Equations and Theories in Plactic Monoids

Daniel Turaev

May 2024

A thesis submitted to the School of Mathematics at the University of East Anglia in partial fulfilment of the requirements for the degree of Master of Science by Research

© This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with the author and that use of any information derived there from must be in accordance with current UK Copyright Law. In addition, any quotation or extract must include full attribution.

Abstract

In this thesis we explore Diophantine equations and first order sentences of the plactic monoids. We present explicit algebraic criteria for certain small equations to have solutions in the plactic monoids. We also construct an interpretation of a plactic monoid of arbitrary finite rank in Presburger arithmetic, which is known to have decidable first order theory, thereby proving that a plactic monoid of any finite rank will have decidable first order theory. This resolves other open decidability problems about the finite rank plactic monoids, such as the Diophantine problem and identity checking. The algorithm generating the interpretations is uniform, which we use to explore the decidability of the Diophantine problem for the infinite rank plactic monoid. We also prove that the interpretation of the plactic monoids into Presburger Arithmetic is in fact a bi-interpretation, hence any two plactic monoids of finite rank are bi-interpretable with one another.

Access Condition and Agreement

Each deposit in UEA Digital Repository is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the Data Collections is not permitted, except that material may be duplicated by you for your research use or for educational purposes in electronic or print form. You must obtain permission from the copyright holder, usually the author, for any other use. Exceptions only apply where a deposit may be explicitly provided under a stated licence, such as a Creative Commons licence or Open Government licence.

Electronic or print copies may not be offered, whether for sale or otherwise to anyone, unless explicitly stated under a Creative Commons or Open Government license. Unauthorised reproduction, editing or reformatting for resale purposes is explicitly prohibited (except where approved by the copyright holder themselves) and UEA reserves the right to take immediate 'take down' action on behalf of the copyright and/or rights holder if this Access condition of the UEA Digital Repository is breached. Any material in this database has been supplied on the understanding that it is copyright material and that no quotation from the material may be published without proper acknowledgement.

Acknowledgements and Dedications

This work is dedicated to Mojżesz Presburger, a victim of the holocaust whose master's thesis forms the bedrock of my own. May his memory be a blessing.

For acknowledgements, I would firstly like to thank Robert Gray. When I first approached him to enquire about a research master's, it wasn't obvious that such a thing even existed at UEA. I am grateful to him for giving me a chance, and for being an excellent supervisor – reading all of the drafts I sent, offering detailed corrections, and encouraging me to keep writing, and to present at seminars and conferences. I am also grateful to Lorna Gregory, for reading my work and helping me with the more model theoretic ideas. In fact, the entire community of researchers and PhD students at UEA was kind, warm, and welcoming. They made my time here very enjoyable, and I am grateful to have become part of that community. I would also like to thank my parents, who were always unfalteringly supportive and loving, as well as their cat Chusik, whose shenanigans were a welcome distraction. I met several other cats during my time at UEA, and the company of each and every one of them will be cherished.

Finally, I can't thank enough my partner Gemini, without whom I do not think I would have managed this. Thank you Gem for keeping me sane, I love you.

Contents

1

Introduction

In this thesis, we concern ourselves with a family of monoids called the *plactic monoids*. This family, originally thought of as a single monoid, has its origin in the work of Knuth [24], which developed the combinatorial algorithm of Schensted [42] into a monoid multiplication operation. First studied in depth by Lascoux and Schützenberger [27, 43, 44], who also gave it the name "le monoïde plaxique", its combinatorial properties were applied to the theory of symmetric polynomials to prove the Littlewood-Richardson rule.

Due to its origins as a monoid of Young tableaux, it has proved useful in various aspects of geometry and representation theory [15]. More recently, it has found application in Kashiwara's crystal basis theory [21], with analogous plactic monoids being defined for different root systems associated to crystal bases [29, 30, 31, 32], and used to study Kostka-Foulkes polynomials [28]. Related, plactic-like monoids have also been defined [1, 13, 17, 37], and used to study the combinatorics and growth properties of the plactic monoid, which itself has some interesting combinatorial structure.

For our focus, however, we concern ourselves with the algorithmic properties of this monoid family. It is known that the plactic monoid has 'nice' algorithms for several classic decision problems. Already, Schensted's multiplication algorithm can be used to decide the word problem for the plactic monoid in quadratic time. Furthermore, it was shown in 1981 that the plactic monoid has decidable conjugacy problem [27]. Cain, Gray, and Malheiro [6] have also shown that the plactic monoids are biautomatic, as are related crystal monoids [5], and related plactic-like monoids such as the Chinese, Hypoplactic, and Sylvester monoids [7]. Biautomaticity also implies a word problem solvable in quadratic time.

A classic generalisation of both the word and conjugacy problems is the Diophantine problem, which has received much attention for free groups [22, 35, 41, 45], where Makanin-Razborov diagrams were used independently by Sela [45] and Kharlampovich and Myasnikov [23] to solve the Tarski problems on the first order theory of free groups[1]. Closely related to Hilbert's tenth problem, the Diophantine problem for a group asks for an algorithm deciding whether a given system of equations, with coefficients in the given group and a finite number of unknowns, has a solution in the group. The problem for monoids is analogous, and has been studied for free monoids [34, 46] and is gaining attention in the study of other monoids [16, 38]. For the case of plactic monoids, the Diophantine problem had remained open.

An active parallel area of research is the question of checking identities in the plactic monoids and their monoid algebras. Progress has been made in the rank 3 case [25, 26], and the plactic monoid, bicyclic monoid, and related plactic-like monoids have been shown to admit faithful representations in terms of matrices over the tropical semiring [4, 8, 11, 19]. This implies that every plactic monoid of finite rank satisfies a nontrivial semigroup identity. There is a natural decision problem underpinning this field of study – is it decidable whether a given identity is satisfied by a plactic monoid?

These two decision problems seem distinct from one another, and indeed they are. But both identities and Diophantine equations[2] are expressible as *first order sentences*. This idea from logic allows us to systemically build a language of sentences, to which we assign a truth value – either they are true or false. Checking the veracity of a first order sentence is itself a decision problem, and a significant generalisation of both the Diophantine and identity checking problems.

[1] For a survey of these results, see [14].

[2] These are often referred to as 'word equations' in the monoid world.

Structures for which this decision problem is solvable are said to have decidable first order theory.

The main result presented in this thesis is that every plactic monoid of finite rank has decidable first order theory. We show this in Chapter 5 by constructing an interpretation of a plactic monoid in Presburger arithmetic, which could open the door to studying the theories of plactic-like classes of monoids via similar interpretations. In Chapter 6, we show that this interpretation is in fact a bi-interpretation, and that certain submonoids of the plactic monoid are definable. This thesis also includes a more detailed exploration of the Diophantine problem in Chapter 4, where we look at the conditions on certain equations being solvable, and Chapter 7, where we discuss the Diophantine problem in certain infinitely generated monoids generalising the plactic monoid.

2

General background

2.1 Monoids

A set M equipped with an associative binary operation $\circ : M \times M \to M$ is called a *monoid* if it has a distinguished identity element $\varepsilon \in M$. Explicitly, that is to say that $(M, \circ, \varepsilon)$ satisfies the following axioms:

- $\forall a, b, c \in M : \; a \circ (b \circ c) = (a \circ b) \circ c.$
- $\forall a \in M : \; a \circ \varepsilon = \varepsilon \circ a = a.$

In the same way that groups function as a model of symmetries (that is, invertible maps), monoids function to model maps from an object to itself which need not be invertible. On the other hand, if one views the multiplication operation as concatenation, monoids function to model *language* – of both a human and non human flavour.

2.1.1 Monoids as languages

Consider A a set of distinct elements, which we will call letters or symbols. This set A is an *alphabet*, over which we may form *words*. A word w is a finite sequence of letters of A, typically written without gaps or commas: $a_1 a_2 \dots a_n$, with each $a_i \in A$.

Example 2.1.1. Choosing A to be the standard Latin alphabet $\{a, b, \dots, z\}$, all English words (for example: cat, cats, kitten) would be words over A, but so would any other string of Latin letters (catcatcat, hgdsghdsbf).

Consider the set of words of any finite length over an alphabet A, with the unique word of length 0 (the empty sequence) denoted by ε. This set is denoted $A^\star$. Any subset of A^* is a possible *language over* A.

We can define on $A^\star$ a concatenation operation $\cdot : A^* \times A^* \to A^*$, where

$$u \cdot v = w \iff u = a_1 \dots a_n,\ v = b_1 \dots b_m,\ \text{and } w = a_1 \dots a_n b_1 \dots b_m.$$

It is quick to see that this operation is associative, and hence A^* is a monoid with ε being the identity.

Definition 2.1.2 (Free Monoid)**.** The set A^* with concatenation is the *free monoid over the alphabet* A.

Throughout the thesis, we will abuse notation to write multiplication in any monoid as concatenation, i.e uv for $u \circ v$ or $u \cdot v$.

Any subset of the free monoid will yield a language, but these various subsets will have different properties to one another. Of most interest to us will be the subsets that inherit a monoid structure, but notice here that this definition of language is also consistent with the notion of a language in logic, which we will discuss later.

Note that the free monoid over any single letter alphabet will be isomorphic to the natural numbers under addition, with a 0 element. Therefore, the set $\mathbb{N}$ will contain 0 throughout this thesis.

2.1.2 Presentations

Analogously to the case of groups, we wish to quotient free monoids by a relation that will allow us to obtain various possible monoids. In this world, the correct structure to choose is the *semigroup congruence*, and like in the groups world, this will allow any monoid to be the quotient of a free monoid by a semigroup congruence.

Definition 2.1.3. Given a monoid M, an equivalence relation $\sim \subseteq M \times M$ is called a *semigroup congruence* if it is compatible with monoid multiplication. That is, if $x \sim y$ and $u \sim v$, then $xu \sim yv$. Given any subset $R \subset M \times M$, the semigroup congruence $\sim_R$ generated by R is the smallest semigroup congruence containing R.

Note that the intersection of two semigroup congruences is again a semigroup congruence, so the notion of 'smallest congruence' is well defined.

Given any monoid M and $\sim$ a semigroup congruence on M, the set $M/\sim$ of equivalence classes under $\sim$ is a well-defined monoid where, given $\overline{x}$ the equivalence class of $x \in M$, we define multiplication in $M/\sim$ by $\overline{x} \cdot \overline{y} = \overline{xy}$. This is known as the *quotient monoid* of M by $\sim$.

A *monoid presentation* is a way of describing a monoid using two pieces of data. Specifically, a presentation is the pair A and R, where A is an alphabet and $R \subset A^* \times A^*$. Typically a presentation is written $\langle A|R \rangle$. We say that a monoid is presented by $\langle A|R \rangle$ if it is isomorphic to the quotient of A^* by the congruence generated by R. That is to say,

$$M = \langle A|R \rangle \implies M \cong A^*/\sim_R .$$

Every monoid admits a monoid presentation[1]. A given monoid M is called *finitely*

[1] Since a monoid presentation describes the monoid elements as equivalence classes, there is a subtle difference between two words in the generators being equal as words, versus them being equal as elements of the monoid. In this thesis, we will use the symbol $=$ for both sorts of equality, as there is never a case where the distinction between the two is particularly meaningful to the argument of the proofs.

presented if one can find A and R both finite such that $M = \langle A|R\rangle$.

In the case of the plactic monoids, we will define them both via the multiplication action on tableaux and via presentations. A useful alternative formulation of monoid presentations, based on the book [3], follows.

Definition 2.1.4. Given an alphabet A:

1. A *string rewriting system* (henceforth rewriting system) on A^* is a set $R \subset A^* \times A^*$ of elements (ℓ, r), usually written $\ell \to r$, called rewrite rules.

2. For two elements $u, v \in A^*$, write $u \to_R v$ if $u = x\ell z$, $v = xrz$, and $(\ell, r) \in R$. The transitive and reflexive closure of $\to_R$, written $\to_R^*$, is called the *reduction relation of R*.

The symmetric closure of $\to_R^*$ is a semigroup congruence, and is in fact the same as $\sim_R$[2]. Therefore, every monoid with presentation $\langle A|R\rangle$ also admits the rewriting system associated to R, which is written as (A, R).

Definition 2.1.5 (Complete Rewriting Systems)**.** A rewriting system is called *Noetherian* if it has no infinite descending chain. That is, there is no sequence $u_1, u_2, \ldots \in A^*$ such that $u_i \to_R u_{i+1}$ for all $i \in \mathbb{N}$. A rewriting system is called *confluent* if it has the property that, whenever $u \in A^*$ is such that $u \to_R^* u'$ and $u \to_R^* u''$, there exists a v such that $u' \to_R^* v$ and $u'' \to_R^* v$. A *complete* rewriting system is one which is both confluent and Noetherian.

Call $u \in (A, R)$ a *reduced word* if there is no subword ℓ of u that forms the left hand side of a rewrite rule in R. By theorem 1.1.12 of [3], if (A, R) is a complete rewriting system, then for every $u \in A^*$ there is a *unique, reduced* $v \in A^*$ such that $u \to_R^* v$. This v is called a *normal form* for u, and forms a cross-section of the monoid $\langle A|R\rangle$, in the sense that every element of the monoid is equal to exactly one reduced word. We may therefore identify a monoid admitting a complete rewriting system with its set of normal forms, and the multiplication being concatenation followed by reducing to normal form.

[2] See [3] for a proof of this result.

2.2 A quick review of first order logic

We will refrain from philosophical discussions here, and consider first order logic as simply the study of first order formulas. For a more detailed introduction to logic, and especially model theory, see [18] or [36]. We will be following the conventions of [36].

The definition of a formula is built up recursively from terms:

- We begin with a set of symbols $\{x_1, x_2, \dots\}$ of a certain cardinality. These will be called our *variables.* Typically in this document we will use lowercase Latin letters to denote them.
- Next we define a *signature* σ. This will determine which first order language we work in, and will depend on our structure. A signature will have three types of symbols in it: *constants, functions,* and *predicates.* Functions and predicates may take arguments, while constants do not.

  An example signature (which will be useful later) is the signature of an ordered monoid. Here, $\sigma = \{\varepsilon, \cdot, \leq\}$, where ε is a constant, $\cdot$ is a function symbol, and $\leq$ is a predicate symbol. The number of arguments function and predicate symbols take is called the symbol's *arity.* In our example, $\cdot$ and $\leq$ both have arity 2.
- A *term* will then be any variable, constant, or string of the form $f(x_1, \dots, x_n)$, where $f \in \sigma$ is a function symbol of arity n, and all x_i are terms. For example, in the language of monoids, ε, a, $a \cdot b$ are all terms.

From terms, we will build formulas as follows:

- For any terms x and y, the string $x = y$ is a formula.
- Given a predicate symbol $\theta \in \sigma$ of arity n, and terms $x_1, \dots, x_n$, the string $\theta(x_1, \dots, x_n)$ is a formula.

The two above types of formula are called *atomic formulas.*

- Now, if ϕ is a formula, then so is $\neg\phi$ (not ϕ).
- If $\phi,\ \psi$ are formulas, then so is $\phi \implies \psi$.
- If ϕ is a formula in which a variable x appears, then $\forall x : \phi$ and $\exists x : \phi$ are formulas.
- If $\phi,\ \psi$ are formulas, then so are $\phi \wedge \psi$ (ϕ and ψ) and $\phi \vee \psi$ (ϕ or ψ).

The set L of all first order formulas for a given signature is the *first order language* of that signature.

If a variable appears in a formula, but does not appear as the argument of a universal or existential quantifier, then it is called a *free variable.* A formula with no free variables is called a *sentence.*

Example 2.2.1. The following are all formulas for the signature $\sigma = \{\varepsilon, \cdot, \leq\}$:

1. $\forall x \exists y : x \cdot y = \varepsilon \wedge y \cdot x = \varepsilon$.
2. $\forall x : m \cdot x = x \cdot m$.
3. $\exists x : x \cdot x = x \wedge x \leq \varepsilon$.
4. $a \cdot b = b \cdot a \implies \neg(a \cdot b \cdot a \cdot b = \varepsilon)$.

Of these, formulas 1 and 3 are sentences, while formulas 2 and 4 are not.

Sentences are the only formulas that may be give a truth value. In theory, the assignment of 'true' or 'false' to each sentence is arbitrary. For our purposes, we will care about assignments that arise from *structures.*

Definition 2.2.2 (Structure)**.** Given L a language of a signature σ, an L-Structure is some set S equipped with:

- For each constant $c \in \sigma$ an element $c_S \in S$.

- For each function $f \in \sigma$ of arity n, a function $f_S : S^n \to S$.
- For each predicate $\theta \in \sigma$ of arity m, a set $\theta_S \subset S^m$.

We will abuse notation and write $c \in S,\ f : S^n \to S$, and $\theta \subset S^m$.

Definition 2.2.3 (First Order Theory)**.** Let L be the language of a given signature. Then the *first order theory* of an L-structure $\mathcal{M}$ is the set of all sentences in L that are true in $\mathcal{M}$.

The question of *deciding a first order theory* asks for an algorithm which, given a first order sentence ϕ, determines whether ϕ is true or false in $\mathcal{M}$ in finite time. If such an algorithm exists, then we call the first order theory of $\mathcal{M}$ decidable.

Less formally, when we say a sentence *is true* or *holds* in $\mathcal{M}$, we mean that the sentence is either some defining axiom of our structure, or a logical consequence of it. For example, in an abelian group the sentences

$$\forall x \forall y \forall z : (xy)z = x(yz)$$
$$\forall x \forall y : xy = yx$$

are axiomatic. Meanwhile, the formula

$$\forall x \forall y \forall z : (yx)z = x(yz)$$

is a logical consequence. All three sentences would be in the first order theory of an abelian group.

We will use the shorthand $FOTh(\mathcal{M})$ to denote the first order theory of $\mathcal{M}$. We will also write $\mathcal{M} \models \phi$ if ϕ is in the first order theory of $\mathcal{M}$.

