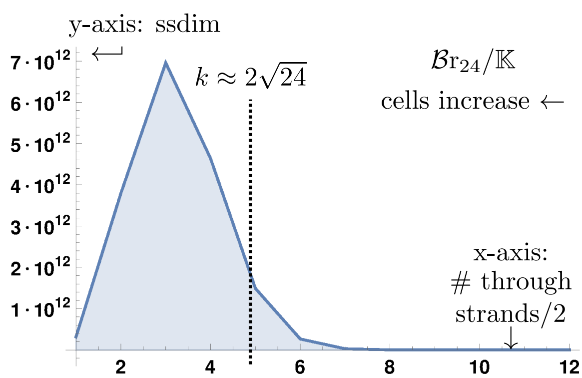
We have $\Delta_k \cong {}_k\Delta$ as $\mathbb{K}$-vector spaces and $\dim_{\mathbb{K}}(\Delta_k) = \dim_{\mathbb{K}}({}_k\Delta) = \binom{n}{k}(n-k-1)!!$.

Proof. Using Proposition 5B.2, the proof is similar to the Temperley–Lieb case. ☐

Proposition 5B.5. *Let K be a simple $\mathcal{S}_k$-representation, and let L_K denote its associated simple $\mathcal{B}\mathrm{r}_n$-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 $\mathcal{S}_k$-representation. ☐

Example 5B.6. The lower bound for the semisimple dimensions of $\mathcal{B}\mathrm{r}_{24}$ can be illustrated by



,

$$\log_{10}(\mathrm{ssdim})\colon \begin{pmatrix} 11.5, 12.5792, 12.8424, 12.6663, 12.1734, 11.4233, \\ 10.4489, 9.26797, 7.88775, 6.30512, 4.50349, 2.44091, 0 \end{pmatrix}.$$

For readability, we took the base 10 log of the actual numbers. This picture again motivates truncation, and we will do this in Section 5C.

Let us discuss the dimensions of simple $\mathcal{B}\mathrm{r}_n$-representations. To the best of our knowledge, the dimensions of simple $\mathcal{B}\mathrm{r}_n$-representations are not known. The best we get is:

Proposition 5B.7. *Let $L_k^{\mathcal{TL}_n}$ denote the kth simple $\mathcal{TL}_n$-representation, cf. Section* 4B*. Let K be a simple $\mathcal{S}_k$-representation and let L_K denote its associated simple $\mathcal{B}\mathrm{r}_n$-representation of apex $\mathcal{J}_k$. We have* $\dim_{\mathbb{K}}(L_K) \geq \dim_{\mathbb{K}}(L_k^{\mathcal{TL}_n})$.

Proof. The Temperley–Lieb monoid $\mathcal{TL}_n$ embeds into $\mathcal{B}\mathrm{r}_n$ by the evident map that diagrammatically is as the one in (4F.9). See also Lemma 5A.3. The proof is thus essentially the same as for $\mathcal{M}\mathrm{o}_n$, see Proposition 4F.8. The difference is that we cannot use Theorem 3D.2 directly, but we instead need to argue slightly differently: First, we use the Brauer algebra $\mathcal{B}\mathrm{r}_n^{lin}(1)$ for circle parameter 1. The monoid algebra of $\mathcal{B}\mathrm{r}_n$ is $\mathcal{B}\mathrm{r}_n^{lin}(1)$, hence, finding dimension bounds for $\mathcal{B}\mathrm{r}_n$ or $\mathcal{B}\mathrm{r}_n^{lin}(1)$ is the same problem. Working with $\mathcal{B}\mathrm{r}_n^{lin}(1)$ 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 [GL96, Section 4]. This can be achieved by using e.g. the Kazhdan–Lusztig bases of the $\mathcal{S}_k$. The sign representation of $\mathcal{S}_k$ in its cell structure corresponds to the bottom cell where there are only through strands. This cell for $\mathcal{B}\mathrm{r}_n^{lin}(1)$ has then $\mathcal{TL}_n^{lin}(1)$ inside and the pairing argument applies. All other simple $\mathcal{B}\mathrm{r}_n^{lin}(1)$-representations associated to $\mathcal{J}_k$ have bigger dimensions, so the proof completes. $\square$

5C. **Truncating the Brauer monoid.** We continue with truncation, which is almost identical as for the Temperley–Lieb monoid in Section 4C.

Lemma 5C.1. *The monoid $\mathcal{B}\mathrm{r}_n$ is regular.*

Proof. The same arguments as in Lemma 5C.1 work. In particular, we can use Lemma 3F.6 and the well-known fact, that is also easy to prove by hand, that $\mathcal{B}\mathrm{r}_n$ has idempotent J-cells, see for example [KMM06, Section 3]. $\square$

Definition 5C.2. Define the *kth truncated Brauer monoid* by

$$\mathcal{B}\mathrm{r}_n^{\leq k} = (\mathcal{B}\mathrm{r}_n)_{\geq \mathcal{J}_k}.$$

Again, let us stress that diagrams in $\mathcal{B}\mathrm{r}_n^{\leq k}$ have at most k through strands. We are almost ready to state our main results, but before we need to discuss extensions.

5D. **Trivial extensions in Brauer monoids.** The following is the same as for $\mathcal{TL}_n$.

Lemma 5D.1. *The monoid $\mathcal{B}\mathrm{r}_n$ is well-connected if $n \geq 5$, and the monoid $\mathcal{B}\mathrm{r}_n^{\leq k}$ is well-connected if $n \geq 5$ and $k \leq 3$.*

Proof. This follows from Lemma 5A.4 and the respective statement about the Temperley–Lieb monoid in Lemma 4D.14. To see this note that the left-connected 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 choose $b = \gamma \circ \sigma_k^{-1} \circ \beta^*$ and get $\gamma \circ id_k \circ \beta \approx_l \gamma \circ \sigma_k \circ \beta$. The same works for right-connected and null-connected. $\square$

We now restrict to a field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) \neq 2$.

Lemma 5D.2. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$. *We have* $\mathrm{H}^1(\mathcal{S}_n, \mathbb{K}) \cong 0$ *for all* $n \in \mathbb{Z}_{\geq 0}$.

