

Semigroups Satisfying $x^{m+n} = x^n$

Nachum Dershowitz*

Department of Computer Science

University of Illinois
Urbana, IL 61801
U.S.A.

nachum@cs.uiuc.edu

Hebrew University
Jerusalem 91904
Israel

nachum@cs.huji.ac.il

Abstract

We summarize recent results on semigroups satisfying the identity $x^{m+n} = x^n$, for $n \geq 0$ and $m \geq 1$, and some rewrite techniques that have contributed to their investigation.

1 Introduction

Ninety years ago, Burnside [1902] posed the question whether every group satisfying the identity $x^m = 1$, and having a finite number of generators, is finite. In 1969, Brzozowski (see the list of open questions in [Brzozowski, 1980]) conjectured that the congruence classes on words generated by $x^{n+1} = x^n$, are all regular sets. Recently, McCammond [1991] extended this conjecture to all semigroups satisfying $x^{m+n} = x^n$ and investigated the decidability of their word problems. These conjectures have been the topic of recent research, which we summarize here.

Consider the set A^* of finite words over some *finite* alphabet A containing at least two letters, and suppose we identify certain repetitious words. (The case $|A| = 1$ is patently uninteresting.) Specifically, a word of the form $ux^{m+n}v$, where x is any subword repeated contiguously $m + n$ times ($n \geq 0$, $m \geq 1$), is equivalent to the shorter word $ux^n v$. Let $\sim_{m,n}$ denote this congruence on words. In other words, we are looking at the algebras $A^*/\sim_{m,n}$, with finite generating set A , and with a binary juxtaposition operation that satisfies the axiom of associativity, $(xy)z = x(yz)$, as well as $x^{m+n} = x^n$. The different cases are portrayed in Table 1.

We are interested in the following three questions:

1. Does $\sim_{m,n}$ have finite index (finitely many congruence classes)? In other words: Is the algebra $A^*/\sim_{m,n}$ finite?
2. Is each of the congruence classes in $A^*/\sim_{m,n}$ a regular (recognizable, rational) set?

*This work was supported in part by a Lady Davis fellowship at the Hebrew University and by the U. S. National Science Foundation under Grants CCR-90-07195, CCR-90-24271, and INT-90-16958.

	$n = 0$	1	2	3	4	5	\dots
$m = 1$	$x = 1$	$xx = x$	$x^3 = xx$	$x^4 = x^3$	$x^5 = x^4$	$x^6 = x^5$	\dots
2	$xx = 1$	$x^3 = x$	$x^4 = xx$	$x^5 = x^3$	$x^6 = x^4$	$x^7 = x^5$	\dots
3	$x^3 = 1$	$x^4 = x$	$x^5 = xx$	$x^6 = x^3$	$x^7 = x^4$	$x^8 = x^5$	\dots
4	$x^4 = 1$	$x^5 = x$	$x^6 = xx$	$x^7 = x^3$	$x^8 = x^4$	$x^9 = x^5$	\dots
5	$x^5 = 1$	$x^6 = x$	$x^7 = xx$	$x^8 = x^3$	$x^9 = x^4$	$x^{10} = x^5$	\dots
6	$x^6 = 1$	$x^7 = x$	$x^8 = xx$	$x^9 = x^3$	$x^{10} = x^4$	$x^{11} = x^5$	\dots
7	$x^7 = 1$	$x^8 = x$	$x^9 = xx$	$x^{10} = x^3$	$x^{11} = x^4$	$x^{12} = x^5$	\dots
8	$x^8 = 1$	$x^9 = x$	$x^{10} = xx$	$x^{11} = x^3$	$x^{12} = x^4$	$x^{13} = x^5$	\dots
9	$x^9 = 1$	$x^{10} = x$	$x^{11} = xx$	$x^{12} = x^3$	$x^{13} = x^4$	$x^{14} = x^5$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
115	$x^{116} = 1$	$x^{117} = x$	$x^{118} = xx$	$x^{119} = x^3$	$x^{120} = x^4$	$x^{121} = x^5$	\dots
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots

Table 1: Semigroups satisfying $x^{m+n} = x^n$.