The language of interest for us is the language of monoids, whose signature is $(\circ, \varepsilon)$. To speak of the first order theory of a given monoid, one classically allows atomic formulas of the form $u = v$ for each $u, v \in \mathcal{M}$. In the finitely generated case (with generating set $A = \{a_1, \ldots, a_n\}$, say) this is equivalent to adding constants

$a_1, \ldots, a_n$ to the signature, and considering the first order theory with constants of $(\mathcal{M}, \circ, \varepsilon, a_1, \ldots, a_n)$.

2.3 Presburger Arithmetic

In 1929, Mojżesz Presburger was tasked with studying the decidability of the integers under addition. In his master's thesis [39], he used quantifier elimination and reasoning about arithmetic congruences to prove that the first order theory of $(\mathbb{N}, 0, 1, +)$ is complete[3] and decidable. Note that we can add a comparison symbol $\leq$ to the signature of Presburger arithmetic without trouble, since $x \leq y$ is equivalent to the statement $\exists z : y = x + z$.[4] This yields the following lemma:

Lemma 2.3.1. *$FOTh(\mathbb{N}, 0, 1, +, \leq)$ is decidable.*

For an English translation of Presburger's work, see [40] or [47].

2.4 Interpretations

Since the main work of the thesis is the construction of an interpretation, we will now define an interpretation, using the conventions of section 1.3 of [36]. Throughout this section, L, L_1, and L_2 will be arbitrary first-order languages.

Definition 2.4.1 (Definable sets)**.** Let $\mathcal{M}$ be an L-structure. A set $S \subseteq \mathcal{M}^n$ is called *definable in* $\mathcal{M}$ if there is a first order formula

$$\phi(x_1, \ldots, x_n, y_1, \ldots, y_m) \in L$$

with free variables $x_1, \ldots, y_m$ such that there exists $(w_1, \ldots, w_m) \in \mathcal{M}^m$ with the property that $\phi(x_1, \ldots, x_n, w_1, \ldots, w_m)$ holds if and only if $(x_1, \ldots, x_n) \in S$. i.e.

[3] i.e. for every ϕ in the first order language of signature $(0, 1, +)$, either ϕ or $\neg\phi$ is in the first order theory of $(\mathbb{N}, 0, 1, +)$, but not both.

[4] We then talk about the first order theory of $\mathbb{N}$ as a given ordered monoid. i.e. we add the generating set $\{1\}$ to the signature of an ordered monoid $(0, +, \leq)$.

S is the set

$$\{\underline{x} \in \mathcal{M}^n | \ \mathcal{M} \models \phi(\underline{x}, w_1, \dots, w_m)\}.$$

Example 2.4.2. In a monoid M, the set of elements that commutes with a given $m \in M$ is definable by the formula $xm = mx$. The centre of M is definable by the formula

$$\forall m : xm = mx.$$

If M is finitely generated by $\{m_1, \dots m_k\}$, then the formula

$$xm_1 = m_1x \wedge xm_2 = m_2x \wedge \cdots \wedge xm_k = m_kx$$

also defines the centre of M. This has the property of being a *positive existential* formula, which is useful in the study of Diophantine equations[5] .

Definition 2.4.3 (Definable functions)**.** A function $f : \mathcal{M}^m \to \mathcal{M}^n$ is *definable* in $\mathcal{M}$ if its graph[6] is definable as a subset of $\mathcal{M}^{m+n}$.

Note that the composition of definable functions is definable.

Definition 2.4.4 (Interpretability)**.** Let $\mathcal{M}$ be an L_1-structure, and $\mathcal{N}$ be an L_2-structure. Then we call $\mathcal{N}$ *interpretable* in $\mathcal{M}$ if there exist some $n \in \mathbb{N}$, some set $S \subseteq \mathcal{M}^n$, and a bijection $\phi : S \to \mathcal{N}$ such that

1. S is definable in $\mathcal{M}$.
2. For every constant, function, and predicate r in the signature of L_2, including the equality relation, the preimage by ϕ of the graph of r is definable in $\mathcal{M}$.

We will use the notation $\phi^{-1}(r)$ for the preimage of the graph of r.

Note that in the above definition we insisted the map ϕ be a bijection, as in section 1.3 of [36]. However, the most general theory of interpretations works with surjections from S onto $\mathcal{N}$. See section 5 of [18] for more details on this.

[5] See, for example, [10].

[6] The graph of a function f is the set of elements $\{(x, f(x)) \mid x \in \mathcal{M}^m\} \subset \mathcal{M}^{m+n}$.

Example 2.4.5. Consider the set $\mathbb{Z}$, with signature $(0, 1, +, -, \leq)$. We can interpret this structure in our Presburger arithmetic $(\mathbb{N}, 0, 1, +, \leq)$ using the set

$$S = \{(a, b) \mid a = 0 \vee b = 0\} \subset \mathbb{N}^2$$

and the bijective map $\phi : S \to \mathbb{Z}$ sending (a, b) to $a - b$.

Proof. We can see that this map is a bijection, which makes straightforward the definability of the preimages of 0, 1, and equality. The preimage of subtraction, which is a unary function sending x to $-x$, is the set

$$\phi^{-1}(-) = \{((a, b), (c, d)) \in \mathbb{N}^4 \mid \phi(a, b) = -\phi(c, d)\}.$$

This is also straightforward to define, since $\phi(a, b) = -\phi(c, d)$ holds precisely when $(c, d) = (b, a)$. Thus the preimage of subtraction is defined by the formula

$$(a = 0 \vee b = 0) \wedge (c = 0 \vee d = 0) \wedge a = d \wedge b = c.$$

For $\phi^{-1}(\leq)$, if $x, y \in \mathbb{Z}$ and $x \leq y$, then if $\phi(a, b) = x$ and $\phi(c, d) = y$ we must have that $a + d \leq c + b$, which is clearly definable.

Now for addition, we are considering the set

$$\phi^{-1}(+) = \{((a, b), (c, d), (e, f)) \in \mathbb{N}^6 \mid \phi(a, b) + \phi(c, d) = \phi(e, f)\}.$$

In other words, we consider elements of $\mathbb{N}^6$ satisfying $a - b + c - d = e - f$. We can rearrange this expression to get a formula of Presburger arithmetic: $a + c + f = e + b + d$. Since we also have the condition that one of e or f must be zero, this formula will uniquely determine e and f in terms of a, b, c, and d. Therefore, this formula will define the graph of the preimage of addition, which finishes the proof that ϕ is an interpretation. $\square$

Next we strengthen the notion of interpretability to bi-interpretability. By the definition of interpretations, it is straightforward to see that interpretations are transitive: if M_1 is interpretable in M_2, and M_2 is interpretable in M_3, then M_1 is interpretable in M_3. This implies that if two structures are *mutually interpretable*, i.e. M_1 and M_2 are each interpretable in the other, then we obtain an interpretation of M_1 in itself, and likewise an interpretation of M_2 in itself.

Definition 2.4.6 (Bi-interpretability)**.** Given M_1 an L_1-structure, and M_2 an L_2-structure, we say M_1 and M_2 are *bi-interpretable* if M_1 and M_2 are mutually interpretable, and the map ϕ_i interpreting M_i in itself is definable in M_i, for $i = 1, 2$.

Returning to our above example, the set $\mathbb{N} \subset \mathbb{Z}$ is definable in $(\mathbb{Z}, 0, 1, +, -, \leq)$ by the formula $0 \leq x$. The identity map ψ on $\mathbb{N}$ is then an interpretation of $(\mathbb{N}, 0, 1, +, \leq)$ in $(\mathbb{Z}, 0, 1, +, -, \leq)$. Composing the map ψ and the map ϕ from example 2.4.5, we get:

1. A map $\psi\phi : T \to \mathbb{N}$, where $T = \{(a, b) \in \mathbb{N}^2 |\ b = 0\} \subset S \subset \mathbb{N}^2$ is definable and $\psi\phi(a, 0) = a$. This map is clearly definable.
2. A map $\phi \circ (\psi \times \psi) : U \to \mathbb{Z}$, where

$$U = \{(a, b) \in \mathbb{Z}^2 |\ 0 \leq a \wedge 0 \leq b \wedge (a = 0 \vee b = 0)\} \subset \mathbb{N}^2 \subset \mathbb{Z}^2$$

   is a definable set, and $\psi \times \psi$ is the map sending (a, b) to $(\psi(a), \psi(b))$. Then we get that $\phi \circ (\psi \times \psi)(a, b) = a - b$, which is also clearly definable.

So we have proved that $(\mathbb{N}, 0, 1, +, \leq)$ and $(\mathbb{Z}, 0, 1, +, -, \leq)$ are bi-interpretable. Indeed, both of these models are referred to as Presburger arithmetic, and we will use the two notions interchangeably, specifying the set if necessary.

The algorithmic reason to care about interpretations is that they allow us to *reduce* certain decision problems to known results. A *reduction* of a decision problem D_1 to another decision problem D_2 is a Turing machine which, given finitely many queries to an oracle for D_2, will yield an algorithm for deciding D_1. Importantly, this means that decidability of D_2 will imply decidability of D_1[7], as such an oracle machine will exist and halt in finite time on each query.

The following result will prove fundamental, and is a consequence of theorem 5.3.2 and its remarks in [18]:

Proposition 2.4.7. *Given M_1 an L_1-structure, and M_2 an L_2-structure, if M_1 is interpretable in M_2, then the problem of deciding $FOTh(M_1)$ is reducible to the problem of deciding $FOTh(M_2)$.*

This namely means that if we build an interpretation of a plactic monoid in Presburger arithmetic, then by lemma 2.3.1 we would prove that the plactic monoids have decidable first order theory.

Let us now move on to introducing the plactic monoid.

[7] And conversely, undecidability of D_1 will imply undecidability of D_2.

3

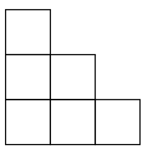
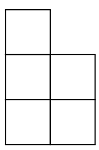
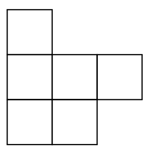
The plactic monoid: background

Originally, plactic monoids were defined in the process of associating Young tableaux to sequences. Young tableaux and Young diagrams are very commonly used in representation theory and combinatorics. Though we will mostly think of the plactic monoids in terms of their presentations, the original algorithmic procedure on tableaux still often proves useful, so let's start there.

3.1 Young tableaux and Schensted's algorithm

We follow the French conventions of Young diagrams having longer rows underneath shorter ones.

Definition 3.1.1. A *Young diagram* is a pictorial representation of a partition of $n \in \mathbb{N}$. It is composed of n boxes, arranged into some number of rows, with row length weakly increasing as you go down the page.

Example 3.1.2.  and  are Young diagrams, and  is not a Young diagram.

Definition 3.1.3. A *Semistandard Young Tableau* (henceforth simply a tableau) is a Young diagram where each box is labelled with a number $n \geq 0$ such that:

- The labels in each row weakly increase left to right.

- The labels in each column strongly decrease top to bottom.

A *standard Young tableau* (henceforth standard tableau) is a Semistandard Young tableau satisfying the additional condition that no label repeats and the set of all labels is $\{1, \dots, n\}$.

Example 3.1.4. $\begin{array}{|c|c|c|}\hline 3&3&3\\\hline 1&2&2\\\hline\end{array}$ is a tableau. $\begin{array}{|c|c|c|c|c|}\cline{1-2} 3&4\\\cline{1-3} 2&3&3\\\hline 1&1&2&4&4\\\hline\end{array}$ is a tableau.

$\begin{array}{|c|c|c|}\cline{1-1} 6\\\cline{1-2} 4&5\\\hline 1&2&3\\\hline\end{array}$ is a standard tableau.

Each tableau t will have some minimal $n \in \mathbb{N}$ such that each label of t is less than or equal to n. This allows us to define the *content* of t to be the list of numbers $c(t) \in \mathbb{N}^n$, where $c_i(t)$ is the number of times i appears as a label of a box in t. This is also sometimes written in the literature as $|t|_i$. Note that a standard tableau t will have $c_i(t) = 1$ for each $i \in \{1, \dots, n\}$.

Conversely, we may also fix some $n \in \mathbb{N}$, and consider the set of all tableaux with labels from $A = \{1, \dots, n\}$. Let t be such a tableau, whose labels are all in A. We associate to t a *row reading* in A^*. Suppose t is a tableau of m rows, labelled top to bottom as $r_1, \dots, r_m$. The labels of the boxes in each row are a weakly increasing sequence, which can be viewed as a word $r_i \in A^*$. The row reading of t is then $w = r_1 r_2 \dots r_m \in A^*$.

We similarly associate a *column reading* to t. Denote the columns of t from left to right by $c_1, \dots, c_m$. Each such column corresponds to a strictly decreasing sequence $c_i \in A^*$. The column reading of t is then $w = c_1 \dots c_m \in A^*$.

Example 3.1.5. The tableau $t = \begin{array}{|c|c|c|c|c|}\cline{1-1} 3\\\cline{1-2} 2&3\\\hline 1&1&2&2&2\\\hline\end{array}$ has row reading

$$32311222 = 3\ 23\ 11222$$

and column reading

$$32131222 = 321\ 31\ 2\ 2\ 2.$$

We now describe Schensted's algorithm. Consider $A = \{1, \ldots, n\}$ a totally ordered alphabet, and $w \in A^*$. We may view w as a finite sequence of numbers. Schensted's algorithm is used to study the longest increasing and decreasing subsequences of w. The algorithm associates a tableau to w with the property that the number of columns of w is the length of the longest *increasing* sequence, and the number of rows is the length of the longest *strictly decreasing* sequence. See [42] or [33] for more details on this combinatorial structure.

Definition 3.1.6 (Schensted's algorithm)**.** We define $P : A^* \to A^*$ to be the map sending a word w to the row reading of a tableau recursively as follows:

Firstly, $P(\varepsilon) = \varepsilon$. Then suppose $w = x_1 \ldots x_\ell \in A^*$ and $P(x_1 \ldots x_{\ell-1}) = r_1 \ldots r_m$, for some rows r_i that form the row reading of a tableau. Then we have:

1. If $r_m x_\ell$ is a row, then we set $P(r_1 \ldots r_m x_\ell) = r_1 \ldots r_m x_\ell$.
2. If not, then we can write $r_m = r_\alpha y r_\beta$, with y being the leftmost letter such that $x_\ell < y$. Such a y must exist, since otherwise $r_m x_\ell$ would be a row. But then $r_\alpha x_\ell r_\beta$ will be a row. So we set

$$P(r_1 \ldots r_m x_\ell) = P(r_1 \ldots r_{m-1} y) r_\alpha x_\ell r_\beta.$$

We call the process in point (2) 'bumping the letter y'. If t has row reading $r_1 \ldots r_m$ and column reading $c_1 \ldots c_k$, then it is straightforward to show that

$$P(r_1 \ldots r_m) = P(c_1 \ldots c_k) = r_1 \ldots r_m.$$

Proposition 3.1.7. *The relation $\sim$ on A^* given by*

$$u \sim v \iff P(u) = P(v)$$

is a semigroup congruence.

A proof is given in [33]. This result means that we can consider the monoid $A^*/\sim$, whose elements are in bijection with tableaux. Indeed, since each $\sim$-class corresponds to a distinct row reading, we can associate a tableau to each element of $A^*/\sim$. On the other hand, since each row reading is a word in A^*, every tableau corresponds to at least one element of $A^*/\sim$, yielding a bijection.

This tableau monoid is our subject of interest.

Definition 3.1.8 (The plactic monoid)**.** Given $A = \{1,\dots,n\}$, the *plactic monoid of rank n*, denoted P_n, is the tableau monoid $A^*/\sim$ defined above, with multiplication given by $u \cdot v = P(uv)$.

There is a useful notion in [27] and [33] of the *standardisation* of a word $w \in A^*$. The standardisation map $Q : A^* \to A^*$ associates a *standard* tableau to each $w \in A^*$ related to $P(w)$. The tableau $Q(w)$ is a Young diagram with the same shape as $P(w)$, but is filled by numbers $\{1, \dots |P(w)|\}$ which denote the order in which the boxes appear in the Young diagram whilst running P.

Example 3.1.9. Suppose $w = 32112322$. Then running P yields the following sequence of tableaux:

$$\begin{array}{l} 3 \end{array},\quad \begin{array}{l} 3 \\ 2 \end{array},\quad \begin{array}{l} 3 \\ 2 \\ 1 \end{array},\quad \begin{array}{ll} 3 & \\ 2 & \\ 1 & 1 \end{array},\quad \begin{array}{lll} 3 & & \\ 2 & & \\ 1 & 1 & 2 \end{array},\quad \begin{array}{llll} 3 & & & \\ 2 & & & \\ 1 & 1 & 2 & 3 \end{array},\quad \begin{array}{llll} 3 & & & \\ 2 & 3 & & \\ 1 & 1 & 2 & 2 \end{array},$$

$$\begin{array}{lllll} 3 & & & & \\ 2 & 3 & & & \\ 1 & 1 & 2 & 2 & 2 \end{array}.$$

Thus we have that $Q(w)$ will be the standard tableau $\begin{array}{lllll} 3 & & & & \\ 2 & 7 & & & \\ 1 & 4 & 5 & 6 & 8 \end{array}$

It is shown in Theorem 2.18 of [27] that the map $w \to (P(w), Q(w))$ is a bijection from the free monoid A^*.

3.2 Presentations of the plactic monoid

In 1970, Knuth [24] exhibited a set of defining relations K for the plactic monoids of the form $xzy = zxy$ and $yxz = yzx$ for $x < y < z,\ x, y, z \in A$ and $xyx = yxx$ and $yyx = yxy$ for $x < y,\ x, y \in A$. That is, we have

$$K = \{xzy = zxy,\ x \leq y < z\} \cup \{yxz = yzx,\ x < y \leq z\}$$

with $P_n = \langle A|K\rangle$. For each finite rank, it follows that P_n will be finitely presented. Note that the Knuth relations are equivalent to running Schensted's algorithm on all words of length 3.

The Knuth relations are *homogeneous*: for each $(\ell, r) \in K,\ |\ell| = |r|$. This namely means that the plactic monoid is multi-homogeneous[1], and the content of an element in P_n is well defined and additive: for each $u, v \in P_n,\ c(uv) = c(u) + c(v)$.