Proof. The cases $n = 0, 1$ are clear, so let $n \geq 2$. Recall from Remark 2B.3 that $\mathrm{H}^1(\mathcal{S}_n, \mathbb{K}) \cong 0$ is trivial if and only if the only homomorphism $\mathcal{S}_n \to \mathbb{K}$ is trivial. To see that this is the case, note that any such homomorphism must send the transposition $(i, i+1)$ of $\mathcal{S}_n = \mathrm{Aut}(\{1, \dots, n\})$ to $k \in \mathbb{K}$ with $2k = 0$, which implies $k = 0$. The claim follows since $\mathcal{S}_n$ is generated by transpositions. $\square$

Let $\mathcal{X}$ be either $\mathcal{B}\mathrm{r}_n$ or $\mathcal{B}\mathrm{r}_n^{\leq k}$ for $k \geq 3$.

Lemma 5D.3. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$. *We have* $\mathrm{H}^1(\mathcal{X}, \mathbb{K}) \cong 0$ *for all* $n \in \mathbb{Z}_{\geq 0}$.

Proof. We will use Lemma 5D.2.

Case ($\mathcal{X} = \mathcal{B}\mathrm{r}_n$). Similar to the proof of Lemma 4D.15 with the difference that elements in $\mathcal{J}_b$ are not generated by idempotents, but rather by idempotents and symmetric group generators. Idempotents are sent to zero, as for the Temperley–Lieb monoid, and the symmetric group generators are also sent to zero. These taken together show the claim.

Case ($\mathcal{X} = \mathcal{B}\mathrm{r}_n^{\leq k}$). The argument is also similar to the proof of Lemma 4D.15. In this case diagrams of width k are of the form $a\sigma_k b^*$ where $\sigma_k \in \mathcal{S}_n$. Keeping this in mind as well as $\mathrm{H}^1(\mathcal{S}_k, \mathbb{K}) \cong 0$, the argument given in the proof of Lemma 4D.15 works mutatis mutandis. □

Remark 5D.4. Lemma 5D.3 actually works in arbitrary characteristic. To elaborate, in [EG17] the authors show that every proper ideal of $\mathcal{B}\mathrm{r}_n$ is generated as a semigroup by idempotents. Now, in general, if $\mathcal{S}$ is a monoid containing an ideal I generated by idempotents as a semigroup, then, for any homomorphism $f\colon \mathcal{S} \to \mathbb{K}$, we have $0 = f(I) = f(\mathcal{S}I) = f(\mathcal{S}) + f(I) = f(\mathcal{S})$. This argument really just needs $\mathrm{Hom}(I, \mathbb{K}) \cong 0$, which is a consequence of I being generated by idempotents as a semigroup, and we get the desired $\mathrm{H}^1(\mathcal{B}\mathrm{r}_n, \mathbb{K}) \cong 0$ as a special case. The same arguments work for the truncated version.

Proposition 5D.5. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$. *Let M be an $\mathcal{X}$-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 4D.16 is that the group of units is $\mathcal{G} \cong \mathcal{S}_n$, but that is taken care of in Lemma 5D.2. □

5E. **Representation gap and faithfulness of the Brauer monoid.** The analog of Section 4E is the weaker statement:

Theorem 5E.1. *Let* $\mathrm{char}(\mathbb{K}) \neq 2$. *We have the following lower bounds:*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{B}\mathrm{r}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}),$$

$$\mathrm{ssgap}_{\mathbb{K}}(\mathcal{B}\mathrm{r}_n^{\leq k}) \geq \begin{cases} \mathrm{ssgap}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}) & \textit{always}, \\ (n-1)!! \in \Theta(n^{n/2}e^{n/2}) & \textit{if } n \gg 0, 0 \leq k \leq 2\sqrt{n}, \end{cases}$$

$$\mathrm{faith}_{\mathbb{K}}(\mathcal{B}\mathrm{r}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{K}}(\mathcal{TL}_n^{\leq k}).$$

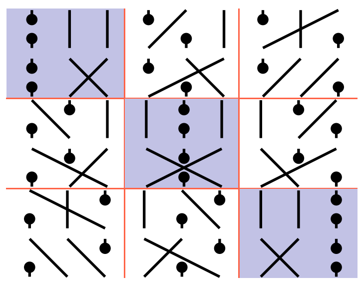
Note that the lower bound $(n-1)!!$ is bigger than the one using $\mathcal{TL}_n$ from Theorem 4E.2.

Proof. Since $\mathcal{TL}_n$ embeds into $\mathcal{B}\mathrm{r}_n$ (see the proof of Proposition 5B.7 or Lemma 5A.3), Proposition 5D.5 and using the arguments from the proof of Proposition 5B.7, most of this theorem follows from the ones for $\mathcal{TL}_n$ or $\mathcal{TL}_n^{\leq k}$. 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 $k = 0$. □

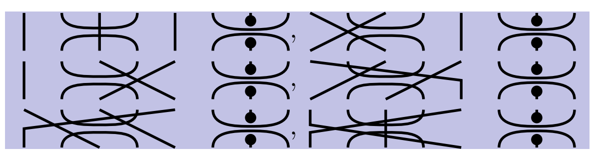
5F. **Other symmetric monoids.** We now discuss the remaining symmetric monoids from (1E.2) in ascending order (of complexity). We will be brief since almost everything follows mutatis mutandis as before. The basics can be found e.g. in [HJ20].

Remark 5F.1. Symmetric monoids have the symmetric groups as H-cells, as we will explain below. As for the planar monoids, the cell structure of the symmetric diagram monoids below is easy to get. See for example [St16, Chapter 9] for many references in the rook monoid case, [HJ20] for the rook-Brauer monoid, and [HR05] for the partition monoid.

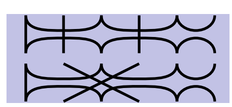
The *symmetric group* was discussed in Example 2A.16, so let us start with the *rook monoid* $\mathcal{R}\mathrm{o}_n$. The rook monoid is the nonplanar version of $\mathrm{p}\mathcal{R}\mathrm{o}_n$ and has $\sum_{k=0}^{n} k!\binom{n}{k}^2$ elements. Its J-cells are again given by through strands. A typical cell is $\mathcal{J}_2$ for $\mathcal{R}\mathrm{o}_3$:

$\mathcal{J}_2$  $\mathcal{H}(e) \cong \mathcal{S}_2$.