3. Is the congruence $\sim_{m,n}$ on A^* decidable? In other words: Is the free word (identity) problem for the variety defined by (associativity and) $x^{m+n} = x^n$ recursively solvable?

The top-left case ($m = 1, n = 0$) of Table 1 is a trivial algebra. The next case of the top row ($m, n = 1$), the (free) idempotent semigroups, are called (*free*) *bands*. The algebras $x^m = 1$ in the first column are called *Burnside groups*. (They are groups, since every element of A has an inverse x^{m-1} .) By extension, the rest of the algebras have been called *Burnside algebras*. We might call the first row *Brzozowski semigroups*, since he proposed the question whether their equivalent words form regular sets.

Before proceeding, it is important to realize that two words may be congruent, though neither contains an instance of x^{m+n} . For example, from $xxx = xx$ one can derive $xyxyxyxyxyxy = yxyxyxy$. The point is that the equation $x^{m+n} = x^n$ on strings has critical pairs with itself (modulo associativity).

A general approach to these three questions is the following: Construct an infinite convergent (terminating, and confluent) string-rewriting system (semi-Thue system) for the theory by looking at longer and longer ground instances of the axiom. If any sufficiently long word is reducible by some rule, then the algebra is finite. If only finitely many rules are needed to rewrite all elements of an equivalence class to normal form, then under certain conditions the class is regular. If there is an effective way of generating a finite set of rules for reducing any given word to normal form, then the word problem is decidable.

For notation and concepts related to rewriting, see [Dershowitz and Jouannaud, 1990].

2 Finiteness

Burnside [1902] showed that the groups $x^m = 1$, for $m = 1, 2, 3$, are finite and asked whether the same was true for all m . Sanov [1940] proved $x^4 = 1$ to be finite and Hall [1957] showed the same for exponent 6. In 1968, Novikov and Adian, in a series of papers, showed that there are *infinite* Burnside groups for all odd $m \geq 4381$; this negative result was extended to odd $m \geq 665$ in Adian's monograph [1979] on the subject (to which [Adian, 1977] serves as an introduction). More recently, the bound was improved to 115, and the conjecture was shown false for all m greater than 2^{13} [Adian, personal communication]. The question remains open for $m = 5, 7, 8, 9, \dots, 113, 114, 116, 118, \dots, 2^{13}$. Much work has been done on this and related questions; it is still an active area of research.

Green and Rees [1952] proved that $x^m = 1$ is finite if and only if the semigroup $x^{m+1} = x$ is. So columns 1 and 2 of Table 1 have identical finiteness properties. In particular, bands ($xx = x$) are finite. In fact, the conditional equation

$$C(y) \subseteq C(x) = C(z) \quad \Rightarrow \quad xyz = xz$$

captures all the infinitely many critical pairs derivable from the defining axiom $xx = x$, where $C(x)$ denotes the set of letters in x . It applies to any subword xyz such that the letters in x and z are the same and include all those in y . See [Howie, 1976, Chap. IV] and [Siekmann and Szabó, 1982]. Finitely generated bands are finite, since there are only finitely many words not equivalent to a shorter word. To see this, suppose a word w contains n letters and is of length $2^{n+1} - 1$. We show, by induction on n , that it must contain an instance of xyz with $C(y) \subseteq C(x) = C(z)$; hence, by the above equation, it is equivalent to a shorter word. Let x be the shortest prefix of w containing all n letters, and z the shortest such suffix. If x and z overlap, or if $w = xz$, then one must be of length at least 2^n and have a subword of length $2^n - 1$ containing only $n - 1$ letters, which, by the inductive hypothesis, can be replaced with a smaller word. If, on the other hand, $w = xyz$, with y non-empty, then $C(y) \subseteq C(x) = C(z)$ and $xyz = xz$. A similar, but more complicated, argument in [Green and Rees, 1952] establishes that the algebra is precisely of size

$$\sum_{k=1}^n \binom{n}{k} \prod_{i=1}^{k-1} (k - i + 1)^{2^i}$$

which, asymptotically, looks more like $(n/e)^{n^2}$ than like the n^{2^n} one gets by the above simplistic reasoning.