It was shown by Cain, Gray, and Malheiro in [6] that the plactic monoid admits a finite complete rewriting system, which we describe here.

We consider two columns α, β as words in A^*. We say that α and β are *compatible*, written $\alpha \succeq \beta$, if $\alpha\beta$ is the column reading of a tableau. Then each pair α, β with $\alpha \not\succeq \beta$ yields a rewrite rule. Consider the tableau associated to $P(\alpha\beta)$. Since the number of columns in $P(\alpha\beta)$ is the length of the longest increasing sequence, and α, β are columns, it follows that $P(\alpha\beta)$ will be a tableau with at most two columns. Therefore this tableau will have column reading $\gamma\delta$, for some columns γ, δ with $\gamma \succeq \delta$, and potentially $\delta = \varepsilon$.

Now consider $\mathcal{C} = \{c_\alpha \mid \alpha \in A^*, \alpha \text{ is a column}\}$ to be a set of symbols corresponding to columns in A^*. Since A is finite and columns are strictly decreasing sequences, $\mathcal{C}$ is also finite. Then define R to be the set of all rewrite rules detailed above

$$R = \{c_\alpha c_\beta \to c_\gamma c_\delta |\ \alpha, \beta \in A^*\ \alpha \not\succeq \beta\}.$$

[1] i.e. that each of its relations is homogeneous.

It is shown in [6] that

Lemma 3.2.1. $(\mathcal{C}, R)$ *is a complete rewriting system for* P_n.

It follows from this that P_n admits normal forms as reduced words in $\mathcal{C}^*$. By the definition of $\succeq$, this normal form will be in the form of column readings $c_{\alpha_1} \dots c_{\alpha_m}$ with each $\alpha_i \succeq \alpha_{i+1}$.

Note that if $\alpha = \alpha_m \dots \alpha_1$ and $\beta = \beta_n \dots \beta_1$, $\alpha_i, \beta_i \in A$, are columns appearing in the column reading of the same tableau (not necessarily adjacent) with α further left than β, then $\alpha \succeq \beta$. Indeed, since α and β are columns of the same tableau, then by the structure of a tableau we have that $m \geq n$. Furthermore, each pair α_i, β_i will be in the same row of the tableau, with α_i appearing earlier than β_i. This will imply that $\alpha_i \leq \beta_i$. But these two conditions imply that $\alpha \succeq \beta$. Thus $\succeq$ is a partial order on $\mathcal{C}$.

We introduce a length-decreasing-lexicographic order on $\mathcal{C}$ extending $\succeq$. For $c_\alpha, c_\beta \in \mathcal{C}$, define:

$$c_\alpha \sqsubseteq c_\beta \iff (|\alpha| > |\beta|) \vee (|\alpha| = |\beta| \wedge (\exists j : \ i < j \implies \alpha_i = \beta_i \wedge \ \alpha_j < \beta_j))$$

With j taken as $n+1$ when $c_\alpha = c_\beta$. Note that $c_\alpha \succeq c_\beta \implies c_\alpha \sqsubseteq c_\beta$. Furthermore, this is clearly a total order. We can therefore enumerate the set $\mathcal{C}$ as $\{c_1, \dots c_k\}$, with $k = |\mathcal{C}| = 2^n - 1$, such that $i \leq j \implies c_i \sqsubseteq c_j$. Then, since $c_\alpha \succeq c_\beta \implies c_\alpha \sqsubseteq c_\beta$, we have that the normal forms of P_n will have the form

$$c_1^{w_1} \dots c_k^{w_k}$$

with $w_i \in \mathbb{N}$ for each i, and for any pair c_i, c_j with $i < j \wedge c_i \not\succeq c_j$, either $w_i = 0$ or $w_j = 0$. Call two columns c_i and c_j *incompatible* if $i < j \wedge c_i \not\succeq c_j$.

Example 3.2.2. P_3 has seven columns:

$$\begin{array}[b]{|c|}\hline 3\\\hline 2\\\hline 1\\\hline\end{array}\,,\ \begin{array}[b]{|c|}\hline 2\\\hline 1\\\hline\end{array}\,,\ \begin{array}[b]{|c|}\hline 3\\\hline 1\\\hline\end{array}\,,\ \begin{array}[b]{|c|}\hline 3\\\hline 2\\\hline\end{array}\,,\ \begin{array}[b]{|c|}\hline 1\\\hline\end{array}\,,\ \begin{array}[b]{|c|}\hline 2\\\hline\end{array}\,,\ \begin{array}[b]{|c|}\hline 3\\\hline\end{array}$$

listed here in length-decreasing-lexicographic order. This list corresponds to symbols $c_1, \ldots, c_7 \in \mathcal{C}$. Note that c_4 and c_5 are incompatible. P_3 is the lowest rank plactic monoid with an incompatible pair.

Example 3.2.3. In P_3, the element $c_1^3 c_2 c_4^2 \in \mathcal{C}^*$ is in normal form and corresponds to the following tableau:

$$\begin{array}{|c|c|c|c|c|c|}\cline{1-3} 3 & 3 & 3 & \multicolumn{3}{c}{} \\\hline 2 & 2 & 2 & 2 & 3 & 3 \\\hline 1 & 1 & 1 & 1 & 2 & 2 \\\hline\end{array}\,.$$

4

An exploration of small equations

4.1 Conjugacy

The conjugacy problem is a classic decision problem in group theory. Given two elements u, v of a group G, the question of whether some $g \in G$ conjugates u to v, that is, $gug^{-1} = v$, is a very natural and important question. For monoids however, the absence of inverse elements means that there is no straightforward way to ask an analogous problem. Several variants of conjugacy for monoids and semigroups exist. A paper of Araújo, Kinyon, Konieczny, and Malheiro [2] gives an overview of some of them. In particular, this paper gives an overview of the notions used to study conjugacy in the plactic monoid.

A simple way to reinterpret conjugation in the monoid world is by rearranging the equation so that there are no inverse elements. This allows us to define *left* and *right* conjugacy: given u, v elements of some monoid M, we call these elements left conjugate, written $u \sim_\ell v$, if for some $X \in M$ we have that $uX = Xv$, and right conjugate, written $u \sim_r v$, if for some $X \in M$ we have that $Xu = vX$. These notions are related, since $u \sim_\ell v$ if and only if $v \sim_r u$. But neither relation is necessarily symmetric. By considering both simultaneously, we obtain $o-$conjugacy, which is precisely when u and v are both left and right conjugate. This turns conjugacy into an equivalence relation, and it is named after Friedrich Otto.

An alternative formulation of conjugacy, called *primary* conjugacy, says that two elements a and b in M are conjugate, written $a \sim_p b$, if the following holds:

$$a \sim_p b \iff \exists u, v : \ a = uv \wedge b = vu.$$

This relation is not transitive, so we again wish to turn p-conjugacy into an equivalence relation. This time, we will take the transitive closure, which we call $\star p$-conjugacy:

$$a \sim_p^\star b \iff \exists u_1, u_2, \ldots, u_n : \ a \sim_p u_1 \wedge u_1 \sim_p u_2 \wedge \cdots \wedge u_n \sim_p b.$$

This notion is stronger than o-conjugacy: if two elements are $\star p$-conjugate then they also must be o-conjugate. Indeed, if a and b are p-conjugate, then there is u, v such that $a = uv$ and $b = vu$. Namely, this also means that $au = uvu = ub$ and $va = vuv = bv$, so a and b are o-conjugate. Since o-conjugacy is an equivalence relation, we then also get that if a and b are $\star p$-conjugate, they most be o-conjugate by transitivity of o-conjugacy.

One can present a conjugacy problem for any of these notions, by asking about the existence of an agorithm that would check the given type of conjugacy between two elements. For the plactic monoid, one can already see that if two elements $u, v \in P_n$ are left conjugate, then they must have the same content: $c(u) = c(v)$, since content is additive under multiplication. So there is a necessary content condition on any pair in the plactic monoid which is conjugate in any of the above ways.

In section 4 of their 1981 paper *le monoïde plaxique* [27], Lascoux and Schützenberger explored, among other things, the $\star p$-conjugacy relation on P_n. They showed that two elements having the same content is in fact a sufficient condition for $\star p$-conjugacy. This namely implies the decidability of the conjugacy problem, since the problem is reduced to simply checking the content of two finite strings.

The result in their paper, which is also presented in more detail in chapter 5 of [33], is far from the main focus, and so is reached in a roundabout way. The idea of their proof is to define the *cyclage* map $\mathcal{C} : P_n \to P_n$ which sends an element $w \in P_n$, written as $w = x_1 \dots x_k$ in row form with each $x_i \in A$, to $\mathcal{C}(w) = P(x_2 \dots x_k x_1)$, where P is the application of Schensted's algorithm. By this construction, it is clear that $w \sim_p \mathcal{C}(w)$. It is then shown that by repeatedly applying this map $\mathcal{C}$ to any element $w \in P_n$, you eventually reach the unique *content row* of w – that is, the unique row r with $c(r) = c(w)$. The proof of this fact is obtained by considering the cocharge of a tableau – a natural number statistic that can be associated to any tableau. This statistic is shown to be well defined using an action of the symmetric group on n elements acting on tableaux, which is said to be acting by so-called "automorphisms on P_n".

All of these ideas are useful when studying the plactic monoid in the context of crystal basis theory, and have as a consequence the sufficiency of content for conjugacy. It turns out, however, that a direct approach will prove the conjugacy result in a simpler, entirely constructive way. What follows is an original approach which will yield a significantly simpler proof of the decidability of conjugacy in the plactic monoid[1].

4.1.1 Deciding when two elements are conjugate

Let $w \in P_n$ be a tableau. Write $w = tb$, with b the bottom row of w.

Lemma 4.1.1. *All occurrences of the letter 1 in w are in b.*

Proof. By definition, columns must be strictly decreasing. So if a letter k is in a certain row, then a letter $k - 1$ must appear in the row below it. But 0 is not a letter, so 1 must be in the bottom row of any tableau word. □

Now, consider the sequence $w_1, w_2, \dots, w_n$ of elements of P_n, where $w_1 = w$ and,

[1]It was discussed in the viva of this thesis that a similar method to the one presented below was used in [9] to show the same result – that two elements in P_n are conjugate when their contents are equal. This is Theorem 17 of their paper. The methods below were developed without knowledge of this result.

given w_i, we write $w_i = t_i b_i$, with b_i the bottom row of w_i, and set $w_{i+1} = P(b_i t_i)$. In this case, $t_1 = t$ and $b_1 = b$.

Lemma 4.1.2. *All occurrences of the letters* $\{1, \ldots, i\}$ *in* w_i *are in the bottom row* b_i.

Proof. By induction, with base case $w_1 = w$, suppose all occurrences of the letters $\{1, \ldots, i-1\}$ are in b_{i-1}. Then in $w_i = P(b_{i-1}t_{i-1})$, any time the letter i appears, it cannot be followed by any $x < i$, since b_{i-1} is a row, and t_{i-1} has no occurrences of any letters in $\{1, \ldots, i-1\}$. Thus no letters i can be bumped in Schensted's algorithm, which means all i's in w_i will be in the bottom row b_i. Furthermore, no letters in t_{i-1} are able to bump any letters in b_{i-1}, so all letters $\{1, \ldots, i-1\}$ will also remain on the bottom row b_i. $\square$

We know that $t_i b_i \sim_p b_i t_i$ as words in the free monoid A^*, so $w_i \sim_p w_{i+1}$ in P_n. Therefore, we have that $w \sim_p^\star w_n$. Furthermore, since w_n has all occurrences of $\{1, \ldots, n\}$ appearing in its bottom row, then we know that w_n is a row with the same content as w. So every $w \in P_n$ is $\star p$-conjugate to the unique row with the same content as w.

Theorem 1. *If* u *and* v *have the same content, then* $u \sim_p^\star v$.

Proof. Let u_n and v_n be the unique rows with the same content as u and v respectively. Then $u \sim_p^\star u_n$ and $v \sim_p^\star v_n$. When u and v have the same content, we have $u_n = v_n$, yielding $u \sim_p^\star v$. $\square$

4.1.2 Constructing a solution when one exists

The above proof yields a natural algorithm for finding a conjugator – that is, given a pair $u, v \in P_n$, an element X such that $uX = Xv$.

Firstly, we associate to u and v sequences $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$, as in Lemma 4.1.2. Write each u_i as $t_{u_i} b_{u_i}$ and each v_i as $t_{v_i} b_{v_i}$, with b_{u_i} and b_{v_i} being the respective bottom rows of the tableaux.

Let $Y_i = b_{v_i}$. Then we have that

$$Y_i v_i = v_{i+1} Y_i$$

for each $i \in \{1, \ldots n-1\}$. Note that the transitivity of left conjugacy implies that

$$aX = Xb,\ bY = Yc \implies aXY = XbY = XYc$$

so it follows that taking $Y = Y_{n-1}Y_{n-2}\ldots Y_2Y_1$, we have that $Yv = Yv_1 = v_nY$.

Let also $X_i = t_{u_i}$ as defined above. Then we have that

$$u_i X_i = X_i u_{i+1}$$

for each $i \in \{1, \ldots, n-1\}$. So, analogously to before, take $X = X_1X_2\ldots X_{n-1}$. Then we have that $uX = u_1X = Xu_n$. Combining these two equalities, we get that

$$uXY = Xu_nY = Xv_nY = XYv.$$

Note that the solution given by this algorithm is not necessarily the only conjugator that exists, nor is it length minimising.

Example 4.1.3. Let Let $u = 3211123$ and $v = 2231113$. Then for u:

- $u = 32\ 11123$, so $X_0 = 32$,
- $u' = 1112332 = 3\ 111223$, so $X_1 = 3$,
- $u'' = 1112233$ which is a content row.

So $X = X_0X_1 = 323$.

Now for v:

- $v = 223\ 1113$, so $Y_0 = 1113$,
- $v' = 1113223 = 3\ 111223$, so $Y_1 = 111223$,
- $v'' = 1112233$ which is a content row.

So $Y = Y_1Y_0 = 1112231113 = 223\ 1111113$.

Now, the solution given by the above algorithm will be

$$Z = XY = 3232231111113 = 33\ 2223\ 1111113.$$

Indeed:

$$uZ = 3211123\ 3322231111113 = 3333\ 222223\ 1111111113.$$

$$Zv = 3322231111113\ 2231113 = 3333\ 222223\ 1111111113.$$

Example 4.1.4. Consider $u = 32211$ and $v = 32112$. Let's use our algorithm to solve $uZ = Zv$.

First we calculate X:

- $u = 322\ 11$ so $X_0 = 322$,
- $u' = 11322 = 3\ 1122$ so $X_1 = 3$,
- $u'' = 11223$ which is a content row.

So $X = 3223$.

Now we calculate Y:

- $v = 32\ 112$ so $Y_0 = 112$,
- $v' = 11232 =\ 3\ 1122$ so $Y_1 = 1122$,
- $v'' = 11223$ which is a content row .

So $Y = 1122112 = 2211112$.

So a solution here would be $XY = 32232211112 = 33\ 2222\ 11112$. Indeed:

$$uXY = 333\ 222222\ 1111112 = XYv.$$

4.2 The right equation

Given a pair of words $u, v \in P_n$, we ask whether there exists an X such that

$$uX = vX.$$

Like in the case of conjugacy, a necessary condition on u and v for this equation to have a solution is that the contents match: $c(u) = c(v)$. We will show that this condition is also sufficient.

Proposition 4.2.1. *For X a variable, and $u, v \in P_n$, the equation $uX = vX$ has a solution in P_n if and only if u and v have the same content.*

Proof. First, let us consider the case of P_2. Here, we will have $u = 2^{u_1}1^{u_2}2^{u_3}$ and $v = 2^{v_1}1^{v_2}2^{v_3}$. The necessary content condition will imply that $u_1 + u_3 = v_1 + v_3$, and $u_2 = v_2$. Consider $k \in \mathbb{N}$ greater than both u_3 and v_3. Then by Schensted's algorithm we will have that

$$u1^k = 2^{u_1+u_3}1^{u_2+k} = 2^{v_1+v_3}1^{v_2+k} = v1^k,$$

so the necessary content condition is also sufficient.

We will continue by induction on the rank of the plactic monoid. Given $u, v \in P_n$, write $u = u_1u_2 \dots u_k$ and $v = v_1v_2 \dots v_j$ in their row readings. Suppose u and v have equal content. Recall by lemma 4.1.1 that the number 1 can only appear in the bottom row of any tableau, so we must have that $u = u_1 \dots u_{k-1}1^x\tilde{u}_k$ and

$v = v_1 \dots v_{j-1} 1^x \tilde{v}_j$, where $x = c_1(u) = c_1(v)$ and $\tilde{u}_k, \tilde{v}_j$ have no occurrences of the number 1.

Let $k \in \mathbb{N}$ be greater than the length of both $\tilde{u}_k$ and $\tilde{v}_j$. Then

$$u1^k = u_1 u_2 \dots u_{k-1} \tilde{u}_k 1^{x+k}$$

and

$$v1^k = v_1 v_2 \dots v_{j-1} \tilde{v}_j 1^{x+k}.$$

This means that we have $\tilde{u} = u_1 \dots u_{k-1} \tilde{u}_k$ and $\tilde{v} = v_1 \dots v_{j-1} \tilde{v}_j$, which are elements of a plactic monoid over the alphabet $\{2, \dots, n\}$ and have equal content. Since this plactic monoid has rank $n - 1$, by our induction hypothesis there is some $Y \in \{2, \dots, n\}^*$ such that $\tilde{u}Y = \tilde{v}Y$.