The *rook-Brauer monoid* $\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n$ is a symmetric version of the Motzkin monoid. The rook-Brauer monoid has $\sum_{k=0}^{n} k!\big(\sum_{t=0}^{n}\binom{n}{k}\binom{n-k}{2t}(2t-1)!!\big)^2$ 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 $\mathcal{J}_3$  $\mathcal{H}(e) \cong \mathcal{S}_3$.

The *partition monoid* $\mathcal{P}\mathrm{a}_n$ 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 $\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n$, the sizes of the cells are very large, so we only illustrate an idempotent (and symmetric) H-cell:

Part of $\mathcal{J}_2$  $\mathcal{H}(e) \cong \mathcal{S}_2$.

Below, if not stated otherwise, let $\mathcal{X}$ be $\mathcal{R}\mathrm{o}_n$, $\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n$ or $\mathcal{P}\mathrm{a}_n$.

Proposition 5F.2. *We have the following.*

(a) *The left and right cells of $\mathcal{X}$ 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

$$\mathcal{R}\mathrm{o}_n\colon |\mathcal{L}| = |\mathcal{R}| = k!\binom{n}{k},$$
$$\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n\colon |\mathcal{L}| = |\mathcal{R}| = k!\sum_{t=0}^{n}\binom{n}{k}\binom{n-k}{2t}(2t-1)!!,$$
$$\mathcal{P}\mathrm{a}_n\colon |\mathcal{L}| = |\mathcal{R}| = k!\sum_{t=0}^{n}\left\{ {n \atop t} \right\}\binom{t}{k}.$$

Here $\left\{ {n \atop t} \right\}$ denotes the Stirling number of the second kind.

(b) *The J-cells $\mathcal{J}_k$ of $\mathcal{X}$ 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 $\mathcal{L} \subset \mathcal{J}_k$ we have*

$$\mathcal{X}\colon |\mathcal{J}_k| = \tfrac{1}{k!}|\mathcal{L}|^2.$$

(c) *Each J-cell of $\mathcal{X}$ is idempotent, and $\mathcal{H}(e) \cong \mathcal{S}_k$ for all idempotent H-cells in $\mathcal{J}_k$. Within $\mathcal{J}_k$ have*

$$\mathcal{X}\colon |\mathcal{H}| = k!.$$

Proof. Easy and omitted, see also [HJ20, Section 3.3]. □

Proposition 5F.3. *The set of apexes for simple $\mathcal{X}$-representations can be indexed* 1:1 *by the poset $\Lambda = (\{n, n-1, \dots\}, >)$, and*

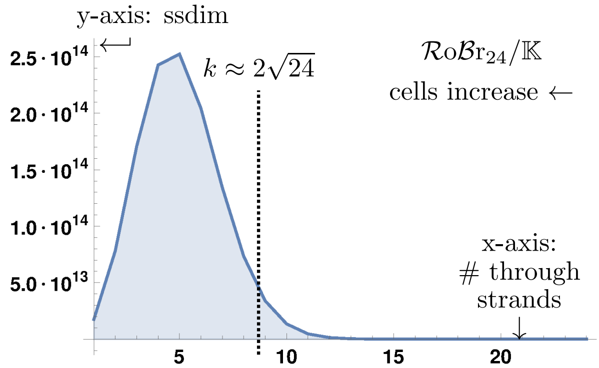
$$\{\textit{simple } \mathcal{X}\textit{-representations of apex } k\}/\cong \xleftrightarrow{1:1} L_{\mathcal{S}_k}/\cong\ .$$

Proof. By Proposition 5F.2. □

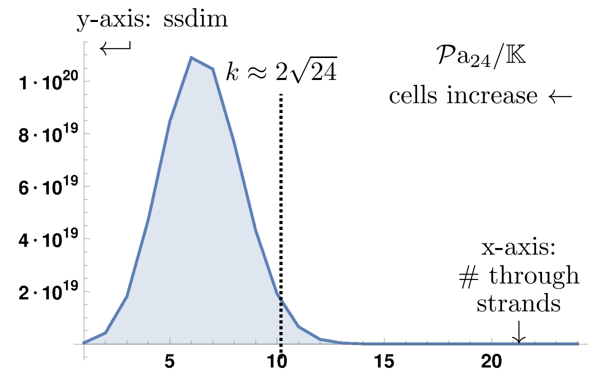
Proposition 5F.4. *Let K be a simple $\mathcal{S}_k$-representation, and let L_K denote its associated simple $\mathcal{X}$-representation of apex $\mathcal{J}_k$. The semisimple dimensions are* $\mathrm{ssdim}_{\mathbb{K}}(L_K) \geq \binom{n}{k}$, $\mathrm{ssdim}_{\mathbb{K}}(L_K) \geq \sum_{t=0}^{n}\binom{n}{k}\binom{n-k}{2t}(2t-1)!!$ *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 5B.5. □

Example 5F.5. As before, let us illustrate the lower bound for the semisimple dimensions:



,



,

$$\text{RoBr } \log_{10}(\text{ssdim}): \begin{pmatrix} 13.2428, 13.8931, 14.2325, 14.3852, 14.4022, 14.3105, \\ 14.1279, 13.8651, 13.5313, 13.1314, 12.671, 12.152, \\ 11.5786, 10.9499, 10.2701, 9.53474, 8.74966, 7.90469, \\ 7.00985, 6.0434, 5.02637, 3.90827, 2.74194, 1.38021, 0 \end{pmatrix},$$

$$\text{Pa } \log_{10}(\text{ssdim}): \begin{pmatrix} 17.6493, 18.6225, 19.2572, 19.6761, 19.9277, 20.0373, \\ 20.0198, 19.8843, 19.6367, 19.2804, 18.8176, 18.2495, \\ 17.5764, 16.7982, 15.9143, 14.9234, 13.8234, 12.6115, \\ 11.2832, 9.83189, 8.24761, 6.51485, 4.60773, 2.47712, 0 \end{pmatrix},$$

where we again took the base 10 log. We have not illustrated the situation for $\mathcal{R}o_n$ as it is the same as for $\mathrm{p}\mathcal{R}o_n$ with semisimple dimensions given by binomial coefficients, cf. (3F).

Let $\mathcal{Y}$ denote $\mathrm{p}\mathcal{R}o_n$, $\mathcal{M}o_n$ or $\mathrm{p}\mathcal{P}a_n$ associated to their respective $\mathcal{X}$.

Lemma 5F.6. *The monoid $\mathcal{X}$ contains $\mathcal{Y}$ as a submonoid, by the analog of* (4F.9).

