Simple equations on binary factorial languages ⋆

A. E. Frid [a]

[a] *Sobolev Institute of Mathematics SB RAS*
Koptyug av., 4, 630090 Novosibirsk, Russia
E-mail: frid@math.nsc.ru

Abstract

We consider equations on the monoid of factorial languages on the binary alphabet. We use the notion of a canonical decomposition of a factorial language and previous results by Avgustinovich and the author to solve several simple equations on binary factorial languages including $X^n = Y^n$, the commutation equation $XY = YX$ and the conjugacy equation $XZ = ZY$. At the end of the paper we discuss the difficulties hindering to reduce equations on factorial languages to equations on words and to enlarge the alphabet considered.

Key words: language equations, commutation, conjugacy, catenation of languages, monoid of factorial languages, canonical decompositions

1 Introduction

Language equations constitute an extensively developing and very non-trivial area. Their behavior shows impressive differences with that of word equations and is much more complicated [11]. Even if we restrict ourselves to single equations involving as an operation only the catenation, many intricate effects appear.

As an example consider the commutation equation. On words, it is easy to completely solve it: if x and y are finite words, we have $xy = yx$ if and only if $x = z^n$ and $y = z^m$ for some word z and some non-negative integers n and m.

⋆ Supported in part by RFBR grant 06-01-00694.

However, on languages, the commutation equation becomes very difficult to solve. In particular, much attention has been paid to the *centralizer* of a language, that is the maximal language commuting with it: the centralizer always exists since the set of languages commuting with a given one is closed under union. Conway [4] conjectured in 1971 that the centralizer of a rational language is rational. However, this conjecture was disproved by Kunc [10] in a very strong sense: the centralizer of a finite language can be not recursively enumerable. At the same time, positive partial results for prefix codes [13], codes [8] and languages with at most three elements [9] are known.

In this paper we consider three simple equations on binary *factorial* languages. A language is called factorial if it contains all factors of each of its elements. The study of the monoid of factorial languages was started by S. V. Avgustinovich and the author in [1] where a theorem of existence and uniqueness of a *canonical* decomposition of a factorial language was proved. Note that no similar result is possible for languages in general [14].

Then we showed that languages occurring in the canonical decomposition of a regular factorial language are always regular [2] and investigated possible forms of the canonical decomposition of the catenation of languages [6]. This latter result allowed to develop a technique for solving some simple equations on binary factorial languages, and that is what we do in this paper. Problems arising when we try to consider languages on a larger alphabet or solve longer equations are described in the last section of this paper.

The results concerning commutation have been reported at DLT 2007 [7]. The results on the first equation, $X^n = Y^n$, and conjugacy, are new.

2 Canonical decompositions

Let Σ be a finite alphabet. A *language* is an arbitrary subset of the set Σ^* of all finite words on Σ. The empty word is denoted by λ.

A word v is called a *factor* of a word u if $u = svt$ for some words s and t (which can be empty). In particular, λ is a factor of any word. The *factorial closure* $\mathrm{Fac}(X)$ of a language X is the set of all factors of all its elements. Clearly, $\mathrm{Fac}(X) \supseteq X$. If $\mathrm{Fac}(X) = X$, that is, if X is closed under taking factors, we say that X is a *factorial* language.

Typical examples of factorial languages include the set of factors of a finite or infinite word; the set of words avoiding a pattern, etc. Clearly, the factorial closure of an arbitrary language is a factorial language; if the initial language is regular, so is its factorial closure. The family of factorial languages is closed under taking union, intersection and catenation; here the catenation of languages is defined naturally as $X_1X_2 = \{u_1u_2|u_1 \in X_1, u_2 \in X_2\}$. Factorial languages equipped with catenation constitute a submonoid of the monoid of all languages, and its unit is the language $\{\lambda\}$. We are interested in properties of this submonoid.

A factorial language X is called *indecomposable* if $X = X_1X_2$ implies $X = X_1$ or $X = X_2$ for any factorial X_1 and X_2. In particular, we have the following

Lemma 1 *[1] For each alphabet Σ, the language Σ^* is indecomposable.*

Other examples of indecomposable languages include $a^* + b^*$ with $a, b \in \Sigma$, and languages of factors of any recurrent infinite word. (Here and below (+) denotes the union of languages.)

A decomposition $X = X_1 \cdots X_k$ of a factorial language X not equal to $\{\lambda\}$ to catenation of factorial languages is called *minimal* if $X_i \neq \{\lambda\}$ for all i and $X \neq X_1 \cdots X_{i-1}X'_iX_{i+1} \cdots X_k$ for any factorial language $X'_i \subset X_i$. A minimal decomposition to indecomposable languages is called *canonical*. For the sake of completeness, we define the canonical decomposition of $\{\lambda\}$ in a trivial way: $\{\lambda\} = \{\lambda\}$.