Now, let $\ell \in \mathbb{N}$ be greater than the length of Y. Then we have that

$$u1^k Y 1^\ell = \tilde{u} 1^{x+k} Y 1^\ell = \tilde{u} Y 1^{x+k+\ell}$$

and

$$v1^k Y 1^\ell = \tilde{v} 1^{x+k} Y 1^\ell = \tilde{v} Y 1^{x+k+\ell}$$

since the ℓ occurrences of 1 will bump the letters of Y above the lowermost row of 1's. But since $\tilde{u}Y = \tilde{v}Y$ this solves the right equation with $X = 1^x Y 1^\ell$. $\square$

From a more constructive viewpoint, the way Schensted's insertion algorithm is defined, when we multiply an element u on the right, all the letters of u will either stay in the row they originally appear, or get bumped to a 'higher' row, in the sense of being further up the page in the tableau. By multiplying both u and v repeatedly by the element 1, we bump all letters except for 1 to a higher row. We repeat this process, bumping all letters that are not 1 or 2 from the bottom two rows, then all letters that are not 1, 2, or 3 from the bottom three rows, and so on, until each occurrence of a letter k is on the k-th row from the bottom in the tableau. This will constructively yield a solution for any pair of words with the same content.

Example 4.2.2. Let $u = 123$ and $v = 321$.

$$\begin{aligned} u &= 123 & v &= 3\ 2\ 1 \\ u2 &= 3\ 122 & v2 &= 3\ 2\ 12 \\ u211 &= 3\ 22\ 111 & v211 &= 3\ 22\ 111 \end{aligned}$$

So $X = 211$ will solve the equation $uX = vX$.

Example 4.2.3. Let's see a bigger example. Let $u = 3211123$ and $v = 2231113$

$$\begin{aligned} u &= 3\ 2\ 11123 & v &= 223\ 1113 \\ u2 &= 3\ 23\ 11122 & v2 &= 2233\ 1112 \\ u211 &= 33\ 222\ 11111 & v211 &= 3\ 2223\ 11111 \\ u21121 &= 33\ 2222\ 111111 & v21121 &= 33\ 2222\ 111111 \end{aligned}$$

So $X = 21121 = 22\ 111$ will solve the equation $uX = vX$.

4.3 The left equation

Analogously to the previous section, we now consider, for a pair of words $u, v \in P_n$, whether there exists some X such that

$$Xu = Xv.$$

As before, the necessary content condition is $c(u) = c(v)$, and we will again show that this condition is also sufficient.

Proposition 4.3.1. *Let $u, v \in P_n$. Then there exists $X \in P_n$ such that $Xu = Xv$ if and only if $c(u) = c(v)$.*

Proof. In analysing this equation, it will be helpful to consider P_n with respect to its column generators $\mathcal{C} = \{c_1, \dots, c_k\}$. Specifically, define for each $i \in A$ the column $f_i \in \mathcal{C}$ corresponding to the decreasing sequence of all the letters n down to i:

$$f_i = \begin{array}{|c|} \hline n \\ \hline n-1 \\ \hline \vdots \\ \hline i \\ \hline \end{array}$$

and consider X of the form $X = f_1^{x_1} f_2^{x_2} \dots f_n^{x_n}$. When we multiply X on the right by some $i \in A$, we get that

$$\begin{aligned} Xi &= f_1^{x_1} \dots f_i^{x_i} f_{i+1}^{x_{i+1}} i \dots f_n^{x_n} \\ &= f_1^{x_1} \dots f_i^{x_i+1} f_{i+1}^{x_{i+1}-1} \dots f_n^{x_n} \end{aligned}$$

because $f_{i+1} i = f_i$, and Schensted's algorithm insists that i bump the leftmost letter in the row that it can.

Now, consider $u \in P_n$ where the number of instances of i in u is less than x_{i+1} for each $i \in A \setminus \{n\}$. That is, $c_i(u) \leq x_{i+1}$ for each $i \in A \setminus \{n\}$. Notice that, in the product Xu, the bottom row of X has at most as many letters $i+1$ as u has letters i, so in the Schensted insertion algorithm, each i from u will bump an $i+1$ from the bottom row of X, regardless of which order the letters are inserted. So we obtain a formula for the product in this case

$$Xu = f_1^{x_1 + c_1(u)} \dots f_i^{x_i - c_{i-1}(u) + c_i(u)} \dots f_n^{x_n - c_{n-1}(u) + c_n(u)}.$$

Notice that this means that all letters that appeared in u will remain in the bottom row of Xu. But that means that, so long as both $c_i(u) \leq x_{i+1}$ and $c_i(v) \leq x_{i+1}$ for all $i \in A \setminus \{n\}$, we only get $Xu \neq Xv$ when $c(u) \neq c(v)$.

Namely, for any $u, v \in P_n$ with $c(u) = c(v)$, we can take some $X = f_1^{x_1} \dots f_n^{x_n}$ with $x_1 = 0$ and $x_i \geq c_{i-1}(u) = c_{i-1}(v)$ for each $i \in \{2, \dots, n\}$. Then we will be exactly in the above case, and so we must have $Xu = Xv$. □

Let's see this process applied to the same examples as in the right equation. In the following examples, elements of P_n written as words in A^* will be in column reading.

Example 4.3.2. Let $u = 123$ and $v = 321$. Then if we take $x_2 \geq 1$ and $x_3 \geq 1$ we will obtain a solution. So take, for example,

$$X = f_2 f_3 = \begin{array}{cc} \boxed{3} & \\ \boxed{2} & \boxed{3} \end{array},$$

then we see that

$$Xu = 323123 = 321\ 32\ 1 = f_1 f_2 f_3.$$

$$Xv = 323321 = 321\ 32\ 1 = f_1 f_2 f_3.$$

Example 4.3.3. Let $u = 3211123$ and $v = 2121313$. Then we need to take $x_2 \geq 3$ and $x_3 \geq 2$ to obtain a solution. So take, for example

$$X = f_2^3 f_3^2 = \begin{array}{ccccc} \boxed{3} & \boxed{3} & \boxed{3} & & \\ \boxed{2} & \boxed{2} & \boxed{2} & \boxed{3} & \boxed{3} \end{array},$$

and we see that

$$Xu = 323232333211123 = 321\ 321\ 321\ 32\ 32\ 3\ 3 = f_1^3 f_2^2 f_3^2.$$

$$Xv = 323232332121313 = 321\ 321\ 321\ 32\ 32\ 3\ 3 = f_1^3 f_2^2 f_3^2.$$

4.4 Intersections of principal ideals

The left and right equations described above are linked to the question of when principal ideals have nonempty intersection.

Definition 4.4.1. Given a monoid M and an element $a \in M$, the *right principal ideal generated by* a, written aM, is the set $\{ax \mid x \in M\} \subseteq M$. Analogously, the *left principal ideal generated by* a, written Ma, is the set $\{xa \mid x \in M\} \subseteq M$.

Given two principal right ideals aM, bM, the question of having nonempty intersection is equivalent to seeking a solution to the equation

$$aX = bY$$

for X, Y variables taking values in M. Analogously, whether two principal left ideals Ma, Mb intersect is equivalent to seeking a solution to the equation

$$Xa = Yb.$$

In the plactic monoids, we obtain the following result.

Proposition 4.4.2. *Any two right (respectively left) principal ideals in the plactic monoid of any finite rank intersect.*

Proof. Given $u, v \in P_n$ any pair of elements, we can find $\alpha, \beta \in P_n$ such that

$$c(u\alpha) = c(\alpha u) = c(\beta v) = c(v\beta).$$

Now, using Proposition 4.2.1 we know that there is some $X \in P_n$ such that

$$u\alpha X = v\beta X,$$

hence the right principal ideals of u and v intersect. Likewise, using Proposition

4.3.1, we know that there is some $Y \in P_n$ such that

$$Y\alpha u = Y\beta V,$$

hence the left principal ideals of u and v intersect. □

We can further show the following nice corollary.

Corollary 4.4.3. *In the infinite rank plactic monoid $P(\mathbb{N})$, any two right (respectively left) principal ideals intersect.*

Where $P(\mathbb{N})$ is the monoid of all Semistandard Young Tableaux, obtained as a union of finite rank plactic monoids

$$P(\mathbb{N}) = \bigcup_{n \in \mathbb{N}} P_n.$$

Proof. Given a pair $u, v \in P(\mathbb{N})$, there must be some $n \in \mathbb{N}$ such that

$$u, v \in P_n \subset P(\mathbb{N}).$$

So, by Proposition 4.4.2, there is some pair $X, Y \in P_n \subset P(\mathbb{N})$ such that

$$uX = vY,$$

so the right ideals intersect in $P(\mathbb{N})$ as well. The argument for left ideals is analogous. □

This result is likely known to researchers in the field, but to the author's knowledge it has not been published before.

4.5 Simultaneous equations

The above discussion of the left and right equation yields the same necessary and sufficient condition to satisfy both equations. A natural question to ask therefore is whether these can be solved simultaneously: does there exist some $X \in P_n$ such that $uX = vX$ and $Xu = Xv$? We will see that the answer is yes.

Suppose that $u, v \in P_n$ have the same content. Then there exists some X such that $uX = vX$ and some Y such that $Yu = Yv$. Now, consider $Z = XY$. Then we see that

$$uZ = uXY = vXY = vZ,$$
$$Zu = XYu = XYv = ZV,$$

by applying the right equation to uX and the left equation to Yu. Thus we see that Z solves both equations simultaneously. So, as long as the contents of u and v match, we can solve the left and right equations simultaneously.

Example 4.5.1. Let's see this for the case of P_2, the plactic monoid generated by $A = \{1, 2\}$.

In the left equation, by our algorithm we will get that X has the form $f_2^{x_2}$, where f_2 is the column $\boxed{2}$. So X will be an element 2^x, with x greater than the number of 1's in the content of u and v.

In the right equation, our procedure reduces to bumping all 2's from the bottom rows of u and v. This can be done by some 1^ℓ for ℓ sufficiently large. So we can take $Y = 1^\ell$ to solve the right equation. Now, taking $Z = YX = 1^\ell 2^x$, we will see that $uZ = vZ$ and $Zu = Zv$.

As an explicit example, take $u = 2^4 1^5 2^5$ and $v = 2^2 1^5 2^7$. Then $Y = 1^7$ and $X = 2^5$

solve the right and left equations respectively, and for $Z = YX = 1^7 2^5$, we get

$$uZ = 2^4 1^5 2^5 \times 1^7 2^5 = 2^9 1^{12} 2^5,$$
$$vZ = 2^2 1^5 2^7 \times 1^7 2^5 = 2^9 1^{12} 2^5.$$
$$Zu = 1^7 2^5 \times 2^4 1^5 2^5 = 2^5 1^{12} 2^9,$$
$$Zv = 1^7 2^5 \times 2^2 1^5 2^7 = 2^5 1^{12} 2^9.$$

4.6 Conjugacy in P_2

4.6.1 Structure of sets of conjugators

Continuing our consideration of the plactic monoid over $A = \{1, 2\}$, let us consider the case of left conjugacy $uX = Xv$ and right conjugacy $Xu = vX$. We will seek to describe the set of all $X \in P_2$ solving either left or right conjugacy for a given pair u, v.

Here, we will benefit from considering P_2 as being generated by the set $\{1, 2, t\}$, where $t = 21$ generates the centre of P_2. This is exactly the column presentation of P_2, in the sense of [6]. The reduced words will then have the form $t^a 1^b 2^c$, for some $(a, b, c) \in \mathbb{N}^3$. We also get a formula for the multiplication of $u = t^{u_1} 1^{u_2} 2^{u_3}$ and $v = t^{v_1} 1^{v_2} 2^{v_3}$, by considering the fact that t is central, so we can move powers of t to the left:

$$\begin{aligned} t^{u_1} 1^{u_2} 2^{u_3} t^{v_1} 1^{v_2} 2^{v_3} &= t^{u_1+v_1} 1^{u_2} 2^{u_3} 1^{v_2} 2^{v_3} \\ &= t^{u_1+v_1} 1^{u_2} 2^{\max(0,u_3-v_2)} t^{\min(u_3,v_2)} 1^{\max(0,v_2-u_3)} 2^{v_3} \\ &= t^{u_1+v_1+\min(u_3,v_2)} 1^{\max(u_2,u_2+v_2-u_3)} 2^{\max(v_3,v_3+u_3-v_2)}. \end{aligned}$$

We will revisit the pair of equations $uX = Xv$ and $Xu = vX$. Supposing these equations have solutions for a given pair of words, there will be sets C_ℓ and C_r of all left (respectively right) conjugators:

$$C_\ell = \{X \in P_n \mid uX = Xv\}$$
$$C_r = \{X \in P_n \mid Xu = vX\}.$$

We seek a description of the elements of these two sets.

Suppose $u = t^{u_1}1^{u_2}2^{u_3}$ and $v = t^{v_1}1^{v_2}2^{v_3}$ are conjugate. Then they must have the same content, so $u_1 + u_2 = v_1 + v_2$ and $u_1 + u_3 = v_1 + v_3$. Suppose that $u_1 \geq v_1$. Then we can write $u = t^a1^b2^c$ and $v = t^{a-k}1^{b+k}2^{c+k}$, for some $k \in \mathbb{N}$.

Let us first consider left conjugacy: Suppose $X = t^x1^y2^z$ solves $uX = Xv$. Then the following equations are satisfied

$$\begin{aligned}
t^a1^b2^ct^x1^y2^z &= t^x1^y2^zt^{a-k}1^{b+k}2^{c+k} \\
t^a1^b2^ct^x1^y2^z &= t^{a+x+\min(c,y)}1^{\max(b,b+y-c)}2^{\max(z,z+c-y)} \\
t^x1^y2^zt^{a-k}1^{b+k}2^{c+k} &= t^{x+a-k+\min(z,b+k)}1^{\max(y,y+b+k-z)}2^{\max(c+k,c+k+z-b-k)}
\end{aligned}$$

Which yields the following system of equations satisfied by x, y, and z

$$a + x + \min(c, y) = x + a - k + \min(z, b + k) \tag{4.6.1}$$
$$\max(b, b + y - c) = \max(y, y + b + k - z) \tag{4.6.2}$$
$$\max(z, z + c - y) = \max(c + k, c + k + z - b - k) \tag{4.6.3}$$

From equation (4.6.1), it follows that x can be any number. The restrictions on y and z then split into four cases

1. $y \leq c$ and $z \leq b + k$: then the equations above reduce to

$$\begin{aligned}
a + y &= a - k + z \\
b &= y + b + k - z \\
z + c - y &= c + k,
\end{aligned}$$

yielding $z = y + k$. This also implies that $y \leq b$, but does not place any further restrictions on y, so we obtain a solution family of the form $t^x 1^y 2^{y+k}$ for each $0 \leq y \leq \min(b, c)$ and any $x \in \mathbb{N}$

2. $y \leq c$ and $z \geq b + k$: the equations above reduce to

$$
\begin{aligned}
a + y &= a - k + b + k \\
b &= y \\
z + c - y &= c + k + z - b - k.
\end{aligned}
$$

These equations yield the sole restriction that $y = b$, which works if and only if $b \leq c$. So when $b \leq c$ we get a solution family $t^x 1^b 2^{b+k+z}$, for any pair $(x, z) \in \mathbb{N}^2$. When $b > c$ we get no solutions of this form.

3. $y \geq c$ and $z \leq b + k$: the equations above reduce to

$$
\begin{aligned}
a + c &= a - k + z \\
b + y - c &= y + b + k - z \\
z &= c + k.
\end{aligned}
$$

Here we get the restriction $z = c + k$, which works if and only if $c \leq b$. This is the converse to case 2 above: when $b \geq c$ we get a solution family $t^x 1^{c+y} 2^{c+k}$, for $(x, y) \in \mathbb{N}^2$, and when $b < c$ we get no solutions of this form.

4. $y \geq c$ and $z \geq b + k$: the equations above reduce to

$$
\begin{aligned}
a + c &= a - k + b + k \\
b + y - c &= y \\
z &= c + k + z - b - k,
\end{aligned}
$$

all three of which reduce to $b = c$. If this equation – which is a condition on u and v – is not satisfied, there are no solutions in this case. Otherwise, as long as $y \geq c$ and $z \geq b + k$, any $t^x 1^y 2^z$ will be a solution.

Using the above cases, we can split the set of conjugators into two parts. For each pair u and v, we may consider C_ℓ as the union of the set of conjugators obtained in case 1, and another set of conjugators obtained from one of cases 2, 3, and 4. This is because which of the cases 2, 3, and 4 yield any solutions depends on the pair u, v we chose. If $b < c$ we will have solutions from case 2 only; if $b > c$ we will have solutions from case 3 only; if $b = c$ then we will have solutions from case 4[2].

Thus, we may write the set of conjugators as $C_\ell = B_\ell \cup U_\ell$, with

$$B_\ell = \left\{X = t^x 1^y 2^{y+k} \in P_n \mid y \leq \min(b,c) \wedge x \in \mathbb{N}\right\}$$
$$U_\ell = \begin{cases} \left\{X = t^x 1^{c+y} 2^{c+k} \in P_n \mid (x,y) \in \mathbb{N}^2\right\}, & b > c \\ \left\{X = t^x 1^{b} 2^{b+k+z} \in P_n \mid (x,z) \in \mathbb{N}^2\right\}, & b < c \\ \left\{X = t^x 1^{b+y} 2^{b+k+z} \in P_n \mid (x,y,z) \in \mathbb{N}^3\right\}, & b = c. \end{cases}$$

Let's now consider right conjugacy. Plugging $X = t^x 1^y 2^z$ into the right conjugacy equation yields the following system of equations satisfied by x, y, z:

$$x + a + \min(z, b) = a - k + x + \min(c + k, y) \tag{4.6.4}$$
$$\max(y, y + b - z) = \max(b + k, b + k + y - c - k) \tag{4.6.5}$$
$$\max(c, c + z - b) = \max(z, z + c + k - y) \tag{4.6.6}$$

but notice that this is the same system of equations as in the case of left conjugacy, up to a relabelling of variables. Swapping b with c and y with z will yield the same equations as in the left conjugacy case.

