REPRESENTATION GAPS OF RIGID PLANAR DIAGRAM MONOIDS

WILLOW STEWART AND DANIEL TUBBENHAUER

Abstract. We define non-pivotal analogs of the Temperley–Lieb, Motzkin, and planar rook monoids, and compute bounds for the sizes of their nontrivial simple representations. From this, we assess the two types of monoids in their relative suitability for use in cryptography by comparing their representation gaps and gap ratios. We conclude that the non-pivotal monoids are generally worse for cryptographic purposes.

Contents

1. Introduction

The main question of this paper is how representations behave when a pivotal structure is relaxed to a rigid, yet non-pivotal, one. Our primary objects of study are (partially) novel diagram categories that serve as non-pivotal analogs of classical diagram categories, such as the Temperley—Lieb category.

1A. **Setting the stage: diagram monoids and representation gaps.** Motivated by the problem of developing cryptographic protocols based on finite noncommutative monoids, [KST24] developed a framework to connect monoidal categories and cryptography. Noncommutative monoids are often vulnerable to *linear attacks*: an attacker can convert a protocol operating in such a monoid into a linear algebra problem, enabling the use of powerful linear algebra techniques to break the encryption; see e.g. [MR15] for examples. Converting such a protocol to linear algebra requires a nontrivial, say simple or faithful, representation of the monoid. In short, a cryptographic protocol based on a noncommutative monoid can be bypassed by targeting the nontrivial simple representations, so if these are too low in dimension, the protocol will not be secure. The security of such a protocol can be roughly measured by the ***representation gap (RepGap)***. As such, it is important to find monoids with large RepGaps. There are also many other reasons to study these numerical invariants of monoids, see, for example, [BG08, Go08].

Monoidal categories provide a wealth of such monoids, since each object X provides an endomorphism monoid $\mathrm{End}(X^{\otimes n})$ for each $n \in \mathbb{Z}_{\geq 0}$, and by the Schur–Weyl dual of [COT24] it is expected that their representations grow exponentially. In particular, [KST24, Section 4 & 5] discusses *diagram monoids*, which arise from endomorphisms of subcategories of the partition category. These are split into the *symmetric* monoids, namely the partition monoid, rook Brauer monoid, Brauer monoid, rook monoid, and symmetric monoid (group), and their *planar* counterparts, the planar

2020 *Mathematics Subject Classification.* Primary: 18D10, 20M30, Secondary: 05A16, 94A60.
Key words and phrases. Diagram categories, monoid/semigroup representations, representation gap, cryptography.

partition monoid, Motzkin monoid, Temperley–Lieb monoid, planar rook monoid, and planar symmetric monoid (the trivial group). The main tools for computing the representations of these monoids and their dimensions are based on *cell theory (a.k.a. Green's relations)* as in [Gr51].

The paper [KST24] primarily explores planar monoids, noting that symmetric monoids may be less suitable for cryptographic applications than their planar counterparts. While this hypothesis remains unproven, it raises the question of how categorical structures, such as symmetry, in a monoidal category influence the RepGap (see e.g. [EGNO15] or, more diagrammatic, [Tub22] for background on such structures). This is where our story starts: The monoidal categories above (excluding the rook categories and those for the groups) are *pivotal*, meaning every object X has a left and right dual, which essentially means that the category is *rigid*, and further the double dual of X is isomorphic to X. A natural generalization is to consider *non-pivotal*, rigid monoidal categories as a potential source of monoids for cryptographic purposes. These are, in a sense, more "complicated" than pivotal monoidal categories: For example, the Temperley–Lieb category is equivalent to the category $Rep(SL_2)$ of finite dimensional representations of the special linear group (a classic result; see [RTW32]) or quantum versions of the group SL_2, and Schur–Weyl duality arguments [Er95, So99, AST18] then imply that the RepGap problem can be solved using representation theory of SL_2. No such equivalence exists for any non-pivotal, rigid monoidal category and finite dimensional representations of any group G.

Remark 1A.1. To avoid confusion, note that in the classical diagram categories under discussion, the object X is self-dual. Relaxing this assumption, while retaining pivotality, would, for example, require introducing an orientation. However, this is *not* what we do here: we break the symmetry of left and right duals, and, as far as we can tell, the categories and monoids we study are (partially) new. Importantly, we expect that passing to oriented versions of the classical diagram categories does not affect the RepGap. For a related result, see [GT25] for the Schur–Weyl dual statement in the context of the Brauer category. ◇

This paper begins the study of this with non-pivotal, rigid analogs of some of the planar diagram monoids above, namely the Temperley–Lieb monoid, Motzkin monoid, and the planar rook monoid. The rigid Temperley–Lieb category, as we define it, has been studied as the free rigid monoidal category, for example in [CSB21, St21, Tub22]. As far as we are aware, there is no existing definition for a rigid analog for the Motzkin monoid. Since the planar rook category has no duals, we treat it as a two-color submonoid of the rigid Motzkin monoid. We directly ignore the planar partition monoid and the planar symmetric monoid, as the former is isomorphic to the even-strand Temperley–Lieb monoids, see [HR05], and the latter is isomorphic to the trivial group.

1B. **Results.** One might assume that a more complicated monoidal category would translate to more secure cryptographic protocols; however, ***surprisingly***, we find that the RepGap and gap ratio (=the RepGap normalized by the order of the monoid; we want this to drop to zero as slow as possible) are largely worse for the non-pivotal diagram monoids. The asymptotic behavior of these is summarized in the table below (more precise results are given in the main body of the paper), with the pivotal monoids on the left and the non-pivotal monoids on the right. We also colored the quantities that are larger when comparing between non-pivotal and pivotal.

Monoid	RepGap	Gap Ratio	Monoid	RepGap	Gap Ratio
TL_{2n}	$\geq \Theta(n^{-5/2} \cdot 4^n)$	$\leq \Theta(n^{-3/4})$	rTL_{2n}	$\leq \Theta(n^{-1/2} \cdot 2^n)$	$\geq \Theta(n^{-1/4} e^{-1/n})$
Mo_{2n}	$\mathrm{Gap}^{1/n} \to 9$	$\mathrm{Ratio}^{1/n} \to 1$	rMo_{2n}	$\mathrm{Gap}^{1/n} \to 4$	$\mathrm{Ratio}^{1/n} \to 1$
pRo_{2n}	$\geq \Theta(n^{-1/2} e^{-1/n} \cdot 4^n)$	$\geq \Theta(n^{-1/4} e^{-1/n})$	$rpRo_{2n}$	$\leq \Theta(n^{-1/2} \cdot 2^n)$	$\leq \Theta(0.87^n)$

Focusing on the Temperley–Lieb monoid, we see that while the gap ratio for the non-pivotal version is slightly better, the RepGap is exponentially worse, illustrated by the Log10-scale plots in Figure 1. For the Motzkin monoids our results are not fine enough to come to a conclusion for the gap ratio, but the RepGap is again much worse.

We ideally aim for a more secure protocol over improved relative security for the computational complexity, so in this case we still say that the pivotal Temperley–Lieb monoid is better for cryptographic purposes than the non-pivotal analog; ditto for the Motzkin monoids. For the remaining case, it is clear that the pivotal monoids are better. With this, we build on the results from [KST24]

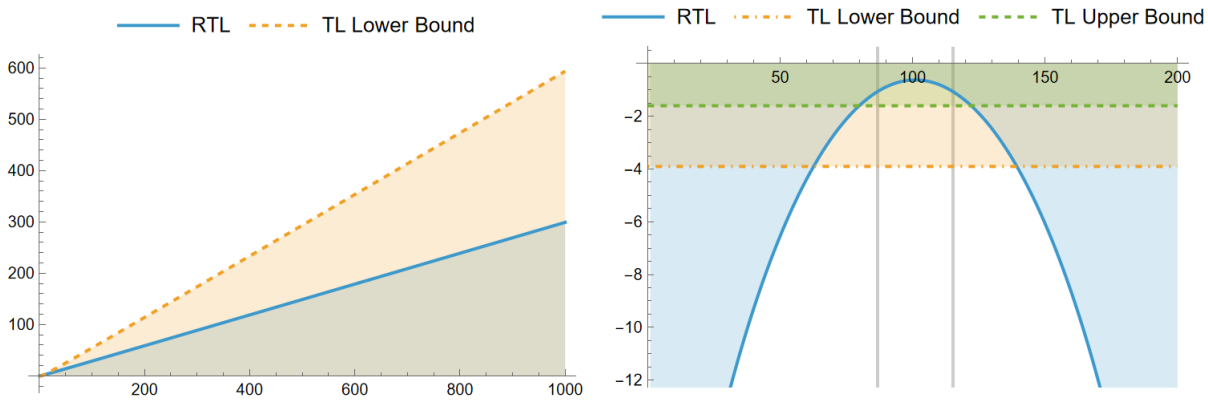


FIGURE 1. Left: comparison of the RepGaps in Log10 scale up to $n = 1000$; Right: comparison of the gap ratios in Log10 scale at $n = 100$, with vertical lines indicating where rTL_n is truncated.

to determine that pivotal planar diagram monoids are generally better for cryptographic purposes than non-pivotal planar diagram monoids.

The results related to the symmetric monoids in [**KST24**, Section 5] are much less precise than those of the planar monoids. This is because there is greater difficulty in computing the dimensions of simple representations for these monoids, although some work toward that has been done in, for example, [**DWH99**, **CdVM09**, **Tu24**]. Future work based on this paper should thus begin from these symmetric monoids, both in the pivotal and non-pivotal cases.

Remark 1B.1. We assume some familiarity with diagrammatic algebras, monoids, and categories, and (sandwich) cellularity a.k.a. Green's relations. There are many references for these, see e.g. [**KST24**, Sections 3 and 4]. (For readers acquainted with diagram algebras such as the Temperley–Lieb algebra, the monoids we study can be obtained by specializing all parameters, i.e., floating components to 1.) ◇

Remark 1B.2. Some parts of this paper are based on computer calculations. For the reader who wants to run these calculations themselves, we have collected all relevant material on GitHub following the link [**St25**]. This applies to all Mathematica and GAP computations in this paper. That page also contains an erratum, which may be empty. ◇

Acknowledgments. This paper is intended to be part of the first author's PhD thesis.

We would like to thank Kevin Coulembier for bringing the rigid Temperley–Lieb category to our attention. WS was supported by the Postgraduate Research Scholarship in Mathematics and Statistics (SC4238). DT was supported by the ARC Future Fellowship FT230100489 and contemplates the various ways their life went awry, taking full responsibility.

2. CELLS AND MONOID REPGAPS

The main representation theory of monoids that we will be using is discussed in detail in [**KST24**, Section 2 & 3], which we follow closely; see also [**St16**]. In this section, we will simply state the main results and tools that we require without proof.

2A. **Monoid representations.** Let M be a finite monoid, and let $\mathbb{K}$ be a field. Except where specified, $\mathbb{K}$ has arbitrary characteristic and representations are left representations over $\mathbb{K}$. We define preorders on M, called *left, right and two-sided cell order*, by

$$(a \leq_l b) \Leftrightarrow \exists c : b = ca,$$
$$(a \leq_r b) \Leftrightarrow \exists c : b = ac,$$
$$(a \leq_{lr} b) \Leftrightarrow \exists c, d : b = cad.$$

Remark 2A.1. There are similar notions of cells in the study of cellular algebras as, e.g., in [GL96, KX12, TV23, Tu24]. As in [KST24, Remark 3.1], 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. ◇

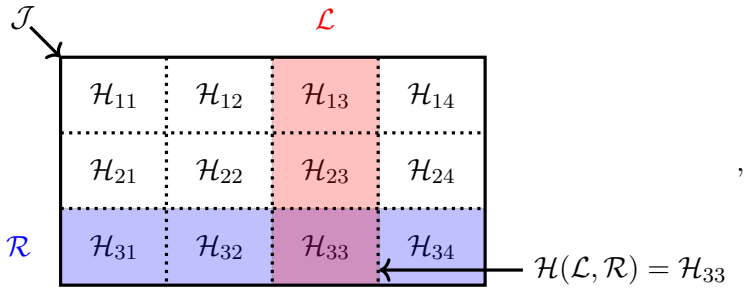
We define equivalence relations, the *left, right and two-sided equivalence*, by

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

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 is

(2A.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 M and cells. For example, the notations $\mathcal{L} \geq_l a$ or $\mathcal{L} \leq_l \mathcal{L}'$ make sense. In particular, for a fixed left cell $\mathcal{L}$ we can define

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

as well as others which we will distinguish by the subscript. 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*.

Notation 2A.3. When $\mathcal{H}(e) \cong 1$ is the trivial group, we say $\mathcal{H}(e)$ is *trivial*. This is the most relevant case for planar diagram monoids (in fact, one might define planar diagram monoids to be those with trivial H-cells). In the following, we will be specifically addressing the case $\mathcal{H}(e) \cong 1$. ◇

We have minimal and maximal J-cells in the $\leq_{lr}$-order. In our illustrations the minimal cell will be at the bottom, so we call it the *bottom cell* $\mathcal{J}_b$, while the maximal cell will be at the top, so we call it the *top cell* $\mathcal{J}_t$.

Lemma 2A.4. *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.* □

Cells can be considered M-representations, called *cell representations* or *Schützenberger representations*, up to higher order terms:

Lemma 2A.5. *Each left cell $\mathcal{L}$ of* M *gives rise to a left* M*-representation $\Delta_{\mathcal{L}} = \mathbb{K}\mathcal{L}$ by*

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

Similarly, right cells give right M*-representations $\Delta_{\mathcal{R}}$ and J-cells give* M*-birepresentations. We have* $\dim(\Delta_{\mathcal{L}}) = |\mathcal{L}|$ *and* $\dim_{\mathbb{K}}(\Delta_{\mathcal{R}}) = |\mathcal{R}|$. □

The top and bottom cells of Lemma 2A.4 correspond to the two trivial representations of the monoid M as in the following definition.

Definition 2A.6. Let $\mathrm{G} \subset \mathrm{M}$ be the subgroup of all invertible elements of M, i.e. G is the group of units. Then we define *trivial representations*

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

An M-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 M-representation M.

Remark 2A.7. With respect to the above, we again 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. ◇

The annihilator $\mathrm{Ann}_{\mathrm{M}}(M) = \{s \in \mathrm{M} | s \,.\, M = 0\}$ of an M-representation M is a two-sided ideal of M. An *apex* of M is a J-cell $\mathcal{J}$ such that, firstly, $\mathcal{J} \cap \mathrm{Ann}_{\mathrm{M}}(M) = \emptyset$, and secondly, all J-cells $\mathcal{J}'$ with $\mathcal{J}' \cap \mathrm{Ann}_{\mathrm{M}}(M) = \emptyset$ 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* M*-representation*:

Lemma 2A.8. *Every simple* M*-representation has a unique apex, and apexes correspond 1:1 to idempotent J-cells.* □

Then, we can classify the simple representations with the *Clifford–Munn–Ponizovskiĭ theorem* or *H-reduction*:

Theorem 2A.9. *For a monoid* M *with only trivial H-cells:*

$$\{\textit{simple } \mathrm{M}\textit{-representations}\}/\cong \overset{1:1}{\longleftrightarrow} \{\textit{idempotent } J\textit{-cells}\}\ ,$$

and the association can be chosen (and we will do this) such that simple M*-representations are mapped to their apex.* □

We can define a partial order, also denoted by $\leq_{lr}$, on the set of simple M-representations by saying that one simple is strictly smaller than another if its apex is strictly smaller.

We can estimate the size of simple representations with the following upper bound:

Lemma 2A.10. *The dimension of the simple* M*-representation $L_{\mathcal{J}}$ associated to the apex $\mathcal{J}$ via Theorem 2A.9 can be bounded by*

$$\dim_{\mathbb{K}}(L_{\mathcal{J}}) \leq |\mathcal{L}|,$$

where $\mathcal{L} \subset \mathcal{J}$ is arbitrary. □

We call $\mathrm{ssdim}_{\mathbb{K}}(L_{\mathcal{J}}) := |\mathcal{L}| = \dim_{\mathbb{K}} \Delta_{\mathcal{L}}$ the *semisimple* dimension of $\mathcal{J}$. This name is justified by the following:

Proposition 2A.11. *The following are equivalent for a monoid* M *with only trivial H-cells.*

- **(a)** *The monoid* M *is semisimple over* $\mathbb{K}$.
- **(b)** *All J-cells are idempotent and square, and we have $\dim_{\mathbb{K}}(L_{\mathcal{J}}) = \mathrm{ssdim}_{\mathbb{K}}(L_{\mathcal{J}})$ for all J-cells $\mathcal{J}$, and $L_{\mathcal{J}} \cong \Delta_{\mathcal{L}}$.* □

2B. **The RepGap.** We now define the main quantities that are important for cryptography. We define them slightly differently when compared to [KST24] (which is the correct definition), but that does not matter for our purposes; see Lemma 2B.2 below.

Definition 2B.1. The *RepGap* $\mathrm{Gap}_{\Bbbk}(\mathrm{M})$ is the dimension of the smallest nontrivial simple representation of M. The *gap ratio* is the quantity $\mathrm{Ratio}_{\Bbbk}(\mathrm{M}) := \mathrm{Gap}_{\Bbbk}(\mathrm{M})/\sqrt{|\mathrm{M}|}$. The *semisimple RepGap* $\mathrm{ssGap}_{\Bbbk}(\mathrm{M})$ is the minimal *semisimple* dimension of the nontrivial simple M-representations. The *semsimple gap ratio* is $\mathrm{ssRatio}_{\Bbbk}(\mathrm{M}) := \mathrm{ssGap}_{\Bbbk}(\mathrm{M})/\sqrt{|\mathrm{M}|}$ ◇

The semisimple RepGap is less important than the RepGap, but easier to compute.

Lemma 2B.2. *The RepGap from Definition 2B.1 is always bigger or equal to the one in* [KST24]. *Moreover, for our reference diagram monoids, Temperley–Lieb, Motzkin and planar rook, the two definitions agree.* □

Our main results will imply that the rigid diagram monoids have a smaller RepGap than their pivotal counterparts, even when using our more generous RepGap definition compared to [KST24]. Hence, by Lemma 2B.2, we can still say that they are worse for our purposes, and therefore we do not have to (and will not) worry about the more subtle definition of the RepGap from [KST24].

Remark 2B.3. The gap ratio roughly measures the ratio of the security of the cryptographic protocol based on the monoid to the computational complexity of the monoid. More precisely, recall that the dimension of a simple representation over an algebraically closed field is at most the square root of the size of the monoid.

If the RepGap is significantly smaller than this upper bound, then the impact from linear attacks is greater; if the monoid is relatively large, the computational complexity for utilizing any encryption protocols based on it is greater, however there is little security gain from this since it can be bypassed by a linear attack, due to the smaller simple representation. In other words, the closer the RepGap is to the square root of the size of the monoid, the less of an impact the linear attack will have. ◇

Remark 2B.4. *Faithfulness* is the minimal dimension of nontrivial faithful representations. We will not compute or discuss it further in this paper, as the RepGap and gap ratio are sufficient for comparing the monoids we are interested in. ◇

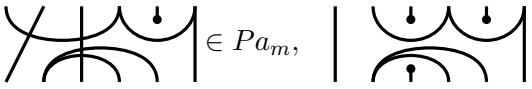
In practice, for cryptographic purposes, we generally look for families of monoids indexed by $n \in \mathbb{Z}_{\geq 0}$ such that the ***RepGap tends to infinity exponentially with n, and the gap ratio does not exponentially tend to zero***. We will discuss examples of such monoids in the next section.

