Commutation and Beyond
Extended Abstract

Štěpán Holub(✉)

Department of Algebra, Charles University, Prague, Czech Republic
holub@karlin.mff.cuni.cz

Abstract. We survey some properties of simple relations between words.

Keywords: Periodicity forcing · Word equations

1 Commutation Forcing

Arguably, the core of the combinatorics on words folklore is the fact that two words commute if and only if they are powers of the same word. In fact, the claim that x and y commute would be written, by a combinatorist on words, most probably as $x, y \in t^*$ (for some t), instead of $xy = yx$.

This fact has a fairly strong and well known generalization: any nontrivial relation of two words forces commutation. This follows easily from the following lemma.

Lemma 1. *Let x and y do not commute and let z be the longest common prefix of xy and yx. Then z is the longest common prefix of any pair of words $u \in x\{x, y\}^*$ and $v \in y\{x, y\}^*$ that are both at least as long as z.*

Another folklore property of words is that every word has a unique *primitive root*: for each word w there is a unique word r such that w is a power of r, and r is a power of itself only. (Therefore, commutation is equivalent to having the same primitive root.) This uniqueness can be also expressed by saying that if

$$s^n = t^m ,$$

then both s and t are powers of some r. Also this fact has several generalizations. The first one is the theorem of Lyndon and Schützenberger [20] (which happens to hold in free groups as well):

Theorem 2. *If $x^n y^m = z^p$ with $n, m, p \geq 2$, then all words x, y and z commute.*

A clever short proof of this classical result was given by Harju and Nowotka [14].

This theorem naturally raises a question: for which words $w \in \{x, y\}^+$ the equality $w = z^p$, $p > 2$ implies that x and y commute? The answer is formulated in the following result.

Š. Holub—Supported by the Czech Science Foundation grant number 13-01832S.

S. Brlek et al. (Eds.): WORDS 2017, LNCS 10432, pp. 1–5, 2017.
DOI: 10.1007/978-3-319-66396-8_1

Theorem 3. *Suppose that $x, y \in A^*$ do not commute and let $X = \{x, y\}$. Let $\mathcal{C}$ be the set of all X-primitive words from $X^* \backslash X$ that are not primitive. Then either $\mathcal{C}$ is empty or there is $k \geq 1$ such that*

$$\mathcal{C} = \{x^i y x^{k-i} \mid 0 \leq i \leq k\} \quad \textit{or} \quad \mathcal{C} = \{y^i x y^{k-i} \mid 0 \leq i \leq k\}.$$

A word is X-primitive if it is primitive when understood as a word over the alphabet X.

A weaker version of the theorem was obtained in a paper by Lentin and Schützenberger [19]. The full claim was proved in a paper by Barin-Le Rest and Le Rest [2], and in the dissertation of Spehner [22]. Although very natural and important, Theorem 3 seems to be not very well known.

Another generalization of Theorem 2 was given by Appel and Djorup [1] who proved that words satisfying

$$x_1^k x_2^k \cdots x_n^k = y^k \tag{1}$$

commute if $n \leq k$. This was further generalized by Harju and Nowotka [15]. For $n > k$, a natural question is whether the equality (1) can be simultaneously satisfied by non-commuting words for several different exponents k. It turns out that this is possible for two different exponents but not for three. For exponents $1 < k_1 < k_2 < k_3$, this was proved by Holub [16]. For $1 = k_1 < k_2 < k_3$, there was only a limited knowledge [12], until the recent complete and elegant proof by Saarela [21].

2 Periodicity Forcing

The equality (1) is related to the equality

$$x_1^k x_2^k \cdots x_n^k = y_1^k y_2^k \cdots y_n^k.$$

Due to the symmetry, this equality is better seen not as a relation between words but rather as a property of two morphisms $g : a_i \mapsto x_i$ and $h : a_i \mapsto y_i$, *viz.* that they agree on the word $a_1^k a_2^k \cdots a_n^k$. This idea leads to a concept of periodicity forcing words and/or languages. A set of words L is said to be *periodicity forcing* if the equality $g(w) = h(w)$ for all $w \in L$ implies (with $g \neq h$) that both morphisms g and h are periodic, that is, all their images commute. For two morphisms g and h, $g \neq h$, we can define their *equality set* as

$$\mathsf{Eq}(g, h) = \{w \mid w \text{ nonempty}, \ g(w) = h(w)\}.$$

Elements of equality sets of non-periodic morphisms are called *equality words*, which is a complementary property to being periodicity forcing. The question whether $\mathsf{Eq}(g, h)$ is nonempty, for given morphisms g and h, is known as the (in general undecidable) *Post Correspondence Problem.* That is why the question whether a given word or language is periodicity forcing is also known as the *Dual Post Correspondence Problem.* The problem was explicitly or implicitly studied in many particular cases, for example in relation with test sets [18]. Recently, the question was investigated also on a general level [5,6].