Proof. Clear, see also Lemma 5A.3. □

Proposition 5F.7. *Let $L_k^{\mathcal{Y}}$ denote the kth simple $\mathcal{Y}$-representation. Let K denote a simple $\mathcal{S}_k$-representation and let L_K denote its associated simple $\mathcal{X}$-representation of apex $\mathcal{J}_k$. We have $\dim_{\mathbb{K}}(L_K^{\mathcal{X}}) \geq \dim_{\mathbb{K}}(L_k^{\mathcal{Y}})$.*

Proof. This follows again by observing that the planar versions embed into their nonplanar counterparts, see Lemma 5F.6. ☐

Proposition 5F.8. *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* $\mathcal{R}\mathrm{o}_n$, *and* $\mathcal{R}\mathrm{o}_n$ *is semisimple.*

Proof. The argument is the same as in Proposition 4F.7 with the additional caveat of the symmetric groups $\mathcal{S}_k$ for $0 \leq k \leq n$ appearing as idempotent H-cells which forces the condition $\mathrm{char}(\mathbb{K}) \nmid n!$. ☐

Lemma 5F.9. *The monoid* $\mathcal{X}$ *is regular.*

Proof. This follows as before from Lemma 3F.6 and a construction of an idempotent for each J-cell. The latter is easy and omitted, but also well-known, see e.g. the references in Remark 5F.1. ☐

Definition 5F.10. Define the *k-l truncated rook monoid* for $k \leq l$ and the *kth truncated rook-Brauer monoid* respectively *k truncated partition monoid* by

$$\mathcal{R}\mathrm{o}_n^{\leq k,<l} = (\mathcal{R}\mathrm{o}_n)_{\geq \mathcal{J}_k}/(> \mathcal{J}_l), \quad \mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n^{\leq k} = (\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n)_{\geq \mathcal{J}_k}, \quad \mathcal{P}\mathrm{a}_n^{\leq k} = (\mathcal{P}\mathrm{a}_n)_{\geq \mathcal{J}_k}.$$

Let $\mathcal{X}$ be either of the above monoids or their truncations. For Theorem 5F.11, note that the *kth truncated planar partition monoid* $\mathrm{p}\mathcal{P}\mathrm{a}_n^{\leq k}$ can be defined in the evident way.

Theorem 5F.11. *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:*

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{R}\mathrm{o}_n^{\leq k,<l}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l}),$$
$$\mathrm{ssgap}_{\mathbb{L}}(\mathcal{R}\mathrm{o}_n^{\leq k,<l}) = \mathrm{ssgap}_{\mathbb{L}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l}), \quad \mathrm{faith}_{\mathbb{L}}(\mathcal{R}\mathrm{o}_n^{\leq k,<l}) \geq \mathrm{faith}_{\mathbb{L}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l}),$$
$$\mathrm{ssgap}_{\mathbb{L}}(\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n^{\leq k}) \geq \begin{cases} \mathrm{ssgap}_{\mathbb{L}}(\mathcal{M}\mathrm{o}_n^{\leq k}) & \textit{always}, \\ \sum_{t=0}^{n} \binom{n}{2t}(2t-1)!! & \textit{if } n \gg 0, 0 \leq k \leq 2\sqrt{n}, \end{cases},$$
$$\mathrm{faith}_{\mathbb{L}}(\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{L}}(\mathcal{M}\mathrm{o}_n^{\leq k}),$$
$$\mathrm{ssgap}_{\mathbb{L}}(\mathcal{P}\mathrm{a}_n^{\leq k}) \geq \begin{cases} \mathrm{ssgap}_{\mathbb{L}}(\mathrm{p}\mathcal{P}\mathrm{a}_n^{\leq k}) & \textit{always}, \\ \sum_{t=0}^{n} \left\{ {n \atop t} \right\} & \textit{if } n \gg 0, 0 \leq k \leq 2\sqrt{n}, \end{cases},$$
$$\mathrm{faith}_{\mathbb{L}}(\mathcal{P}\mathrm{a}_n^{\leq k}) \geq \mathrm{faith}_{\mathbb{L}}(\mathrm{p}\mathcal{P}\mathrm{a}_n^{\leq k}).$$

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

$$\mathrm{gap}_{\mathbb{K}}(\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathcal{M}\mathrm{o}_n^{\leq k}), \quad \mathrm{gap}_{\mathbb{K}}(\mathcal{P}\mathrm{a}_n^{\leq k}) \geq \mathrm{gap}_{\mathbb{K}}(\mathrm{p}\mathcal{P}\mathrm{a}_n^{\leq k}),$$

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 5F.6. The first uses additionally Proposition 5F.8 which also holds for the truncation.

The equality $\mathrm{ssgap}_{\mathbb{K}}(\mathcal{R}\mathrm{o}_n^{\leq k,<l}) = \mathrm{ssgap}_{\mathbb{K}}(\mathrm{p}\mathcal{R}\mathrm{o}_n^{\leq k,<l})$ is clear by Proposition 5F.2. For the semisimple gaps of $\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n$ and $\mathcal{P}\mathrm{a}_n^{\leq k}$ one can use the same arguments as in Theorem 5E.1. ☐

Remark 5F.12. The exact value for $\mathrm{faith}_{\mathbb{L}}(\mathcal{R}\mathrm{o}_n^{\leq k,<l})$ can be computed using [MS12b, Theorems 15 and 17]. The methods from that paper together with [EMRT17] may also be used to compute the faithfulness of other diagram monoids and their truncations.

Conclusion 5F.13. As with the planar monoids, all of the symmetric monoids $\mathcal{R}\mathrm{o}_n$, $\mathcal{B}\mathrm{r}_n$, $\mathcal{R}\mathrm{o}\mathcal{B}\mathrm{r}_n$ and $\mathcal{P}\mathrm{a}_n$ 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 $\mathcal{S}_k$. In fact most of our arguments above use the planar versions to derive bounds.

Acknowledgments

The third author would like to thank Robert Spencer for freely sharing ideas and computations, patiently answering questions and helpful discussions, and twenty-one green bricks for moral support. Special thanks to James East, Joel Gibson, Gus Lehrer, Alexander Moretó, and Geordie Williamson for very helpful comments, several clarifications and many useful reference suggestions. Last but not least, we would like to thank the referee for their careful reading of the manuscript, wonderful suggestions, freely sharing ideas and very useful pointers to the literature. The referee's comments improved the mathematical quality and the exposition of the paper a lot, and, indeed, some of the proofs, examples and remarks are due to the referee.