3. Diagram categories and monoids

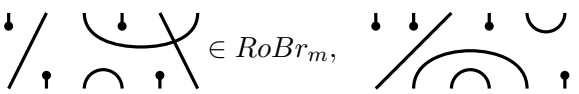
Martin [Mar91] and Jones [Jo94] discovered the partition algebra as a generalization of the Temperley–Lieb algebra, extending the construction that relates the Temperley–Lieb algebra to the Potts model in statistical mechanics; see [HR05] for a self-contained summary. Specializing the parameter yields the partition monoid and its associated category.

3A. **Pivotal diagram categories.** The *diagram monoids* we refer to are submonoids of the partition monoid. For $m \in \mathbb{Z}_{\geq 0}$ the picture to keep in mind, taken from [Tu24], is:

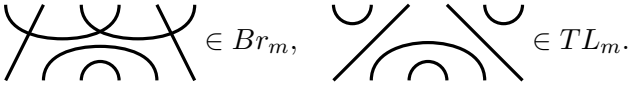
- The *partition monoid* Pa_m of all diagrams of partitions of a $2m$-element set. The *planar partition monoid* pPa_m is the respective planar submonoid of Pa_m.



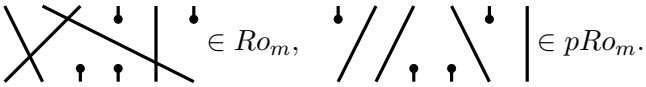
- The *rook-Brauer monoid* $RoBr_m$ consisting of all diagrams with components of size 1 or 2. The planar rook-Brauer monoid $pRoBr_m = Mo_m$ is also called the *Motzkin monoid*.



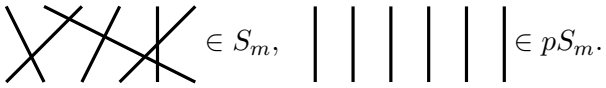
- The *Brauer monoid* Br_m consisting of all diagrams with components of size 2. The planar Brauer monoid $pBr_m = TL_m$ is known as the *Temperley–Lieb monoid* (sometimes TL_m is called *Jones monoid* or *Kauffman monoid*).



- The *rook monoid* or *symmetric inverse semigroup* Ro_m consisting of all diagrams with components of size 1 or 2, and all partitions have at most one component at the bottom and at most one at the top. The *planar rook monoid* pRo_m is the corresponding submonoid.



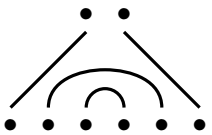
- The *symmetric monoid/group* S_m consisting of all matchings with components of size 1. The *planar symmetric group* is trivial $pS_m \cong 1$.



We will only be considering the planar monoids, however we included the non-planar ("symmetric") monoids above for completeness. We also focus on TL_m, Mo_m and pRo_m, since pS_m is trivial and $pPa_m \cong TL_{2m}$ by [**HR05**, (1.5)].

These monoids each have corresponding monoidal categories, with objects made up of words in a single letter $\bullet$ of length $m \in \mathbb{Z}_{\geq 0}$, and morphism sets consisting of diagrams like the above with each letter in the object acting as a node. The endomorphism sets on objects of length m recover the original monoids. Composition is given by stacking diagrams on top of each other, as long as the objects in the middle are the same, then reducing based on the final pairings of each node (i.e. the partition of nodes). When the diagrams are endomorphisms, this is the same composition as in the original monoids.

For example, for the Temperley–Lieb category, TL, we have:



$\in \mathrm{Hom}_{TL}(\bullet\bullet\bullet\bullet\bullet\bullet, \bullet\bullet)$.

Remark 3A.1. Further details about these monoids can be found in numerous sources; see, for example, [**HR05**]. Since the partition category can be identified with cobordisms modulo certain relations, [**Ko04**] provides a convenient framework for translating these monoids into categorical language, see [**Hu19**] for an explicit summary. ◇

We also pick particular values m for these monoids, for reasons that will become clear in the following section. From now

we will simply write $\mathrm{TL}_n, \mathrm{Mo}_n$, and pRo_n to mean endomorphisms on $(\bullet\bullet)^{\otimes n}$ instead,

which is equivalent to $\mathrm{TL}_m, \mathrm{Mo}_m$, and pRo_m for $m = 2n$ using the previous definitions. We also truncate the monoids to keep only the representations that are sufficiently large, following [**KST24**, Section 4].

Remark 3A.2. One key advantage of monoids over groups is their flexibility: we can truncate them either from below, by annihilating small cells and adjoining a unit, or from above, by collapsing large cells to an adjoint zero. This allows us to strategically eliminate representations that are too small, and we will do this throughout. ◇

Recall that this works as follows. Let D be any of our diagram monoids. Then the J-cells of D are a subset of $\mathbb{Z}_{\geq 0}$, where every J-cell corresponds to a fixed number $k \in \mathbb{Z}_{\geq 0}$ being the number of through strands. We can then define $D^{a \leq k \leq b}$ as the Rees factor (adjoining a unit, if necessary) supported on the cells with $a \leq k \leq b$ through strands. In this paper, we use $TL_n^T := TL_n^{0 \leq k \leq 2\sqrt{2n}}$, $Mo_n^T := Mo_n^{0 \leq k \leq 2\sqrt{2n}}$, and $pRo_n^T := pRo_n^{n-\sqrt{2n} \leq k \leq n+\sqrt{2n}}$.

Theorem 3A.3. *Assuming that* $\operatorname{char}\mathbb{K} = 0$ *for* Mo_n *and* TL_n*, we have the following inequalities for the asymptotics of the RepGaps and gap ratios:*

$$2^{-5/2} \cdot n^{-5/2} \cdot 4^n \leq \operatorname{Gap}_{\mathbb{K}} TL_n^T \leq 2^{-5/2} \cdot n^{-3/2} \cdot 4^n,$$

$$f(n) \cdot 9^n \leq \operatorname{Gap}_{\mathbb{K}} Mo_n^T \leq 2^{-3/2} \cdot n^{-3/2} \cdot 4^n,$$

$$\pi^{-1/2} e^{-2-\frac{1}{3n}} \cdot n^{-1/2} \cdot 4^n \leq \operatorname{Gap}_{\mathbb{K}} pRo_n^T \leq \pi^{-1/2} \cdot n^{-1/2} \cdot 4^n,$$

for some function f *in* n *asymptotically smaller than* $(2n)^{-3/2}$*. The ratios are*

$$2^{-7/4}\pi^{3/4} \cdot n^{-7/4} \leq \operatorname{Ratio}_{\mathbb{K}} TL_n^T \leq 2^{-3/4}\pi^{3/4} \cdot n^{-3/4},$$

$$\pi^{1/4} 4^{-1} 3^{-3/4} \cdot f(n) n^{3/4} \leq \operatorname{Ratio}_{\mathbb{K}} Mo_n^T \leq \sqrt{2}\pi^{1/4} 3^{-3/4} \cdot n^{-3/4},$$

$$\pi^{-1/4} 2^{1/4} e^{-2-\frac{1}{3n}} \cdot n^{-1/4} \leq \operatorname{Ratio}_{\mathbb{K}} pRo_n^T \leq \pi^{-1/4} 2^{1/4} \cdot n^{-1/4},$$

for the same f*.*

Proof. For TL_n^T the bounds on the RepGap come from [KST24, Theorem 4E.2], noting that the upper bound is from the semisimple RepGap. The pRo_n^T asymptotics come from the formulas in [KST24, Section 4F]. The asymptotics for the gap ratios then follow easily when dividing by the asymptotics of $|TL_n|$ and $|pRo_n|$, since the latter are straightforward binomials whose asymptotics can be calculated directly in Mathematica.

For Mo_n^T, the result that the exponential growth factor of the RepGap is 3^{2n}, and that it is worse than $3^{2n}(2n)^{-3/2}$, is found in [Ar25].

To obtain an asymptotic for $|Mo_n|$, we can start with the recurrence for the Motzkin numbers in [Be99], which naturally leads to a generating function and an asymptotic for the Motzkin numbers. The sequence of sizes of the Motzkin monoid is a bisection of the Motzkin numbers, so we can finally use [FS09] to obtain the asymptotic of $|Mo_n|$. [Ko12] has already calculated this to be $|Mo_n| \sim (3^{4n+3/2})/(16\sqrt{\pi}n^{3/2})$, from which we can get the gap ratio. □

Remark 3A.4. Strictly speaking, we should be taking the size of the truncated monoid on the denominator in the gap ratios, however in the above we have used the full size of the monoids. We justify this by observing that the asymptotic growth up to the exponential factor is the same for the full monoid and truncated monoid. Indeed, if $M_n = \sum_{k=0}^{n} f(n,k)$ is the size of the monoid, then taking $m(n) := \max\{f(n,k) | k = 0, 1, ..., n\}$, we have $m(n) \leq M_n \leq nm(n)$. Taking the nth root to find the exponential growth, $(nm(n))^{1/n} \to (m(n))^{1/n}$ since the contribution from n is negligible, so by the sandwich theorem $M_n^{1/n} \to (m(n))^{1/n}$ (note that for all the monoids we are dealing with, $f(n,k)$ is continuous in n and k).

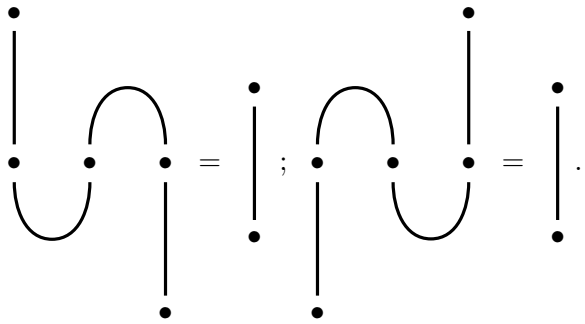
Therefore, as long as M_n^T contains $m(n)$, which it does by design in the cases above, the asymptotic of the *nth* root will be $m(n)$, meaning they have the same exponential growth factor. As a result, we can simply use the size of the monoid itself in the above ratios, when doing otherwise would be computationally difficult, as long as n is sufficiently large. ◇

3B. **Non-pivotal diagram categories.** Define left and right duals in the usual way, e.g. following [EGNO15, Section 2].

Definition 3B.1. A monoidal category is *rigid* if every object has a left and right dual. An object X in a rigid monoidal category with a dual X^* is *pivotal* if $X^{**} \cong X$. A rigid monoidal category is called *pivotal* if every object is pivotal. ◇

Remark 3B.2. We have simplified the definition, however one should keep in mind that each dual is actually a monoidal functor, and the isomorphisms are isomorphisms of monoidal functors. ◇

A key feature of the categories described above is that they are all pivotal. This follows from the fact that the object • is self-dual, which is just the zigzag equations:



In the following sections, we will compute the RepGaps and gap ratios for *rigid, non-pivotal* counterparts to the familiar categories above, and compare them to the results for the original pivotal versions. This will give some indication of which, between pivotal and non-pivotal, are more suitable for use in cryptography.

The exploration of non-pivotal analogs is justified with the following result:

Lemma 3B.3. *Let R, P be rigid monoidal categories and $F : R \to P$ a full monoidal functor. If $Y \in Obj(P)$ such that Y is pivotal, then $\exists X \in Obj(R)$ such that X is pivotal. Moreover, if P is a pivotal monoidal category and F is additionally faithful, then R is also a pivotal monoidal category.*

Proof. Since $Y \in P$ is pivotal, Y is the left dual of Y^*, so there is an evaluation morphism $\mathrm{ev}_Y : Y \otimes Y^* \to \mathbb{1}_P$. Since F is a full monoidal functor, $\exists X \in Obj(R)$ and $\mathrm{ev}_X : X \otimes X^* \to \mathbb{1}_R$ such that $F(\mathrm{ev}_X) : F(X) \otimes F(X^*) \to F(\mathbb{1}_R) = \mathrm{ev}_Y : Y \otimes Y^* \to \mathbb{1}_P$. Similarly, there is a corresponding co-evaluation morphism in R, which means that X is a left dual of X^*, and since duals are unique up to (unique) isomorphism [**EGNO15**, Proposition 2.10.5], this means $X \cong X^{**}$ so X is pivotal.

If P is pivotal, the above argument gives a pivotal $X \in Obj(R)$ for every $Y \in Obj(P)$, and if F is faithful then this means that this is all the objects in R, i.e., every $X \in Obj(R)$ is pivotal. □

Let G be a group and $Rep(G)$ be the monoidal category of all finite dimensional representations of G. Since $V^{**} \cong V$ for any finite dimensional vector space V, $Rep(G)$ is pivotal.

Corollary 3B.4. *Let R be a non-pivotal rigid monoidal category. Then there is no fully faithful monoidal functor from R to $Rep(G)$.* □

This shows that a non-pivotal counterpart to the Temperley–Lieb, Motzkin, and planar rook categories is meaningfully different, since the pivotal versions do have category equivalences to $Rep(G)$ for some group G; for example, the Temperley–Lieb category (when the circle is evalauted to 2 instead of 1) is equivalent to $Rep(SL_2)$ via the functor that sends • to the standard two-dimensional SL_2-representation.

Remark 3B.5. The categories we use where the parameter is evaluated to 1 are actually equivalent to representations of quantum groups (or rather quantum enveloping algebras) and not groups, but the difference wll not play a role for us. ◇

This result also suggests that the monoids from non-pivotal categories will in some sense be more complicated than those from the pivotal categories. When designing encryption protocols, it would be more desirable to have more complicated, less easily described monoids, since that would hopefully make it harder to decrypt. This is incredibly imprecise; however, the RepGap and gap ratio are useful concrete tools to determine which monoids will likely be more effective for use in cryptography.

In the next three sections, we prove the following bounds on the RepGaps and gap ratios for the non-pivotal TL, Mo, and pRo monoids:

Theorem 3B.6. *We have the following inequalities for the asymptotics of the RepGaps and gap ratios:*

$$\boxed{2^{-1/2}\pi^{-1/2}e^{-1-\frac{1}{3n}}} \cdot \boxed{n^{-1/2}} \cdot \boxed{2^n} \leq \mathrm{Gap}_{\mathbb{K}}\, rTL_n^T \leq \boxed{2^{-1/2}\pi^{-1/2}} \cdot \boxed{n^{-1/2}} \cdot \boxed{2^n},$$

$$\boxed{\pi^{-1/2}e^{-\frac{1}{n}}}\cdot\boxed{n^{-3/2}}\cdot\boxed{4^n}\leq \mathrm{ssGap}_{\mathbb{K}}rMo_n^T\leq\boxed{4\sqrt{2}\pi^{-1/2}e^{-\frac{1}{n}}}\cdot\boxed{n^{-1}}\cdot\boxed{4^n},$$

$$\boxed{\sqrt{2}\pi^{-1/2}e^{-4-\frac{16}{3n}}}\cdot\boxed{n^{-1/2}}\cdot\boxed{2^n}\leq \mathrm{Gap}_{\mathbb{K}}\,rpRo_n^T\leq\boxed{\sqrt{2}n^{-1/2}\pi^{-1/2}}\cdot\boxed{2^n},$$

$$\boxed{2^{1/4}\pi^{-1/4}e^{-1-\frac{1}{3n}}}\cdot\boxed{n^{-1/4}}\leq \mathrm{Ratio}_{\mathbb{K}}\,rTL_n^T\leq\boxed{2^{1/4}\pi^{-1/4}}\cdot\boxed{n^{-1/4}},$$

$$\boxed{\pi^{-1/2}e^{-\frac{1}{n}}}\cdot\boxed{n^{-3/2}}\leq \mathrm{ssRatio}_{\mathbb{K}}rMo_n^T\leq\boxed{4\sqrt{2}\pi^{-1/2}}\cdot\boxed{n^{-1}},$$

$$\mathrm{Ratio}_{\mathbb{K}}\,rpRo_n^T\leq\boxed{2^{3n/2}3^{3n/4}5^{-5n/4}}\approx\boxed{0.87^n}.$$

Theorem 3B.6 will be proven case by case in the next sections. Note that Theorem 3B.6 implies that the table in the introduction holds.

4. The rigid Temperley–Lieb monoid

We start with our first non-pivotal diagram monoid.

4A. **Definition of rTL_n.** We now define a non-pivotal analog of the Temperley–Lieb category, a rigid monoidal category that we call the ***rigid Temperley–Lieb category*** and denote by rTL.

Definition 4A.1. The objects, morphisms, and tensor product of rTL are defined as follows:

(a) The collection of *objects* $Obj(rTL)$ consists of all finite words $X_{i_1}X_{i_2}...X_{i_n}$ in the alphabet $\{X_i : i\in\mathbb{Z}\}$. We will typically only write the subscripts, for example the object $X_1X_2X_1X_1$ will often simply be written $1\,2\,1\,2$. The *empty word* is denoted $\mathbb{1}$.

(b) The *length* of an object $X=X_{i_1}X_{i_2}...X_{i_n}$ is $\mathrm{length}(X)=n$, that is, the number of letters used to make up the word. The length of $\mathbb{1}$ is zero.

(c) The collection of *morphisms* between two objects $Hom(X,Y)$, for $X=X_{i_1}X_{i_2}...X_{i_n}$ and $Y=X_{j_1}X_{j_2}...X_{j_m}$, consists of all partitions of $\{1,2,...,m,-1,-2,...,-n\}$ into ordered pairs (a,b), with the following properties:

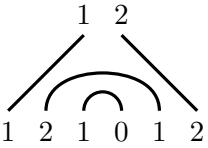
(i) (a,b), $a*b<0$, is a valid pair $\iff j_{-b}=i_a$,

(ii) (a,b), $a>0,b>0$, is a valid pair $\iff i_b=i_a+1$,

(iii) (a,b), $a<0,b<0$, is a valid pair $\iff j_{-b}=j_{-a}-1$,

(iv) the partition is *planar*, meaning there are no pairs $[a,b],[u,v]$ such that $a<u<b<v$.

(d) It will be useful to represent such morphisms as *diagrams*, drawn vertically from $j_1,...,j_m$ to $i_1,...,i_n$ (i.e. just keeping the subscripts of the two objects, drawing from bottom to top), connecting each pair via an unbroken line, we call a *string*. For example, the morphism $[(1,-1),(2,-6),(-2,-5),(-3,-4)]$ from $X_1X_2X_1X_0X_1X_2\to X_1X_2$ would be represented by:



$\in \mathrm{Hom}_{TL}(1\,2\,1\,0\,1\,2, 1\,2)$.