As such, the set C_r will have the same structure as C_ℓ, though with slightly modified solution families due to the coordinate relabelling in the equations. Explicitly, we

[2]Note that the solutions obtained in case 2 and 3 would also be obtained from case 4.

will obtain a decomposition $C_r = B_r \cup U_r$, with

$$B_r = \Big\{X = t^x 1^{z+k} 2^z \in P_n \mid z \leq \min(b,c) \wedge x \in \mathbb{N}\Big\}$$

$$U_r = \begin{cases} \left\{X = t^x 1^{c+k+y} 2^c \in P_n \mid (x,y) \in \mathbb{N}^2\right\}, & b > c \\ \left\{X = t^x 1^{b+k} 2^{b+z} \in P_n \mid (x,z) \in \mathbb{N}^2\right\}, & b < c \cdot \\ \left\{X = t^x 1^{b+k+y} 2^{b+z} \in P_n \mid (x,y,z) \in \mathbb{N}^3\right\}, & b = c \end{cases}$$

Note that in the above arguments we assumed that $u_1 \geq v_1$. So our descriptions of C_ℓ and C_r are specifically associated to a pair (u, v) with $u_1 \geq v_1$. Call these $C_\ell^{(u,v)}$ and $C_r^{(u,v)}$. If for a pair of words $w, t \in P_2$ we have $w_1 < t_1$, then we can rearrange $wX = Xt$ to $Xt = wX$ and $Xw = tX$ to $tX = Xw$. Thus, by considering the pair (t, w) we see that $C_\ell^{(t,w)}$ is the set of *right* conjugators for the pair (w, t), and $C_r^{(t,w)}$ is the set of *left* conjugators for the pair (w, t). So the description of the two sets of conjugators swaps.

4.6.2 Power conjugacy

A generalisation of left (respectively right) conjugacy would be considering equations of the form $uX^n = X^n v$ (respectively $X^n u = vX^n$) for some $n \in \mathbb{N}$. We will call this 'power conjugacy'.

Clearly, a necessary condition to be power conjugate is for u and v to be conjugate in the first place, but it is not obvious that this should be a sufficient condition, as there is not a known general formula for calculating roots in the plactic monoid. But in the case of P_2, we can use our classification of conjugators to show this condition is sufficient.

Proposition 4.6.1. *Suppose u and v are conjugate in P_2. Then there exists a solution to $uX^n = X^n v$ for each $n \in \mathbb{N}$.*

Proof. First, suppose that u, v are such that $u_1 \geq v_1$. By the discussion above, there will be at least one family of the form $1^\alpha 2^{\beta+z}$ or $1^{\alpha+y}2^\beta$ in U_ℓ of u and v, for some fixed α, β, and y, z arbitrary natural numbers. In the case that this is $1^\alpha 2^{\beta+z}$, fix some $z_1 > \alpha$ and let $X = 1^\alpha 2^{\beta+z_1}$ Then

$$X^2 = t^\alpha 1^\alpha 2^{\beta+z_2}$$

with $z_2 = 2z_1 - \alpha + \beta > z_1 > \alpha$. This is again a conjugator in U_ℓ. Then, by induction, if $X^{n-1} \in U_\ell$, and $z_{n-1} > \alpha$, we get that

$$X^n = t^{(n-1)\alpha} 1^\alpha 2^{\beta+z_n}$$

with $z_n = 2z_{n-1} - \alpha + \beta > z_{n-1} > \alpha$. So for any $n \in \mathbb{N}$ we pick, we see that $X^n \in U_\ell$.

In the case of $1^{\alpha+y}2^\beta$, fix some $y_1 > \beta$ and let $X = 1^{\alpha+y_1}2^\beta$. An analogous argument shows that

$$X^n = t^{(n-1)\beta} 1^{\alpha+y_n} 2^\beta$$

with $y_n > y_{n-1} > \cdots > y_1 > \beta$, and hence $X^n \in U_\ell$ for all $n \in \mathbb{N}$.

Now, suppose $u_1 < v_1$. Then the set of left conjugators corresponding to u and v will be the set $C_r^{(v,u)}$. But here again there will be at least one family of the form $1^\alpha 2^{\beta+z}$ or $1^{\alpha+y}2^\beta$ in the U_r corresponding to (v, u), for fixed α, β, and $y, z \in \mathbb{N}$ allowed to vary. So by an analogous argument, we will see that X^n will be in U_r for any $n \in \mathbb{N}$. $\square$

Note that by swapping u and v in the left power conjugacy equation, we get the same argument showing the result for right power conjugacy $X^n u = vX^n$.

4.7 Further questions on generalisation

There are still more questions that can be explored in the world of small equations over plactic monoids. A natural question from the previous section would be to explore the set of conjugators for plactic monoids on more than 2 generators. Furthermore, does a conjugate pair $u, v \in P_n$ have solutions to power conjugacy in any other plactic monoids? If so, what would these solutions look like? One could also consider whether these sets of conjugators have any grammatical structure, in the sense of formal languages.

One can also further this exploration by considering larger Diophantine equations in one variable. Suppose we wish to find an $X \in P_n$ that satisfies an arbitrary equation

$$u_1 X u_2 X \dots u_n X u_{n+1} = v_1 X \dots v_m X v_{m+1}$$

where all u_i, v_i are members of P_n. What sort of condition is sufficient for such an equation to have a solution, and what would the set of solutions look like?

We do have some necessary conditions on the content of our coefficients:

- if $n = m$, then we must have

  $$\sum_{i=1}^{n+1} c_j(u_i) = \sum_{i=1}^{n+1} c_j(v_i)$$

  for each $j \in A$

- if without loss of generality $n > m$, then we must have

  $$\sum_{i=1}^{n+1} c_j(u_i) \leq \sum_{i=1}^{n+1} c_j(v_i)$$

  for each $j \in A$

but neither condition is sufficient, in general.

Example 4.7.1. $1X = 21$ has no solution. Indeed, content arguments show that X must be 2. But $12 \neq 21$.

Example 4.7.2. $1X2 = 21X$ has no solution. Here, we will examine the bottom row of each side of the equation. Suppose $X = r_1 \dots r_m$ as a row reading. Then the bottom row of $21X$ will be $1r_m$, which will always be a row. On the other hand, the bottom row of $1X2$ will be the bottom row of $1r_m2$. If this is itself a row, then $|1r_m2| > |1r_m|$ so they cannot be equal. If this is not a row, then by Schensted's algorithm we have $r_m = r_\alpha x r_\beta$, with $x > 2$, and $r_\alpha \in P_2$. Then we get that $1r_m = 1r_\alpha x r_\beta$, and the bottom row of $1r_m2$ is $1r_\alpha 2 r_\beta$. Then since $x \neq 2$, these two rows cannot be equal.

Of course, since any single variable Diophantine equation is a first order formula, the next section will show that the question of whether it has solutions is decidable. What this means is that an algorithmic exploration of this question is entirely feasible, should we wish to undertake it.

5

On the first order theory of plactic monoids

In this chapter, our key result is that P_n is interpretable in Presburger arithmetic for any $n \in \mathbb{N}$, and hence will have decidable first order theory. An important corollary of this is that the Diophantine problem is decidable (since Diophantine equations are positive existential first order sentences) and so is the problem of checking semigroup identities (since these correspond to positive universal first order sentences). Our proof will work by induction, with our base case being the plactic monoid on two letters P_2.

5.1 Interpreting P_2 in Presburger Arithmetic

First, we will explicitly treat the case $n = 2$ of tableaux on two letters. As before, we will consider the tableaux to be generated by columns $\mathcal{C} = \{t, 1, 2\}$, and our rewriting system becomes:

$$R = \{21 \to t \ , \ 2t \to t2 \ , \ 1t \to t1\}.$$

By the two commutativity rules, and the fact that any factor 21 would not appear in a reduced word, each reduced word $w \in (\mathcal{C}, R)$ is in the form $t^{w_1}1^{w_2}2^{w_3}$. Thus, by completeness of the rewriting system, each element of P_2 corresponds to a triple $(w_1, w_2, w_3) \in \mathbb{N}^3$, associated to a normal form $t^{w_1}1^{w_2}2^{w_3}$. Likewise, each such triple corresponds to a tableau, hence an element of P_2.

We will take the $\mathbb{Z}$ version of Presburger arithmetic, to make use of subtraction. Consider the map $\phi : S \to P_2$, where $S = \mathbb{N}^3 \subset \mathbb{Z}^3$ is definable by the formula

$$(0 \leq x_1) \wedge (0 \leq x_2) \wedge (0 \leq x_3)$$

and $\phi(x_1, x_2, x_3) = t^{x_1} 1^{x_2} 2^{x_3}$. This is a bijection from a definable set in $(\mathbb{Z}, 0, 1, +, -, \leq)$, and the inverse graph of equality will be

$$\begin{aligned}\phi^{-1}(=) &= \left\{(a_1, a_2, a_3, b_1, b_2, b_3) \in \mathbb{N}^6 \mid t^{a_1} 1^{a_2} 2^{a_3} = t^{b_1} 1^{b_2} 2^{b_3}\right\} \\ &= \left\{(a_1, a_2, a_3, b_1, b_2, b_3) \in \mathbb{N}^6 \mid a_1 = b_1,\ a_2 = b_2,\ a_3 = b_3\right\} \subset \mathbb{Z}^6\end{aligned}$$

which is definable by the formula $(\underline{a} \in S) \wedge (\underline{b} \in S) \wedge \bigwedge_{i \in \{1,2,3\}} (a_i = b_i)$.

next we check the preimage of the graph of multiplication

$$\phi^{-1}(\circ) = \left\{(\underline{a}, \underline{b}, \underline{c}) \in S^3 \mid t^{a_1} 1^{a_2} 2^{a_3} t^{b_1} 1^{b_2} 2^{b_3} = t^{c_1} 1^{c_2} 2^{c_3}\right\}.$$

Using the multiplication formula from the previous chapter, we get that

$$\begin{aligned} t^{a_1} 1^{a_2} 2^{a_3} t^{b_1} 1^{b_2} 2^{b_3} &= t^{a_1+b_1} 1^{a_2} 2^{a_3} 1^{b_2} 2^{b_3} \\ &= \begin{cases} t^{a_1+b_1+a_3} 1^{a_2+b_2-a_3} 2^{b_3}, & a_3 \leq b_2 \\ t^{a_1+b_1+b_2} 1^{a_2} 2^{b_3+a_3-b_2}, & b_2 \leq a_3 \end{cases}\end{aligned}$$

thus obtaining the following formula for $\phi^{-1}(\circ)$

$$\begin{aligned}(\underline{a} \in S) \wedge (\underline{b} \in S) \wedge (\underline{c} \in S) \wedge [&(a_3 \leq b_2 \wedge c_1 = a_1 + b_1 + a_3 \wedge c_2 = a_2 + b_2 - a_3 \wedge c_3 = b_3) \\ &\vee (b_2 \leq a_3 \wedge c_1 = a_1 + b_1 + b_2 \wedge c_2 = a_2 \wedge c_3 = b_3 + a_3 - b_2)]\end{aligned}$$

where $\underline{a} \in S$ is a shorthand for$(a \leq x_1) \wedge (0 \leq a_2) \wedge (0 \leq a_3)$. It follows then that ϕ is an interpretation of P_2 in Presburger arithmetic. This yields the following result.

Theorem 2. *P_2 has decidable first order theory.*

Proof. Since ϕ above is an interpretation of P_2 in $(\mathbb{Z}, 0, 1, +, -, \leq)$, every first order formula of P_2 is interpreted as a first order formula of Presburger arithmetic, which is decidable by 2.3.1. □

Note that this argument is closely related to the proof that the bicyclic monoid $B = \langle a, b \mid ba = \varepsilon \rangle$ has decidable first order theory (see section 2.4 of [12]). Indeed, the map $\psi : P_2 \to B$ sending 1 to a, 2 to b, and t to ε is a monoid homomorphism, and $\psi \circ \phi : S \to B$ is an interpretation of the bicyclic monoid in Presburger arithmetic, in the sense of surjections.

5.2 Interpreting P_n in Presburger Arithmetic

Throughout this section, let $k = |\mathcal{C}| = 2^n - 1$. Index $\mathcal{C}$ by $i \in \{1, \ldots, k\}$ with $i < j \iff c_i \sqsubset c_j$.

Let $S \subseteq \mathbb{N}^k$ be the set of all $(v_1, \ldots, v_k)$ such that $c_1^{v_1} \ldots c_k^{v_k}$ is the normal form of a tableau, and let $\phi : S \to P_n$ be the natural bijection. The normal form of any tableau will obey compatibility conditions: for each pair

$$(a, b) \in \{1, \ldots, k\} \times \{1, \ldots, k\}$$

such that $a < b$ and $c_a \not\leq c_b$, we have that either $v_a = 0$ or $v_b = 0$. Let $I \subset \{1, \ldots, k\}^2$ be the set of all such pairs. Then $S \subset \mathbb{Z}^k$ is defined by the formula

$$\bigwedge_{i \in \{1, \ldots, k\}} (0 \leq x_i) \wedge \bigwedge_{(a,b) \in I} [(x_a = 0) \vee (x_b = 0)] \, .$$

We claim that ϕ is an interpreting map of P_n in Presburger arithmetic. Again, we check the diagonal:

$$\phi^{-1}(=) = \{(\underline{a}, \underline{b}) \in S^2 \mid \phi(\underline{a}) = \phi(\underline{b})\},$$

which is definable by $(\underline{a} \in S) \wedge (\underline{b} \in S) \wedge \bigwedge_{i \in \{1,\ldots,k\}} (a_i = b_i)$ as in the $n = 2$ case. It remains to check whether the preimage of the multiplication graph

$$\phi^{-1}(\circ) = \left\{(\underline{a}, \underline{b}, \underline{c}) \in S^3 \mid \phi(\underline{a})\phi(\underline{b}) = \phi(\underline{c})\right\} \subset \mathbb{Z}^{3k}$$

is definable.

5.2.1 Multiplication – the idea

Using section 5.1 as a base case, we will proceed with the induction hypothesis that, for each $2 \leq i \leq n-1$, we have a formula η_i in Presburger arithmetic defining multiplication in P_i.

We first consider the structure of multiplication in P_n. The recursive nature of Schensted's algorithm yields a characterisation of multiplication in P_n via bottom rows and top tableaux.

Definition 5.2.1. We call a tableau $t \in P_n$ a *top tableau* if its row reading is a word over $\{2, \ldots, n\}^*$. i.e. there are no 1's appearing in the tableau word representing t.

Note that each $u \in P_n$ will have an associated top tableau: if $u = r_1 \ldots r_l$, where each r_i is a row, then $r_1 \ldots r_{l-1}$ will be a top tableau.

For $u, v \in P_n$, the product uv will be computed by first running an insertion algorithm into the bottom row of u, and then inserting any bumped letters into the top tableau associated to u. We will make this idea more precise.

Definition 5.2.2. Define the following maps:

1. The top map $T : P_n \to P_n$ maps an element w with row form $r_1 \ldots r_l$ in A^*

to its corresponding top tableau $T(w) = r_1 \dots r_{l-1}$.

2. The bottom map $B : P_n \to P_n$ maps an element w as above to its bottom row $B(w) = r_l$.

Example 5.2.3. Let $t = \begin{array}{|c|c|c|c|c|}\cline{1-2} 3 & 4 & \multicolumn{3}{c}{} \\ \cline{1-3} 2 & 3 & 3 & \multicolumn{2}{c}{} \\ \hline 1 & 1 & 2 & 4 & 4 \\ \hline \end{array}$. Then $T(t) = 34\ 233$ and $B(t) = 11244$.

For $u, v \in P_n$, by the structure of Schensted's algorithm, the product uv will run an insertion algorithm first into $B(u)$, followed by any letters that are bumped being inserted into $T(u)$. This yields the following characterisation of the top and bottom of the product:

$$T(uv) = T(u)T(B(u)v),$$
$$B(uv) = B(B(u)v),$$

where equality is taken to mean equality in P_n, not equality of words. Note that the set of top tableaux, which is equivalently the image of T, is a submonoid isomorphic to P_{n-1} over the alphabet $\{2, \dots, n\}$. Thus by our induction hypothesis the product of top tableaux will be definable via η_{i-1}. Therefore, if we can define the row $B(uv)$, and a way of stitching $T(uv)$ and $B(uv)$ into one tableau uv, we will obtain η_i a formula defining multiplication in P_n.

Definition 5.2.4. The stitch map $\Sigma : P_n \times P_n \to P_n$ is defined as follows. For $u \in P_n$ a top tableau with row reading $r_1 \dots r_n \in A^*$ and v a row with row reading $r_v \in A^*$, $\Sigma(u, v) = uv$ if $r_1 \dots r_n r_v$ is the row reading of a tableau. Otherwise, $\Sigma(u, v) = \varepsilon$.

If Σ has nontrivial output, we call u and v *compatible*, and uv the "stitched" tableau.

Example 5.2.5. Suppose $u = 43322234$ and $v = 11113$. Then $\Sigma(u, v) = uv$, with corresponding tableau

$$\begin{array}{|c|c|c|c|c|}
\cline{1-1} 4 \\
\cline{1-2} 3 & 3 \\
\hline 2 & 2 & 2 & 3 & 4 \\
\hline 1 & 1 & 1 & 1 & 3 \\
\hline
\end{array}.$$

Note that $\Sigma(T(u), B(u)) = u$. We can thus characterise multiplication via the above maps as follows

$$\begin{aligned}
uv &= \Sigma(T(uv), B(uv)) \\
&= \Sigma(T(u)T(B(u)v), B(B(u)v)).
\end{aligned}$$

Let us consider the structure of $w \in P_n$ as a word in normal form in $\mathcal{C}^*$. We have that $w = c_1^{w_1} c_2^{w_2} \dots c_k^{w_k}$ for some $w_i \in \mathbb{N}$ for each i, satisfying some compatibility conditions. But consider now each block c_i^m for some $m \in \mathbb{N}$ as a tableau word in row form in the presentation $\langle A|K \rangle$. Then for $c_i = x_1 x_2 \dots x_r$ in row form in A^*, we have that $c_i^m = x_1^m x_2^m \dots x_r^m$ in row form in A^*. For each c_i, this row form is unique, since each column corresponds to a unique decreasing sequence in A^*. This will give us a useful way to write the column form of w as a word in A^*.