References

[An19] Henning Haahr Andersen, *Simple modules for Temperley-Lieb algebras and related algebras*, J. Algebra **520** (2019), 276–308, DOI 10.1016/j.jalgebra.2018.10.035. MR3881749

[AST18] Henning Haahr Andersen, Catharina Stroppel, and Daniel Tubbenhauer, *Cellular structures using U_q-tilting modules*, Pacific J. Math. **292** (2018), no. 1, 21–59, DOI 10.2140/pjm.2018.292.21. MR3708257

[AST17] H. H. Andersen, C. Stroppel, and D. Tubbenhauer, *Semisimplicity of Hecke and (walled) Brauer algebras*, J. Aust. Math. Soc., **103** (2017), no. 1, 1–44. `arXiv:1507.07676`, DOI 10.1017/S1446788716000392.

[AAG99] Iris Anshel, Michael Anshel, and Dorian Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Lett. **6** (1999), no. 3-4, 287–291, DOI 10.4310/MRL.1999.v6.n3.a3. MR1713130

[BMKS16] Mohammad Bardestani, Keivan Mallahi-Karai, and Hadi Salmasian, *Minimal dimension of faithful representations for p-groups*, J. Group Theory **19** (2016), no. 4, 589–608, DOI 10.1515/jgth-2016-0003. MR3518394

[BH14] Georgia Benkart and Tom Halverson, *Motzkin algebras*, European J. Combin. **36** (2014), 473–502, DOI 10.1016/j.ejc.2013.09.010. MR3131911

[Be98] D. J. Benson, *Representations and cohomology. I*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, Cambridge, 1998. Basic representation theory of finite groups and associative algebras. MR1644252

[Bi01] S. J. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. **14** (2001), no. 2, 471–486. `arXiv:math/0005038`, DOI 10.1090/S0894-0347-00-00361-1.

[BHMV95] C. Blanchet, N. Habegger, G. Masbaum, and P. Vogel, *Topological quantum field theories derived from the Kauffman bracket*, Topology **34** (1995), no. 4, 883–927, DOI 10.1016/0040-9383(94)00051-4. MR1362791

[Bo20] Elijah Bodish, *Web calculus and tilting modules in type C_2*, Quantum Topol. **13** (2022), no. 3, 407–458, DOI 10.4171/qt/166. MR4537310

[BG08] Jean Bourgain and Alex Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2) **167** (2008), no. 2, 625–642, DOI 10.4007/annals.2008.167.625. MR2415383

[Br37] Richard Brauer, *On algebras which are connected with the semisimple continuous groups*, Ann. of Math. (2) **38** (1937), no. 4, 857–872, DOI 10.2307/1968843. MR1503378

[Br55] Wm. P. Brown, *An algebra related to the orthogonal group*, Michigan Math. J. **3** (1955), 1–22. MR72122

[CGGS20] R. Casals, E. Gorsky, M. Gorsky, and J. Simental, *Algebraic weaves and braid varieties*, 2020. URL: `arXiv:math/0209020`, 2020.

[CKR11] Shane Cernele, Masoud Kamgarpour, and Zinovy Reichstein, *Maximal representation dimension of finite p-groups*, J. Group Theory **14** (2011), no. 4, 637–647, DOI 10.1515/JGT.2010.071. MR2818953

[CP61] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups. Vol. I*, Mathematical Surveys, No. 7, American Mathematical Society, Providence, RI, 1961, xv+224 pp.

[CP67] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups. Vol. II*, Mathematical Surveys, No. 7, American Mathematical Society, Providence, RI, 1967, xv+350 pp.

[CPS88] E. Cline, B. Parshall, and L. Scott, *Finite-dimensional algebras and highest weight categories*, J. Reine Angew. Math. **391** (1988), 85–99. MR961165

[CC19] Alain Connes and Caterina Consani, *Homological algebra in characteristic one*, High. Struct. **3** (2019), no. 1, 155–247. MR3939048

[CCN$^+$85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, $\mathbb{ATLAS}$ *of finite groups*, Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups; With computational assistance from J. G. Thackray. MR827219

[DEG17] Igor Dolinka, James East, and Robert D. Gray, *Motzkin monoids and partial Brauer monoids*, J. Algebra **471** (2017), 251–298, DOI 10.1016/j.jalgebra.2016.09.018. MR3569186

[Du20] M. Durcheva, *Semirings as building blocks in cryptography*, 1st ed., Cambridge Scholars Publishing, Newcastle Upon Tyne, England, 2020.

[Ea21] J. East, *Presentations for Temperley–Lieb algebras*, Q. J. Math. **72** (2021), no. 4, 1253–1269. `arXiv:2101.02862`, DOI 10.1093/qmath/haab001.

[EG17] James East and Robert D. Gray, *Diagram monoids and Graham-Houghton graphs: idempotents and generating sets of ideals*, J. Combin. Theory Ser. A **146** (2017), 63–128, DOI 10.1016/j.jcta.2016.09.001. MR3574225

[EMRT17] James East, James D. Mitchell, Nik Ruškuc, and Michael Torpey, *Congruence lattices of finite diagram monoids*, Adv. Math. **333** (2018), 931–1003, DOI 10.1016/j.aim.2018.05.016. MR3818094

[EST16] M. Ehrig, C. Stroppel, and D. Tubbenhauer, *Generic $\mathfrak{gl}_2$-foams, web and arc algebras*, `arXiv:1601.08010`, 2016.

[EST17] Michael Ehrig, Catharina Stroppel, and Daniel Tubbenhauer, *The Blanchet-Khovanov algebras*, Categorification and higher representation theory, Contemp. Math., vol. 683, Amer. Math. Soc., Providence, RI, 2017, pp. 183–226, DOI 10.1090/conm/683. MR3611714

[ET21] M. Ehrig and D. Tubbenhauer, *Relative cellular algebras*, Transform. Groups **26** (2021), no. 1, 229–277. `arXiv:1710.02851`, DOI 10.1007/S00031-019-09544-5.