The other algebras of the table are all infinite, since there exist infinitely many square-free words (words not of the form $uxxv$). Since neither side of the axiom $x^{m+n} = x^n$, for $n \geq 2$, can apply to any of these words, each square-free word is in a different class, of which there are infinitely many. It was Axel Thue [1912] who first constructed an infinite square-free word over a three letter alphabet, as well as an infinite cube-free word in a binary alphabet. The infinite sequence of square-free words in Figure 1 is due to Aršon [Aršon, 1937]: Each word is obtained from the previous by substituting $a \mapsto abc$, $b \mapsto bca$, and $c \mapsto cab$ for letters in odd positions, and $a \mapsto cba$, $b \mapsto acb$, and $c \mapsto bac$, for letters in even positions. To obtain a sequence of cube-free words over two letters, 0 and 1, one can apply the map: $a \mapsto 01$, $b \mapsto 010$, and $c \mapsto 0110$. For details, see [Adian, 1979, Chap. I].

Since there are only finitely many square-free words over a binary alphabet, this argument does not work for $n = 2$ and $|A| = 2$. Nevertheless, Brzozowski, Culik and

a
 abc
 $abc\ acb\ cab$
 $abc\ acb\ cab\ cba\ cab\ acb\ cab\ cba\ bca$
 \vdots

Figure 1: Square-free words.

$[0]$
 $[001]$
 $[001\ 001\ 100]$
 $[001\ 001\ 100\ 001\ 001\ 100\ 100\ 001\ 001]$
 \vdots

Figure 2: Congruence classes for $x^3 = xx$.

Gabrielian [1971] showed that the congruence induced by $x^3 = xx$ has infinitely many classes, as shown in Figure 2, where each class is obtained from the previous representative by applying the morphism $0 \mapsto 001$, $1 \mapsto 100$. No sequence of applications of the axiom can equate the representative elements of distinct classes.

When the algebra is finite, ordered completion (see [Hsiang and Rusinowitch, 1987; Dershowitz, 1992; Bachmair and Dershowitz, 199?]) can be used to generate its multiplication table. One computes critical pairs with the axioms, and, at the same time, normal forms of successively larger and larger words. This works provided one can determine when sufficiently many rules have been generated from the axioms for words of any given length. For example, for bands ($xx = x$) and $A = \{a, b\}$, one starts with $a \rightarrow 1$, $b \rightarrow 2$, $ba \rightarrow 3$, and $ab \rightarrow 4$. Since aab has two normal forms, 14 and 4, we get $14 \rightarrow 4$. Eventually, one gets the six elements in Table 2 (as predicted by the formula on the previous page). Pedersen [1988] performed some experiments with such a method.

	1	2	3	4	5	6
1	1	4	6	4	4	6
2	3	2	3	5	5	3
3	3	5	3	5	5	3
4	6	4	6	4	4	6
5	3	5	3	5	5	3
6	6	4	6	4	4	6

Table 2: The free band on two generators.

3 Regularity

If an algebra is finite, then each equivalence class is regular, since each congruence class can be identified with a state, congruent prefixes being interchangeable. By the same token, if all prefixes (or all suffixes, let alone all subwords) of words in a particular class belong to a finite number of classes, then that class is regular.

Brzozowski, Culik, and Gabrielian [1971] showed that each of the classes in Figure 2 is regular which lent support to the conjecture that such is the case for all equivalence classes for the semigroup varieties $x^{n+1} = x^n$. Imre Simon, in unpublished notes (see [Brzozowski, 1980]), contributed to this problem. The first solution, for $n \geq 5$, was by de Luca and Varricchio [1990] who believed their method could be extended to $n = 4$. McCammond [1991] generalized the question to all Burnside semigroups $x^{m+n} = x^n$, and—taking a different approach—solved it for all $m \geq 1$ and $n \geq 6$. Most recently, do Lago [1992] (for his Master’s thesis) refined the approach of de Luca and Varricchio, showing regularity for all $m \geq 1$ and $n \geq 4$, and leaving hope that the method applies to $n = 3$, too.