Define $\alpha = (\alpha_1, \dots, \alpha_\ell)$ to be the finite sequence of letters in A which first outputs in order the letters in the row form of c_1, then the letters of the row form of c_2, and so on. We also define $\beta = (\beta_1, \dots, \beta_\ell)$ to be the finite sequence, taking values in $\{1, \dots, k\}$, with $\beta_i = j$ when α_i is a letter from column c_j. Note that these sequences only depend on the rank of P_n, as it is defined using the columns generating P_n. Now, a straightforward check using Schensted's algorithm verifies that the word $\alpha_1^{w_{\beta_1}} \dots \alpha_\ell^{w_{\beta_\ell}} \in A^*$ is equal to $w = c_1^{w_1} c_2^{w_2} \dots c_k^{w_k}$ in the plactic monoid, where w_{β_i} is the coefficient of column c_{β_i} in the normal form of w.

Example 5.2.6. The seven columns of P_3:

$$\begin{array}{|c|}\hline 3\\\hline 2\\\hline 1\\\hline\end{array}, \begin{array}{|c|}\hline 2\\\hline 1\\\hline\end{array}, \begin{array}{|c|}\hline 3\\\hline 1\\\hline\end{array}, \begin{array}{|c|}\hline 3\\\hline 2\\\hline\end{array}, \begin{array}{|c|}\hline 1\\\hline\end{array}, \begin{array}{|c|}\hline 2\\\hline\end{array}, \begin{array}{|c|}\hline 3\\\hline\end{array}, \text{ yield}$$

$$\alpha = 3, 2, 1, 2, 1, 3, 1, 3, 2, 1, 2, 3$$

$$\beta = 1, 1, 1, 2, 2, 3, 3, 4, 4, 5, 6, 7.$$

For an example word $w = c_1^3 c_2 c_3 c_6$, we get the corresponding sequence

$$3^3 2^3 1^3 2^1 1^1 3^1 1^1 3^0 2^0 1^0 2^1 3^0 = 33322211121312,$$

which after running Schensted's algorithm becomes the tableau

$$\begin{array}{|c|c|c|ccc}\cline{1-3} 3 & 3 & 3 & \multicolumn{3}{c}{} \\ \cline{1-5} 2 & 2 & 2 & \multicolumn{1}{c|}{2} & \multicolumn{1}{c|}{3} & \\ \hline 1 & 1 & 1 & \multicolumn{1}{c|}{1} & \multicolumn{1}{c|}{1} & \multicolumn{1}{c|}{2} \\ \hline\end{array}.$$

Lemma 5.2.7. *Consider $u, v, w \in P_n$. Suppose v has normal form $c_1^{v_1} \dots c_k^{v_k}$. Then $w = uv$ is equivalent to the following:*

There exist $u_0, u_1, \dots, u_\ell \in P_n$ such that $u_0 = u$, $u_\ell = w$, and we have a recursive formula for u_i

$$u_i = u_{i-1} \alpha_i^{v_{\beta_i}}.$$

This result is immediate from the structure of the insertion algorithm and the fact $v = \alpha_1^{v_{\beta_1}} \dots \alpha_\ell^{v_{\beta_\ell}}$.

Definition 5.2.8. For each $x \in A$ the map $\mu_x : \mathbb{N} \times S \to S$ is such that $\phi(\mu_x(m, \underline{a})) = \phi(\underline{a}) x^m$.

Corollary 5.2.9. *$\phi^{-1}(\circ)$ is definable if the maps μ_x are definable for each $x \in A$.*

Proof. Restating lemma 5.2.7 in terms of elements of S, given $\underline{u}, \underline{v}, \underline{w} \in S$, we have that $\phi(\underline{w}) = \phi(\underline{u})\phi(\underline{v})$ if and only if there are some $\underline{u}^0, \dots, \underline{u}^\ell$ such that

$\underline{u}^0 = \underline{u}$, $\underline{u}^\ell = \underline{w}$, and

$$\phi(\underline{u}^i) = \phi(\underline{u}^{i-1})\alpha_i^{v_{\beta_i}}.$$

By the definition of μ_x, we can rephrase the above condition as

$$\underline{u}^i = \mu_{\alpha_i}(v_{\beta_i}, \underline{u}^{i-1}),$$

so the preimage of the graph of multiplication becomes a composition of finitely many applications of μ_x, which will be definable if each μ_x is definable. $\square$

5.2.2 The formula defining μ_x

Henceforth, x is a fixed letter in A.

Recall that if $\underline{b} = \mu_x(m, \underline{a})$, then

$$\begin{aligned}\phi(\underline{b}) &= \phi(\underline{a})x^m \\ &= \Sigma(T(\phi(\underline{a}))T(B(\phi(\underline{a}))x^m), B(B(\phi(\underline{a}))x^m)).\end{aligned}$$

So we wish to obtain a formula of Presburger arithmetic describing

$$\underline{b} = \phi^{-1}\Sigma(T(\phi(\underline{a}))T(B(\phi(\underline{a}))x^m), B(B(\phi(\underline{a}))x^m)).$$

We can break this down into a composition of several maps. First, define $\underline{a}^1$ and $\underline{a}^2$ such that

$$\begin{aligned}\underline{a}^1 &= \phi^{-1}T\phi(\underline{a}), \\ \underline{a}^2 &= \phi^{-1}B\phi(\underline{a}).\end{aligned}$$

Next, considering $R \subset P_n$ the set of row words, we define two maps

$\rho_1, \rho_2 : \mathbb{N} \times \ R \ \rightarrow \ S$ such that, for $r \in R$ we have

$$\phi(\rho_1(m, r)) = T(rx^m) \text{ and } \phi(\rho_2(m, r)) = B(rx^m).$$

Then since $\phi(\underline{a}^2)$ is a row, we can define $\underline{a}^3$ and $\underline{a}^4$ to be such that

$$\underline{a}^3 = \rho_1(m, \phi(\underline{a}^2)),$$
$$\underline{a}^4 = \rho_2(m, \phi(\underline{a}^2)).$$

That is, $\phi(\underline{a}^3) = T(B(\phi(\underline{a}))x^m)$ and $\phi(\underline{a}^4) = B(B(\phi(\underline{a}))x^m)$.

Next, define $\underline{a}^5$ to be such that

$$\phi(\underline{a}^5) = T(\phi(\underline{a}))T(B(\phi(\underline{a}))x^m) = \phi(\underline{a}^1)\phi(\underline{a}^3).$$

By our induction hypothesis, this will be definable in Presburger arithmetic, as the coefficients in $\underline{a}^5$ will either be calculated by the formula η_{n-1}, or will equal zero.

Finally, we have that

$$\underline{b} = \phi^{-1}\Sigma(\phi(\underline{a}^5), \phi(\underline{a}^4)).$$

Since the composition of definable maps is definable, we have that μ_x is definable precisely when $\phi^{-1}T\phi(\underline{a}), \phi^{-1}B\phi(\underline{a}), \rho_1, \rho_2$, and $\phi^{-1}\Sigma(\phi(\ ), \phi(\ ))$ are definable. This will be the subject of the following three lemmas.

Lemma 5.2.10. *The following maps are definable:*

(i) $\phi^{-1}B\phi : S \rightarrow S$.

(ii) $\phi^{-1}T\phi : S \rightarrow S$.

Proof. (i) Define the finite sets B_m for each $m \in A$ by

$$B_m = \{j \in \{1, \ldots, k\} \mid c_j = x_m \ldots x_1 \wedge x_1 = m\}$$

which are nonempty for each m. Then we get that $\underline{b} = \phi^{-1}(B(\phi(\underline{a}))$ if and only if the following formula holds:

$$\bigwedge_{i\in\{1,\ldots,k-n\}} (b_i = 0) \wedge \bigwedge_{i\in\{1,\ldots,n\}} \left(b_{k-n+i} = \sum_{j\in B_i} a_j \right).$$

The first part of the formula denoting the coefficient of each column of size ≥ 2 being zero, and the second part denoting the fact that each column $x_m \ldots x_1$ in $\phi(\underline{a})$ contributes to the coefficient of the x_1 letter in the bottom row.

(ii) Define the similar sets T_i for each $i \in \{1, \ldots, k\}$ by

$$T_i = \{j \in \{1, \ldots, k\} \mid c_j = x_m \ldots x_1 \wedge x_m \ldots x_2 = c_i\}.$$

Note that if $i \in B_1$, then $T_i = \varnothing$. Now, we have that $\underline{b} = \phi^{-1}(T(\underline{a}))$ if and only if the following formula holds:

$$\bigwedge_{i\in\{1,\ldots,k\}} \left(b_i = \sum_{j\in T_i} a_j \right)$$

where we take the sum over an empty indexing set to be 0. □

Note that the sets T_i and B_m can be constructed algorithmically for any given n. Given the set of columns as decreasing sequences, we can check membership in each B_m by considering the minimal element of a column, and we can check membership in each T_i by considering the column without its minimal element. Note also that $\{B_m : m \in A\}$ and $\{T_j : j \in \{1, \ldots, k\},\ T_j \neq \varnothing\}$ are partitions of $\{1, \ldots, k\}$.

Next, we move on to defining the maps $\phi^{-1}T(rx^m)$ and $\phi^{-1}B(rx^m)$. Here, we consider $S_R \subset S$ to be the subset of normal forms corresponding to rows (i.e. S_R is the preimage of $R \subset P_n$).

Lemma 5.2.11. *The following maps are definable:*

1. $\rho_1\phi : \mathbb{N} \times S_R \to S$ *taking* $\phi^{-1}(r)$ *with parameter* $m \in \mathbb{N}$ *to* $\phi^{-1}T(rx^m)$.

2. $\rho_2\phi : \mathbb{N} \times S_R \to S$ *taking* $\phi^{-1}(r)$ *with parameter* $m \in \mathbb{N}$ *to* $\phi^{-1}B(rx^m)$.

We will abuse notation and write $\rho_1(r)$ for $\rho_1\phi(m, \phi^{-1}(r))$, which is equivalently $\rho_1(m, r)$ (and analogously for $\rho_2(r)$).

Proof. First note that S_R is a subset definable by

$$\bigwedge_{i\in\{1,\ldots,k-n\}} x_i = 0$$

and $\rho_1\phi$, $\rho_2\phi$ will be maps from S_R to S_R. Indeed, for $\rho_2\phi$ this is immediate, but for $\rho_1\phi$ note that by [42] the number of rows after running Schensted's algorithm on any $w \in A^*$ is equal to the length of the longest strictly decreasing subsequence of w. Now, since r is non-decreasing as a sequence in A^*, the longest strictly decreasing subsequence of rx^m viewed as a word in A^* can have length at most 2. Thus the top $T(rx^m)$ can have at most one row, meaning the image of $\rho_1\phi$ must be in S_R.

Now, write $\underline{r} = \phi^{-1}(r) = (0, \ldots, 0, r_1, r_2, \ldots, r_n)$. We will describe explicitly $\underline{c} = (0, \ldots, 0, c_1, \ldots, c_n)$ and $\underline{d} = (0, \ldots, d_1, \ldots, d_n)$ such that $\underline{c} = \rho_1(r)$ and $\underline{d} = \rho_2(r)$.

2. We will first consider the $\rho_2\phi$ case, which corresponds to $B(rx^m)$. In the setting of the presentation $\langle A|K\rangle$, we will have x^m inserted into

$$r = 1^{r_1}2^{r_2}\ldots(x+1)^{r_{x+1}}(x+2)^{r_{x+2}}\ldots n^{r_n}.$$

   It will bump m letters from this row, starting at $x + 1$. This means that $d_i = r_i$ for $i < x$ and $d_x = r_x + m$. We will now consider the later entries of $\underline{d}$, which will split into several cases depending on the size of m.

   In the first case, suppose $m \leq r_{x+1}$. Then we will bump m letters $x + 1$ and replace them with letters x. This yields the effect that $d_{x+1} = r_{x+1} - m$ and $d_i = r_i$ for all $i > x + 1$.

   In the next case, suppose $r_{x+1} \leq m \leq r_{x+1} + r_{x+2}$. Then all letters $x + 1$ are bumped, as are $m - r_{x+1}$ letters $x + 2$. Thus we have that $d_{x+1} = 0$, $d_{x+2} =$

$r_{x+2} + r_{x+1} - m$, and $d_i = r_i$ for all $i > x + 2$.

Generalising the above, suppose, for some $i \leq n - x$, we have

$$\sum_{j=1}^{i-1} r_{x+j} \leq m \leq \sum_{j=1}^{i} r_{x+j}.$$

Then in this case, $d_{x+j} = 0$ for each $0 < j < i$, and $d_{x+i} = \sum_{j=1}^{i} r_{x+j} - m$, and all later entries remain unchanged.

The last case to consider is when

$$\sum_{j=1}^{n-x} r_{x+j} \leq m,$$

in which case all letters bigger than x will be bumped and we have $d_{x+j} = 0$ for all j.

Each case yields a formula in terms of $\leq$, addition, and subtraction. Then the disjunction of the above cases, which will be a finite formula, will define $\underline{d}$ such that $\phi(\underline{d}) = B(rx^m)$, hence $\underline{d} = \rho_2(r)$.

1. Let us now consider $\rho_1\phi$, which corresponds to $T(rx^m)$. This will be the row of bumped letters, which will mean that $c_i = 0$ for any $i \leq x$. For the later entries of $\underline{c}$, we will again have cases corresponding to the size of m.

   Suppose that as above, we have some $1 \leq i \leq n - x$ such that

$$\sum_{j=1}^{i-1} r_{x+j} \leq m \leq \sum_{j=1}^{i} r_{x+j}.$$

   Then we will bump all letters $x+1, \ldots, x+i-1$, as well as some letters $x+i$. Therefore $c_{x+j} = r_{x+j}$ for $0 < j < i$, and $c_{x+i} = m - \sum_{j=1}^{i-1} r_{x+j}$.

   Now suppose we are in the case

$$\sum_{j=1}^{n-x} r_{x+j} \leq m.$$

   Then we will have that $c_{x+j} = r_{x+j}$ for each $0 < j < n - x$.

As above, the disjunction of these cases yields a formula defining $\underline{c} = \rho_1(r)$.

$\square$

We will now show the definability of the stitch map.

Lemma 5.2.12. *The map $\phi^{-1}\Sigma(\phi(\ ), \phi(\ )) : S^2 \to S$ is definable.*

Proof. The condition for Σ to have nontrivial action is definable via the following formula:

Suppose $\underline{a}$, $\underline{b} \in S$. Consider the set $B_1 = \{i \in \{1, \dots, k\} \mid c_i = x_m \dots x_1 \wedge x_1 = 1\}$ as in Lemma 5.2.10. Then $\phi(\underline{a})$ being a top tableau is definable by $\left(\bigwedge_{i \in B_1} a_i = 0 \right)$. Also, $\phi(\underline{b})$ being a row is definable by the formula $\left(\bigwedge_{i \in \{1,\dots,k-n\}} b_i = 0 \right)$.

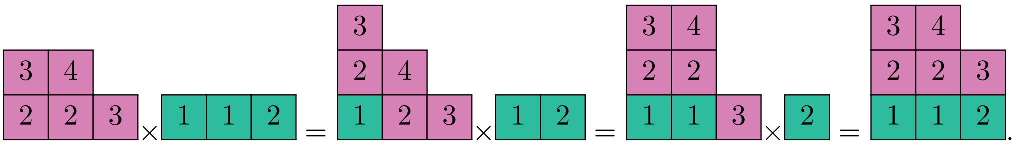
Now, let $e_m = \sum_{i \in B_m} a_i$. In order for it to be possible to stitch two inputs, we need $e_2 \leq b_{k-n+1}$, $e_3 \leq b_{k-n+2} + b_{k-n+1} - e_2$, and so on. We can rearrange this to get the following compatibility condition:

$$\underline{a} \in S \wedge \underline{b} \in S \wedge \left(\bigwedge_{i \in B_1} a_i = 0 \right) \wedge \bigwedge_{i \in \{1,\dots,k-n\}} (b_i = 0) \wedge \bigwedge_{i \in \{2,\dots,n\}} \left(\sum_{j=2}^{i} e_i \leq \sum_{j=1}^{i-1} b_{k-n+j} \right)$$

Where we take empty sums to be 0. Note that all sums used are finite, so we obtain a valid formula in Presburger arithmetic. Denote this compatibility formula $\gamma(\underline{a}, \underline{b})$.

When γ is satisfied, we wish to construct $\underline{d} = \phi^{-1}\Sigma(\phi(\underline{a}), \phi(\underline{b}))$. In order to do this, we first briefly discuss what happens at each step during the multiplication algorithm in this case.