The above conditions, when translated to the language of these diagrams, are:

(i) (a,b), with $ab<0$ and $j_{-b}=i_a$, is called a *through strand*,

(ii) (a,b), with $a>0,b>0$ and $i_b=i_a+1$, is called a *cup*, denoted $\mathrm{cup}_{x,x+1}$,

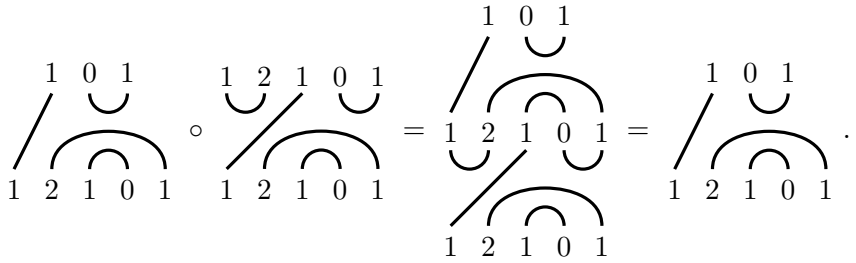
(iii) (a,b), with $a<0,b<0$ and $j_{-b}=j_{-a}-1$, is called a *cap*, denoted $\mathrm{cap}_{x,x-1}$,

(iv) and the partition being planar simply means that the diagram is planar, that is, no strings are allowed to intersect.

Henceforth we will consider diagrams and partitions interchangeably.

(e) The *size* of a diagram $f:X\to Y$ is $\mathrm{size}(f)=\big(\mathrm{length}(X),\mathrm{length}(Y)\big)$.

(f) *Composition* of two morphisms $f : X \to Y$ and $g : Y \to Z$, $f \circ g : X \to Z$, is given by vertically placing the diagram f on top of the diagram g, then obtaining a new partition by creating pairs that are connected by strings (noting that a string is not broken by a subscript). For example:



(g) The identity morphism on $X \in Obj(rTL)$, denoted 1_X, is simply the diagram consisting only of through strands, that is, every subscript in X at the bottom of the diagram is connected to its corresponding subscript at the top via a vertical line. $1_{\mathbb{1}}$ is defined as there being no diagram, the empty diagram (or empty partition $[]$).

(h) Define a functor $\bigotimes : rTL \times rTL \to rTL$ by:

(i) If $X = X_{i_1}X_{i_2}...X_{i_n}$, $Y = X_{j_1}X_{j_2}...X_{j_m} \in Obj(rTL)$, then

$$X \otimes Y = X_{i_1}X_{i_2}...X_{i_n}X_{j_1}X_{j_2}...X_{j_m}$$

that is, we simple concatenate the words X and Y, and

(ii) if $f : X \to Y \in Hom_{rTL}(X, Y)$, $g : A \to B \in Hom_{rTL}(A, B)$, then we obtain $f \otimes g \in Hom_{rTL}(X \otimes A, Y \otimes B)$ by placing the diagram g to the right of f, that is, concatenating the diagrams horizontally.

We call the resulting construction the (set-theoretic) rigid Temperley–Lieb category. ◇

Lemma 4A.2. *With the structure above, rTL is a rigid monoidal category, and no object is pivotal.*

Proof. The composition of morphisms in rTL is clearly associative, since we can simply stack all multiplied diagrams and obtain the result by following the strings from their top-most objects to the bottom-most objects they are connected to. Moreover, $\bigotimes$ defines a monoidal product, with the empty word and diagram $(\mathbb{1}, 1_{\mathbb{1}})$ being the monoidal unit. So rTL is a monoidal category.

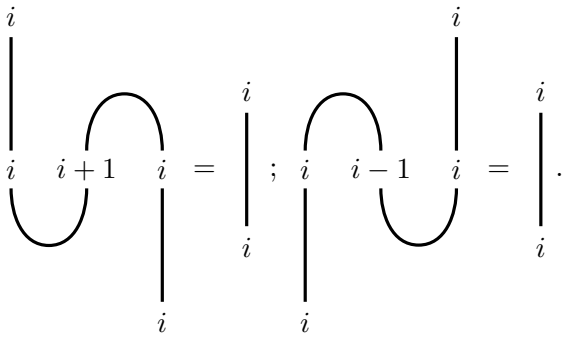
For every $i \in \mathbb{Z}$, we have:

(a) The *left dual* of X_i is $(X_i^* = X_{i-1}, \mathrm{cup}_{i-1,i}, \mathrm{cap}_{i,i-1})$, and

(b) the *right dual* of X_i is $({}^*X_i = X_{i+1}, \mathrm{cup}_{i,i+1}, \mathrm{cap}_{i+1,i})$,

which follows from the familiar zigzag equations:

(4A.3)



Therefore, given an object $X = X_{i_1}X_{i_2}...X_{i_n}$, the left dual of X is the object $X^* = X_{i_n-1} \otimes X_{i_n-1-1} \otimes ... \otimes X_{i_2-1} \otimes X_{i_1-1}$, along with the evaluation and coevaluation morphisms, $\mathrm{cup}_{X^*,X}$ and cap_{X,X^*}, defined by vertically concatenating cups and caps on the corresponding subscripts of X and X^*. The right dual is found similarly, and hence rTL is a rigid monoidal category.

Finally, $X_i^{**} \cong X_{i+2} \ncong X_i$ and ${}^{**}X_i \cong X_{i-2} \ncong X_i$, for all $i \in \mathbb{Z}$, and hence no object in rTL is pivotal. □

We have defined rTL, the ***rigid Temperley–Lieb category***, a rigid, non-pivotal analog of the Temperley–Lieb category, and from this we pick the monoid of endomorphisms

$$rTL_n := End_{rTL}(1\,2)^{\otimes n}$$

to analyze for cryptographic purposes. We call rTL_n the ***rigid Temperley–Lieb monoid***.

Remark 4A.4. The above definition does not include all endomorphisms in rTL of length $2n$. This is because, unlike in TL, we have multiple different objects of the same length, meaning the endomorphisms cannot be composed. As a result, the best we can do is pick one object for our endomorphism monoid; the alternative would be to take a direct sum $\bigoplus_{X\in Obj(rTL),(X)=m} \mathrm{End}_{rTL}(X)$, however this would require performing a completely different, generally nontrivial, calculation for each different endomorphism monoid, for no discernible extra benefit.

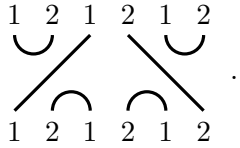
The choice of $(1\,2)^{\otimes n}$ as our object is because it captures enough of the structure of endomorphisms in rTL, while being relatively easier to compute cells. ◇

4B. **Computing cells for rTL_n.** We have the following sandwich factorization:

Lemma 4B.1. *Every diagram $d \in rTL_n$ with k through strands can be written as $\tau \circ 1_{\alpha(k)} \circ \beta$, where τ and β are diagrams of size (n,k) and (k,n) respectively, and $\alpha(k) = 1\,2...1\,2$ is of length k, where k is an even positive integer.*

Proof. Firstly, clearly it is impossible to have a diagram with zero through strands, since there is no valid cap arrangement on $1\,2...1\,2$. Moreover, there cannot be a negative number of through strands, so k must be a positive integer.

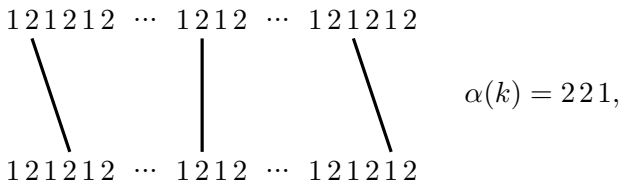
Now, consider the possibilities for through strands of a diagram in rTL_n. Let k be the number of through strands, and $\alpha(k)$ the sequence, of length k, of the letters paired by the through strands, read from left to right. For example, the following diagram has the sequence $1\,2$:



If the leftmost through strand pairs two 2s, then on the left we will have an odd number of letters on both the top and bottom. Since this is the leftmost through strand, the letters in the top must be paired up independently from the letters in the bottom, and vice versa. This is clearly impossible, since the number of letters in each is odd. A similar argument holds for the rightmost through strand.

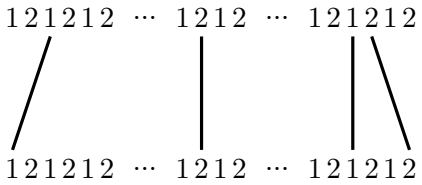
If there is a through strand to the left that pairs the same letters as the through strand to its right, then we will also have an odd number of letters on both the top and bottom, and the same reasoning holds again. This therefore shows that the sequence $\alpha(k)$ must be of the form $1\,2...1\,2$, which is necessarily of even length.

The above reasoning is illustrated below, first with a "bad" sequence of through strands, which cannot occur for any diagram in rTL_n:



$$\alpha(k) = 2\,2\,1,$$

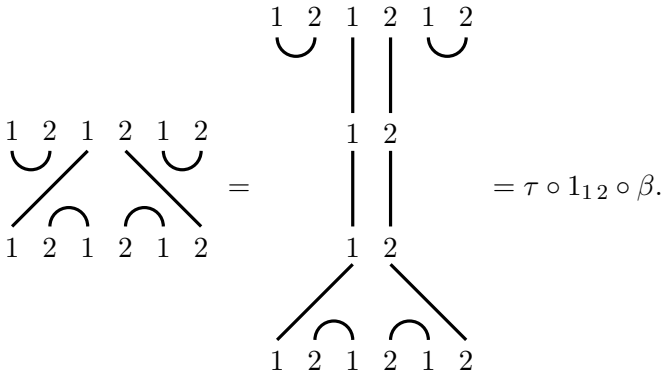
then with a "good" sequence that does appear in some diagrams in rTL_n.



$\alpha(k) = 1\,2\,1\,2.$

Note that this is only a necessary condition for the sequence of through strands; for example, it is also required that the leftmost through strand connects to the leftmost 1 on the bottom, and the rightmost through strand connects to the rightmost 2 on the bottom.

Finally, the factorisation into $\tau \circ 1_{\alpha(k)} \circ \beta$ follows from observing that the result of a composition depends only on the final pairings between the numbers in the very top object and very bottom object, so we can "stretch out" the through strands like so:



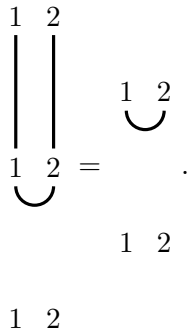
$= \tau \circ 1_{1\,2} \circ \beta.$

□

We will write $1_{\alpha(k)} = 1_k$, with k the number of through strands, since the meaning is clear. For $x \in rTL_n$, write k_x for the number of through strands in x.

Lemma 4B.2. *If $x, y \in rTL_n$, then $k_x \geq k_{xy}$ and $k_x \geq k_{yx}$. (The number of through strands cannot decrease.)*

Proof. In the composition xy, each strand arises from a strand in x and a strand in y, such that there is a continuous line between the top object of x and the bottom object of y. Therefore, it is not possible to increase the number of through strands in xy compared to x. It is possible to decrease the number of through strands, since for example we have



Hence, $1_{k_{xy}} \leq 1_{k_x}$, and similarly $1_{k_{yx}} \leq 1_{k_x}$. □

With the above two lemmas, we can describe the cells of rTL_n:

Proposition 4B.3. *The cells of rTL_n have the following properties:*

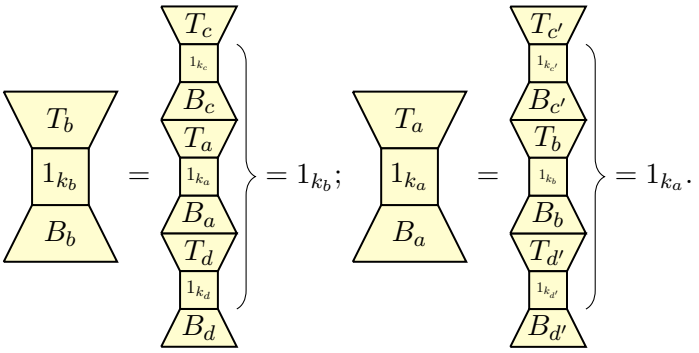
- **(a)** *The J-cells of rTL_n are indexed by the number of through strands, with order $2 <_{lr} \ldots <_{lr} 2n$. That is, number of through strands k is the apex of the J-cell.*
- **(b)** *The size of the left and right cells of rTL_n is given by the number of diagrams possible when fixing the top and bottom half, respectively.*

(c) *Every J-cell in rTL_n is idemptotent.*

Proof. The sandwich pictures below, which we will use from now on, are meant to show the factorization in Lemma 4B.1. The reader unfamiliar with these illustrations is referred to [**Tu24**].

Fix a J-cell $\mathcal{J}$, and suppose $a, b \in J$, meaning $a \leq_{lr} b$ and $b \leq_{lr} a$. This means $\exists c, c', d, d' \in rTL_n$ such that $b = cad$ and $a = c'bd'$.

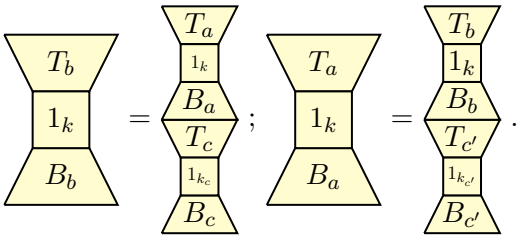
Using Lemma 4B.1, we have:



In the left equation, the middle of the right hand side must resolve to 1_{k_b}, and since 1_{k_a} is contained within that middle, $k_a \geq k_b$ (using Lemma 4B.2. Similarly, $k_b \geq k_)$, and thus $k_a = k_b$. This proves (a).

Clearly, if $k_a = k_b$, then $a \leq_{lr} b$ and $b \leq_{lr} a$, and hence the J-cells of rTL_n are completely determined by the number of through strands. Moreover, the above argument shows that $a \leq_{lr} b \implies 1_{k_a} \leq 1_{k_b}$, making $\leq_{lr}$ a total order on the J-cells.

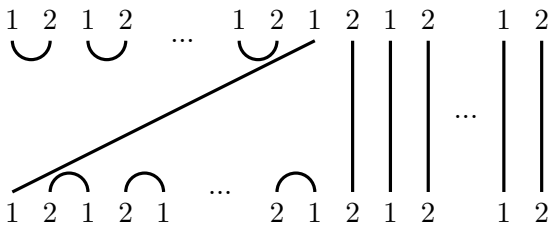
The argument for right and left cells is similar. If we have $a, b \in J$, with k through strands, then the condition for $a \sim_r b$ is:



which shows that $a \sim_r b \iff T_a = T_b$, i.e. the top halves of the diagrams are the same. Similar reasoning shows that $a \sim_l b \iff B_a = B_b$, proving (b).

Finally, suppose we have a fixed J-cell $\mathcal{J}$ of apex k through strands. If $k = 2n$ then the identity is an idempotent in $\mathcal{J}$.

Suppose now that $2 \leq k < 2n$. Then there exists a diagram of the form:



where we have simply moved all caps and cups as far to the left as possible. Stacking this diagram on top of itself shows that this diagram is idempotent, and hence every J-cell contains an idempotent. □

Remark 4B.4. $k = 2n$ corresponds to the bottom J-cell and bottom trivial representation, and $k = 2$ corresponds to the top J-cell and top trivial representation. Those familiar with the representations of TL_n might be surprised, since the top trivial representation typically corresponds to $k = 0$, which

is missing for rTL_n. This can be reconciled by noting that $k = 0$ corresponds to the maximal number of cups and caps in a Temperley-Lieb diagram, while $k = 2$ does the same in rTL_n. ◇

Example 4B.5. For rTL_3 and rTL_5 the cells are illustrated in Figure 2. It is explained in [St25] how to produce these pictures in GAP. ◇

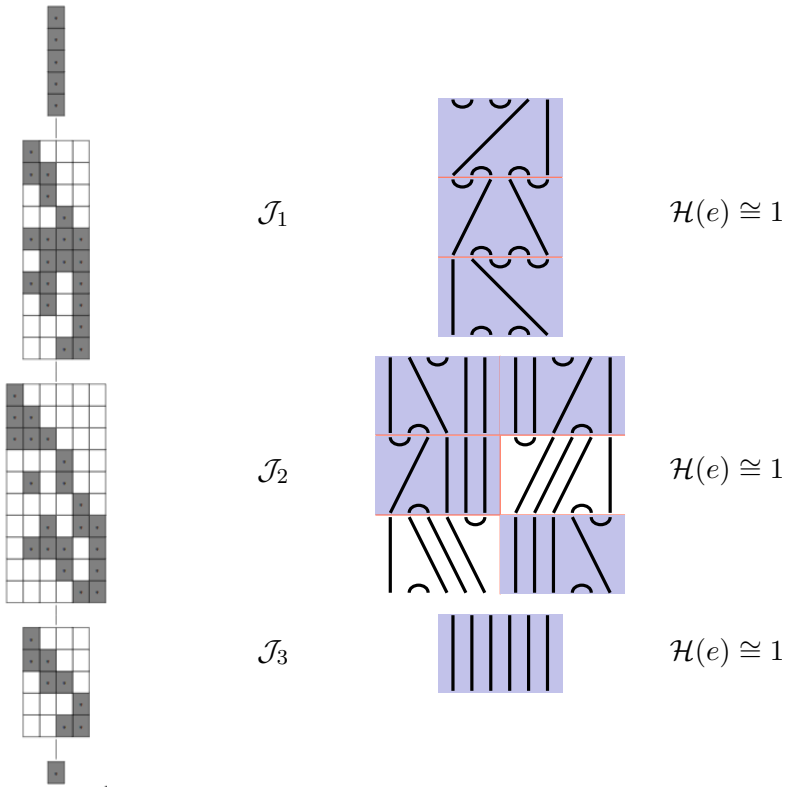


FIGURE 2. Left: the cell structure of rTL_5, produced with the Semigroups package in GAP (adjusted to match our conventions): every block represents a J-cell, and every shaded box an $\mathcal{H}$-cell containing an idempotent. Right: the cell structure of rTL_3, with each $\mathcal{H}$-cell written explicitly.

Now, we calculate the sizes of the left and right cells.

Proposition 4B.6. *For a fixed number of through strands k, we have:*

$$|\mathcal{R}_n^k| = \binom{n-1}{\frac{2n-k}{2}}, \quad |\mathcal{L}_n^k| = \binom{n}{\frac{2n-k}{2}},$$

moreover, the total number of elements in rTL_n is $\binom{2n-1}{n}$.

Proof. Fix k through strands, and fix the letters in the diagram that each through strand pairs up. Then, all that's left is to arrange the cups and caps on the top and bottom respectively, and the arrangements on the top and bottom are independent of each other.

Consider the bottom first. There are n letters on the bottom, and only $\frac{2n-2}{2} = n - 1$ spots a cap can be placed (with no nesting allowed), since on the far left and far right we have 12. Of the $2n$ total letters in the diagram, k are already paired up, so there are only $\frac{2n-k}{2}$ remaining on each of the bottom and top words.

Once we place the caps, there is only one possible arrangement of the through strands, since the diagrams in rTL_n are planar. Hence, the number of different bottom half diagrams is equal to the number of ways to choose $(2n - k)/2$ pairs of letters (i.e. 1s and 2s) to be placed in the $n - 1$ valid cap positions. This is equal to $\binom{n-1}{\frac{2n-k}{2}}$, proving the formula for $|\mathcal{R}_n^k|$.

The size of the left cells can be computed similarly, noting that the far left 1 and the far right 2 can be used for cups on the top.