The following theorem is the starting point of our technique.

Theorem 1 *[1] For each factorial language X, a canonical decomposition exists and is unique.*

Example 1 If X is indecomposable, its canonical decomposition is just $X = X$. The canonical decomposition of the language $a^*b^* + b^*a^*$ is $(a^* + b^*)(a^* + b^*)$.

In what follows, the canonical decomposition of a factorial language X is denoted by $\overline{X}$. A canonical decomposition can be interpreted as a word on the infinite alphabet $\mathcal{F}$ of all indecomposable factorial languages (although not all words on that alphabet are allowable canonical decompositions). We write $\overline{X_1} \doteq \overline{X_2}$ to mark that the canonical decompositions are equal and in general will overline variables when they denote words on $\mathcal{F}$. Clearly, $\overline{X_1} \doteq \overline{X_2}$ if and only if $X_1 = X_2$, and this is our main tool.

We should also know what happens to the canonical decomposition when we catenate languages: given $\overline{X_1}$ and $\overline{X_2}$, how can we describe $\overline{X_1X_2}$? The answer has been described in [6], and in the next section we give it among other properties of canonical decompositions.

3 Preliminary facts

First of all, let us observe the following easy fact.

Lemma 2 *Let X, Y, Z, W be factorial languages satisfying $Z \subset X$ and $W \subset Y$. Then $ZW \subset XY$.*

Proof. The unstrict inclusion is clear; to see the strict one, consider words $x \in X \backslash Z$ and $y \in Y \backslash W$. Then $xy \in XY \backslash ZW$ since the longest prefix of xy belonging to Z is shorter than x and the longest suffix of xy belonging to W is shorter than y. □

For a factorial language X, we define the subalphabets

$$\Pi(X) = \{x \in \Sigma | Xx \subset X\} \text{ and } \Delta(X) = \{x \in \Sigma | xX \subset X\}.$$

So, $\Pi(X)$ is defined as the greatest subalphabet such that each word from X can be extended to the right by any letter of $\Pi(X)$; and $\Delta(X)$ is defined symmetrically in the left direction.

Remark 1 If $\Pi(X) = \Sigma$ or $\Delta(X) = \Sigma$, then clearly $X = \Sigma^*$. If Σ is the binary alphabet, $\Sigma = \{a, b\}$, this implies that Π and Δ of any language not equal to Σ^* can be equal to $\{a\}, \{b\}$, or $\emptyset$.

Example 2 If $X = a^*b^*$, then $\Delta(X) = \{a\}$ and $\Pi(X) = \{b\}$. If $X = a^* + b^*$, then $\Delta(X) = \Pi(X) = \emptyset$. We also have $\Delta(X) = \Pi(X) = \emptyset$ for each finite language X.

Lemma 3 *[6] If $\overline{X} \doteq \overline{Y} \cdots \overline{Z}$, $\overline{Y}, \overline{Z} \in \mathcal{F}^+$, then $\Pi(X) = \Pi(Z)$ and $\Delta(X) = \Delta(Y)$.*

Now, given a factorial language X and a subalphabet Δ, let the operators L and R on factorial languages be defined by

$$L_\Delta(X) = \mathrm{Fac}(X \backslash \Delta X) \text{ and } R_\Delta(X) = \mathrm{Fac}(X \backslash X\Delta).$$

The meaning of these sets is described by the following lemma.

Lemma 4 *[6] For factorial languages X and Y we have $R_{\Delta(Y)}(X)Y = XY$, and $R_{\Delta(Y)}(X)$ is the minimal factorial set with this property: it is equal to the intersection of all factorial languages Z such that $ZY = XY$. Symmetrically, $YL_{\Pi(Y)}(X) = YX$, and $L_{\Pi(Y)}(X)$ is the minimal factorial language with this property.*

Note that $Y = \Sigma^*$ implies that $XY = Y$ for all X, and $\Delta(Y) = \emptyset$ implies that for all X, the minimal language giving XY when catenated with Y is X itself. So, in the binary case the situation is non-trivial only if $\Delta(Y) = \{x\}$ for some symbol x. In what follows we write R_x and L_x instead of $R_{\{x\}}$ and $L_{\{x\}}$ for a symbol $x \in \Sigma$.

Let us list several staightforward properties of the operators L and R.