When a top tableau t is multiplied by a compatible bottom row r, by the bumping property of Schensted's algorithm and the compatibility condition, each letter bumped by a letter of r will bump the letter directly above it, which in turn bumps the letter directly above it, and so on until an entire column of t has been bumped up by one space. As an example, consider $t = 34223$ and $r = 112$. The multiplication algorithm will bump columns as follows:



In this way, the columns of t are always bumped up in turn from left to right. Due to this left-to-right bumping process, and the ordering of the coefficients $d_1, \ldots, d_k$, running Schensted's algorithm will first calculate d_1, then d_2 and so on. Furthermore, as the algorithm runs, it will insert letters (which are themselves columns) of r into columns of t. We will call this insertion "using up" columns of r and t. Suppose we use up k columns c_i^k of t and k columns c_j^k of r. Then the corresponding coefficients a_i and b_j will need to be changed to $a_i - k$ and $b_j - k$ respectively. We can formalise this as a recursive process to compute $\underline{d}$:

Suppose we have calculated the coefficients $d_1, \ldots, d_{i-1}$, and have obtained modified elements $\underline{a}^{i-1}$ and $\underline{b}^{i-1}$ in S representing all columns that have not yet been used up in the stitch. We calculate the coefficient d_i as follows:

d_i is the coefficient of $c_i \in \mathcal{C}$, which we can write as $c_i = x_m \ldots x_1 \in A^*$. Then $x_m \ldots x_2$ and x_1 are two columns, which we denote respectively by c_{i_T} and c_{i_B} in $\mathcal{C}$. Denote the coefficients corresponding to c_{i_T} in $\underline{a}^{i-1}$ and c_{i_B} in $\underline{b}^{i-1}$ by $a_{i_T}^{i-1}$ and $b_{i_B}^{i-1}$ respectively. By the structure of Schensted's algorithm it is straightforward to see that $d_i = \min(a_{i_T}^{i-1}, b_{i_B}^{i-1})$, which is definable in Presburger arithmetic by

$$(a_{i_T}^{i-1} \leq b_{i_B}^{i-1} \wedge d_i = a_{i_T}^{i-1}) \vee (b_{i_B}^{i-1} \leq a_{i_T}^{i-1} \wedge d_i = b_{i_B}^{i-1}).$$

Now define $a_j^i = a_j^{i-1}$ for $j \neq i_T$, and $a_{i_T}^i = a_{i_T}^{i-1} - d_i$. Likewise, define $b_j^i = b_j^{i-1}$ for $j \neq i_B$ and $b_{i_B}^i = b_{i_B}^{i-1} - d_i$. This corresponds to the fact that these columns have now been used up in a stitch. Note that we will always get one of these coefficients being set to zero. This is clearly definable in Presburger arithmetic, and we will denote the formula for obtaining $\underline{a}^i$ and $\underline{b}^i$ from $\underline{a}^{i-1}$ and $\underline{b}^{i-1}$ by δ_i. Note that when $i = 1$, we take $\underline{a}^0 = \underline{a}$ and $\underline{b}^0 = \underline{b}$, which allows us to calculate d_1 in terms of $\underline{a}^0$ and $\underline{b}^0$.

Now we get that $\phi^{-1}\Sigma(\phi(\ ), \phi(\ ))$ has graph consisting of all $(\underline{a}, \underline{b}, \underline{d})$ satisfying:

$$\gamma(\underline{a}, \underline{b}) \wedge \exists \underline{a}^0 \dots \exists \underline{a}^k \exists \underline{b}^0 \dots \exists \underline{b}^k : (\underline{a}^0 = \underline{a}) \wedge (\underline{b}^0 = \underline{b}) \wedge \left(\bigwedge_{i \in \{1,\dots,k\}} d_i = \min(a_{i_T}^{i-1}, b_{i_B}^{i-1}) \wedge \delta_i \right).$$

□

With the above lemmas in hand, we can now prove the following result.

Proposition 5.2.13. *For any $x \in A$, the map μ_x is definable.*

Proof. By the discussion before Lemma 5.2.10, μ_x is a composition of the maps $\phi^{-1}B\phi$, $\phi^{-1}T\phi$, $\rho_1\phi$, $\rho_2\phi$, $\phi^{-1}\Sigma(\phi(\ ), \phi(\ ))$, and multiplication of top tableaux. By Lemmas 5.2.10, 5.2.11, and 5.2.12, all five required maps are definable.

To define $\underline{a}^5 = \phi^{-1}(T(\phi(\underline{a}))T(B(\phi(\underline{a}))x^m))$, first note that since $\underline{a}^5$ denotes a top tableau, we have that $a_i^5 = 0$ for each $i \in B_1$ as defined in lemma 5.2.10. Furthermore, for each $i \notin B_1$, we have that a_i^5 is determined by the formula η_{n-1} applied to $\phi^{-1}(T(\phi(\underline{a})))$ and $\phi^{-1}(T(B(\phi(\underline{a}))x^m))$. This determines η_n by induction, with base case η_2 as detailed in section 5.1. This completes the proof. □

Combining Proposition 5.2.13 and Corollary 5.2.9, we obtain that $\phi^{-1}(\circ)$ is definable. Thus proving the following theorem:

Theorem 3. *The map $\phi : S \to P_n$ as defined above is an interpretation of P_n in Presburger arithmetic.*

This reduces $FOTh(P_n)$ to the first order theory of Presburger arithmetic, which is decidable by lemma 2.3.1, hence yielding the following result as a corollary.

Theorem 4. *For any $n \in \mathbb{N}$, the first order theory of P_n decidable.*

6

Definable submonoids and bi-interpretability

In a plactic monoid of any rank, the centre of P_n will be generated by the column $c_1 \in \mathcal{C}$ corresponding to the decreasing sequence $n(n-1)\dots 21 \in A^*$. We have seen that the centre of any monoid is a definable subset, so we have $Z(P_n) = \{c_1^n \mid n \in \mathbb{N}\}$ a definable subset of P_n isomorphic to $(\mathbb{N}, 0, 1, +, \leq)$, with $a \leq b$ in $\mathbb{N}$ corresponding to the formula $\exists y : c_1^a y = c_1^b$, and addition corresponding to monoid multiplication.

We can therefore take for any n, the map $\psi : Z(P_n) \to \mathbb{N}$ to be an interpreting map of Presburger arithmetic in P_n. In this chapter, we will show that these mutually interpretable structures are, in fact, bi-interpretable.

6.1 The case for P_2

In the style of section 5.1, take $\mathcal{C} = (t, 1, 2)$ with $Z(P_2) = \{t^n \mid n \in \mathbb{N}\}$. Firstly, note that $\phi : \mathbb{N}^3 \to P_2$ as defined in that section is also an interpreting map of P_2 into the $\mathbb{N}$ version of Presburger arithmetic, by rearranging any subtraction formulas $a = b - c$ to $a + c = b$.

Let $\psi : Z(P_2) \to \mathbb{N}$ be the interpretation of Presburger arithmetic in P_2 described above. Then taking S as the definable subset $\{(n, 0, 0) \mid n \in \mathbb{N}\} \subset \mathbb{N}^3$, the map $\psi\phi : S \to \mathbb{N}$ is the isomorphism sending $(n, 0, 0)$ to n, which is clearly definable.

Now, consider $\phi\psi : Z(P_2)^3 \to P_2$, sending (t^a, t^b, t^c) to $w = t^a 1^b 2^c$. To show that this is definable, we will first show that the sets $N_1 = \{1^n | \; n \in \mathbb{N}\}$ and $N_2 = \{2^n | \; n \in \mathbb{N}\}$ are definable in P_2.

First, consider the set S_ℓ of elements that can be multiplied on the left to yield a central element

$$S_\ell = \{x \in P_2 \mid \exists y : yx \in Z(P_2)\}$$

and analogously, the set S_r of elements that can be multiplied on the right to yield a central element

$$S_r = \{x \in P_2 \mid \exists y : xy \in Z(P_2)\}.$$

Since we know that 1 can be multiplied on the left to become central, and 2 can be multiplied on the right to become central, it is straightforward to see that $S_\ell = \{t^a 1^b | \; a, b \in \mathbb{N}\}$ and $S_r = \{t^a 2^b | \; a, b \in \mathbb{N}\}$.

Notice that in S_ℓ (respectively S_r), each element is written as a product of a central element with an element of N_1 (respectively N_2). So if we insist that the central element in this product is always the identity, we will obtain the elements of N_1 (respectively N_2). In symbols, we can formalise this as the following conditions

$$x \in N_1 \iff [x \in S_\ell \wedge \forall y \forall z : z \in Z(P_2) \wedge x = zy \implies z = \varepsilon]$$
$$x \in N_2 \iff [x \in S_r \wedge \forall y \forall z : z \in Z(P_2) \wedge x = zy \implies z = \varepsilon]$$

so both sets N_1 and N_2 are definable.

Now, given t^b we can define $x = 1^b$ as the element of N_1 such that there is some $z \in N_2$ such that $zx = t^b$. Likewise, given t^c we can define $y = 2^c$ as the element of N_2 such that there is some $z \in N_1$ such that $yz = t^c$.

Then we take the image of $(t^a, t^b, t^c) \in Z(P_2)^3$ to be $\phi\psi(t^a, t^b, t^c) = t^a xy$, with $x, \; y$ calculated as above. This is clearly definable, which completes the proof that this is in fact a bi-interpretation.

6.2 Submonoids generated by columns

Notice that in the above section we showed that the submonoids $t^*, 1^*$, and 2^* generated by each of the columns are definable in P_2. We will now show that this is a general fact in any plactic monoid, which will be useful for constructing a bi-interpretation.

Theorem 5. *For any plactic monoid P_n with column generating set $\mathcal{C}$, for each $c_i \in \mathcal{C}$, the submonoid $c_i^* = \{c_i^n \mid n \in \mathbb{N}\}$ is definable in P_n.*

Proof. We will proceed by induction, with base case P_2 from the previous section.

As before, consider the set S_ℓ of all elements that can be multiplied on the left to yield a central element

$$S_\ell = \{x \in P_n \mid \exists y : yx \in Z(P_n)\}.$$

Note that the centre of any monoid is definable, so S_ℓ is a definable set. We claim that any element of S_ℓ will have all its columns in the form

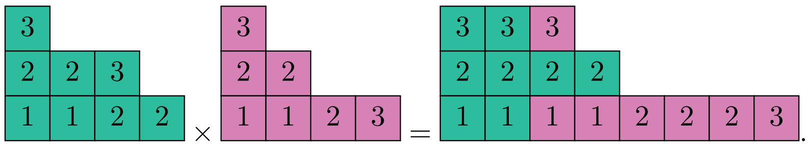
$$u_i = \begin{array}{|c|}\hline i \\ \hline i-1 \\ \hline \vdots \\ \hline 1 \\ \hline \end{array}$$

i.e. a general $X \in S_\ell$ will be of the form $u_n^{x_n} \dots u_1^{x_1}$. Indeed, for each such X we have a $Y = f_n^{x_{n-1}} f_{n-1}^{x_{n-2}} \dots f_2^{x_1}$, where

$$f_i = \begin{array}{|c|}\hline n \\ \hline n-1 \\ \hline \vdots \\ \hline i \\ \hline \end{array}$$

and YX is central, so X is a member of S_ℓ.

To show that there are no other elements in S_ℓ, consider the structure of Schensted's algorithm. Given two elements $u, v \in P_n$, for each $x \in A$ that appears in the row reading of v, the corresponding x in the row reading of uv will either be on the same row as it started in v, or on a lower row. As an example, in P_3, consider the product of $u = 3\ 223\ 1122$ and $v = 3\ 22\ 1123$, here written in row reading. Then after running Schensted's algorithm with colour coding, we can see that



This will be true in general because when you run Schensted's algorithm on a string in A^*, a letter may only be bumped by other letters further to the right in the string. So any x that started in v will only be moved by other letters of v, even in the product uv. But since each letter must bump the leftmost letter in the row, it might happen that x will not be bumped as many times in the product as it was in v, in which case it might end up on a lower row. Most importantly, any x that started on a given row of v cannot be in a higher row of uv than the row it started in.

Note that in a central element (a power of c_1), any $x \in A$ must appear in the row that is x-th from the bottom[1]. The columns of the form u_i are all the columns in $\mathcal{C}$ where each x appears only on the x-th row from the bottom.

Now, suppose $w \in P_n$ is a tableau with at least one of its columns not in the form of some u_i. Then there will be some letter x in the tableau of w which is lower than the x-th row from the bottom. But because multiplication on the left cannot move letters of w to a higher row, for any Y we must have an x in Yw in a row lower than x-th from the bottom. Hence Yw is never central, so w is not a member of S_ℓ.

Next, notice that any $X \in S_\ell$ can be written as the product of $\tilde{X} = u_n^{x_n} \dots u_2^{x_2}$ and

[1] i.e. all 1's appear on the bottom row, all 2's on the second from bottom row, and so on.

$u_1^{x_1}$. This is useful, because $\tilde{X}$ commutes with the generator 2, while $u_1^{x_1}$ does not. Furthermore, the column u_1 corresponds to the generator 1. So, similar to the case of P_2, we may define the submonoid 1^* as the set satisfying the formula

$$x \in S_\ell \wedge \forall y \forall z : z2 = 2z \wedge x = zy \implies z = \varepsilon.$$

Since $\tilde{X}$ commutes with 2, the formula above will insist that $\tilde{X} = \varepsilon$, leaving only the elements of S_ℓ of the form u_1^x. Therefore, this is precisely the set $1^* = \{1^m \mid m \in \mathbb{N}\}$, as in the P_2 case.

Using this, we can define the set satisfying the formula

$$\forall x \forall y \forall z : w = xyz \wedge (y \in 1^*) \implies y = \varepsilon.$$

This formula disallows any instance of the generator 1, so defines the subset of P_n generated by $\{2, \ldots, n\}$. This is a submonoid isomorphic to P_{n-1}.

Since it is definable in P_n, any set definable in this submonoid is also definable in P_n. By our induction hypothesis, any column generated submonoid of P_{n-1} is definable in P_{n-1}. Therefore, by this hypothesis we get that x^* is definable in P_n for any $x \in A = \{1, \ldots, n\}$.

Now, we know that each column $c_i \in \mathcal{C}$ will correspond to a nonempty subset of A. Of these, every column except c_1 will have at least one letter $x \in A$ omitted. But since x^* is definable in P_n for each x, we can define a submonoid isomorphic to P_{n-1} generated by $A \setminus \{x\}$, using a similar formula to the one above:

$$\forall x \forall y \forall z : w = xyz \wedge y \in x^* \implies y = \varepsilon.$$

Each $c_i \in \mathcal{C}$ except c_1 will be an element of at least one of these definable submonoids. Then, using our induction hypothesis, it follows that c_i^* is definable in P_n for each $c_i \in \mathcal{C}$ except c_1. But c_1^* is the centre of P_n, which is also definable, thus completing the proof. $\square$

6.3 A bi-interpretation for plactic monoids

Theorem 6. *P_n and Presburger Arithmetic are bi-interpretable for each $n \in \mathbb{N}$.*

Proof. We start with the map $\phi : S \to P_n$ from section 5.2, which by Theorem 3 is an interpretation, and the interpretation $\psi : Z(P_n) \to \mathbb{N}$.

Taking $T \subset S$ corresponding to the preimage of $Z(P_n)$, we have that

$$T = \{(x, 0, \dots, 0) \mid x \in \mathbb{N}\}.$$

Thus $\psi\phi : T \to \mathbb{N}$ is the obvious bijection sending $(n, \dots, 0)$ to n, and clearly an isomorphism in the language of Presburger arithmetic.

On the other hand, considering the reverse composition we have $\phi\psi : V \to P_n$, where $V \subset Z(P_n)^k$ is the subset defined through the incompatibility conditions on columns, which simply insist that certain entries be identity. This map $\phi\psi$ will identify a tuple $\underline{a} = (c_1^{a_1}, c_1^{a_2}, \dots, c_1^{a_k})$ with an element $c_1^{a_1} c_2^{a_2} \dots c_k^{a_k} \in P_n$.

By the argument in lemma 5.2.7, this is equivalent to identifying $\underline{a}$ with an element $\alpha_1^{a_{\beta_1}} \alpha_2^{a_{\beta_2}} \dots \alpha_t^{a_{\beta_t}}$. Since the sequences α and β are fixed, this means that as long as we can identify c_1^a with x^a for each $x \in A$, we can define the element $\alpha_1^{a_{\beta_1}} \alpha_2^{a_{\beta_2}} \dots \alpha_t^{a_{\beta_t}}$ in terms of $\underline{a}$. Namely, this will show that the map $\phi\psi$ is definable in the language of P_n, which will complete the proof that we have built a bi-interpretation.

Recall the columns of the form u_i and f_i from the proof of theorem 5. Note that for each $x \in A$ we have that

$$f_{x+1} x u_{x-1} = c_1.$$

Furthermore, by theorem 5, we know that x^*, u_{x-1}^*, and f_{x+1}^* are definable subsets of P_n. So, if we consider $w \in x^*$, $y \in f_{x+1}^*$, and $z \in u_{x-1}^*$, we will have that

$ywz = c_1^a$ precisely when $w = x^a$. So, the formula

$$w \in x^* \wedge \exists y \exists z : y \in f_{x+1}^* \wedge z \in u_{x-1}^* \wedge ywz = c_1^a$$

defines x^a in terms of c_1^a. Hence the image $\alpha_1^{a_{\beta_1}} \alpha_2^{a_{\beta_2}} \ldots \alpha_t^{a_{\beta_t}}$ of $\underline{a}$ under $\phi\psi$ is definable in the language of P_n. $\square$

Due to the transitivity of interpretations, we also have the following nice corollary.

Corollary 6.3.1. *For any $m, n \in \mathbb{N}$, P_n and P_m are bi-interpretable.*

7

Infinitely generated plactic monoids

We note that the above interpretations were constructed algorithmically in a uniform way. That is to say, there will exist an effective procedure which, given n, will construct the interpreting map for P_n. The procedure runs as follows:

1. Generate the interpretation for P_{n-1}.
2. Given n, generate the power set of $\{1, \ldots, n\}$ except the empty set.
3. Enumerate the set $\mathcal{P}(\{1, \ldots, n\}) \setminus \varnothing$ by the order $\sqsubseteq$ on columns. Since each column is a decreasing sequence of elements in $\{1, \ldots, n\}$, each column corresponds to a unique element of the power set.
4. Run Schensted's algorithm on each pair of columns. If the output of running Schensted's algorithm on $c_i c_j$ is not $c_i c_j$, then (i, j) is an incompatible pair.
5. Generate the formula defining S by conjuncting with $x_i = 0 \vee x_j = 0$ for each incompatible pair discovered in step 3.
6. Generate the formula defining equality in terms of the formula defining S.
7. Generate the formula for μ_x in terms of the interpretation for P_{n-1}.
8. Generate the sequences α and β from lemma 5.2.7. Steps 7 and 8 yield a formula defining multiplication.

Step 1 will repeat recursively until we reach P_2, which can be written explicitly as in section 5.1.

7.1 The plactic monoid of all tableaux

We consider $A = \mathbb{N} \setminus \{0\}$ with $K_{\mathbb{N}}$ the set of Knuth relations for all triples $(x, y, z) \in \mathbb{N}^3$. Then the associated plactic monoid $P(\mathbb{N})$ is the monoid of *all* semistandard Young tableaux. Despite the work in this thesis, the question of deciding the theory of $P(\mathbb{N})$ remains open. However, we present an algorithm, by uniformity, for deciding the Diophantine problem for $P(\mathbb{N})$.