Finally, since the top and bottom are independent once we've fixed k through strands (note that k must be even, by Lemma 4B.1), the total number of possible diagrams is

$$\sum_{\substack{k=0\\ k \text{ even}}}^{2n} |\mathcal{R}_n^k||\mathcal{L}_n^k| = \sum_{k=0}^{n} \binom{n-1}{\frac{2n-2k}{2}} \binom{n}{\frac{2n-2k}{2}} = \sum_{k=0}^{n} \binom{n-1}{n-k} \binom{n}{k} = \binom{2n-1}{n},$$

where the final step follows from the Chu–Vandermonde identity. □

4C. **RepGap and gap ratio of rTL_n.** We are on the final round in our proof of Theorem 3B.6 for rTL_n. As a first step:

Proposition 4C.1. *The simple rTL_n-representation are indexed and ordered by $2 <_{lr} \ldots <_{lr} 2n$. Moreover, the right representations $\Delta_{\mathcal{R}_n^k}$ are all simple, and provide a complete list, up to isomorphism, of the simple representations of rTL_n.*

Proof. The first statement is immediate from Theorem 2A.9 and Proposition 4B.3

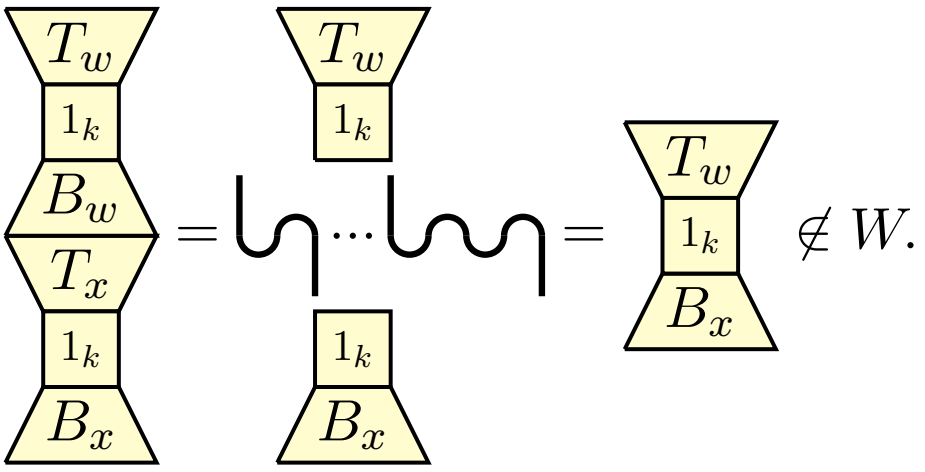
Suppose W is a nontrivial subspace of $\Delta_{\mathcal{R}_n^k}$ such that $W \neq \Delta_{\mathcal{R}_n^k}$. Let $w \in \text{basis}(W)$ such that w has at least one cap (this always exists since W is nontrivial). Then, we find an $x \in rTL_n = \text{basis}(\Delta_{\mathcal{R}_n^k})$ such that $wx \in rTL_n \setminus \text{basis}(W)$, which shows that W cannot be rTL_n-invariant, proving that $\Delta_{\mathcal{R}_n^k}$ is simple.

Using Lemma 4B.1, we can write $w = T_w \circ 1_k \circ B_w$, where $T_w = T$ is the fixed top half of the diagrams in rTL_n.

Then, we define $x = T_x \circ m_x \circ B_x$ to have:

- **(a)** k through strands, so $m_x = 1_k$,
- **(b)** $B_x \neq B_y$ for any $y \in W$, which is always possible to define since $W \subsetneq R_n^k$,
- **(c)** and T_x such that there is a cup placed directly to the left of every cap in B_w, which is always possible since w has at least one cap, and there can be no caps on the far left of the object $1\,2\,1\,2\ldots$.

Then, using the zigzag equations (4A.3), $B_w \circ T_x$ is reduced to the identity on k through strands, while T_w remains unchanged on the top. Therefore, $xw = T_w \circ 1_k \circ B_x \in R_n^k$, so $xw \neq 0$, but $xw \notin W$ by definition of B_x, hence W cannot be rTL_n-invariant. This is illustrated below:



Finally, the fact that this is all the simple representations of rTL_n follows from the classification Theorem 2A.9. □

Remark 4C.2. All cell representations are semisimple, but the monoid rTL_n is not semisimple: being semisimple would imply that the sum of the squares of the simple representations is the order of the monoid, but that is not true as our J-cells are not squares; cf. Proposition 4B.6. However, we can

think of rTL_n as being almost semisimple: only the slight asymmetry in its left and right cells sizes prevents it from being semisimple. ◇

Following [KST24], we will now truncate rTL_n, similarly to TL_n. From Proposition 4B.6 we find that the maximum of $|\mathcal{R}_n^k|$ occurs at $k = n+1$ (simply by the properties of the binomial coefficient). We consider the interval $n+1-\sqrt{2n} \leq k \leq n+1+\sqrt{2n}$, which has a width on the order of $\sqrt{2n}$, up to a scalar, and is centered around the peak at $k = n+1$. This is illustrated in Figure 3. To avoid unwieldy superscripts, as with the pivotal monoids, we will denote this truncated monoid by rTL_n^T.

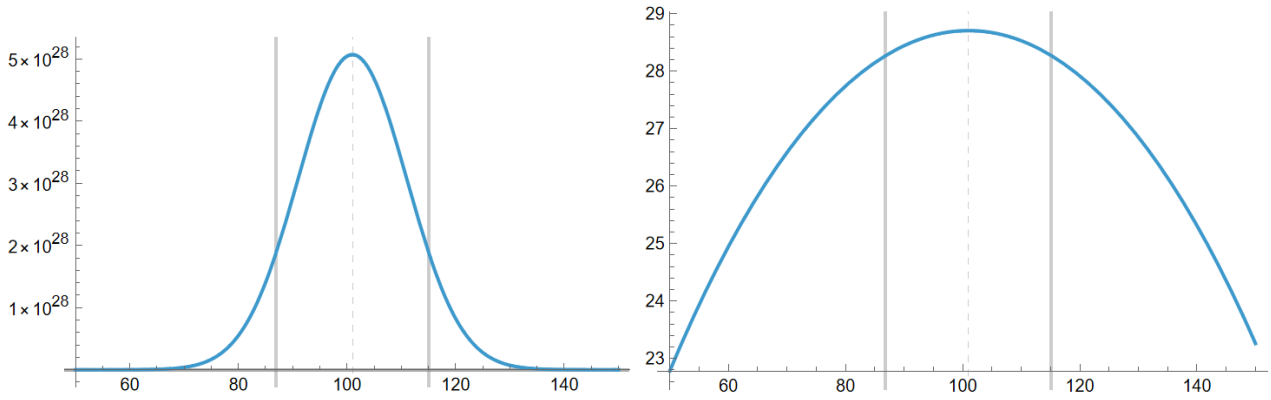


FIGURE 3. Left: The dimension of the simple representations over k, for $n = 100$, with vertical lines marking the truncation end points. Right: A Log10 version of the same graph.

Now we can find the RepGap and gap ratio, and compare the results with those for TL_n.

Theorem 4C.3. *We have the following inequalities for the RepGaps and gap ratios of* rTL_n^T

$$\boxed{2^{-1/2}\pi^{-1/2}e^{-1-\frac{1}{3n}}} \cdot \boxed{n^{-1/2}} \cdot \boxed{2^n} \leq \operatorname{Gap}_{\mathbb{K}} rTL_n^T \leq \boxed{2^{-1/2}\pi^{-1/2}} \cdot \boxed{n^{-1/2}} \cdot \boxed{2^n},$$

$$\boxed{2^{1/4}\pi^{-1/4}e^{-1-\frac{1}{3n}}} \cdot \boxed{n^{-1/4}} \leq \operatorname{Ratio}_{\mathbb{K}} rTL_n^T \leq \boxed{2^{1/4}\pi^{-1/4}} \cdot \boxed{n^{-1/4}}.$$

This is true over an arbitrary field $\mathbb{K}$.

Proof. The simple representations have dimension $\binom{n-1}{\frac{1}{2}(2n-k)}$ (combining the previous two propositions), which obviously has a maximum of $\binom{n-1}{\frac{1}{2}(n-1)}$. Due to the symmetry of the binomial coefficient, the minium will be at the two end points of the truncated interval, i.e. $k = n+1 \pm \sqrt{2n}$. Picking the lower endpoint, we can easily find the asymptotics of these using Mathematica.

Finally, due to the reasoning in Remark 3A.4, the bounds on the gap ratio are calculated based on $|rTL_n|$. □

Combining this with Theorem 3A.3, we have the following conclusion for $\operatorname{char}\mathbb{K} = 0$ (which is only needed for TL_n itself, see Remark 4C.5).

Corollary 4C.4. *Assume* $\operatorname{char}\mathbb{K} = 0$. *Then:*

$$\operatorname{Gap}_{\mathbb{K}} rTL_n^T \leq \boxed{n^2} \cdot \boxed{2^{-n}} \cdot \operatorname{Gap}_{\mathbb{K}} TL_n^T,$$

$$\operatorname{Ratio}_{\mathbb{K}} rTL_n^T \geq \boxed{e^{-1-\frac{1}{3n}}} \cdot \boxed{n^{1/2}} \cdot \operatorname{Ratio}_{\mathbb{K}} TL_n^T.$$

Thus, we get the table entries as in the introduction. □

Although rTL_n is slightly better than TL_n in terms of the gap ratio, the fact that it is significantly worse in terms of RepGap makes it less suitable for cryptographic purposes. Also, rTL_n is essentially semisimple over an arbitrary field, see Remark 4C.2, and for these reasons it may be too easy for cryptography purposes.

Remark 4C.5. The behavior of the monoid TL_n/category TL is very different in prime characteristic compared to $\operatorname{char}\mathbb{K} = 0$, see e.g. [**An19**, **Sp23**, **STWZ23**] (where we specialize so that the circle parameter is one in these papers). In contrast, surprisingly, rTL_n is characteristic free. ◇

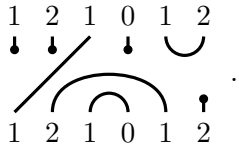
5. The rigid Motzkin monoid

In this section we define a non-pivotal version of the Motzkin algebra/monoid as, for example, in [**BH14**]. This will be done in a similar way to the previous section, so we will be brief whenever appropriate.

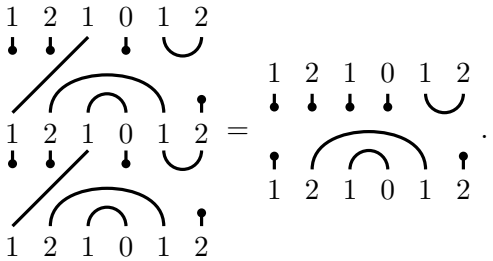
5A. Definition of rMo_n.

Similarly to rTL_n we define:

Definition 5A.1. The ***rigid Motzkin category*** rMo has objects the same as those in rTL, and morphisms defined as partitions of those objects, similarly to rTL, however we also allow parts of size 1, i.e. we allow unpaired partitions. In diagram form, this would be denoted by a *top dot* or *bottom dot*, generally referred to as *dots*, as seen in the following example:



Composition of diagrams is defined similarly to rTL, for example:



Everything else, such as the tensor product, tensor unit, duals, etc., are defined in the same way as in rTL. Finally, the ***rigid Motzkin monoid*** is

$$rMo_n := \operatorname{End}_{rMo}(1\,2)^{\otimes n},$$

where, as before, our object of choice is $(1\,2)^{\otimes n}$. ◇

We leave it to the reader to formulate and verify that rMo shares the same categorical properties as rTL.

5B. Computing cells for rMo_n.

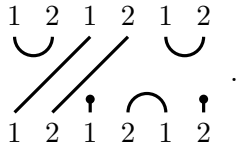
We proceed analogously to rTL:

Lemma 5B.1. *Any $d \in rMo_n$ can be written*

$$d = \tau \circ 1_{\alpha(k)} \circ \beta \tag{5B.2}$$

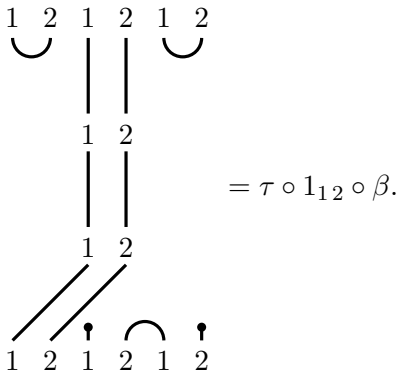
for diagrams $\tau, \beta \in rMo$ and some sequence $\alpha(k)$ of length k in 1 and 2, $0 \leq k \leq 2n$.

Proof. If $d \in rMo_n$ has k through strands, define the sequence $\alpha(k)$ as the sequence of through strands read from left to right; explicitly, $\alpha(k)_i = 1$ if the ith through strand pairs two 1s, and $\alpha(k)_i = 2$ if the ith through strand pairs two 2s. For example, the following diagram has the sequence 1 2:



Note that, unlike rTL_n, the number of through strands can be any integer $0 \leq k \leq 2n$.

Given the sequence $\alpha(k)$, the result follows via the same argument as that used for Lemma 4B.1, as once again only the final partition matters when determining the result of a composition. For example, the above diagram with $\alpha(k) = 1\,2$ becomes:



$= \tau \circ 1_{1\,2} \circ \beta.$

The proof is complete. □

Now, for $n \geq 0$ fix a sequence of k through strands $\alpha(k)$. Since the diagrams in rMo_n are planar, the through strands create an ordered partition of both the top and bottom objects. For the above example, $\alpha(k)$ partitions the bottom and top object into the blocks $[[], [], [1\,2\,1\,2]]$ and $[[1\,2], [], [1\,2]]$ respectively, including the empty blocks.

Denote by j_i, $1 \leq i \leq k+1$, the size of the block to the left of the through strand $\alpha(k)_i$. Then we have an ordered partition

$$j_1 + j_2 + ...j_{k+1} = 2n - k. \tag{5B.3}$$

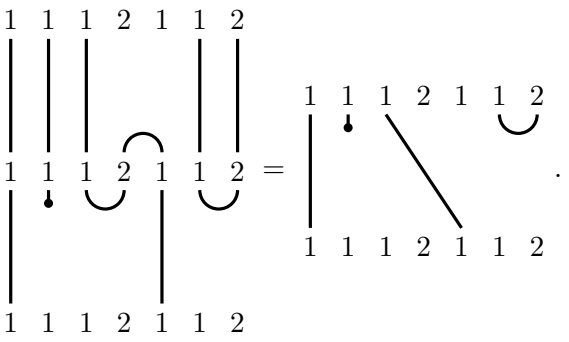
Define a partial order on the sequences $\alpha(k)$ by $\alpha(k) \leq \beta(k') \iff \alpha(k)$ is a subsequence of $\beta(k')$. Let k_x denote the number of through strands in the diagram x, and $\alpha(k_x)$ the corresponding sequence.

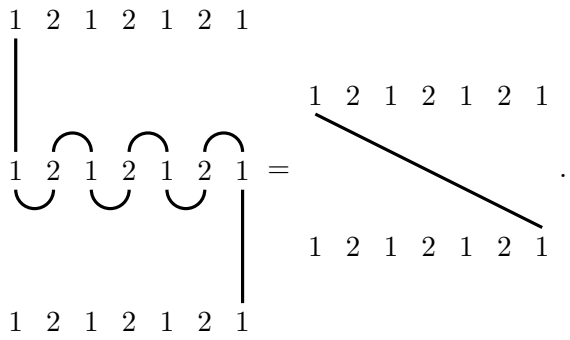
Lemma 5B.4. *For any diagrams $x, y \in rMo_n$, $\alpha(k_x) \geq \alpha(k_{xy})$ and $\alpha(k_x) \geq \alpha(k_{yx})$.*

Proof. This follows by observing that composing two diagrams can never add any through strands, while they can remove them. Through strands only occur in the composition xy when a number in the top object of x is connected to a number in the bottom object of y via a continuous line. Therefore, each through strand in xy is a result of a composition between a through strand in x and a through strand in y, possibly with some caps and cups in the middle.

This naturally means that there is no way to add any new through strands via composition, since they each must correspond to a pair of through strands from x, y. In all other cases, the through strand from x or y will disappear in xy, to become either a cap, cup, or dot, since there is no continuous line between the top object of x and the bottom object of y.

As a result, the resulting sequence of through strands of xy must be a subsequence of both $\alpha(k_x)$ and $\alpha(k_y)$. The diagrams below summarize some of the possible cases for compositions involving through strands:





The general pattern is similar. □

Proposition 5B.5. *The cells of rMo_n have the following properties:*

- **(a)** *The J-cells of rMo_n are uniquely determined by the sequence of through strands $\alpha(k)$. That is, each J-cell is of apex $\alpha(k)$, with a partial order given by the partial order on sequences.*
- **(b)** *Within each J-cell, sizes of the right and left cells can be found by counting the number of diagrams when fixing the top respectively bottom half. Explicitly, we have*

$$|\mathcal{R}_n^{\alpha(k)}| = \sum_{\substack{j_1+\ldots+j_{k+1}\\=2n-k}} \prod_{i=1}^{k+1} B_{j_j}^0$$

and

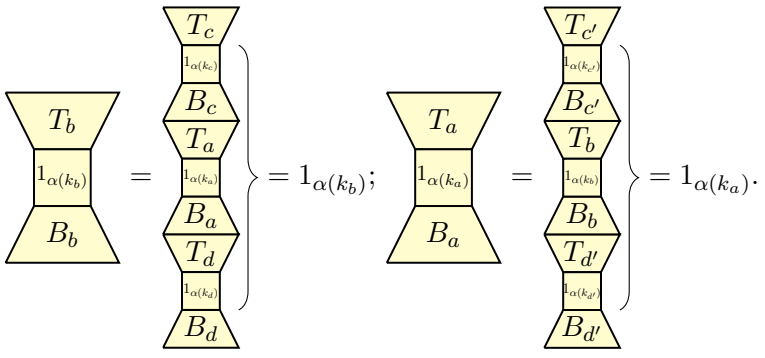
$$|\mathcal{L}_n^{\alpha(k)}| = \sum_{\substack{j_1+\ldots+j_{k+1}\\=2n-k}} \prod_{i=1}^{k+1} T_0^{j_j}$$

where the sum is over the partition of through strands (5B.3), and $B_{j_i}^0$ and $T_0^{j_i}$ denote the number of possible diagrams on the block of the bottom respectively top object of size j_i.

- **(c)** *Every J-cell of rMo_n is idempotent.*

Proof. Fix a J-cell $\mathcal{J}$, and suppose $a, b \in J$, meaning $a \leq_{lr} b$ and $b \leq_{lr} a$. This means $\exists c, c', d, d' \in rMo_n$ such that $b = cad$ and $a = c'bd'$.

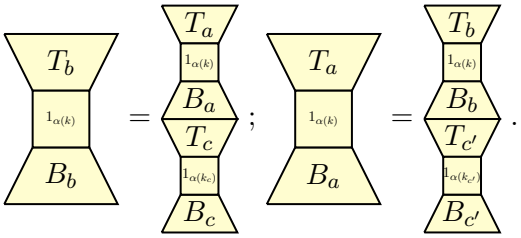
Using Lemma 5B.1, we have:



In the left equation, the middle of the right hand side must resolve to $1_{\alpha(k_b)}$, and since $1_{\alpha(k_a)}$ is contained within that middle, $\alpha(k_a) \geq \alpha(k_b)$ (using Lemma 5B.4. Similarly, $\alpha(k_b) \geq \alpha(k_a)$, and thus $\alpha(k_a) = \alpha(k_b)$.

