Parameterized Rewriting on Words

Benjamin Monate

LRI, CNRS UMR 8623, Bât. 490 - Université Paris-Sud, Centre d'Orsay
91405 Orsay Cedex, France
monate@lri.fr

1 Introduction

Basic rewriting techniques are widely used to perform automatic proofs about equational specifications. For example the symmetric groups $\mathcal{S}_n$ are studied as the quotient of a free structure by some well chosen equations. The Knuth-Bendix completion automatically computes a convergent finite rewriting that leads to an efficient decision algorithm for equality : the normalization. One can exhibit a convergent rewriting system for *each* $\mathcal{S}_n$, n being in $\mathbb{N}$. The completion cannot be done in practice for very large symmetric groups *i.e.* for large values of n, because its complexity is exponential in the number of equations. Our goal in this paper is to perform proofs about this kind of equational specification without instantiating the parameters. Therefore the system $\mathcal{S}_n$ is directly presented as a parameterized word rewriting system :

$$\begin{aligned}\mathcal{S}_n \ = \{&a_i^2 = \epsilon \mid 1 \leq i \leq n-1 \\ &a_i a_j = a_j a_i \mid i - j \geq 2 \wedge 1 \leq i, j \leq n-1 \\ &(a_i a_{i+1})^3 = \epsilon \mid 1 \leq i \leq n-2\}\end{aligned}$$

In Section 1 of the paper we define the syntax of parameterized rewriting. In Section 2 give a critical pair theorem in this setting and conclude with an extension to some other kind of parameterization.

An extended version of this abstract with complete proofs and more precise explanations (in French) is available at `http://www.lri.fr/~monate/ftp/prw.html`

2 Basic notions of parameterized rewriting

We define a formal syntax for parameterized signatures. For $\mathcal{S}_n$ we want to define the signature as $\Sigma = \{a_i|_I 1 \leq i \leq N-1\}_{\{N\}}$ where I is an infinite countable set of variables (containing i) and N is a parameter. The general definition is

Definition 1 *A parameterized signature is a 4-tuple* $\Sigma = (a, I, \varphi, \mathcal{N})$ *denoted by* $\Sigma = \{a_i|_I\, \varphi\}_{\mathcal{N}}$ *such that*

- *a is a generic arbitrary symbol*

- *$\mathcal{N}$ is a countable set of parameters.*
- *I is a countable set of variables such that $\mathcal{N} \cap I = \emptyset$ and $i \in I$.*
- *φ is a formula of Presburger's arithmetic [2] whose variables are in $I \cup \mathcal{N}$.*

We need to give an interpretation to a parameterized signature that links the notion of parameterized signatures to the notion of alphabets. We define a function $[\![\,]\!]$ which associates an infinite family of alphabets with any parameterized signature. For the example of $\mathcal{S}_n$ the interpretation has to satisfy

$$[\![\Sigma]\!] = (\emptyset; \{a_1\}; \{a_1; a_2\}; \cdots; \{a_1; a_2; \cdots; a_k\} \cdots)$$

Definition 2 *For any substitution $\nu : N \to \mathbb{N}$ the function $[\![.]\!]_\nu$ is defined by*

$$[\![\{a_i|_I\varphi\}_{\mathcal{N}}]\!]_\nu = \bigcup_{\substack{\mu : I \to \mathbb{N} \\ \nu(\mu(\varphi)) \text{ is true}}} \{a_{\nu(\mu(i))}\}$$

This function is called ν-interpretation *and associates an alphabet that may be infinite, empty or finite with every parameterized signature. One can define the interpretation of a signature Σ by the countable family $([\![\Sigma]\!]_\nu)_{\nu : N \to \mathbb{N}}$.*

From now on we will implicitly refer to the signature $\Sigma = \{a_i|_I\varphi\}_{\mathcal{N}}$.

Parameterized words are intuitively words build over a parameterized signature. In the case of $\mathcal{S}_n$ one has to handle words like a_1 (which exists only when $n \geq 2$) or $a_i a_j | i - j \geq 2$. The formal definition handles these cases.

Definition 3 *A* parameterized word *is either $a_{i_0} \ldots a_{i_k}|\psi$ or $\epsilon|\psi$ such that*

- *ψ is a formula of Presburger's arithmetic whose variables are in $I \cup \mathcal{N}$*
- *k is a non-negative integer*
- *$i_0 \cdots i_k$ are elements of I*

The ν-interpretation of a parameterized word is a set of words built over the alphabet $[\![\Sigma]\!]_\nu$.

Definition 4 *The ν-interpretation of a parameterized word is defined by*

$$[\![a_{i_0} \cdots a_{i_k}|\psi]\!]_\nu = \bigcup_{\substack{\mu : I \to \mathbb{N} \\ \nu(\mu(\psi)) \text{ is true} \\ j \in [0;k] a_{\nu(\mu(i_j))} \in [\![\Sigma]\!]_\nu}} \{a_{\nu(\mu(i_0))} \cdots a_{\nu(\mu(i_k))}\}$$

and $[\![\epsilon|\psi]\!]_\nu = \begin{cases} \{\epsilon\} & \text{if } \nu(\psi) \text{ is satisfiable} \\ \emptyset & \text{if } \nu(\psi) \text{ is not satisfiable} \end{cases}$.