Lemma 7.1.1. *For any $n \in \mathbb{N}$ the map $\phi : P(\mathbb{N}) \to P_n$, defined on generators as $\phi(k) = k$ if $k \leq n$ and $\phi(k) = \varepsilon$ if $k > n$ and extended to words in the natural way, is a homomorphism.*

Proof. Considered as a map from $\mathbb{N}^*$ to $\{1, \dots, n\}^*$, ϕ is clearly a homomorphism. It only remains to show that ϕ is well defined as a map from $P(\mathbb{N})$ to P_n. We will show this by proving that each Knuth relation in $K_{\mathbb{N}}$ will map to a relation that holds in P_n.

Suppose $u = xzy$ and $v = zxy$, for $x \leq y < z$. If $z \leq n$ then $\phi(u) = u$, $\phi(v) = v$, and $u = v$ in P_n so there is nothing to prove. If $z > n$ then $\phi(u) = \phi(x)\phi(y) = \phi(v)$, as $\phi(z) = \varepsilon$. Thus $\phi(u) = \phi(v)$ will always hold in P_n. An analogous argument shows $\phi(u) = \phi(v)$ for $u = yxz$ and $v = yzx$ with $x < y \leq z$. □

Theorem 7. *The Diophantine problem for $P(\mathbb{N})$ is decidable.*

Proof. Suppose we are given some equation $u_1 X_1 \dots X_n u_{n+1} = v_1 Y_1 \dots Y_m v_{m+1}$. Denote this equation by φ. Define the *support* of an element $u \in P(\mathbb{N})$ to be the set of all numbers appearing in u. Further, define the support of φ to be all letters appearing in the supports of u_i and v_i

$$supp(\varphi) = \bigcup_{i \leq n+1} supp(u_i) \cup \bigcup_{j \leq m+1} supp(v_j).$$

Let $k = \max(supp(\varphi))$. Then by the above proposition there exists a homomorphism $\phi : P(\mathbb{N}) \to P_k$. Since each u_i and v_j is an element of P_k, we get that $\phi(u_i) = u_i$ and $\phi(v_j) = v_j$.

Now, suppose φ has a solution $(x_1, \dots, x_n, y_1, \dots, y_m) \in P(\mathbb{N})^{m+n}$.

Then $(\phi(x_1), \dots \phi(x_n), \phi(y_1), \dots, \phi(y_m)) \in P_k^{n+m}$ will also be a solution to φ, since ϕ is a homomorphism. Thus φ has a solution in $P(\mathbb{N})$ if and only if it has a solution in P_k.

Now, since there is a uniform algorithm for deciding first order sentences in P_k for any k, we obtain the following procedure for solving Diophantine problems in $P(\mathbb{N})$:

1. Given φ as input, calculate $k = \max(supp(\varphi))$.
2. Generate the interpretation of P_k into Presburger arithmetic.
3. Interpret the sentence

$$\exists X_1 \dots \exists X_n \exists Y_1 \dots \exists Y_m : u_1 X_1 \dots X_n u_{n+1} = v_1 Y_1 \dots Y_m v_{m+1}$$

   in Presburger arithmetic using the interpretation of P_k, and check whether it holds.

$\square$

7.2 A plactic monoid on integers

We need not restrict ourselves to plactic monoids generated by $\mathbb{N}$.

Let's consider instead tableaux with labels taken from $\mathbb{Z}$. By the total order on $\mathbb{Z}$ we obtain a set $K_{\mathbb{Z}}$ of Knuth relations on triples $(x, y, z) \in \mathbb{Z}^3$. Define the plactic monoid on integers to be $P(\mathbb{Z}) = \langle \mathbb{Z} \mid K_{\mathbb{Z}} \rangle$. This is an infintely generated plactic monoid, but note that $P(\mathbb{N})$ and $P(\mathbb{Z})$ are not isomorphic.

Indeed, suppose $\psi : P(\mathbb{Z}) \to P(\mathbb{N})$ were an isomorphism. Then for some $y \in P(\mathbb{Z})$

we have $\psi(y) = 1$. Since 1 is irreducible, we must have $y \in \mathbb{Z}$. Consider $x < y < z$, $x, y, z \in \mathbb{Z}$. Then by irreducibility, $\psi(x), \psi(z) \in \mathbb{N}$. Thus we have some $a, b \in \mathbb{N}$ such that $1ab = 1ba$. Such an equality cannot hold in $P(\mathbb{N})$.

Given φ a Diophantine equation in $P(\mathbb{Z})$, we will have $supp(\varphi)$ a finite totally ordered set. This set will have some smallest element $a \in \mathbb{Z}$ and some largest element $b \in \mathbb{Z}$. Then the interval $[a, b] \subset \mathbb{Z}$ has size $k = b - a + 1$, and we can define an order preserving injective map from $supp(\varphi)$ to $\{1, \dots, k\}$. We will extend this map to a homomorphism.

Lemma 7.2.1. *Let $\{z_1 < z_2 < \cdots < z_n\}$ be a finite set of integers with their standard order. Then the map $\phi : P(\mathbb{Z}) \to P_k$, with $k = z_n - z_1 + 1$ defined on generators by*

$$\phi(z) = \begin{cases} \varepsilon, \ z < z_1 \\ z - z_1 + 1, \ z \in [z_1, z_n] \\ \varepsilon, \ z > z_n \end{cases}$$

and extended to words in the natural way, is a homomorphism.

Proof. As in lemma 7.1.1, consider $u = xzy$ and $v = zxy$, for $x \leq yz$. If more than one letter in $\{x, y, z\}$ is mapped to ε, there is nothing to prove. Likewise if no letters are mapped to ε. If only one letter is mapped to ε, then this is either x, yielding $\phi(u) = \phi(z)\phi(y) = \phi(v)$, or this letter is z, yielding $\phi(u) = \phi(x)\phi(y) = \phi(v)$. An analogous argument holds for all other Knuth relations. $\square$

Thus, as in the case above, any Diophantine equation φ is solvable in $P(\mathbb{Z})$ if and only if it has a solution in a fixed finite rank plactic monoid. Therefore, by uniformity of the above algorithm, we obtain the following corollary.

Corollary 7.2.2. *The Diophantine problem for $P(\mathbb{Z})$ is decidable.*

7.3 Some open questions

1. Is the first order theory of $P(\mathbb{N})$ decidable? It is known that this monoid satisfies no identities [19], and the above proof shows it has decidable Diophantine problem. Can this be extended to the whole theory? What about in the $P(\mathbb{Z})$ case?

2. Do infinite rank plactic monoids defined on other generating sets have decidable Diophantine problem? For example, does $P(\mathbb{Q}) = \langle \mathbb{Q} \mid K_{\mathbb{Q}} \rangle$ have decidable Diophantine problem? What about $P(L)$ for an arbitrary recursive total order? More generally, do such monoids have decidable theory as well?

Bibliography

[1] A. Abram and C. Reutenauer. The stylic monoid. *Semigroup Forum*, 105:1–45, June 2022. ISSN: 1432-2137.

[2] J. Araújo, M. Kinyon, J. Konieczny, and A. Malheiro. Four notions of conjugacy for abstract semigroups. *Proceedings of the Royal Society of Edinburgh: Section A Mathematics*, 147(6):1169–1214, 2017.

[3] R. V. Book and F. Otto. *String-rewriting systems*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993. ISBN: 0-387-97965-4.

[4] A. J. Cain, G. Klein, Ł. Kubat, A. Malheiro, and J. Okniński. A note on identities in plactic monoids and monoids of upper-triangular tropical matrices, 2017. arXiv: `1705.04596 [math.CO]`.

[5] A. J. Cain, R. D. Gray, and A. Malheiro. Crystal monoids & crystal bases: rewriting systems and biautomatic structures for plactic monoids of types A_n, B_n, C_n, D_n, and G_2. *Journal of Combinatorial Theory. Series A*, 162:406–466, 2019. ISSN: 0097-3165,1096-0899.

[6] A. J. Cain, R. D. Gray, and A. Malheiro. Finite Gröbner-Shirshov bases for plactic algebras and biautomatic structures for plactic monoids. *Journal of Algebra*, 423:37–53, 2015. ISSN: 0021-8693,1090-266X.

[7] A. J. Cain, R. D. Gray, and A. Malheiro. Rewriting systems and biautomatic structures for Chinese, hypoplactic, and Sylvester monoids. *International Journal of Algebra and Computation*, 25(1-2):51–80, 2015. ISSN: 0218-1967,1793-6500.

[8] A. J. Cain, M. Johnson, M. Kambites, and A. Malheiro. Representations and identities of plactic-like monoids. *Journal of Algebra*, 606:819–850, 2022. ISSN: 0021-8693,1090-266X.

[9] C. Choffrut and R. Mercaş. The lexicographic cross-section of the plactic monoid is regular. In *Combinatorics on words*. Volume 8079, Lecture Notes in Comput. Sci. Pages 83–94. Springer, Heidelberg, 2013. ISBN: 978-3-642-40579-2; 978-3-642-40578-5.

[10] L. Ciobanu and A. Garreta. Group Equations With Abelian Predicates. *International Mathematics Research Notices. IMRN*, (5):4119–4159, 2024. ISSN: 1073-7928,1687-0247.

[11] L. Daviaud, M. Johnson, and M. Kambites. Identities in upper triangular tropical matrix semigroups and the bicyclic monoid. *Journal of Algebra*, 501:503–525, 2018. ISSN: 0021-8693,1090-266X.

[12] V. Diekert and M. Lohrey. Word equations over graph products. *International Journal of Algebra and Computation*, 18(3):493–533, 2008. ISSN: 0218-1967,1793-6500.

[13] G. Duchamp and D. Krob. Plactic-growth-like monoids. In *Words, languages and combinatorics, II (Kyoto, 1992)*, pages 124–142. World Sci. Publ., River Edge, NJ, 1994. ISBN: 981-02-1609-2.

[14] B. Fine, A. Gaglione, G. Rosenberger, and D. Spellman. The Tarski problems and their solutions. *Advances in Pure Mathematics*, 5(04):212–231, 2015.

[15] W. Fulton. *Young Tableaux: With Applications to Representation Theory and Geometry*, volume 35 of *London Mathematical Society Student Texts*. Cambridge University Press, 1996. ISBN: 0-521-56144-2; 0-521-56724-6.

[16] A. Garreta and R. D. Gray. On equations and first-order theory of one-relator monoids. *Information and Computation*, 281:Paper No. 104745, 19, 2021. ISSN: 0890-5401,1090-2651.

[17] F. Hivert, J.-C. Novelli, and J.-Y. Thibon. An analogue of the plactic monoid for binary search trees. In *Proceedings of WORDS'03*, volume 27 of *TUCS Gen. Publ.* Pages 27–35. Turku Cent. Comput. Sci., Turku, 2003. ISBN: 952-12-1211-X.

[18] W. Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993. ISBN: 0-521-30442-3.

[19] M. Johnson and M. Kambites. Tropical representations and identities of plactic monoids. *Transactions of the American Mathematical Society*, 374(6):4423–4447, 2021. ISSN: 0002-9947,1088-6850.

[20] P. T. Johnstone. *Notes on logic and set theory*. Cambridge Mathematical Textbooks. Cambridge University Press, Cambridge, 1987. ISBN: 0-521-33502-7; 0-521-33692-9.

[21] M. Kashiwara. On crystal bases of the Q-analogue of universal enveloping algebras. *Duke Mathematical Journal*, 63(2):465–516, 1991. ISSN: 0012-7094,1547-7398.

[22] O. Kharlampovich and A. Myasnikov. Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz. *Journal of Algebra*, 200(2):472–516, 1998. ISSN: 0021-8693,1090-266X.

[23] O. Kharlampovich and A. Myasnikov. Tarski's problem about the elementary theory of free groups has a positive solution. *Electronic Research Announcements of the American Mathematical Society*, 4:101–108, 1998. ISSN: 1079-6762.

[24] D. E. Knuth. Permutations, matrices, and generalized Young tableaux. *Pacific Journal of Mathematics*, 34:709–727, 1970. ISSN: 0030-8730,1945-5844.

[25] Ł. Kubat and J. Okniński. Identities of the plactic monoid. *Semigroup Forum*, 90(1):100–112, 2015. ISSN: 0037-1912,1432-2137.

[26] Ł. Kubat and J. Okniński. Plactic algebra of rank 3. *Semigroup Forum*, 84(2):241–266, 2012. ISSN: 0037-1912,1432-2137.

[27] A. Lascoux and M.-P. Schützenberger. Le monoıde plaxique. In *Noncommutative structures in algebra and geometric combinatorics (Naples, 1978)*. Volume 109, Quad. "Ricerca Sci." Pages 129–156. CNR, Rome, 1981.

[28] C. Lecouvey. Combinatorics of crystal graphs and Kostka-Foulkes polynomials for the root systems B_n, C_n and D_n. *European Journal of Combinatorics*, 27(4):526–557, 2006. ISSN: 0195-6698,1095-9971.

[29] C. Lecouvey. Schensted-type correspondence, plactic monoid, and jeu de taquin for type C_n. *Journal of Algebra*, 247(2):295–331, 2002. ISSN: 0021-8693,1090-266X.

[30] C. Lecouvey. Schensted type correspondence for type G_2 and computation of the canonical basis of a finite dimensional $U_q(G_2)$-module, 2002. arXiv: `math/0211443 [math.CO]`.

[31] C. Lecouvey. Schensted-type correspondences and plactic monoids for types B_n and D_n. *Journal of Algebraic Combinatorics. An International Journal*, 18(2):99–133, 2003. ISSN: 0925-9899,1572-9192.

[32] P. Littelmann. A plactic algebra for semisimple Lie algebras. *Advances in Mathematics*, 124(2):312–331, 1996. ISSN: 0001-8708,1090-2082.

[33] M. Lothaire. *Algebraic Combinatorics on Words*, volume 90 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2002. ISBN: 0-521-81220-8.

[34] G. S. Makanin. The problem of the solvability of equations in a free semigroup. *Matematicheskiı Sbornik. Novaya Seriya*, 103(145)(2):147–236, 319, 1977. ISSN: 0368-8666.

[35] G. S. Makanin. Equations in a free group. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 46(6):1199–1273, 1982. ISSN: 0373-2436.

[36] D. Marker. *Model Theory : An Introduction*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781475777321.

[37] J.-C. Novelli. On the hypoplactic monoid. *Discrete Mathematics*, 217(1):315–336, 2000. ISSN: 0012-365X.

[38] C.-F. Nyberg-Brodda. A word-hyperbolic special monoid with undecidable diophantine problem, 2022. arXiv: `2205.01056 [math.GR]`.

[39] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchen die Addition als einzige Operation hervortritt. *Comptes Rendus Premier Congrès des Mathématicienes des Pays Slaves, Varsovie 1929 / Sprawozdanie z I Kongresu matematyków krajów słowiańskich, Warszawa 1929*:92–101, 1929.

[40] M. Presburger. On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation. *History and Philosophy of Logic*, 12(2):225–233, 1991. ISSN: 0144-5340,1464-5149. Translated from the German and with commentaries by Dale Jacquette.

[41] A. A. Razborov. On systems of equations in a free group. *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 48(4):779–832, 1984. ISSN: 0373-2436.

[42] C. Schensted. Longest increasing and decreasing subsequences. *Canadian Journal of Mathematics*, 13:179–191, 1961. ISSN: 0008-414X,1496-4279.

[43] M.-P. Schützenberger. La correspondance de Robinson. In *Combinatoire et représentation du groupe symétrique.* Volume 579, Lecture Notes in Math. Pages 59–113. Springer, Berlin-New York, 1977.

[44] M. P. Schützenberger. Sur une construction de Gilbert de B. Robinson. *Séminaire Dubreil. Algèbre et théorie des nombres*, 25(1):1–4, 1971-1972.

[45] Z. Sela. Diophantine geometry over groups. I. Makanin-Razborov diagrams. *Publications Mathématiques. Institut de Hautes Études Scientifiques*, (93):31–105, 2001. ISSN: 0073-8301,1618-1913.

[46] Z. Sela. Word equations I: Pairs and their Makanin-Razborov Diagrams, 2016. arXiv: `1607.05431 [math.GR]`.

[47] R. Stansifer. Presburger's Article on Integer Airthmetic: Remarks and Translation. Technical report TR84-639, Cornell University, Computer Science Department, Sept. 1984.

A

A theoretical computer

Despite most of the results in this thesis being results about algorithms, and hence about computers, the author has made no attempt to define what model of theoretical computation we are using, nor indeed what it means to provide an 'algorithm' for a problem. Mainly, this is because any reasonable and intuitive definition of 'a procedure of applying certain rules in an order' suffices to show our results. Furthermore, most reasonable models of computation are Turing equivalent. Nonetheless, for the sake of completeness what follows is the definition of a *register machine*, or *Minsky machine*. These machines are named after Marvin Minsky, the computer scientist who first described them. The definition is taken from Chapter 4 of Peter Johnstone's book [20] – an excellent reference text on logic.

Definition (Register Machine)**.** A Register machine will firstly have countably many *registers* $R_1, R_2, R_3, \ldots$, each of which may store a natural number. To begin with, each register will store 0. We then specify a program to run on the registers by giving a list of states $S_0, S_1, \ldots, S_n$, for some $n \in \mathbb{N}$. These states each store one of the following instructions:

- The state S_0 stores the instruction "HALT".
- A nonzero state may have the instruction $(i, +, j)$, in which case we add 1 to the number in register R_i, and move to the state S_j.
- A nonzero state may alternatively have the instruction $(i, -, j, k)$, in which

case we check whether register R_i has a nonzero entry. If it does, we subtract 1 from it and move to state S_j. If R_i has a zero entry, we do nothing and move to state S_k.

This register machine takes as input some tuple $(n_1, \ldots, n_k) \in \mathbb{N}^k$, and will start in state S_1. When the machine is in a given state, it executes the instruction stored in the state. If it moves into state S_0, the machine executes 'HALT', meaning the computation is finished. The output of the register machine will then be the number stored in the register R_1.