Clearly, if $\alpha(k_a) = \alpha(k_b)$, then $a \leq_{lr} b$ and $b \leq_{lr} a$, and hence the J-cells of rMo_n are completely determined by the sequences of through strands.

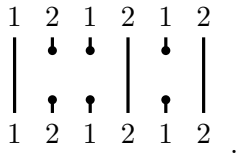
The argument for right and left cells is similar. If we have $a, b \in J$, with sequence of through strands $\alpha(k)$, then the condition for $a \sim_r b$ is:



which shows that $a \sim_r b \iff T_a = T_b$, i.e. the top half of the diagrams is the same. Similar reasoning shows that $a \sim_l b \iff B_a = B_b$.

Given this, we know that the through strands of a diagram partition both the top and bottom into blocks, with sizes given by (5B.3). For a fixed partition, these blocks are independent of each other, thus the number of diagrams is the product of the number of diagrams within each block. Taking the sum over all partitions gives the desired result.

Finally, if there are k through strands, the J-cell of apex $\alpha(k)$ contains an idempotent that has pairs of dots everywhere there are no through strands (in general there are multiple of these for each sequence of through strands). For example, if $n = 3$ and $\alpha(k) = 1\,2\,2$, then the following diagram is an idempotent in the corresponding J-cell:



The general case can be verified similarly. □

Remark 5B.6. In general, we cannot compare all J-cells of rMo_n, so there is no total order like with rTL_n, only the partial order determined by the sequences of through strands: $J_{\alpha(k_1)} < J_{\alpha(k_2)} \iff \alpha(k_1)$ is a subsequence of $\alpha(k_2)$. As a result, we have a more complicated (or exciting) cell structure, seen in Figure 4. ◇

With this set up, we will continue to focus on the right cells, and the results for the left cells follow similarly.

Proposition 5B.7. *For all $m \in \mathbb{Z}_{\geq 0}$, the number of possible diagrams on the bottom object $1\,2\,1\,2\ldots$ of length m is given by:*

$$A^0_m = C\left(\left\lfloor \frac{m+1}{2} \right\rfloor\right) \tag{5B.8}$$

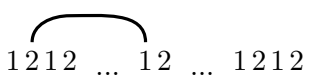
where $C(l)$ denotes the lth Catalan number. Moreover, if instead we have $2\,1\,2\,1$ of length m, then the number of diagrams is A^0_{m+2} if m is even and A_{m+1} if m is odd.

Proof. Let $m = 2l$ be even, and note that $A^0_0 = 1$ (the only option is the empty diagram $1_{\mathbb{1}}$). We claim that:

$$A^0_{2l} = \sum_{i=1}^{l} A^0_{2i-2} A^0_{2l-2i} \tag{5B.9}$$

which is the familiar recurrence relation for the Catalan numbers, so assuming (5B.9), we obtain $A^0_{2l} = C(l) = C(m/2)$. Observe also that if we consider $1\,2\,1\,2\ldots1\,2\,1$ of length $2l-1$, adding a 2 to the right changes nothing, since it cannot pair with anything to the left, and there is no 1 to the right to pair with. Therefore, $A^0_{2l-1} = A^0_{2l}$ so we finally have $A^0_m = C\left(\lfloor \frac{m+1}{2} \rfloor\right)$.

Now, to prove (5B.9), consider the possibilities for the first 2 in $1\,2\,1\,2\ldots1\,2$ (of length $2l$):



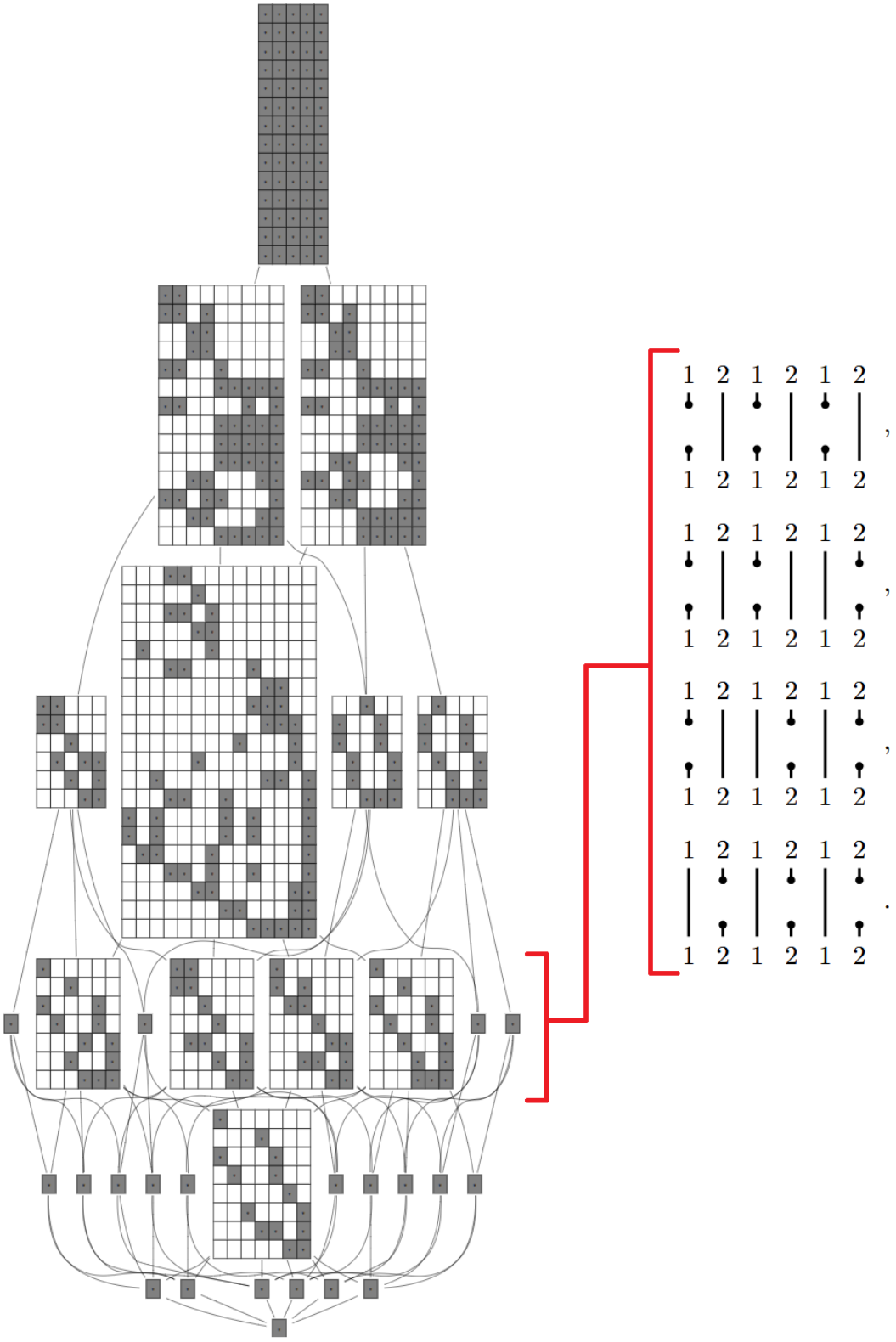
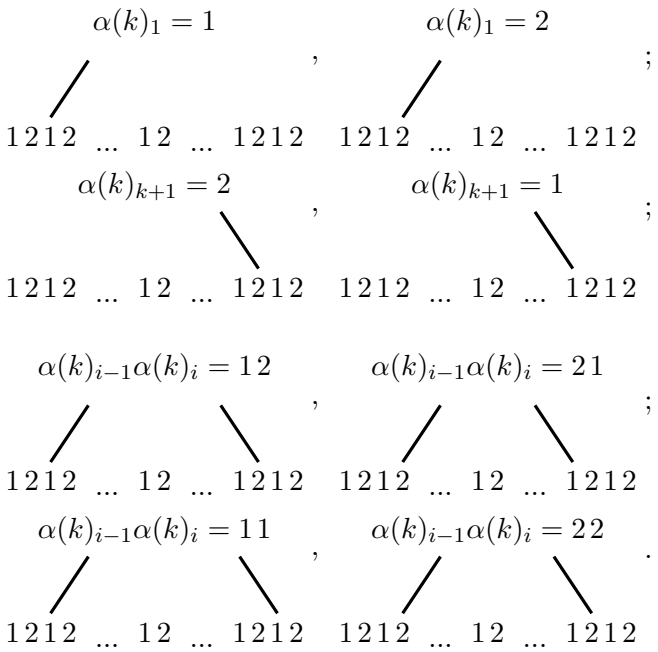


FIGURE 4. Left: The cell structure for rMo_3. Right: explicit diagrams representing the single elements of the four J-cells of size 1 for $k = 3$.

If we pair the first 2 with the ith 1 following that 2, we have $1\,2...1\,2$ of length $2i-2$ under the cap, and $1\,2...1\,2$ of length $2l-2i$ remaining outside the cap, noting that the interruption where the cap is placed can be ignored, since the diagram is planar and thus we treat inside and outside the cap separately. These can be arranged independently in $A^0_{2i-2}A^0_{2l-2i}$ ways. Setting $i = l$ for the case where the first 2 remains unpaired, we thus conclude the recurrence relation (5B.9).

Finally, if we have $1\,2\,1\,2...1\,2$ of length $m+2$, the first 1 and the final 2 must remain unpaired, so the number of diagrams A^0_{m+2} on this object is the same as the number of diagrams on $2\,1\,2\,1...2\,1$ of length m. In the case $2\,1\,2\,1...2\,1\,2$ of length m (i.e. odd), the final 2 must remain unpaired, so the number of ways is the same as $2\,1\,2\,1...2\,1$ of length $m-1$, which is A^0_{m+1}. □

Consider now the following cases for $\alpha(k)$:



where $2 \leq i \leq k+1$. Recall from (5B.3) that the through strands partition the bottom object into $k+1$ blocks of size ≥ 0. Each block is of size j_i and corresponds to the block to the left of the ith through strand, except for block $k+1$, which corresponds to the block to the right of the kth through strand. We summarise the above cases for each block, using Proposition 5B.7, in the following table:

(5B.10)

Case	Block	Block Shape	No. Diagrams
$\alpha(k)_1 = 1$	j_1 even, $j_1 \geq 0$	$1\,2...1\,2$	$C(j_1/2)$
$\alpha(k)_1 = 2$	j_1 odd, $j_1 \geq 1$	$1\,2...1\,2\,1$	$C((j_1+1)/2)$
$\alpha(k)_{k+1} = 2$	j_{k+1} even, $j_{k+1} \geq 0$	$1\,2...1\,2$	$C(j_{k+1}/2)$
$\alpha(k)_{k+1} = 1$	j_{k+1} odd, $j_{k+1} \geq 1$	$2\,1...2\,1\,2$	$C((j_{k+1}+1)/2)$
$\alpha(k)_{i-1}\alpha(k)_i = 12$	j_i even, $j_i \geq 0$	$2\,1...2\,1$	$C(j_i/2+1)$
$\alpha(k)_{i-1}\alpha(k)_i = 21$	j_i even, $j_i \geq 0$	$1\,2...1\,2$	$C(j_i/2)$
$\alpha(k)_{i-1}\alpha(k)_i = 11$	j_i odd, $j_i \geq 1$	$2\,1...2\,1\,2$	$C((j_i+1)/2)$
$\alpha(k)_{i-1}\alpha(k)_i = 22$	j_i odd, $j_i \geq 1$	$1\,2...1\,2\,1$	$C((j_i+1)/2)$

Observe that for all even j_i, except if $\alpha(k)_{i-1}\alpha(k)_i = 12$, the number of diagrams is equal to $C(j_i/2)$, and for all odd j_i, the number of diagrams is equal to $C((j_i+1)/2)$. For this reason, we need the following lemma.

Lemma 5B.11. *Let $\alpha(k)$ be a sequence of k through strands with j occurrences of the block $1\,2$. Then, we have:*

- **(a)** *all such sequences $\beta(k)$ with j occurrences of $1\,2$ have the same numbers of odd and even blocks, and*
- **(b)** *the number of such sequences is equal to $\binom{k+1}{2j+1}$.*

Proof. For part (a), we begin with a sequence $\alpha(k)$ with j $1\,2$ blocks, then we show that if we create a new sequence $\beta(k)$ by changing a 1 into a 2 or a 2 into a 1, we either preserve the counts outlined in the proposition, or the number of $1\,2$ blocks changes. We have the following cases:

- **(a)** The first number is a 1 and $\alpha(k) = \mathbf{1}\,1...1\,2\,\alpha(k)_{i\geq m+1}$ where we have only considered up to the first appearance of a 2 at $i = m$. Then if we set $\beta(k) = \mathbf{2}\,1...1\,2\,\alpha(k)_{i\geq m+1}$, the number

of 1 2 blocks hasn't changed, the first block has changed from even to odd, and the second block has changed from odd to even. Hence, the required counts remain the same.

(b) The first number is a 2 and $\alpha(k) = \mathbf{2}\,2...2\,1\,1...1\,2\,\alpha(k)_{i\geq m+1}$.
Then, if $\beta(k) = \mathbf{1}\,2...2\,1...1\,2\,\alpha(k)_{i\geq m+1}$ we have increased the number of 1 2 blocks.

(c) The last number is a 1 and in $\beta(k)$ we change this 1 into a 2. Then there are two cases:
- **(i)** $\alpha(k) = \alpha(k)_{i\leq k-2}\,2\,\mathbf{1}$, then if $\beta(k) = \alpha(k)_{i\leq k-2}\,2\,\mathbf{2}$, we have changed the final block from odd to even and changed the second last block from even to odd, leaving the rest unchanged.
- **(ii)** $\alpha(k) = \alpha(k)_{i\leq k-2}\,1\,\mathbf{1}$, then if $\beta(k) = \alpha(k)_{i\leq k-2}\,1\,\mathbf{2}$, we have increased the number of 1 2 blocks.

(d) The last number is a 2 and in $\beta(k)$ we change this 2 into a 1. Then there are two cases:
- **(i)** $\alpha(k) = \alpha(k)_{i\leq k-2}\,2\,\mathbf{2}$, then if $\beta(k) = \alpha(k)_{i\leq k-2}\,2\,\mathbf{1}$, we have changed the final block from even to odd and changed the second last block from odd to even, so the overall counts remain unchanged.
- **(ii)** $\alpha(k) = \alpha(k)_{i\leq k-2}\,1\,\mathbf{2}$, then if $\beta(k) = \alpha(k)_{i\leq k-2}\,1\,\mathbf{1}$, we have decreased the number of 1 2 blocks.

(e) $\alpha(k) = \alpha(k)_{i\leq m-1}\mathbf{1}\alpha(k)_{i\geq m+1}$, and $\beta(k) = \alpha(k)_{i\leq m-1}\mathbf{2}\alpha(k)_{i\geq m+1}$. Then, there are four cases:
- **(i)** $\alpha(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{1}\,1\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{2}\,1\alpha(k)_{i\geq m+2}$, then we have increased the number of 1 2 blocks.
- **(ii)** $\alpha(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{1}\,2\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{2}\,2\alpha(k)_{i\geq m+2}$, then we have lost a 1 2 block in the the $m+1$st position and an odd block in the $m-1$st position, but gained a 1 2 block in the $m-1$st position and an odd block in the $m+1$st position, so the overall counts remain unchanged.
- **(iii)** $\alpha(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{1}\,1\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{2}\,1\alpha(k)_{i\geq m+2}$, then we have lost an even block in the $m-1$st position and an odd block in the $m+1$st position, but gained an odd block in the $m-1$st position and an even block in the $m+1$st position, so the overall counts remain unchanged.
- **(iv)** $\alpha(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{1}\,2\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{2}\,2\alpha(k)_{i\geq m+2}$, then we have decreased the number of 1 2 blocks.

(f) $\alpha(k) = \alpha(k)_{i\leq m-1}\mathbf{2}\alpha(k)_{i\geq m+1}$, and $\beta(k) = \alpha(k)_{i\leq m-1}\mathbf{1}\alpha(k)_{i\geq m+1}$. Then, there are four cases:
- **(i)** $\alpha(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{2}\,1\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{1}\,1\alpha(k)_{i\geq m+2}$, then we have decreased the number of 1 2 blocks.
- **(ii)** $\alpha(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{2}\,2\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}1\,\mathbf{1}\,2\alpha(k)_{i\geq m+2}$, then we have lost a 1 2 block in the $m-1$st position and an odd block in the $m+1$st position, but gained an odd block in the $m-1$st position and a 1 2 block in the $m+1$st position, so the overall counts remain unchanged.
- **(iii)** $\alpha(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{2}\,1\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{1}\,1\alpha(k)_{i\geq m+2}$, then we have lost an odd block in the $m-1$st position and an even block in the $m+1$st position, but gained an even block in the $m-1$st position and an odd block in the $m+1$st position, so the overall counts remain unchanged.
- **(iv)** $\alpha(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{2}\,2\alpha(k)_{i\geq m+2}$. If $\beta(k) = \alpha(k)_{i\leq m-2}2\,\mathbf{1}\,2\alpha(k)_{i\geq m+2}$, then we have increased the number of 1 2 blocks.

Hence, since this covers every case for changing a 1 into a 2 or a 2 into a 1 for $\alpha(k)$, we have shown that the numbers of odd and even blocks remain unchanged if the number of 1 2 blocks remains unchanged.

Now, for part (b), consider a sequence $\alpha(k)$ of length k, made only of 1s and 2s, with j occurrences of the substring 1 2. Firstly, observe that if $j = 0$, the number of possible sequences is clearly

$k+1 = \binom{k+1}{1}$, since it's the number of sequences of the form 2 2...2 1 1...1 (including the sequences of all 2s and all 1s).

Now suppose $1 \leq j \leq \lfloor \frac{k}{2} \rfloor$. Suppose the first 1 is in the ith position, $1 \leq i \leq k-2j+1$, and suppose there is a sequence of 1s of length l (including the first 1), $1 \leq l \leq k-i-2j+1$:

$$\overbrace{\underbrace{2\,2...2}_{i-i}\,\underbrace{1\,1...1\,1}_{l}\,\underbrace{*\,*\,*}_{k-i-l+1}}^{k}$$

Then, we are placing $2j-1$ 1s and 2s (including the first 2 after the 1s) somewhere inside the remaining sequence of length $k-i-l+1$, which can be done in $\binom{k-i-l+1}{2j-1}$ ways.

Thus, the total number of ways is $\sum_{i=1}^{k-2j+1}\sum_{l=1}^{k-i-2j+2}\binom{k-i-l+1}{2j-1}$. Using the Hockey-Stick identity, we obtain:

$$\begin{aligned}\sum_{i=1}^{k-2j+1}\sum_{l=1}^{k-i-2j+2}\binom{k-i-l+1}{2j-1} &= \sum_{i=1}^{k-2j+1}\binom{k-i+1}{2j} \\ &= \binom{k+1}{2j+1}\end{aligned}$$

as required. □

Remark 5B.12. Lemma 5B.11 shows that to find the sizes of right cells, we only need to consider the sequence of the form 1 2 1 2...1 2 2...2, for each number of 1 2 blocks j, $0 \leq j \leq \lfloor \frac{k}{2} \rfloor$. Furthermore, we see that the 1 2 blocks have $C(j_i/2+1)$ possible diagrams, which is larger than any of the other blocks, and the number of different partitions (5B.3) also increases as j increases. We prove the latter fact when discussing the planar rook monoid below (see Proposition 6B.1). Thus, the total number of possible diagrams increases as j increases, with a minimum at $j=0$. This means that when finding the semisimple RepGap, we will need to focus on the $j=0$ case. ◇

We denote by $\mathcal{R}_n^{k,j}$ the right cell arising from this particular sequence.