The family of all ν-interpretations of a word is called the interpretation *of the word.*

For example we have $[a_1]_{n\to 2} = \{a_1\}$, $[a_1]_{n\to 0} = \emptyset$ and $[a_j a_i | i-j \geq 2]_{n\to 5} = \{a_1 a_3; a_1 a_4; a_2 a_4\}$. The ν-interpretation of a parameterized word can be infinite if the ν-interpretation of the signature is an infinite alphabet.

We introduce a syntactical definition that let us write rules like $u_i u_j \to u_j u_i | i - j \geq 2$. Note that such a rule represents the set of rules $u_i u_j \to u_j u_i$ for all integers i and j satisfying the constraint.

Definition 5 *A parameterized rule is a triplet (u, v, ψ) denoted $(u \to v)|\psi$ such that*

- *u and v are two parameterized words without constraint*
- *ψ is formula of Presburger's arithmetic*

A parameterized rewriting system is a finite set of parameterized rules. As usual u is the left member of the rule and r the right member. ψ is the constraint of the rule.

The ν-interpretation of a rule is a set of rules built over the ν-interpretation of the signature. For example $[u_i u_j \to u_j u_i | i-j \geq 2]_{N\to 4} = \{u_3 u_1 \to u_1 u_3\}$.

Definition 6 *The* ν-interpretation *of a rule is defined by*

$$[\![(u = v)|\psi]\!]_\nu = \bigcup_{\substack{\mu : I \to \mathbb{N} \\ \nu(\mu(\psi)) \text{ is true}}} \{\nu(\mu(u)) \to \nu(\mu(v))\}$$

The ν-interpretation of a rewriting system is the union of the ν-interpretation of its rules.

The main property of the parameterized rewriting is that it is preserved by interpretation in the sense that if $u \to_R v$ for parameterized rewriting then for all $u_0 \in [u]_\nu$ and $v_0 \in [\![v]\!]_\nu$ the rewriting system $R_0 = [\![R]\!]_\nu$ reduces u_0 into v_0. Moreover every v_0 is obtained by the reduction from an u_0. The following definition for the rewriting relation has this property.

Definition 7 *In the signature $\Sigma = \{a_i|_I \varphi\}_N$, the parameterized word $u|\psi$ rewrites into $v|\chi$ by the rule $l \to r|\xi$ at position $p \in \mathbb{N}$ with the substitution $\sigma : I \to Expr(I, N)$ and we denote*

$$u|\psi \xrightarrow[p,\sigma]{l\to r|\xi} v|\chi \quad \textit{if and only if}$$

1. *Matching conditions:*
   (a) *u has a subword of length $|l|$ at position p* i.e.
   $u = a_{i_1} \cdots a_{i_{p-1}}\ a_{i_p} \cdots a_{i_{p+|l|-1}}\ a_{i_{p+|l|}} \cdots a_{i_m}$
   $l = a_{i'_1} \cdots a_{i'_{|l|}}$
   (b) *$\psi \Rightarrow i_p = \sigma(i'_1)$, ... , $\psi \Rightarrow i_{p+|l|-1} = \sigma(i'_{|l|})$ are valid formulae of Presburger's arithmetic.*

(c) *Denoting* $\{x_1; \ldots ; x_n\} = Var(\sigma(\xi)) \setminus Var(\psi)$, *the formula* $\psi \Rightarrow \exists x_1 \ldots x_n \sigma(\xi)$ *is valid.*

2. *Production conditions:*
   (a) $v = a_{\sigma(i_1)} \cdots a_{\sigma(i_{p-1})} \sigma(r) a_{\sigma(i_{p+|l|})} \cdots a_{\sigma(i_m)}$
   (b) $\sigma(\chi) \Leftrightarrow \psi \wedge \sigma(\xi)$ *is valid.*

This definition has been proved to have the previously mentioned preservation property. For example the term $a_{i+3}a_i|i \geq 1 \wedge i+3 \leq n-1$ reduces into $a_i a_{i+3}|i \geq 1 \wedge i+3 \leq n-1$. The latter is not reducible.

3 Completion for parameterized rewriting

We can now define the notion of critical pair of rules by enumerating all possible overlaps between the left members of rules and prove a critical pair lemma.

Theorem 1 *A parameterized rewriting system is locally confluent if and only if its critical pairs are locally confluent.*

This theorem is interesting because local confluence is preserved by ν-interpretation. But on the contrary even all ν-interpretation can be confluent whereas the parameterized system is not.

We have an algorithm to perform completion on parameterized rewriting systems. As always one needs to find suitable orderings on parameterized words. An implementation is currently under development in the software C*i*ME [1]. We have also extended the syntax of words in order to allow *exponents* in words in order to describe systems like $a_i^n \to \epsilon$ and perform completion on such systems. This is a very promising extension as presentations of algebraic structures often use exponents. For example the presentation of $\mathcal{S}_n$ with a transposition and an n-cycle contains $a^n = \epsilon$.

References

1. Evelyne Contejean, Claude Marché, Benjamin Monate, and Xavier Urbain. Cime version 2, 2000. Prerelease available at `http://www.lri.fr/~demons/cime.html`.
2. M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In *Comptes Rendus du premier Congrès des Mathématiciens des Pays slaves*, Warszawa, 1929.