[ETW18] Michael Ehrig, Daniel Tubbenhauer, and Paul Wedrich, *Functoriality of colored link homologies*, Proc. Lond. Math. Soc. (3) **117** (2018), no. 5, 996–1040, DOI 10.1112/plms.12154. MR3877770

[El15] B. Elias, *Light ladders and clasp conjectures*, `arXiv:1510.06840`, 2015.

[El16] Ben Elias, *The two-color Soergel calculus*, Compos. Math. **152** (2016), no. 2, 327–398, DOI 10.1112/S0010437X15007587. MR3462556

[EK10] Ben Elias and Mikhail Khovanov, *Diagrammatics for Soergel categories*, Int. J. Math. Math. Sci., posted on 2010, Art. ID 978635, 58, DOI 10.1155/2010/978635. MR3095655

[EMTW20] Ben Elias, Shotaro Makisumi, Ulrich Thiel, and Geordie Williamson, *Introduction to Soergel bimodules*, RSME Springer Series, vol. 5, Springer, Cham, [2020] ©2020, DOI 10.1007/978-3-030-48826-0. MR4220642

[EW16] Ben Elias and Geordie Williamson, *Soergel calculus*, Represent. Theory **20** (2016), 295–374, DOI 10.1090/ert/481. MR3555156

[EGNO15] Pavel Etingof, Shlomo Gelaki, Dmitri Nikshych, and Victor Ostrik, *Tensor categories*, Mathematical Surveys and Monographs, vol. 205, American Mathematical Society, Providence, RI, 2015, DOI 10.1090/surv/205. MR3242743

[FG95] S. Fishel and I. Grojnowski, *Canonical bases for the Brauer centralizer algebra*, Math. Res. Lett. **2** (1995), no. 1, 15–26, DOI 10.4310/MRL.1995.v2.n1.a3. MR1312974

[FLM88] Igor Frenkel, James Lepowsky, and Arne Meurman, *Vertex operator algebras and the Monster*, Pure and Applied Mathematics, vol. 134, Academic Press, Inc., Boston, MA, 1988. MR996026

[GMS09] O. Ganyushkin, V. Mazorchuk, and B. Steinberg, *On the irreducible representations of a finite semigroup*, Proc. Amer. Math. Soc., **137** (2009), no. 11, 3585–3592. `arXiv:0712.2076`, DOI 10.1090/S0002-9939-09-09857-8.

[Go08] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387, DOI 10.1017/S0963548307008826. MR2410393

[GL96] J. J. Graham and G. Lehrer, *Cellular algebras*, Invent. Math. **123** (1996), no. 1, 1–34, DOI 10.1007/BF01232365.

[Gr51] J. A. Green, *On the structure of semigroups*, Ann. of Math. (2) **54** (1951) no. 1, 163–172. DOI 10.2307/1969317.

[GS14] Dima Grigoriev and Vladimir Shpilrain, *Tropical cryptography*, Comm. Algebra **42** (2014), no. 6, 2624–2632, DOI 10.1080/00927872.2013.766827. MR3169729

[GS19] Dima Grigoriev and Vladimir Shpilrain, *Tropical cryptography II: extensions by homomorphisms*, Comm. Algebra **47** (2019), no. 10, 4224–4229, DOI 10.1080/00927872.2019.1581213. MR3976001

[GW15] Nicolas Guay and Stewart Wilcox, *Almost cellular algebras*, J. Pure Appl. Algebra **219** (2015), no. 9, 4105–4116, DOI 10.1016/j.jpaa.2015.02.010. MR3336000

[HJ20] Tom Halverson and Theodore N. Jacobson, *Set-partition tableaux and representations of diagram algebras*, Algebr. Comb. **3** (2020), no. 2, 509–538, DOI 10.5802/alco.102. MR4099006

[HR05] Tom Halverson and Arun Ram, *Partition algebras*, European J. Combin. **26** (2005), no. 6, 869–921, DOI 10.1016/j.ejc.2004.06.005. MR2143201

[Hu92] Bertram Huppert, *A remark on the character-degrees of some p-groups*, Arch. Math. (Basel) **59** (1992), no. 4, 313–318, DOI 10.1007/BF01197044. MR1179454

[JZM02] A. Jaikin-Zapirain and Alexander Moretó, *Character degrees and nilpotence class of finite p-groups: an approach via pro-p groups*, Trans. Amer. Math. Soc. **354** (2002), no. 10, 3907–3925, DOI 10.1090/S0002-9947-02-02992-6. MR1926859

[Ja05] Christoph Jansen, *The minimal degrees of faithful representations of the sporadic simple groups and their covering groups*, LMS J. Comput. Math. **8** (2005), 122–144, DOI 10.1112/S1461157000000930. MR2153793

[Ja70] G. J. Janusz, *Faithful representations of p groups at characteristic p. I*, J. Algebra **15** (1970), 335–351, DOI 10.1016/0021-8693(70)90063-3. MR265482

[KL94] Louis H. Kauffman and Sóstenes L. Lins, *Temperley-Lieb recoupling theory and invariants of 3-manifolds*, Annals of Mathematics Studies, vol. 134, Princeton University Press, Princeton, NJ, 1994, DOI 10.1515/9781400882533. MR1280463

[Kh04] Mikhail Khovanov, *sl(3) link homology*, Algebr. Geom. Topol. **4** (2004), 1045–1081, DOI 10.2140/agt.2004.4.1045. MR2100691

[KK20] M. Khovanov and N. Kitchloo, *A deformation of Robert–Wagner foam evaluation and link homology*, `arXiv:2004.14197`, 2020.

[KL09] Mikhail Khovanov and Aaron D. Lauda, *A diagrammatic approach to categorification of quantum groups. I*, Represent. Theory **13** (2009), 309–347, DOI 10.1090/S1088-4165-09-00346-X. MR2525917

[KL10] Mikhail Khovanov and Aaron D. Lauda, *A categorification of quantum* $\mathrm{sl}(n)$, Quantum Topol. **1** (2010), no. 1, 1–92, DOI 10.4171/QT/1. MR2628852

[KL11] Mikhail Khovanov and Aaron D. Lauda, *A diagrammatic approach to categorification of quantum groups II*, Trans. Amer. Math. Soc. **363** (2011), no. 5, 2685–2700, DOI 10.1090/S0002-9947-2010-05210-9. MR2763732

[KS15] M. Khovanov and R. Sazdanovic, *Categorifications of the polynomial ring*, Fund. Math., **230** (2015), no. 3, 251–280. `arXiv:1101.0293`, DOI 10.4064/fm230-3-3.