The following combinatorial result from Fine and Wilf [1965] is essential to obtaining these results: If w is a word with periods p and q (that is, if $u'w = u^p$ and $v'w = v^q$ for some suffixes u' of u and v' of v), then w also has a period $\gcd(p, q)$, the greatest common divisor of its two periods—provided w is of length at least $p + q - \gcd(p, q)$. This is used in [do Lago, 1992] to show that all the critical pairs $l \rightarrow r$, have a special form: the right-hand (shorter) side r is a suffix of the left side l ($l = ur$), as well as a prefix of l ($l = rv$), the remainder of which (v) is of the form w^m , for the given m , where w is the *shortest* periodic suffix of r . For example, the reduced critical pair, $(01)^2(10101)^2 \rightarrow (01)^2(10101)$, formed from the instances $(01)^3 \rightarrow (01)^2$ and $(10101)^3 \rightarrow (10101)^2$ of the axiom (for $m = 1$ and $n = 2$), is of the desired form. In general, for the critical pairs to have this form, $n \geq 4$ is required. By analyzing the structure of derivations (with the closure set of reduced critical pairs of this form), it can be shown that the set of normal forms of subwords of elements of any one class is finite, establishing regularity. See [de Luca and Varricchio, 1990; do Lago, 1992].

4 Decidability

When an algebra is finite, there is a finite (unconditional) rewrite system to decide its word problem, that is, validity of ground equations over a finite set of generators. For bands, for example, one need only include a rule $w \rightarrow w'$, where w' is the shortest word equivalent to w , whenever w is of length up to $2^{n+1} - 1$ and $w \neq w'$. (See [Benninghofen *et al.*, 1987, Chap. II].) Longer rules have reducible left-hand sides, and contribute nothing. Siekmann and Szabó [1982] give a simple decision procedure for free bands using the following conditional string-rewriting system:

$$\begin{array}{l} xx \rightarrow x \\ C(y) \subseteq C(x) = C(z) \mid xyz \rightarrow xz \end{array}$$

for which they give a proof of the convergence (that is, termination and confluence). There are infinitely many “square-free” words to which the first rule does not apply, but

the second does. (An extension of this system, for the join of bands and commutative semigroups, is given in [Nordahl, 1992].)

Even the infinite Burnside groups, odd $n \geq 665$, $m = 1$, have decidable free word problems (see [Adian, 1979, Chap. VI]). The word problem is also decidable for finitely presented groups whose relations are all of the form $w^n = 1$, with n is sufficiently large [Adian, 1979, Preface].

The identity problems for all the cases known to be regular, namely $n \geq 4$, $m \geq 1$, are similarly decidable, since there is an effective way of constructing just the rewrite rules up to the size needed to map an element of A^* to its normal form, rather than generate the whole, infinite system for the theory. See [de Luca and Varricchio, 1990] and [do Lago, 1992].

5 Discussion

Much of the work we have described considers *production* rules $r \rightarrow l$, rather than *reduction* rules $l \rightarrow r$, as we have. In these papers, termination of reduction is invariably based simply on word length. The notions of local and global confluence do play an important role in the work on regularity of the Burnside semigroups. The notion of critical pair is also central, but less explicit. (The “closure under reductions” of [do Lago, 1992], for example, is exactly closure under critical pair generation.)