Proposition 5B.13. *Fix $n \in \mathbb{Z}_{\geq 0}$, $0 \leq k \leq n$, and sequence of through strands $\alpha(k)$ with j 1 2 blocks, $0 \leq j \leq \lfloor \frac{k}{2} \rfloor$. Then, the size of the corresponding right cell is:*

$$|\mathcal{R}_n^{k,j}| = \sum_{r=0}^{k-j}(-1)^r \frac{k-r+1}{2n+k-r+1}\binom{k-j}{r}\binom{2n+k-r+1}{n} \tag{5B.14}$$

the size of the corresponding left cell is:

$$|\mathcal{L}_n^{k,j}| = \sum_{r=0}^{k-j+1}(-1)^r \frac{k-r+1}{2n+k-r+3}\binom{k-j+1}{r}\binom{2n+k-r+3}{n+1} \tag{5B.15}$$

and the size of the monoid is:

$$|rMo_n| = \sum_{k=0}^{2n}\sum_{j=0}^{\lfloor \frac{k}{2} \rfloor}\binom{k+1}{2j+1}|\mathcal{R}_n^{k,j}||\mathcal{L}_n^{k,j}|. \tag{5B.16}$$

Proof. We have the sequence

$$\alpha(k) = \underbrace{1\,2\,1\,2...1\,2}_{2j}\,\underbrace{2\,2...2}_{k-2j}$$

creating an ordered partition of the bottom object, with sizes $j_1, j_2, ..., j_{k+1}$ such that

$$j_1 + j_2 + ...j_{k+1} = 2n-k.$$

With reference to the table (5B.10), the blocks of the partition are as follows:

(a) j_1 is even, $j_1 \geq 0$, and the number of possible diagrams in the block is $C(j_1/2)$

(b) j_{k+1} is even, $j_{k+1} \geq 0$, and the number of possible diagrams in the block is $C(j_{k+1}/2)$

(c) j_{2l} is even, $j_{2l} \geq 0$, and the number of possible diagrams in the block is $C(j_{2l}/2+1)$ for $l = 1, 2, ..., j$

(d) j_{2m+1} is even, $j_{2m+1} \geq 0$, and the number of possible diagrams in the block is $C(j_{2m+1}/2)$ for $m = 1, 2, ..., j-1$

(e) j_p is odd, $j_p \geq 1$, and the number of possible diagrams in the block is $C((j_p+1)/2)$ for $p = 2j+1, 2j+2, ..., k$

Hence, using Proposition 5B.5, we obtain

$$|\mathcal{R}_n^{k,j}| = \sum_{\substack{j_1+...+j_{k+1} \\ =2n-k}} C(j_1/2)C(j_2/2+1)C(j_3/2)...C(j_{2j}/2+1)C((j_{2j+1}+1)/2)...C((j_k+1)/2)C(j_{k+1}/2).$$

Now set $x_1 = \frac{j_1}{2}$, $x_{2l} = \frac{j_{2l}}{2} + 1$ for $l = 1, ..., j$, $x_{2m+1} = \frac{j_{2m+1}}{2}$ for $m = 1, ..., j-1$, $x_p = \frac{j_p+1}{2}$ for $p = 2j+1, ..., k$, and $x_{k+1} = \frac{x_{k+1}}{2}$. Then, the above becomes

$$|\mathcal{R}_n^{k,j}| = \sum_{x_1+...+x_{k+1}=n} C(x_1)C(x_2)...C(x_{k+1}).$$

This is almost the definition of the Catalan k-fold convolution, however we have $x_{2l} \geq 1$ and $x_p \geq 1$ for $l = 1, ..., j$ and $p = 2j+1, ...k$, so we instead need an alternating sum of Catalan k-fold convolutions (noting that $C(0) = 1$):

$$\begin{aligned}|\mathcal{R}_n^{k,j}| = \sum_{\substack{x_1+...+x_{k+1}=n \\ x_i \geq 0}} C(x_1)...C(x_{k+1}) - \binom{k-j}{1} \sum_{\substack{x_1+...+x_{k+1}=n \\ x_i \geq 0 \\ x_2=0}} C(x_1)...C(x_{k+1}) \\ +... + (-1)^{k-j}\binom{k-j}{k-j} \sum_{\substack{x_1+...+x_{k+1}=n \\ x_i \geq 0 \\ x_{2l},x_p=0}} C(x_1)...C(x_{k+1})\end{aligned}$$

where in each term we have set r of the $k-j$ x_i that are ≥ 1 to zero, noting that the formula will remain the same regardless of which we choose, so we can simply multiply by a binomial coefficient. From [**LS25**, Proposition 1.2], the formula for the Catalan k-fold convolution is

$$\sum_{\substack{m_1+...m_k=n \\ m_i \geq 0}} C(m_1)...C(m_k) = \frac{k}{2n+k}\binom{2n+k}{n}$$

which finally gives

$$|\mathcal{R}_n^{k,j}| = \sum_{r=0}^{k-j} (-1)^r \frac{k-r+1}{2n+k-r+1}\binom{k-j}{r}\binom{2n+k-r+1}{n}$$

as required. The argument for left cells is similar.

Finally, observe that if we fix the sequence $\alpha(k)$, the top half and bottom half of the diagrams become independent of each other. Thus, the number of possible diagrams in the monoid for each sequence $\alpha(k)$ is the number of bottom half diagrams multiplied by the number of bottom half diagrams, then to find the total $|rMo_n|$ by taking the sum over all sequences $\alpha(k)$, then another sum over all k, $0 \leq k \leq 2n$.

Using Lemma 5B.11, we can then simplify this to give

$$|rMo_n| = \sum_{k=0}^{2n} \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k+1}{2j+1} |\mathcal{R}_n^{k,j}||\mathcal{L}_n^{k,j}|.$$

□

5C. **Semisimple RepGap and gap ratio of rMo_n.** As we have seen above, although rMo_n can largely be treated in the same way as Mo_n, certain differences make rMo_n more intricate. This trend will continue in this section.

Remark 5C.1. By Lemma 2A.10, the semisimple RepGap is an upper bound for the RepGap, and we will see that this upper bound alone is enough to determine that rMo_n is less suitable for cryptography than Mo_n. It is worth noting, however, that this upper bound is strictly larger than the RepGap.

Using [**Tu24**, Proposition 2D.7], we can compute the dimensions of the simple representations by computing the ranks of corresponding Gram matrices. Setting $n = 3$ and $k = 2$, we obtain ranks $4, 5, 5$, and 12, in increasing order of dimension (using GAP). The semisimple dimension can be easily computed via Proposition 5B.13, which gives 5 for $j = 0$ and 14 for $j = 1$.

This shows first and foremost that the RepGap is strictly smaller than the semisimple RepGap in general, and it also reveals that there are further distinguishing features of the sequence of through strands apart from simply the number of $1\,2$ pairs when we are at the level of simple representations. In this case, the minimal simple dimension corresponds to the sequence $2\,1$. ◇

We now compute the asymptotics of the semisimple RepGap for rMo_n. Using Mathematica, we can simplify the equations from Proposition 5B.13 for the sizes of the left and right cells to:

$$|\mathcal{R}_n^{k,j}| = \frac{k+1}{2n+k+1}\binom{2n+k+1}{n}{}_2F_1(j-k,-1-k-n,-k-2n,1) + \frac{k-j}{2n+k}\binom{2n+k}{n}{}_2F_1(j-k+1,-k-n,1-k-2n,1),$$

$$|\mathcal{L}_n^{k,j}| = \frac{k+1}{2n+k+3}\binom{2n+k+3}{n+1}{}_2F_1(j-k-1,-2-k-n,-2-k-2n,1) + \frac{k-j+1}{2n+k+2}\binom{2n+k+2}{n+1}{}_2F_1(j-k,-1-k-n,-1-k-2n,1).$$

Here, and throughout, ${}_2F_1$ denotes the hypergeometric series:

$${}_2F_1(a,b,c,z) = \sum_{n=0}^{\infty}\frac{(a)_n(b)_n}{(c)_n}\frac{z^n}{n!}.$$

where $(x)_n = x(x+1)(x+2)...(x+n-1)$ is the *Pochhammer symbol* or *rising factorial*. In particular, for $m > 0$,

$$ {}_2F_1(-m,b,c,z) = \sum_{n=0}^{m}(-1)^n\binom{m}{n}\frac{(b)_n}{(c)_n}z^n \tag{5C.2}$$

Note that, in our case, $c \in \mathbb{Z}_{<0}$, which creates some difficulties, as explained in the following remark:

Remark 5C.3. Typically, one leaves Pochhammer symbols undefined for negative integers, and Gauss' hypergeometric series undefined for negative integers c. However, we are able to extend both to negative integers in this case.

Firstly, for $x \in \mathbb{Z}_{>0}$, define $(-x)_n = (-x)(-x+1)...(-x+n-1)$. It's easy to see that $(-x)_n = (-1)^n\prod_{r=0}^{n}(x-r) = (-1)^n(x-n+1)_n$, allowing us to return to the familiar Pochhammer symbol. With this, noting that $(-x)_n = 0$ if $n > x$, we obtain the finite sum (5C.2).

${}_2F_1(a,b,c,z)$ has been defined in some cases where $c \in \mathbb{Z}_{<0}$, when $a < 0$ or $b < 0$, such as for Krawtchouk polynomials (introduced in [**Kr29**], later reformulated in terms of the hypergeometric function [**AW85**, Appendix]). Some work has also been done towards generalizing this in [**Gr17**]. In our case, we can simply consider ${}_2F_1(-m,b,c+\epsilon,z)$ for some small $\epsilon > 0$, then take the limit as $\epsilon \to 0$. Since all our sums are finite, we can write our arguments without the ϵ, implicitly assuming we are taking limits. ◇

Next we have the Chu–Vandermonde identity for the hypergeometric series.

Lemma 5C.4. *Let $m \in \mathbb{Z}_{>0}$ and b, c such that $m + c - 1 \neq 0$. Then*

$$ {}_2F_1(-m, b, c, 1) = \frac{(c-b)_m}{(c)_m}.$$

Proof. This is probably well-known, but we were not able to find a reference, so we give a proof. We follow the proof from [Si05], which uses the method of Wilf–Zeilberger pairs. Define:

$$f(m) := \frac{(c)_m}{(c-b)_m} {}_2F_1(-m, b, c, 1) = \sum_{k=0}^{m} \frac{(-m)_k (b)_k (c)_n}{k!(c)_k (c-b)_n}$$

We also define for $0 \leq k \leq m$:

$$F(m,k) = \frac{(-m)_k (b)_k (c)_m}{k!(c)_k (c-b)_m}$$

$$G(m,k) = \frac{k(1-c-k)}{m(m+c-1)}$$

and

$$H(m,k) = F(m,k)G(m,k).$$

Then, we have the following equalities (noting that $F(m,k) \neq 0$):

$$\begin{aligned} \frac{F(m,k) - F(m-1,k)}{F(m,k)} &= \frac{(-m)_k (b)_k (c)_m - (-m+1)_k (b)_k (c)_{m-1}(c-b+m-1)}{(-m)_k (b)_k (c)_m} \\ &= \frac{(m-k)(c+m-1) - m(c-b+m-1)}{(m-k)(c+m-1)} \\ &= \frac{bm + k(c-b+m-1)}{m(c+m-1)} \end{aligned}$$

and

$$\begin{aligned} \frac{F(m,k+1)G(m,k+1)}{F(m,k)} - G(m,k) &= \frac{(-m)_{k+1}(b)_{k+1}(c)_k}{(-m)_k (b)_k (c)_{k+1}} \frac{(-c-k)}{m(m+c-1)} + \frac{k(k+c-1)}{m+c-1} \\ &= \frac{(m-k)(b+k) + k(k+c-1)}{m(m+c-1)} \\ &= \frac{bm + k(c-b+m-1)}{m(c+m-1)}. \end{aligned}$$

Thus, $F(m,k) - F(m-1,k) = F(m,k+1)G(m,k+1) - F(m,k)G(m,k) = H(m,k+1) - H(m,k)$, and therefore

$$f(m) - f(m-1) = \sum_{k=0}^{m} F(m,k) - F(m-1,k) = \sum_{k=0}^{m} H(m,k+1) - H(m,k).$$

The sum on the right is a telescoping sum that resolves to $H(m,m+1) - H(m,0)$, and observing that

$$(-m)_{m+1} = (-m)(-m+1)...(-m+m-1)(-m+m) = 0 \implies F(m,m+1) = 0$$

and

$$\frac{0(1-c-0)}{m(m+c-1)} = 0 \implies G(m,0) = 0$$

gives that $f(m) - f(m-1) = 0$.

Hence, $f(m)$ is constant for all $m \in \mathbb{Z}_{>0}$, so $f(m) = f(0) = 1$, and finally we rearrange

$$1 = \frac{(c)_m}{(c-b)_m} {}_2F_1(-m, b, c, 1)$$

to give the desired result. □

Remark 5C.5. Typical proofs of the Chu–Vandermonde identity use Gauss' hypergeometric theorem (see e.g. [AAR99, Corollary 2.2.3]), however these all require that $Re(c-a+b) > 0$, which is insufficient for our purposes, hence the alternate, more general proof. ◇

Using Lemma 5C.4 and $(-x)_n = (-1)^n(x-n+1)_n$, noting that the conditions in the lemma hold for all the hypergeometric series involved in the simplification above, we can rewrite our formulas for $|\mathcal{R}_n^{k,j}|$ and $|\mathcal{L}_n^{k,j}|$ in terms of Pochhammer symbols of nonnegative integers, which have much more straightforward asymptotic behavior.

$$\begin{aligned}|\mathcal{R}_n^{k,j}| &= \frac{k+1}{2n+k+1}\binom{2n+k+1}{n}\frac{(1+j-k+n)_{k-j}}{(2+j+2n)_{k-j-1}} \\ &\quad + \frac{k-j}{2n+k}\binom{2n+k}{n}\frac{(2+j-k+n)_{k-j-1}}{(2+j+2n)_{k-j-2}} \\ &= \frac{(1-j+2k)\Gamma(1+j+2n)}{\Gamma(1+j-k+n)\Gamma(2+k+n)},\end{aligned}$$

$$\begin{aligned}|\mathcal{L}_n^{k,j}| &= \frac{k+1}{2n+k+3}\binom{2n+k+3}{n+1}\frac{(n-k+j)_{k-j+1}}{(2n+j+2)_{k-j+1}} \\ &\quad + \frac{k-j+1}{2n+k+2}\binom{2n+k+2}{n+1}\frac{(n-k+j+1)_{k-j}}{(2n+j+2)_{k-j}} \\ &= \frac{(2-j+2k)\Gamma(2+j+2n)}{\Gamma(1+j-k+n)\Gamma(3+k+n)}.\end{aligned}$$

As with Mo_n, we truncate rMo_n to include the bulk of the monoid, while ensuring the representations grow sufficiently quickly. Since they have similar shapes, we truncate at the same point: $k \leq 2\sqrt{2n}$. See Figure 5.

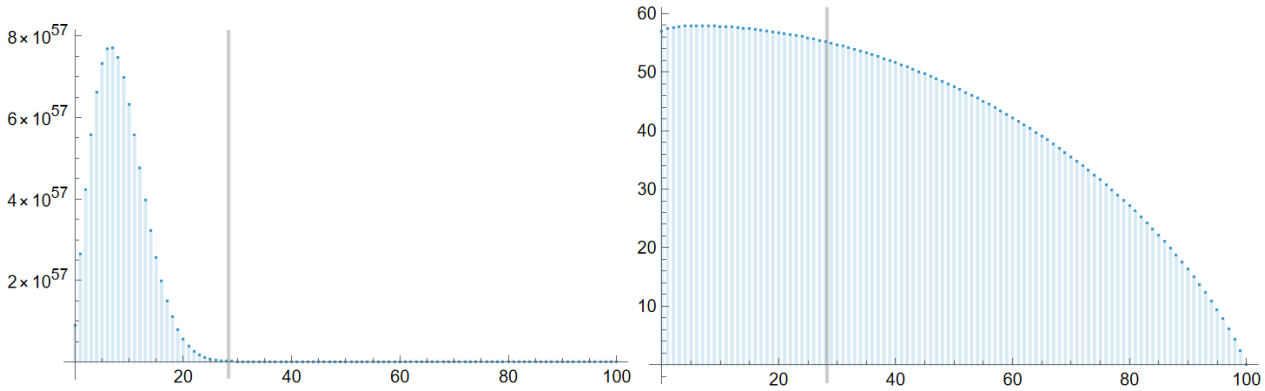


FIGURE 5. Left: the semisimple dimension over k, for $n = 100$, with a vertical line showing the rightmost truncation endpoint. Right: A Log10 version of the same graph.

We again denote this truncated monoid by rMo_n^T.

Theorem 5C.6. *We have the following.*

$$\boxed{\pi^{-1/2}e^{-\frac{1}{n}}}\cdot\boxed{n^{-3/2}}\cdot\boxed{4^n} \leq \mathrm{ssGap}_{\mathbb{K}} rMo_n^T \leq \boxed{4\sqrt{2}\pi^{-1/2}e^{-\frac{1}{n}}}\cdot\boxed{n^{-1}}\cdot\boxed{4^n},$$

$$\boxed{\pi^{-1/2}e^{-\frac{1}{n}}}\cdot\boxed{n^{-3/2}} \leq \mathrm{ssRatio}_{\mathbb{K}} rMo_n^T \leq \boxed{4\sqrt{2}\pi^{-1/2}}\cdot\boxed{n^{-1}}.$$

Proof. We use the right cells and set $j = 0$ for the semisimple RepGap, since that gives the minimal cell size. For fixed n over $0 \leq k \leq 2\sqrt{2n}$, $\frac{(1+k)\Gamma(1+2n)}{\Gamma(1-k+n)\Gamma(2+k+n)}$ has a maximum somewhere strictly in $0 < k < 2\sqrt{2n}$, and is monotone increasing from 0 to the maximum, and monotone decreasing after the maximum to $2\sqrt{2n}$. The minimum will therefore be at one of $k = 0$ or $k = 2\sqrt{2n}$.

Using Stirling's approximation for the Gamma function, we get:

$$\begin{aligned}|\mathcal{R}_n^{k,j}| &\sim \frac{e}{\sqrt{2\pi}}(1-j+2k)(j-k+n)^{-1/2-j+k-n}(1+k+n)^{-3/2-k-n}(j+2n)^{1/2+j+2n}\\ &\sim \frac{2^{j+n}(1-j+2k)}{n^{3/2}\sqrt{\pi}}e^{-\frac{j+j^2-4jk+4(1+k+k^2)}{4n}}\\ &\geq \frac{4^n e^{-8-\frac{1}{n}-\frac{2\sqrt{2}}{\sqrt{n}}}}{n^{3/2}\sqrt{\pi}}(4\sqrt{2n}+1), \text{ substituting } j=0 \text{ and } k=2\sqrt{2n},\\ &\text{or} \geq \frac{4^n e^{-\frac{1}{n}}}{n^{3/2}\sqrt{\pi}}, \text{ substituting } j=0 \text{ and } k=0.\end{aligned}$$

The ratio of the $k=0$ case to the $k=2\sqrt{2n}$ case asymptotically approaches $e^{8+\frac{2\sqrt{2}}{\sqrt{n}}}/(1+4\sqrt{2n})$, which approaches 0, so our lower bound is $4^n e^{-\frac{1}{n}}/n^{3/2}\sqrt{\pi}$.