The most simple nontrivial version of the problem is the question on equality words over the binary alphabet. Although the binary Post Correspondence Problem is decidable in polynomial time [13], classification of binary equality words turns out to be surprisingly difficult. For instance, it is presently not known whether *abbaaaa* is an equality word or not. Binary equality languages were first studied by Čulík II and Karhumäki [3] almost forty years ago. Soon it was shown that binary equality languages are generated either by one word, or by two words, or are of a special form $\alpha\gamma^*\beta$ [7]. The latter possibility, however, was conjectured to be impossible. The conjecture was confirmed in 2003 [16]. Moreover, it was shown that the only possible form of a two-generated binary equality language is (up to the symmetry of letters) $\{a^ib, ba^i\}$ [17].

There is a series of papers studying words that can be generators of binary equality sets [4,8,10,11]. The current state of the art is captured in the Ph.D. thesis of Jana Hadravová [9] by the Fig. 1 below. Coordinates represent the number of a's and b's in the potential equality word. Black dots indicate that there is a known equality set generator with this numbers of letters, and the grey area delimits cases where all equality words are known. The asymmetry is

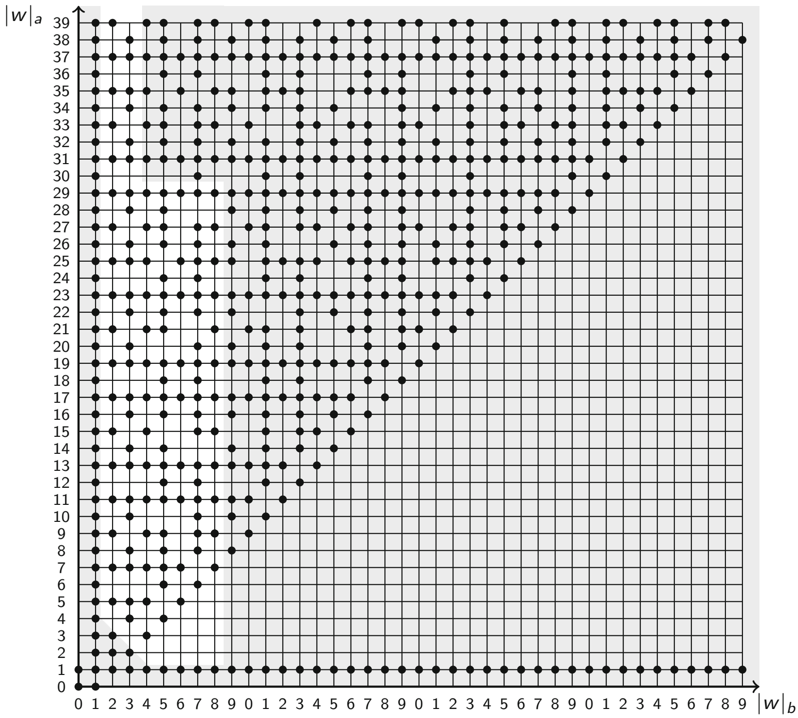

Fig. 1. Binary equality words

given by the assumption that $h(b)$ is not shorter than the other three images $g(a)$, $g(b)$ and $h(a)$.

Example 4. We give an example illustrating how to read the figure. No generator with ten b's and twelve a's is recorded in the figure. The corresponding empty place is within the gray area which means that we can prove that no such generator exists.

On the other hand, there is a dot for five b's and six a's. In fact, we know three such generators: a^6b^5, b^5a^6 and $(ab)^5a$. The coordinate $(5, 6)$ is not in the gray area, which means that we are not presently sure that there is no other word (although we believe so).

Note that also $(b^5a^6)^2$ is a binary equality word, which may seem to be at odds with our first example. But that word is not a generator of an equality language since any two morphisms agreeing on $(b^5a^6)^2$ agree also on b^5a^6 as one can easily see.