There are many other questions about semigroups (let alone richer algebraic structures) to which rewriting techniques have been applied. For example, Ehrenfeucht, Hausler, and Rozenberg [1983] give the following generalization of the Myhill-Nerode Theorem: A subset of a semigroup S is regular if and only if it closed with respect to some well-quasi-order \preceq on S that has the replacement property: $x \preceq y$ implies $uxv \preceq uyv$ for all (empty or nonempty) words x, y, u, v . (A well-quasi-order \preceq is a reflexive-transitive binary relation that has no infinite descending sequences $s_1 \succ s_2 \succ \dots$ and no infinite antichains of incomparable elements.) From this, it follows that a language (over a finite alphabet) is regular if and only if it is produced by a string-rewriting relation \rightarrow whose derivation relation \rightarrow^* is a well-quasi-order of A^* [Ehrenfeucht *et al.*, 1983; de Luca and Varricchio, 1992]. Higman’s Lemma is generalized in [Ehrenfeucht *et al.*, 1983] to show that certain productions give a well-quasi-order. See de Luca and Varricchio [1992] for additional applications of rewrite relations and well-quasi-orders to regular languages.

See Benninghofen, Kemmerich, and Richter’s [1987] monograph and Book’s [1987] survey for various applications of rewriting to questions of formal languages and decidability in semigroups. They also point out the limitations of the rewriting approach (see, for example, [Squier, 1987]).

Other applications of rewriting to the investigation of semigroups includes the use of ordered completion—and the introduction of new operators—by Pedersen [1989] to construct new decision procedures for some one-relation monoids. Decidability for one-relation Burnside varieties has not been investigated.

Acknowledgement

I thank Sergei Adian for enlightening conversations, Gregory Kucherov and John Pedersen for their comments, and Michaël Rusinowitch for his encouragement.

References

- [Adian, 1977] Sergei I. Adian. Classifications of periodic words and their application in group theory. In J. L. Mennicke, editor, *Proceedings of a Workshop on Burnside Groups*, pages 1–40, Bielefeld, Germany, 1977. Vol. 806 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin.
- [Adian, 1979] Sergei I. Adian. *The Burnside Problem and Identities in Groups*. Springer-Verlag, Berlin, 1979. Translated from the Russian.
- [Aršon, 1937] S. E. Aršon. Proof of the existence of n -valued infinite asymmetric sequences. *Matematicheskii Sbornik*, 2(44):769–779, 1937.
- [Bachmair and Dershowitz, 199?] Leo Bachmair and Nachum Dershowitz. Equational inference, canonical proofs, and proof orderings. *J. of the Association for Computing Machinery*, 199?. To appear. Available as Technical Report DCS-R-92-1746, Department of Computer Science, University of Illinois, Urbana, IL.
- [Benninghofen *et al.*, 1987] Benjamin Benninghofen, Susanne Kemmerich, and Michael M. Richter. *Systems of Reductions*, volume 277 of *Lecture Notes in Computer Science*. Springer, Berlin, 1987.
- [Book, 1987] Ronald V. Book. Thue systems as rewriting systems. *J. Symbolic Computation*, 3(1&2):39–68, February/April 1987.
- [Brzozowski, 1980] Janusz Brzozowski. Open problems about regular languages. In R. Book, editor, *Formal Language Theory: Perspectives and Open Problems*, pages 23–47. Academic Press, New York, 1980.
- [Brzozowski *et al.*, 1971] Janusz Brzozowski, Karl Culik II, and A. Gabrielian. Classification of non-counting events. *J. of Computer and System Sciences*, 5:41–53, 1971.
- [Burnside, 1902] W. Burnside. On an unsettled question in the theory of discontinuous groups. *Quarterly J. of Pure and Applied Mathematics*, 33:230–238, 1902.
- [Dershowitz, 1992] Nachum Dershowitz. Rewriting methods for word problems. In M. Ito, editor, *Words, Languages & Combinatorics (Proceedings of the International Colloquium, Kyoto, Japan, August 1990)*, pages 104–118, Singapore, 1992. World Scientific.
- [Dershowitz and Jouannaud, 1990] Nachum Dershowitz and Jean-Pierre Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science B: Formal Methods and Semantics*, chapter 6, pages 243–320. North-Holland, Amsterdam, 1990.
- [Ehrenfeucht *et al.*, 1983] Andrzej Ehrenfeucht, David Haussler, and G. Rozenberg. On regularity of context-free languages. *Theoretical Computer Science*, 27(3):311–332, December 1983.
- [Fine and Wilf, 1965] N. J. Fine and M. S. Wilf. Uniqueness theorems for periodic functions. *Proceedings of the American Mathematical Society*, 16:109–114, 1965.
- [Green and Rees, 1952] J. A. Green and D. Rees. On semigroups in which $x^r = x$. *Proceedings of the Cambridge Philosophical Society*, 48:35–40, 1952.
- [Hall, 1957] M. Hall, Jr. Solution of the Burnside problem for exponent 6. In *Proceedings of the National Academy of Sciences of the USA*, volume 43, pages 751–753, 1957.