[KS21] Mikhail Khovanov and Radmila Sazdanovic, *Diagrammatic categorification of the Chebyshev polynomials of the second kind*, J. Pure Appl. Algebra **225** (2021), no. 6, Paper No. 106592, 23, DOI 10.1016/j.jpaa.2020.106592. MR4171760

[KT19] M. Khovanov and Y. Tian, *How to categorify the ring of integers localized at two*, Quantum Topol. **10** (2019), no. 4, 723–775. `arXiv:1702.07466`, DOI 10.4171/qt/130.

[KLC+00] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park, *New public-key cryptosystem using braid groups*, Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 1880, Springer, Berlin, 2000, pp. 166–183, DOI 10.1007/3-540-44598-6_10. MR1850042

[Ko98] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer-Verlag, Berlin, 1998. With an appendix by Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato. DOI 10.1007/978-3-662-03642-6.

[Kr02] D. Krammer, *Braid groups are linear*, Ann. of Math. (2) **155** (2002), no. 1, 131–156, `arXiv:math/0405198`, DOI 10.2307/3062152.

[KMM06] Ganna Kudryavtseva, Victor Maltcev, and Volodymyr Mazorchuk, *$\mathcal{L}$- and $\mathcal{R}$-cross-sections in the Brauer semigroup*, Semigroup Forum **72** (2006), no. 2, 223–248, DOI 10.1007/s00233-005-0511-3. MR2216091

[Ku96] Greg Kuperberg, *Spiders for rank 2 Lie algebras*, Comm. Math. Phys. **180** (1996), no. 1, 109–151. MR1403861

[LFG06] Kwok Wai Lau and D. G. FitzGerald, *Ideal structure of the Kauffman and related monoids*, Comm. Algebra **34** (2006), no. 7, 2617–2629, DOI 10.1080/00927870600651414. MR2240396

[La10] Aaron D. Lauda, *A categorification of quantum* sl(2), Adv. Math. **225** (2010), no. 6, 3327–3424, DOI 10.1016/j.aim.2010.06.003. MR2729010

[Li08] Nicolas Libedinsky, *Sur la catégorie des bimodules de Soergel* (French, with French summary), J. Algebra **320** (2008), no. 7, 2675–2694, DOI 10.1016/j.jalgebra.2008.05.027. MR2441994

[LPWW98] S. Linton, R. Parker, P. Walsh, and R. Wilson, *Computer construction of the Monster*, J. Group Theory, **1** (1998), no. 4, 307–337, DOI 10.1515/jgth.1998.023.

[MMMT20] Marco Mackaay, Volodymyr Mazorchuk, Vanessa Miemietz, and Daniel Tubbenhauer, *Trihedral Soergel bimodules*, Fund. Math. **248** (2020), no. 3, 219–300, DOI 10.4064/fm566-3-2019. MR4046957

[MMM+19] M. Mackaay, V. Mazorchuk, V. Miemietz, D. Tubbenhauer, and X. Zhang, *Simple transitive 2-representations of Soergel bimodules for finite Coxeter types*, `arXiv:1906.11468`, 2019.

[MMM+21] Marco Mackaay, Volodymyr Mazorchuk, Vanessa Miemietz, Daniel Tubbenhauer, and Xiaoting Zhang, *Finitary birepresentations of finitary bicategories*, Forum Math. **33** (2021), no. 5, 1261–1320, DOI 10.1515/forum-2021-0021. MR4308630

[MT19] Marco Mackaaij and Daniel Tubbenhauer, *Two-color Soergel calculus and simple transitive 2-representations*, Canad. J. Math. **71** (2019), no. 6, 1523–1566, DOI 10.4153/cjm-2017-061-2. MR4028468

[Ma99] Andrew Mathas, *Iwahori-Hecke algebras and Schur algebras of the symmetric group*, University Lecture Series, vol. 15, American Mathematical Society, Providence, RI, 1999, DOI 10.1090/ulect/015. MR1711316

[MS12a] Stuart Margolis and Benjamin Steinberg, *Quivers of monoids with basic algebras*, Compos. Math. **148** (2012), no. 5, 1516–1560, DOI 10.1112/S0010437X1200022X. MR2982439

[MSS21] Stuart Margolis, Franco V. Saliola, and Benjamin Steinberg, *Cell complexes, poset topology and the representation theory of algebras arising in algebraic combinatorics and discrete geometry*, Mem. Amer. Math. Soc. **274** (2021), no. 1345, xi+135, DOI 10.1090/memo/1345. MR4365944

[MSS15] Stuart Margolis, Franco Saliola, and Benjamin Steinberg, *Combinatorial topology and the global dimension of algebras arising in combinatorics*, J. Eur. Math. Soc. (JEMS) **17** (2015), no. 12, 3037–3080, DOI 10.4171/JEMS/579. MR3429159

[Ma17] V. Mazorchuk, *Classification problems in 2-representation theory*, São Paulo J. Math. Sci., **11** (2017), no. 1, 1–22. `arXiv:1703.10093`, DOI 10.1007/s40863-017-0059-7.

[MS12b] Volodymyr Mazorchuk and Benjamin Steinberg, *Effective dimension of finite semigroups*, J. Pure Appl. Algebra **216** (2012), no. 12, 2737–2753, DOI 10.1016/j.jpaa.2012.04.014. MR2943755

[Mo21] A. Moretó, *On the minimal dimension of a faithful linear representation of a finite group*, `arXiv:2102.01463`, 2021.