The upper bound comes directly from the asymptotic computed by Mathematica, $2^{j+2n}(1-j+2k)/n^{3/2}\sqrt{\pi}$, substituting $j=0$ and $k=2\sqrt{2n}$. $j=0$ is to ensure we are still comparing the smallest cells for each k, and it's easy to see that this asymptotic is maximal at $k=2\sqrt{2n}$ within the bounds of the truncated monoid.

To compute the asymptotic of $|rMo_n^T|$, we first obtain a lower bound using the method in Remark 3A.4. Take $k=2\sqrt{2n}$, which is not the maximum of $\binom{k+1}{2j+1}|\mathcal{R}_n^{k,j}||\mathcal{L}_n^{k,j}|$ for fixed j and n, however it is close. Then, obtaining the asymptotic of the summand via Stirling's approximation and Mathematica, we obtain

$$\begin{aligned}&\frac{4^{3+2n}e^{-16-\frac{6\sqrt{2}}{\sqrt{n}}}}{n^2\pi}(1+2\sqrt{2n})_2F_1(\frac{1}{2}-\sqrt{2n},-\sqrt{2n},\frac{3}{2},4e^{\frac{4\sqrt{2}}{\sqrt{n}}})\\ &\quad\sim 3^{1+2\sqrt{2n}}4^{1+2n}e^{-\frac{32}{3}-\frac{6\sqrt{2}}{\sqrt{n}}}(\sqrt{2}+4\sqrt{n})n^{-5/2}\pi^{-1/2},\end{aligned}$$

which has the exponential factor 16^n. Thus, $|rMo_n^T| \geq 16^n$.

For the upper bound, we do the same thing with Stirling's approximation, except without taking $k=\sqrt{2n}$:

$$\binom{k+1}{2j+1}|\mathcal{R}_n^{k,j}||\mathcal{L}_n^{k,j}| \sim \frac{2^{1+2j+4n}(-1+j-2k)(j-2(1+k))}{n^3\pi}e^{-\frac{(7+(j-2k)^2+6k}{2n}}\binom{1+k}{1+2j}.$$

The maximum of $e^{-((7+(j-2k)^2+6k)/2n}$ is $e^{-7/2n}$. Thus, taking the sum over $0 \leq j \leq \lfloor \frac{k}{2} \rfloor$ and $0 \leq k \leq 2\sqrt{2n}$, then taking the asymptotic in Mathematica, we obtain:

$$|rMo_n^T| \leq O\left(\frac{25 \times 2^{1+4n} \times 9^{\sqrt{2n}}}{n^2\pi}\right)$$

which clearly has exponential growth factor 16^n. Therefore, $\Omega(16^n) \leq |rMo_n^T| \leq O(16^n)$.

Using 16^n as the size of the monoid, the semisimple gap ratio follows easily using the upper bounds of the semisimple RepGap already obtained. □

Remark 5C.7. The asymptotic of the nth root of $|rMo_n^T|$ is 16, however, unlike for rTL and the pivotal planar monoids, this is significantly smaller than the size of the full monoid. Since $|rMo_n|$ is monotone increasing in n, we can use a direct calculation in Mathematica for $n=500$ to see that 20 is a lower bound for the limit of $|rMo_n|^{1/n}$ as $n \to \infty$.

The reason for this discrepancy comes from the peculiar cell structure of rMo_n, which results in a large number of small cells. For $R_n^{k,0}$, n fixed, the peak over k is significantly different to the peak over k of the monoid size $|rMo_n^k| = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor}\binom{k+1}{2j+1}|\mathcal{R}_n^{k,j}||\mathcal{L}_n^{k,j}|$. This is visualized in Figure 6. Due to this, the size of the truncated monoid is relatively small, since we need to truncate where the peak of the right cells are.

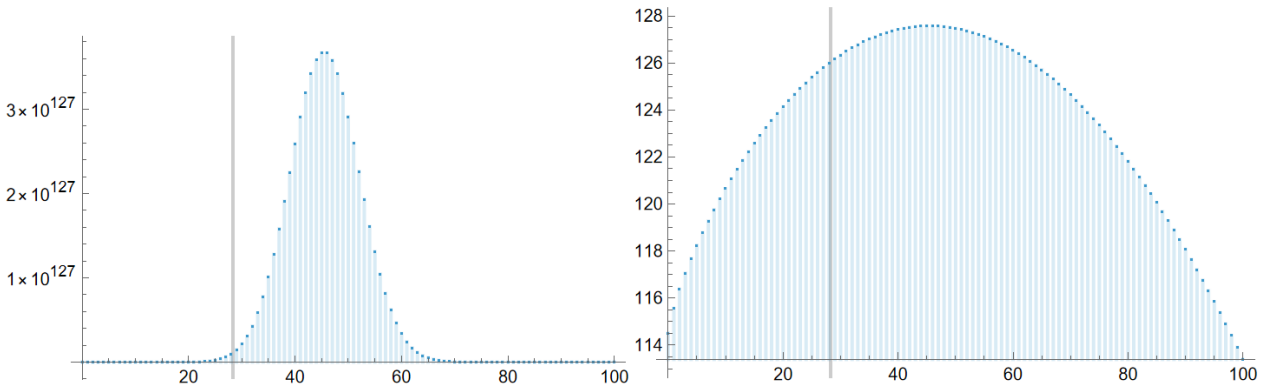


FIGURE 6. Left: the bulk of the monoid rMo_n, with the rightmost truncation endpoint marked by a vertical line, showing the truncation is much smaller than the monoid size. Right: A Log10 version of the same graph.

This also reveals that the asymptotic of the nth root of the ratio of the RepGap to the square root of the size of the monoid is less than 1, in contrast with the pivotal diagram monoids. Therefore, the simple representations are significantly smaller than their upper bound, in the context of Remark 2B.3. While truncating the monoid does result in a (semisimple) gap ratio of ~ 1, we also lose the bulk of the monoid. ◇

Combining this with Theorem 3A.3, we have the following conclusion:

Corollary 5C.8. *Assume* $\operatorname{char}\mathbb{K} = 0$. *For all* $\epsilon > 0$ *and sufficiently large* n,

$$\boxed{\Omega\big((4-\epsilon)^n\big)} \leq \operatorname{ssGap}_{\mathbb{K}} rMo_n^T \leq \boxed{O\big((4+\epsilon)^n\big)} < \boxed{\Omega\big((9-\epsilon)^n\big)} \leq \operatorname{Gap}_{\mathbb{K}} Mo_n^T,$$

$$\boxed{\Omega\big((1-\epsilon)^n\big)} \leq \operatorname{ssRatio}_{\mathbb{K}} rMo_n^T \leq \boxed{O\big((1+\epsilon)^n\big)} \ni \operatorname{Ratio}_{\mathbb{K}} Mo_n^T.$$

Thus, we get the table entries as in the introduction. □

Therefore, rMo_n is significantly less suitable for cryptographic purposes than its pivotal counterpart, since the semisimple gap is much worse, and the semisimple gap ratio is at best the same, up to the exponential factor. Since the semisimple dimension is an upper bound for the simple dimension, and in light of Remark 5C.1, we expect the RepGap and gap ratio to be even worse.

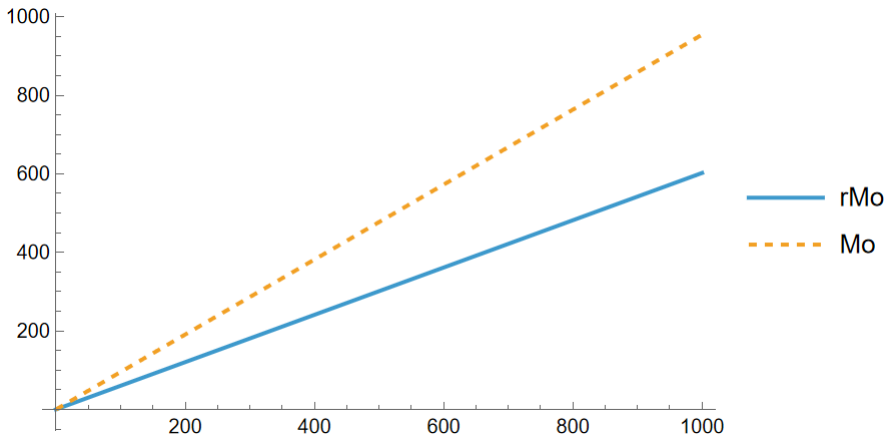


FIGURE 7. Visual comparison of the RepGaps between the non-pivotal and pivotal Motzkin monoid, on a Log10 plot.

Remark 5C.9. As before, the characteristic assumption in Corollary 5C.8 is needed for Mo_n itself. Indeed, the Motzkin category is Schur–Weyl dual to $\mathfrak{sl}_2$ [**BH14**, **CG23**], similarly to the Temperley–Lieb category but with a different generating representation (namely the vector plus the trivial representation), so the same comment as in Remark 4C.5 applies. ◇

6. The "rigid" planar rook monoid

The planar rook monoid and its associated category have been discovered many times, see, e.g., [**So02**, **KS15**], and we will now define a non-pivotal version of it.

6A. **Definition of $rpRo_n$.** The planar rook monoid has no duals so it is naturally not possible to define a non-pivotal analog. We instead define it as follows, which is more of a two-color variant of the planar rook monoid:

Definition 6A.1. The ***"rigid" planar rook category*** (we drop the quotation marks from now on) $rpRo$ is the subcategory of rMo that contains only through strands and dots. As before,

$$rpRo_n := \mathrm{End}_{rpRo}(1\,2)^{\otimes n},$$

is the ***rigid planar rook monoid***. ◇

Remark 6A.2. Like the planar rook monoid, the planar symmetric monoid (the trivial group) also has no rigid analog, however the two-color submonoid of rTL_n consisting of only through strands is isomorphic to the usual version, so we omit it from the discussion. ◇

Remark 6A.3. Inspired by the rigid planar rook monoid, it is potentially worth investigating two-color or n-color versions of the other diagram monoids, as somewhat of an intermediate between pivotal and rigid. ◇

6B. **Computing cells for $rpRo_n$.** The arguments for the rigid planar rook monoid, $rpRo_n$, are very similar to those used for rMo_n.

We find the sizes of the left and right cells of $rpRo_n$ via the same partition method used for rMo_n, however, it is much easier since each block has only one possible diagram (all dots). Moreover, there is no longer a difference between the left and right cells.

Proposition 6B.1. *For each n, number of through strands k, and number of occurrences j of $1\,2$ in the sequence of through strands $\alpha(k)$, the sizes of the left and right cells are:*

$$|L_n^{k,j}| = |R_n^{k,j}| = \binom{n+j}{k}.$$

Furthermore, we have

$$|rpRo_n| = \sum_{k=0}^{2n} \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k+1}{2j+1} \binom{n+j}{2}^2.$$

Proof. Since each block only has one possible diagram, the count simply becomes the number of partitions $j_1 + ... + j_{k+1} = 2n - k$. Using the results from rMo_n, we know that j_1, j_{k+1}, and j_m for $m = 2, 3, ...2j$ are all even, and the remaining $k - 2j$ are odd. Therefore, we can write $j_i = 2y_i$ for $i = 1, 2, ..., 2j, k+1$, and $j_i = 2y_i + 1$ for $i = 2j+1, ...k$, where each $y_i \geq 0$. So, the partition becomes:

$$2y_1 + 2y_2 + ...2y_{2j} + 2y_{2j+1} + 1 + ...2y_k + 1 + 2y_{k+1} = 2n - k \implies y_1 + ...y_{k+1} = n - k + j.$$

Hence, $|\mathcal{L}_n^{k,j}| = |\mathcal{R}_n^{k,j}|$ is just the number of weak compositions of $n - k + j$ into $k + 1$ parts, which is, by, for example, [**Bo16**, Theorem 5.2]:

$$\binom{n-k+j+k+1-1}{k+1-1} = \binom{n+j}{k}.$$

The final equation for $|rpRo_n|$ follows from the exact same argument used for $|rMo_n|$. □

Remark 6B.2. Once again, like in rMo_n, the sizes of the right cells (and left cells) increase with the number of 1 2 blocks, meaning we need to focus on the $j = 0$ case for the RepGap. Moreover, this proves the fact used previously in Remark 5B.12 that the number of different partitions increases as j increases. As seen in Figure 8, we have a similar cell structure to rMo. ◇

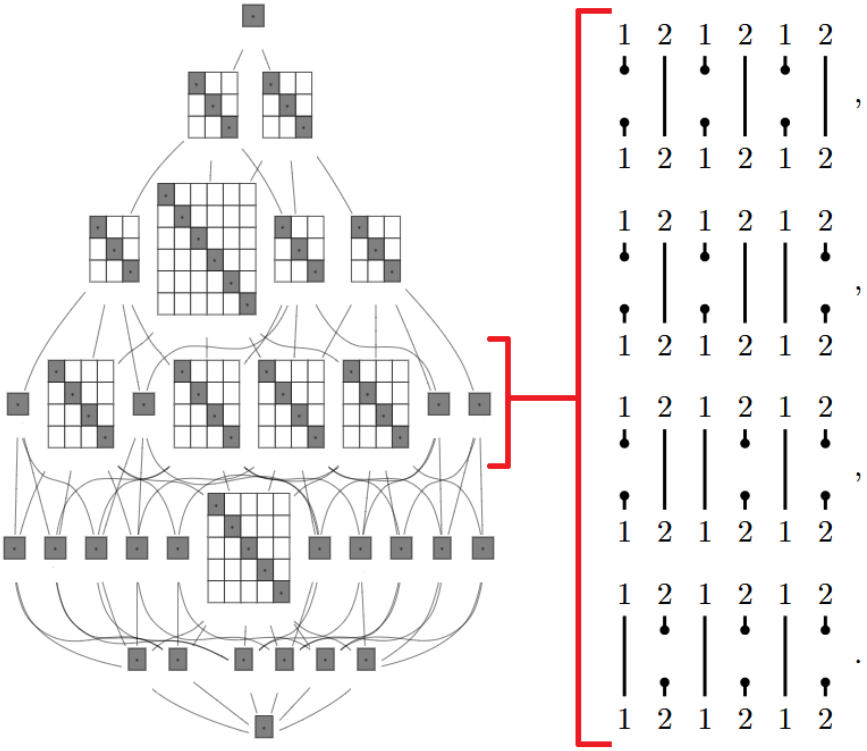


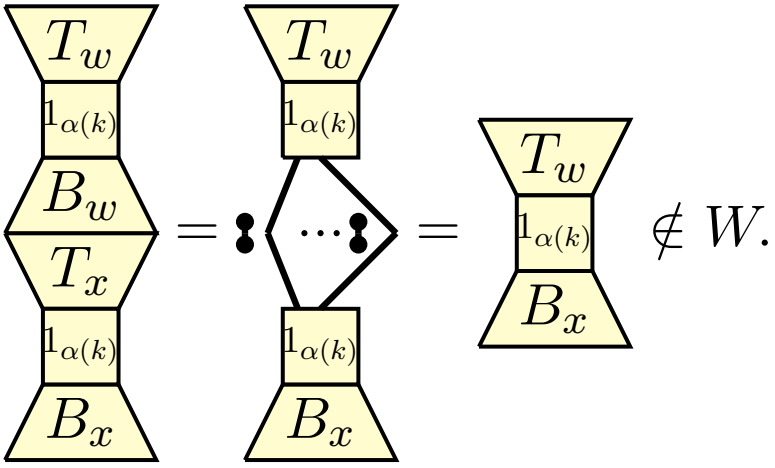
FIGURE 8. Left: The cell structure for $rpRo_3$. Right: explicit diagrams representing the single elements of the four J-cells of size 1 for $k = 3$.

6C. **RepGap and gap ratio of $rpRo_n$.** The key difference between $rpRo_n$ rMo_n is that $rpRo_n$ is semisimple, and this follows from the following.

Proposition 6C.1. *The right representations $\Delta_{R_n^{\alpha(k)}}$ are all simple, and form a complete list of the simple right representations of $rpRo_n$, up to isomorphism.*

Proof. The argument is very similar to that used for rTL_n. Fix a sequence of through strands $\alpha(k)$ and the corresponding J cell $J_n^{\alpha(k)}$. Then we have right representations $\Delta_{R_n^{\alpha(k)}}$. Let W be a nontrivial subspace of $\Delta_{R_n^{\alpha(k)}}$ such that they are nonequal, and let $w \in \text{basis}(W)$. $w = T_w \circ 1_{\alpha(k)} \circ T_b$, using Lemma 5B.1. Define $x \in R_n^{\alpha(k)} \setminus basis(W)$ by $x = T_x \circ 1_{\alpha(k)} \circ B_x$ such that $B_x \neq B_y$ for any $y \in W$, and $T_x = B_w^*$, where $\_^*$ denotes the anti-involution of the diagram $B_w \in rMo$ that flips the diagram upside down (see [**Tu24**] for more details on $\_^*$).

Then, in the middle, each through strand and dot in B_w perfectly lines up with their counterpart in T_x, resulting in the exact same sequence of through strands. Furthermore, T_w remains the same. Therefore, $xw = T_w \circ 1_{\alpha(k)} \circ B_x \in R_n^{\alpha(k)}$, so $xw \neq 0$, however due to the definition of B_x we have $xw \notin W$, and hence W cannot be $rpRo_n$-invariant. This is illustrated below:



Finally, the fact that this is all the simple representations of $rpRo_n$ follows from the classification Theorem 2A.9. □

Remark 6C.2. The above proposition applies to left representations as well, as the arguments used apply similarly to multiplication on the left. ◇

Corollary 6C.3. *$rpRo_n$ is semisimple over (arbitrary) $\mathbb{K}$.* □

Proof. Every J-cell is idempotent by the same argument used in Proposition 5B.5 (in fact we construct the same idempotents) and every J-cell is square, by Proposition 6B.1. Finally, combining these facts with Proposition 6C.1 and Proposition 2A.11 proves that $rpRo_n$ is semisimple over $\mathbb{K}$. □

As with pRo_n, we truncate $rpRo_n^T := rpRo_n^{\frac{n}{2}-\sqrt{2n}\leq k\leq \frac{n}{2}+\sqrt{2n}}$. See Figure 9.