- [Howie, 1976] J. M. Howie. *An Introduction to Semigroup Theory*. Academic Press, London, 1976.
- [Hsiang and Rusinowitch, 1987] Jieh Hsiang and Michaël Rusinowitch. On word problems in equational theories. In T. Ottmann, editor, *Proceedings of the Fourteenth EATCS International Conference on Automata, Languages and Programming*, pages 54–71, Karlsruhe, West Germany, July 1987. Vol. 267 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin.
- [do Lago, 1992] Alair Pereira do Lago. On the Burnside semigroups $x^n = x^{n+m}$. In I. Simon, editor, *Proceedings of the First Latin American Symposium on Theoretical Informatics*, pages 329–343, São Paulo, Brazil, April 1992. Vol. 583 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin.
- [de Luca and Varricchio, 1990] Aldo de Luca and Stefano Varricchio. On non counting regular classes. In M. Paterson, editor, *Proceedings of the Seventeenth International Colloquium on Automata, Languages and Programming*, Warwick, June 1990. EATCS. Vol. 443 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin; to appear in *Theoretical Computer Science*.
- [de Luca and Varricchio, 1992] Aldo de Luca and Stefano Varricchio. Some regularity conditions based on well quasi-orders. In I. Simon, editor, *Proceedings of the First Latin American Symposium on Theoretical Informatics*, pages 356–371, São Paulo, Brazil, April 1992. Vol. 583 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin.
- [McCammond, 1991] J. McCammond. The solution to the word problem for the relatively free semigroups satisfying $t^a = t^{a+b}$ with $a \geq 6$. *Intl. J. of Algebra and Computation*, 1:1–32, 1991.
- [Nordahl, 1992] Thomas E. Nordahl. On the join of the variety of all bands and the variety of all commutative semigroups via conditional rewrite rules. In M. Ito, editor, *Words, Languages & Combinatorics (Proceedings of the International Colloquium, Kyoto, Japan, August 1990)*, pages 365–372, Singapore, 1992. World Scientific.
- [Pedersen, 1988] John Pedersen. Computer solution of word problems in universal algebra. In M. Tangora, editor, *Computers in Algebra*, pages 103–128. 1988. Vol. 111 of *Lecture Notes in Pure and Applied Mathematics*, Marcel-Dekker, New York.
- [Pedersen, 1989] John Pedersen. Morphocompletion for one-relation monoids. In N. Dershowitz, editor, *Proceedings of the Third International Conference on Rewriting Techniques and Applications*, pages 574–578, Chapel Hill, NC, April 1989. Vol. 355 *Lecture Notes in Computer Science*, Springer, Berlin.
- [Sanov, 1940] I. N. Sanov. Solution of the Burnside problem for exponent 4. *Učen. Zap. Leningrad Univ.*, 10:166–170, 1940.
- [Siekman and Szabó, 1982] Jorg Siekman and P. Szabó. A Noetherian and confluent rewrite system for idempotent semigroups. *Semigroup Forum*, 25(1/2):83–110, 1982.
- [Squier, 1987] Craig Squier. Word problems and a homological finiteness condition for monoids. *J. of Pure and Applied Algebra*, 49:201–217, 1987.
- [Thue, 1912] Axel Thue. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen. *Norske Videnskabselskabets Skrifter I Mat. Nat. Kl.*, 1:1–67, 1912.