[MPS17] Scott Morrison, Emily Peters, and Noah Snyder, *Categories generated by a trivalent vertex*, Selecta Math. (N.S.) **23** (2017), no. 2, 817–868, DOI 10.1007/s00029-016-0240-3. MR3624901

[MR15] Alexei Myasnikov and Vitaliĭ Roman'kov, *A linear decomposition attack*, Groups Complex. Cryptol. **7** (2015), no. 1, 81–94, DOI 10.1515/gcc-2015-0007. MR3341508

[MSU05] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov, *A practical attack on a braid group based cryptographic protocol*, Advances in cryptology—CRYPTO 2005, Lecture Notes in Comput. Sci., vol. 3621, Springer, Berlin, 2005, pp. 86–96, DOI 10.1007/11535218_6. MR2237301

[MSU08] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov, *Group-based cryptography*, Advanced Courses in Mathematics. CRM Barcelona, Birkhäuser Verlag, Basel, 2008. MR2437984

[MSU11] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov, *Non-commutative cryptography and complexity of group-theoretic problems*, Mathematical Surveys and Monographs, vol. 177, American Mathematical Society, Providence, RI, 2011. With an appendix by Natalia Mosina, DOI 10.1090/surv/177. MR2850384

[Ni71] William R. Nico, *Homological dimension in semigroup algebras*, J. Algebra **18** (1971), 404–413, DOI 10.1016/0021-8693(71)90070-6. MR277626

[Pu98] Mohan S. Putcha, *Complex representations of finite monoids. II. Highest weight categories and quivers*, J. Algebra **205** (1998), no. 1, 53–76, DOI 10.1006/jabr.1997.7395. MR1631310

[RS21] N. Rahman and V. Shpilrain, *MOBS (Matrices Over Bit Strings) public key exchange*, `arXiv:2106.01116`, 2021.

[RS09] John Rhodes and Benjamin Steinberg, *The q-theory of finite semigroups*, Springer Monographs in Mathematics, Springer, New York, 2009, DOI 10.1007/b104443. MR2472427

[RSA14] David Ridout and Yvan Saint-Aubin, *Standard modules, induction and the structure of the Temperley-Lieb algebra*, Adv. Theor. Math. Phys. **18** (2014), no. 5, 957–1041. MR3281274

[RW20] Louis-Hadrien Robert and Emmanuel Wagner, *A closed formula for the evaluation of foams*, Quantum Topol. **11** (2020), no. 3, 411–487, DOI 10.4171/qt/139. MR4164001

[Ro18] Vitaly Roman'kov, *Two general schemes of algebraic cryptography*, Groups Complex. Cryptol. **10** (2018), no. 2, 83–98, DOI 10.1515/gcc-2018-0009. MR3871466

[Ro08] R. Rouquier, 2-*Kac–Moody algebras*, `arXiv:0812.5023`, 2008.

[RTW32] G. Rumer, E. Teller, and H. Weyl, *Eine für die Valenztheorie geeignete Basis der binären Vektorinvarianten* (German), Nachrichten von der Ges. der Wiss. Zu Göttingen. Math.-Phys. Klasse, 1932, pp. 498–504.

[Se11] P. Selinger, *A survey of graphical languages for monoidal categories*, New structures for physics, Lecture Notes in Phys., vol. 813, Springer, Heidelberg, 2011, pp. 289–355, DOI 10.1007/978-3-642-12821-9_4. MR2767048

[SZ06] V. Shpilrain and G. Zapata, *Combinatorial group theory and public key cryptography*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 3-4, 291–302. URL: `arXiv:math/0410068`, DOI 10.1007/s00200-006-0006-9.

[Si20] M. Sitaraman, *Topological actions of Temperley–Lieb algebras and representation stability*, `arXiv:2008.09636`, 2020.

[So92] Wolfgang Soergel, *The combinatorics of Harish-Chandra bimodules*, J. Reine Angew. Math. **429** (1992), 49–74, DOI 10.1515/crll.1992.429.49. MR1173115

[Sp20] Robert A. Spencer, *The modular Temperley-Lieb algebra*, Rocky Mountain J. Math. **53** (2023), no. 1, 177–208, DOI 10.1216/rmj.2023.53.177. MR4585987

[Sp21] R. A. Spencer, *Modular valenced Temperley–Lieb algebras*, `arXiv:2108.10011`, 2021.

[St14] B. Steinberg, *On the Burnside–Brauer–Steinberg theorem*, `arXiv:1409.7632`, 2014.

[St16] Benjamin Steinberg, *Representation theory of finite monoids*, Universitext, Springer, Cham, 2016, DOI 10.1007/978-3-319-43932-7. MR3525092

[St05] E. Stickel, *A new method for exchanging secret keys*, Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), vol. 2, IEEE Computer Society, Washington, DC, 2005, pp. 426–430.

[STWZ21] Louise Sutton, Daniel Tubbenhauer, Paul Wedrich, and Jieru Zhu, SL_2 *tilting modules in the mixed case*, Selecta Math. (N.S.) **29** (2023), no. 3, Paper No. 39, 40, DOI 10.1007/s00029-023-00835-0. MR4587641

[TV17] Vladimir Turaev and Alexis Virelizier, *Monoidal categories and topological field theory*, Progress in Mathematics, vol. 322, Birkhäuser/Springer, Cham, 2017, DOI 10.1007/978-3-319-49834-8. MR3674995

[Tu22] D. Tubbenhauer, *Sandwich cellularity and a version of cell theory*, `arXiv:2206.06678`, 2022.

[TV21] Daniel Tubbenhauer and Pedro Vaz, *Handlebody diagram algebras*, Rev. Mat. Iberoam. **39** (2023), no. 3, 845–896, DOI 10.4171/rmi/1356. MR4603639

[TW21] Daniel Tubbenhauer and Paul Wedrich, *Quivers for* SL_2 *tilting modules*, Represent. Theory **25** (2021), 440–480, DOI 10.1090/ert/569. MR4273168

[TW22] D. Tubbenhauer and P. Wedrich, *The center of* SL_2 *tilting modules*, Glasg. Math. J. **64** (2022), no. 1, 165–184. `arXiv:2004.10146`, DOI 10.1017/S001708952100001X.

[WM85] Neal R. Wagner and Marianne R. Magyarik, *A public-key cryptosystem based on the word problem*, Advances in cryptology (Santa Barbara, Calif., 1984), Lecture Notes in Comput. Sci., vol. 196, Springer, Berlin, 1985, pp. 19–36, DOI 10.1007/3-540-39568-7_3. MR820010

[Wa08] Lawrence C. Washington, *Elliptic curves*, 2nd ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008. Number theory and cryptography, DOI 10.1201/9781420071474. MR2404461

Department of Mathematics, Columbia University, New York, New York 10027
Email address: `khovanov@math.columbia.edu`

Department of Mathematics, Columbia University, New York, New York 10027
Email address: `maithreya@math.columbia.edu`

School of Mathematics and Statistics F07, The University of Sydney, Office Carslaw 827, New South Wales 2006, Australia
Email address: `daniel.tubbenhauer@sydney.edu.au`
URL: `www.dtubbenhauer.com`
ORCID: 0000-0001-7265-5047