Lemma 5 *Let X be a binary factorial language on $\Sigma = \{a, b\}$. Then for any symbol $x \in \Sigma$ we have $\{\lambda\} = L_\Sigma(X) \subseteq L_x(X) \subseteq L_\emptyset(X) = X$ and $\{\lambda\} = R_\Sigma(X) \subseteq R_x(X) \subseteq R_\emptyset(X) = X$.* □

Lemma 6 *For all factorial languages $X \subseteq \Sigma^*$ and subalphabets $\Delta \subseteq \Sigma$ the equality $R_\Delta(R_\Delta(X)) = R_\Delta(X)$ holds.* □

Lemma 7 *Let Y be a factorial language with $Y = R_\Delta(Y)$ ($Y = L_\Pi(Y)$) for a given $\Delta, \Pi \subset \Sigma$. Then $Y = R_\Delta(X)$ ($Y = L_\Pi(X)$) for a factorial language X if and only if we have $Y \subseteq X \subseteq Y\Delta^*$ (respectively, $Y \subseteq X \subseteq \Pi^* Y$).*

Lemma 8 *[6] Let X be a factorial language with $\overline{X} \doteq X_1 \cdots X_k$, $X_i \in \mathcal{F}$, and $\Delta(X) = \{x\}$. Then*

$$\overline{L_x(X)} \doteq \begin{cases} X_2 \cdots X_k, & \textit{if } X_1 = x^*, \\ \overline{X}, & \textit{otherwise.} \end{cases}$$

The symmetric statement for $\Pi(X)$ and X_k also holds.

The following lemma is a corollary of Lemmas 2 and 4.

Lemma 9 *[6] For all factorial languages X and Y, the canonical decomposition of XY is either $\overline{XY} \doteq \overline{R_{\Delta(Y}(X)}\ \overline{Y}$ or $\overline{XY} \doteq \overline{X}\ \overline{L_{\Pi(X)}(Y)}$. If $R_{\Delta(Y)}(X) \neq X$, the first equality holds, and if $L_{\Pi(X)}(Y) \neq Y$, the second equality holds.*

Example 3 If $X = a^*b^*$ and $Y = b^*a^*$, then $\Pi(X) = \Delta(Y) = \{b\}$ and $\overline{XY} = a^*b^*a^*$; here both equalities from Lemma 9 hold since it does not matter which of the b^*s was erased according to Lemma 8.

Example 4 Let us consider $F_a = \mathrm{Fac}(\{a, ab\}^*)$, which means that F_a is the language of all binary words which do not contain two successive bs. Then F_a is indecomposable, $\Pi(F_a) = \Delta(F_a) = \{a\}$, and $L_a(F_a) = R_a(F_a) = F_a$, so that $\overline{F_aF_a} \doteq \overline{F_a}\ \overline{F_a}$, which is consistent with Lemma 8. Here F_aF_a is the language of all words containing the factor bb at most once.

Lemma 10 *[6] Let X be a factorial language with $\overline{X} \doteq X_1 \cdots X_m$, $X_i \in \mathcal{F}$. Consider a subalphabet $\Delta \subset \Sigma$ and the factorial language $Y = R_\Delta(X)$. Then* *the canonical decomposition* $\overline{Y} \doteq Y_1 \cdots Y_n$, $Y_j \in \mathcal{F}$, *is obtained by deleting* $\{\lambda\}$ *entries from the decomposition* $\overline{U_1} \cdots \overline{U_m}$, *where* $\overline{U_i} \in \mathcal{F}^*$ *and subalphabets* $\Delta_i \subseteq \Sigma$ *are defined iteratively as follows:* $\Delta_m = \Delta$, *and for each* i *from* m *to* 1 *we put*

$$U_i = R_{\Delta_i}(X_i) \text{ and } \Delta_{i-1} = \Delta(U_i), \text{ if } X_i \not\subseteq \Delta_i^*,$$
$$U_i = \{\lambda\} \text{ and } \Delta_{i-1} = \Delta_i, \text{ otherwise.}$$

In other terms, there exist integers $0 = i_0 \leq \ldots \leq i_{m-1} \leq i_m = n$ *such that* $Y_{i_{k-1}+1} \cdots Y_{i_k} \subseteq X_k$ *for all* $k = 1, \ldots, m$. *More precisely, for each* $k < m$ *we have* $Y_1 \cdots Y_{i_k} = R_{\Delta(Y_{i_k+1})}(X_1 \cdots X_k)$ *and* $Y_{i_k+1} \cdots Y_n = R_\Delta(X_{k+1} \cdots X_m)$.