References

1. Appel, K.I., Djorup, F.M.: On the equation $z_1^n z_2^n z_k^n = y_n$ in a free semigroup. Trans. Am. Math. Soc. **134**(3), 461–470 (1968)
2. Barbin-Le Rest, E., Le Rest, M.: Sur la combinatoire des codes à deux mots. Theor. Comput. Sci. **41**, 61–80 (1985)
3. Karel Culik, I.I., Karhumäki, J.: On the equality sets for homomorphisms on free monoids with two generators. RAIRO ITA **14**(4), 349–369 (1980)
4. Czeizler, E., Holub, Š., Karhumäki, J., Laine, M.: Intricacies of simple word equations: an example. Internat. J. Found. Comput. Sci. **18**(6), 1167–1175 (2007)
5. Day, J.D., Reidenbach, D., Schneider, J.C.: On the dual post correspondence problem. Int. J. Found. Comput. Sci. **25**(8), 1033–1048 (2014)
6. Day, J.D., Reidenbach, D., Schneider, J.C.: Periodicity forcing words. Theor. Comput. Sci. **601**, 2–14 (2015)
7. Ehrenfeucht, A., Karhumäki, J., Rozenberg, G.: On binary equality sets and a solution to the test set conjecture in the binary case. J. Algebra **85**(1), 76–85 (1983)
8. Hadravová, J.: A length bound for binary equality words. Commentat. Math. Univ. Carol. **52**(1), 1–20 (2011)
9. Hadravová, J.: Structure of equality sets. Ph.D. thesis, Charles University, Prague (2015)
10. Hadravová, J., Holub, Š.: Large simple binary equality words. Int. J. Found. Comput. Sci. **23**(06), 1385–1403 (2012)
11. Hadravová, J., Holub, Š.: Equation $x^i y^j x^k = u^i v^j u^k$ in Words. In: Dediu, A.-H., Formenti, E., Martín-Vide, C., Truthe, B. (eds.) LATA 2015. LNCS, vol. 8977, pp. 414–423. Springer, Cham (2015). doi:10.1007/978-3-319-15579-1_32
12. Hakala, I., Kortelainen, J.: On the system of word equations $x_1^i x_2^i \ldots x_m^i = y_1^i y_2^i \ldots y_n^i (i = 1, 2, \ldots)$ in a free monoid. Acta Informatica **34**(3), 217–230 (1997)
13. Halava, V., Holub, Š.: Binary (generalized) post correspondence problem is in P. Technical report 785, Turku Centre for Computer Science (2006)
14. Harju, T., Nowotka, D.: The equation $x^i = y^j z^k$ in a free semigroup. Semigroup Forum **68**(3), 488–490 (2004)

15. Harju, T., Nowotka, D.: On the equation $x^k = z_1^{k_1} z_2^{k_2} \cdots z_n^{k_n}$ in a free semigroup. Theor. Comput. Sci. **330**(1), 117–121 (2005)
16. Holub, Š.: Local and global cyclicity in free semigroups. Theor. Comput. Sci. **262**(1), 25–36 (2001)
17. Holub, Š.: A unique structure of two-generated binary equality sets. In: Ito, M., Toyama, M. (eds.) DLT 2002. LNCS, vol. 2450, pp. 245–257. Springer, Heidelberg (2003). doi:10.1007/3-540-45005-X_21
18. Holub, Š., Kortelainen, J.: Linear size test sets for certain commutative languages. Theor. Inform. Appl. **35**(5), 453–475 (2001)
19. Lentin, A., Schützenberger, M.-P.: A combinatorial problem in the theory of free monoids. In: Algebraic Theory of Semigroups. North-Holland Pub. Co., Amsterdam, New York (1979)
20. Lyndon, R.C., Schützenberger, M.-P.: The equation $a^m = b^n c^p$ in a free group. Michigan Math. J. **9**(4), 289–298 (1962)
21. Saarela, A.: Word equations where a power equals a product of powers. In: STACS: Leibniz International Proceedings in Informatics, vol. 66, pp. 55:1–55:9. Dagstuhl, Germany (2017)
22. Spehner, J.-P.: Quelques problèmes d'extension, de conjugaison et de presentation des sous-monoïdes d'un monoïde libre. PhD thesis, Université Paris VII, Paris (1976)