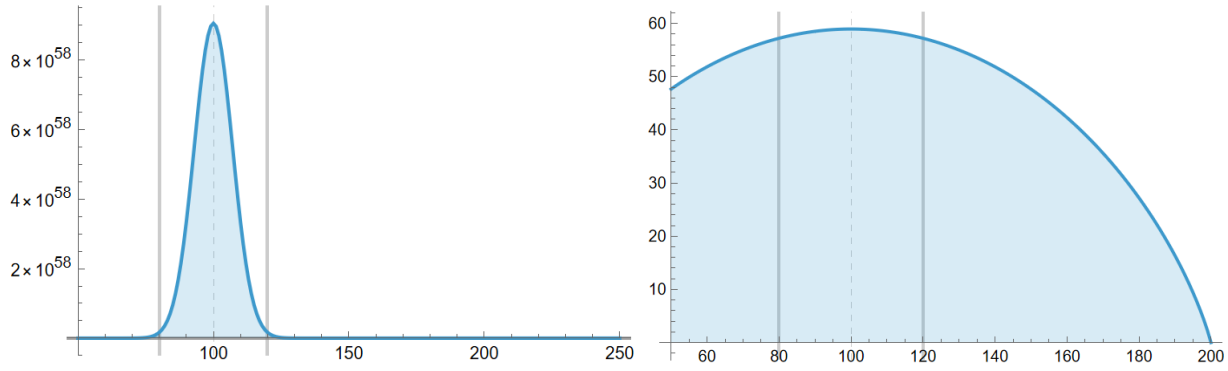


FIGURE 9. Left: the dimension of the simple representations over k, for $n = 200$, with vertical lines marking the truncation end points. Right: A Log10 version of the same graph.

Theorem 6C.4. *The asymptotics of the RepGap and gap ratio of $rpRo_n^T$ have the following inequalities:*

$$\boxed{\sqrt{2}\pi^{-1/2}e^{-4-\frac{16}{3n}}} \cdot \boxed{n^{-1/2}} \cdot \boxed{2^n} \leq \mathrm{Gap}_{\mathbb{K}}\, rpRo_n^T \leq \boxed{\sqrt{2}n^{-1/2}\pi^{-1/2}} \cdot \boxed{2^n},$$

$$\mathrm{Ratio}_{\mathbb{K}}\, rpRo_n^T \leq \boxed{2^{3n/2}3^{3n/4}5^{-5n/4}} \approx \boxed{0.87^n}.$$

Proof. As with rMo, we take $j = 0$ to get the minimal dimension of the representations.

The upper bound of the RepGap corresponds to $k = \frac{n}{2}$, i.e. the maximum of the binomial $\binom{n+0}{k}$. The lower bound corresponds to $k = \frac{n}{2}-\sqrt{2n}$, i.e. one of the endpoints of the truncated monoid. Since these are straightforward binomial coefficients, we can easily find their asymptotics in Mathematica.

For the ratio, to obtain the upper bound we consider the maximal RepGap, i.e. when $k = \frac{n}{2}$. Clearly, $\sqrt{|rpRo_n^T|} \geq \binom{5n/4}{n/2}$, where we have taken only the summand, and substituted $j = \frac{k}{2}$ and $k = \frac{n}{2}$. Then, we have an upper bound for the gap ratio

$$\mathrm{Ratio}_{\mathbb{K}}\, rpRo_n^T \leq \binom{n}{n/2} \Big/ \binom{5n/4}{n/2} \sim 2^{3n/2} 3^{3n/4} 5^{-5n/4}$$

using Mathematica again for the asymptotic. □

Remark 6C.5. As with rMo, the truncated monoid is much smaller than the full monoid, since the location of the right cell peak is different to the location of the monoid peak, over k through strands, seen in Figure 10. We can again find a lower bound for the asymptotic of $|rpRo_n|^{1/n}$ by observing

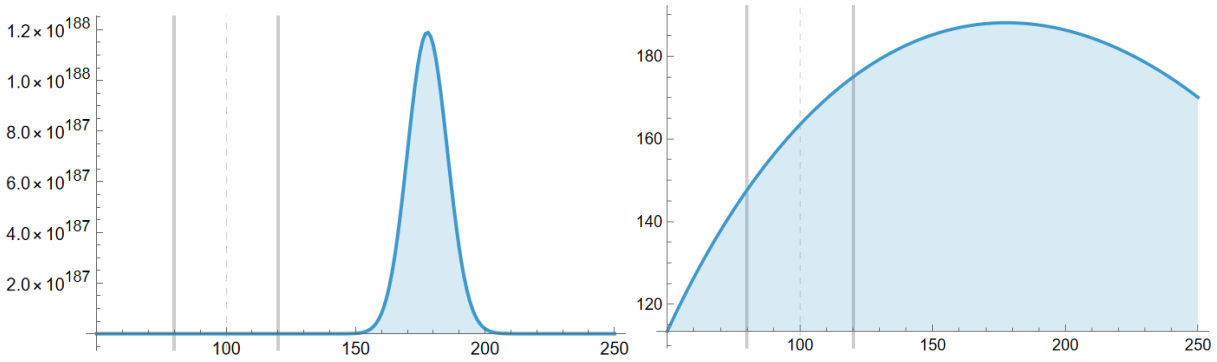


FIGURE 10. Left: the bulk of the monoid $rpRo_n$, with truncation endpoints marked by vertical lines, showing the truncation is much smaller than the monoid size. Right: A Log10 version of the same graph.

that it is monotone increasing in n, and calculating the result for $n = 500$ in Mathematica. We therefore have $|rpRo_n| \geq \Omega(8.9^n)$, meaning we once again have the nth root of the ratio of the RepGap to the square root of the size of the monoid being less than 1. ◇

Remark 6C.6. The upper bound for the gap ratio is quite coarse, since we are picking only one (non-maximal) term in the double sum that makes up $|rpRo_n^T|$. As a result, $rpRo_n$ is significantly worse for cryptographic purposes than pRo_n. In fact, since the gap ratio tends to zero exponentially with n, $rpRo_n$ is substantially worse than all other diagram monoids that appear in this paper. ◇

Corollary 6C.7. *For sufficiently large n:*

$$\mathrm{Gap}_{\mathbb{K}}\, rpRo_n^T \leq \boxed{\sqrt{2}e^{2+\frac{1}{3n}}} \cdot \boxed{2^{-n}} \cdot \mathrm{Gap}_{\mathbb{K}}\, pRo_n^T,$$

$$\mathrm{Ratio}_{\mathbb{K}}\, rpRo_n^T \leq \boxed{\pi^{1/4} e^{2+\frac{1}{3n}}} \cdot \boxed{n^{1/4}} \cdot \boxed{0.87^n} \cdot \mathrm{Ratio}_{\mathbb{K}}\, pRo_n^T.$$

Thus, we get the table entries as in the introduction. □

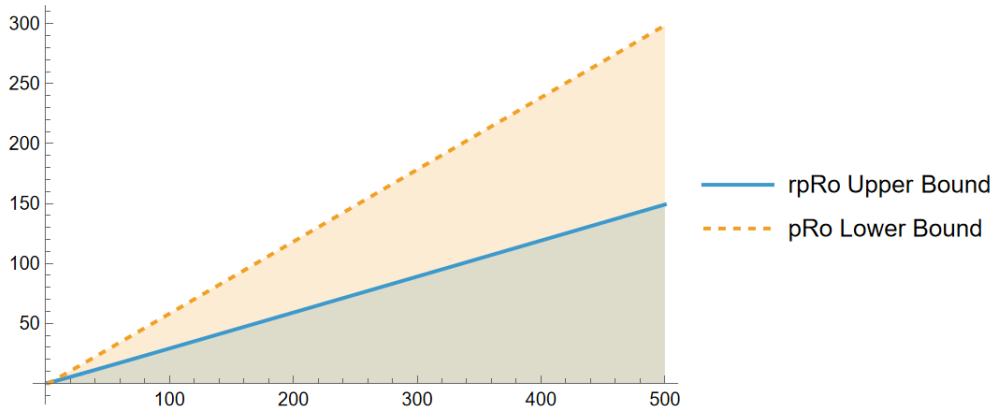


FIGURE 11. Visual comparison of the RepGaps between the non-pivotal and pivotal planar rook monoid, on a Log10 plot.

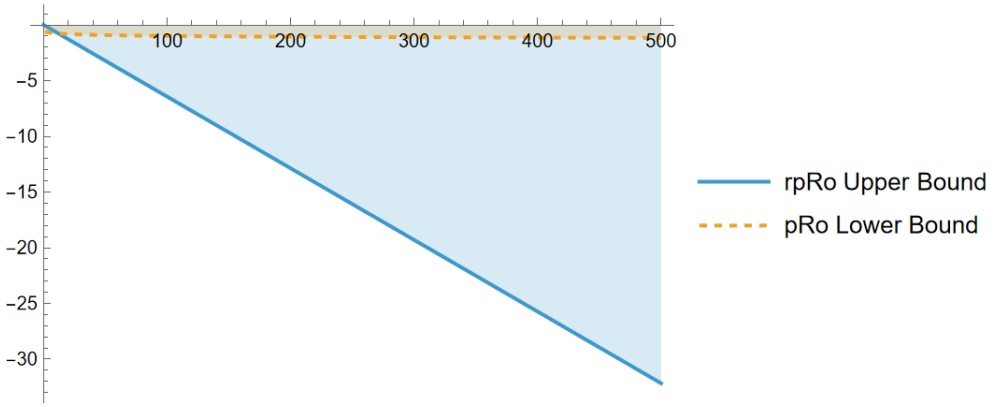


FIGURE 12. Visual comparison of the gap ratios between the non-pivotal and pivotal planar rook monoid, on a Log10 plot.

REFERENCES

[An19] H.H. Andersen. Simple modules for Temperley–Lieb algebras and related algebras. *J. Algebra*, 520:276–308, 2019. URL: https://arxiv.org/abs/1709.00248, doi:10.1016/j.jalgebra.2018.10.035.

[AST18] H.H. Andersen, C. Stroppel, and D. Tubbenhauer. Cellular structures using U_q-tilting modules. *Pacific J. Math.*, 292(1):21–59, 2018. URL: https://arxiv.org/abs/1503.00224, doi:10.2140/pjm.2018.292.21.

[AAR99] GE. Andrews, R. Askey and R. Roy. Special Functions. *Cambridge University Press*, 1999. URL: doi:10.1017/CBO9781107325937.

[Ar25] K. Arms. Representation gaps of the Motzkin monoid. 2025 (to appear). *University of Sydney: Bachelor of Science (Advanced) (Honours)*.

[AW85] R. Askey and J. Wilson. Some basic hypergeometric orthogonal polynomials that generalize Jacobi polynomials. *Memoirs of the American Mathematical Society* 54(319), 1985. URL: doi:10.1090/memo/0319.

[BH14] G. Benkart and T. Halverson. Motzkin algebras. *European J. Combin.*, 36 (2014), 473–502. URL: https://arxiv.org/abs/1106.5277, doi:10.1016/j.ejc.2013.09.010.

[Be99] F. Bernhart. Catalan, Motzkin, and Riordan numbers. *Discrete Mathematics* 204(1–3):73–112, 1999. URL: doi:10.1016/S0012-365X(99)00054-0.

[Bo16] M. Bóna. A Walk Through Combinatorics: An Introduction to Enumeration and Graph Theory, 4th Edition. *World Scientific*, 2016. URL: doi:10.1142/10258.

[BG08] J. Bourgain and A. Gamburd. Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$. *Ann. of Math. (2)*, 167(2):625–642, 2008. URL: doi:10.4007/annals.2008.167.625.

[COT24] K. Coulembier, V. Ostrik, and D. Tubbenhauer. Growth rates of the number of indecomposable summands in tensor powers. *Algebr. Represent. Theory* 27 (2024), no. 2, 1033–1062. URL: https://arxiv.org/abs/2301.00885, doi:10.1007/s10468-023-10245-7.

[CSB21] K. Coulembier, R. Street, and M. van de Bergh. Freely Adjoining Dual Modules. *Math. Struct. Comp. Sci.*, 31:748–768, 2021. URL: https://arxiv.org/abs/2004.09697, doi:10.1017/S0960129520000274.

[CdVM09] A. Cox, M. de Visscher, and P. Martin. The blocks of the Brauer algebra in characteristic zero. *Represent. Theory*, 13 (2009), 272—308. URL: https://arxiv.org/abs/math/0601387, doi:10.1090/S1088-4165-09-00305-7.

[DWH99] W.F. Doran, D.B. Wales, and P.J. Hanlon. On the semisimplicity of the Brauer centralizer algebras. *J. Algebra*, 211 (1999), no. 2, 647-–685. URL: doi:10.1006/jabr.1998.7592.

[CG23] S. Doty, and A. Giaquinto. The partial Temperley–Lieb algebra and its representations. *J. Comb. Algebra*, 7 (2023), no. 3-4, 401–439. URL: https://arxiv.org/abs/2208.04296, doi:10.4171/jca/74.

[Er95] K. Erdmann. Tensor products and dimensions of simple modules for symmetric groups. *Manuscripta Math.*, 88(3):357–386, 1995. doi:10.1007/BF02567828.

[EGNO15] P. Etingof, S. Gelaki, D. Nikshych, and V. Ostrik. Tensor Categories. *American Mathematical Society: Mathematical Surveys and Monographs*, Online Ed. 2331-7159, v. 205, 2015. ISBN: 978-1-4704-2024-6 978-1-4704-2349-0. URL: math.mit.edu/~etingof/egnobookfinal.pdf.

[FS09] P. Flajolet and R. Sedgewick. Analytic Combinatorics. *Cambridge University Press*, 2009. ISBN: ISBN 978-0-521-89806-5. URL: ac.cs.princeton.edu/home/AC.pdf.

[Go08] W.T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008. URL: https://arxiv.org/pdf/0710.3877.pdf, doi:10.1017/S0963548307008826.

[GL96] J.J. Graham and G. Lehrer. Cellular algebras. *Invent. Math.*, 123(1):1–34, 1996. doi:10.1007/BF01232365.

[Gr51] J.A. Green. On the structure of semigroups. *Ann. of Math. (2)*, 54:163–172, 1951. URL: doi:10.2307/1969317.

[Gr17] F. Grondin. Hypergeometric series with negative integer at the denominator. 2017. URL: doi:10.13140/RG.2.2.11546.03529.

[GT25] J. Gruber, and D. Tubbenhauer. Growth problems in diagram categories 2025. URL: https://arxiv.org/abs/2503.00685.

[HR05] T. Halverson and A. Ram. Partition algebras. *European J. Combin.*, 26(6):869–921, 2005. URL: https://arxiv.org/abs/math/0401314, doi:10.1016/j.ejc.2004.06.005.

[Hu19] M. Hu. Presentations of diagram categories. *PUMP Undergrad. Research* 3:1–25, 2019. URL: https://arxiv.org/abs/1910.11784, .

[Jo94] V.F.R. Jones. The Potts model and the symmetric group. *Subfactors* (Kyuzeso, 1993), 259–267. World Scientific Publishing Co., Inc., River Edge, NJ, 1994.

[KS15] M. Khovanov and R. Sazdanovic. Categorifications of the polynomial ring. *Fund. Math.*, 230(3):251–280, 2015. URL: https://arxiv.org/abs/1101.0293, doi:10.4064/fm230-3-3.

[KST24] M. Khovanov, M. Sitaraman, and D. Tubbenhauer. Monoidal Categories, representation Gap and cryptography. *Trans. Amer. Math. Soc. Ser. B*, 11:329–395, 2024. URL: https://arxiv.org/abs/2201.01805, doi:10.1090/btran/151.

[Ko04] J. Kock. Frobenius algebras and 2D topological quantum field theories. *London Math. Soc. Stud. Texts*, 59 Cambridge University Press, Cambridge, 2004. xiv+240 pp. URL: https://mat.uab.es/~kock/TQFT.html.

[KX12] S. König and C. Xi. Affine cellular algebras. *Adv. Math.*, 229(1):139–182, 2012. doi:10.1016/j.aim.2011.08.010.

[Ko12] V. Kotesovec. OEIS, The on-Line encyclopedia of integer sequences: Sequence A026945. Asymptotic formula on this page. URL: https://oeis.org/A026945. Accessed: 2025-04-28.

[Kr29] M. Krawtchouk. Sur une généralisation des polynomes d'Hermite. *Comptes Rendus de L'Académie des Sciences, Paris* 189:620–622, 1929. In French.

[LS25] T. Li and S. Starr. Multifold Convolutions, Generating Functions and 1d Random Walks. 2025. URL: https://arxiv.org/abs/2410.22486.

[Mar91] P. Martin. Potts models and related problems in statistical mechanics. *Ser. Adv. Statist. Mech.*, 5 World Scientific Publishing Co., Inc., Teaneck, NJ, 1991. xiv+344 pp. URL: doi:10.1142/0983.

[MR15] A. Myasnikov and V. Roman'kov. A linear decomposition attack. *Groups Complex. Cryptol.*, 7(1):81–94, 2015. URL: https://arxiv.org/abs/1412.6401, doi:10.1515/gcc-2015-0007.

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

[Si05] D. Sills. Hypergeometric series. *Rutgers University: Introductory Theory of Functions of a Complex Variable*, Second Supplement, 2005. URL: http://home.dimacs.rutgers.edu/~asills/teach/spr05/hypergeom.pdf, home.dimacs.rutgers.edu/~asills/teach/spr05/. Accessed: 2025-04-28.

[So99] W. Soergel. Character formulas for tilting modules over quantum groups at roots of one. In *Current developments in mathematics, 1997 (Cambridge, MA)*, pages 161–172. Int. Press, Boston, MA, 1999.

[So02] L. Solomon. Representations of the rook monoid. *J. Algebra.* 256 (2002), no. 2, 309–342. URL: doi:10.1016/S0021-8693(02)00004-2.

[Sp23] R.A. Spencer. The modular Temperley–Lieb algebra. *Rocky Mountain J. Math.* 53 (2023), no. 1, 177–208. URL: https://arxiv.org/abs/2011.01328, doi:10.1216/rmj.2023.53.177.

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

[St25] W. Stewart. GitHub page for the code used in the paper "Representations gaps of rigid planar diagram monoids." 2025. URL: https://github.com/WillowStewart/RepGapsRigidPlanar.

[St21] W. Stewart. Ideals in the free rigid monoidal category. 2021. *University of Sydney: Bachelor of Science (Advanced) (Honours).*

[STWZ23] L. Sutton, D. Tubbenhauer, P. Wedrich, and J. Zhu. SL2 tilting modules in the mixed case. *Selecta Math.* (N.S.) 29 (2023), no. 3, Paper No. 39, 40 pp. URL: https://arxiv.org/abs/2105.07724, doi:10.1007/s00029-023-00835-0.

[Tub22] D. Tubbenhauer. Quantum topology without topology. 2022. URL: https://www.dtubbenhauer.com/qinvariants.pdf.

[Tu24] D. Tubbenhauer. Sandwich cellularity and a version of cell theory. *Rocky Mountain J. Math.*, 54(6):1733–1773, 2024. URL: https://arxiv.org/abs/2206.06678, doi:10.1216/rmj.2024.54.1733.

[TV23] D. Tubbenhauer and P. Vaz. Handlebody diagram algebras. *Rev. Mat. Iberoam.*, 39(3):845–896, 2023. URL: https://arxiv.org/abs/2105.07049, doi:10.4171/rmi/1356.

W.S.: The University of Sydney, School of Mathematics and Statistics F07, Office Carslaw 807, NSW 2006, Australia, www.maths.usyd.edu.au/ut/people?who=W_Stewart, ORCID: 0009-0000-2854-2256

Email address: W.Stewart@maths.usyd.edu.au

D.T.: The University of Sydney, School of Mathematics and Statistics F07, Office Carslaw 827, NSW 2006, Australia, www.dtubbenhauer.com, ORCID 0000-0001-7265-5047

Email address: daniel.tubbenhauer@sydney.edu.au