Note that in the binary case, the described situation can be non-trivial only if Δ is of cardinality one, and U_i may be not equal to X_i only if $\Delta_i \neq \Delta(X_{i+1})$, which means that we had $\Delta(X_{i+1}) = \emptyset$.

Example 5 Consider $X = (a^* + b^*)^{2k}$ and $\Delta = \{a\}$. Then $U_{2k} = R_a(a^* + b^*) = b^*$, $\Delta_{2k-1} = \{b\}$, $U_{2k-1} = R_b(a^* + b^*) = a^*$, $\Delta_{2k-2} = \{a\}$, etc., so that we have $\overline{R_a(X)} \doteq (a^* b^*)^k$. Consequently, $\overline{X a^*} \doteq (a^* b^*)^k a^*$.

The following several lemmas are also important tools of our technique.

Lemma 11 *Let* Δ *be a subalphabet and* X *and* Y *be factorial languages with* $Y = R_\Delta(X)$, $Y \neq \{\lambda\}$. *Then* $\Delta(Y) \supseteq \Delta(X)$.

PROOF. We shall consider a symbol $d \in \Delta(X)$ and prove that $d \in \Delta(Y)$. Let $u \in Y$ be a non-empty word from Y: it exists since $Y \neq \{\lambda\}$. The equality $Y = R_\Delta(X)$ means that $uv \in X$ for some word v such that the last symbol of uv is not from Δ. By the definition of $\Delta(X)$, we have $duv \in X$. Since the last symbol of duv is not from Δ, we see that $du \in R_\Delta(X) = Y$.

The word u was chosen as an arbitrary non-empty element of Y; for $u = \lambda$, we have $du = d \in Y$ since Y is factorial and non-empty words starting from d occur in it. So, $du \in Y$ for all $u \in Y$, which means that $d \in \Delta(Y)$. □

The next lemma is valid only for the binary alphabet, and this is the main reason why our technique does not work for greater alphabets.

Lemma 12 *Let* X *be a binary factorial language with* $\#\Delta(X) = 1$. *Consider the language* $Y = R_x(X)$ *for some* $x \in \{a, b\}$. *If* $Y \neq \{\lambda\}$, *then* $\Delta(Y) = \Delta(X)$.

PROOF. By the previous lemma, we have $\Delta(Y) \supseteq \Delta(X)$; but $\Delta(Y) \supset \Delta(X)$ would mean that $\Delta(Y) = \{a, b\}$, which is possible only if $Y = \{a, b\}^*$. This is impossible since $Y \subseteq X$ and $X \neq \{a, b\}^*$. □

The following lemma is non-trivial in the binary case only when Δ and Π are of cardinality one, but we just prove it for the general case.

Lemma 13 *Let X be a factorial language. Then for all subalphabets $\Delta, \Pi \subset \Sigma$ the equality $L_\Pi(R_\Delta(X)) = R_\Delta(L_\Pi(X))$ holds.*

PROOF. If a non-empty word u belongs to $L_\Pi(R_\Delta(X))$, then there exists v (which can be empty) such that vu starts with a symbol from $\Sigma\backslash\Pi$ and belongs to $R_\Delta(X)$. This, in its turn, means that there exists a word w (which can be empty) such that the last symbol of the word vuw belongs to $\Sigma\backslash\Delta$, and $vuw \in X$.

We see that the obtained condition is symmetric with respect to the order of applying the operators L_Π and R_Δ, so, we get it another time if we consider an arbitrary word $u \in R_\Delta(L_\Pi(X))$. Thus, these two sets are equal. $\square$

Lemma 14 *Suppose that $Y = R_\Delta(X)$ (or $Y = L_\Delta(X)$) for some $\Delta \subset \Sigma$, $\overline{X} \doteq X_1 \cdots X_n$, $X_i \in \mathcal{F}$, and $\overline{Y} \doteq X_{\sigma(1)} \cdots X_{\sigma(n)}$ for some permutation σ. Then $X = Y$.*

PROOF. The assertion of the lemma means that each indecomposable factorial language occurs in the canonical decompositions of X and Y an equal number of times.

For the sake of convenience, let us denote $X_{\sigma(i)} = Y_i$. Due to Lemma 10, there exist integers $0 = i_0 \le \ldots \le i_{n-1} \le i_n = n$ such that $Y_{i_{k-1}+1} \cdots Y_{i_k} \subseteq X_k$ for all $k = 1, \ldots, n$. We wish to prove that $i_k = k$ for all k, and all the inclusions are in fact equalities (of the form $Y_i = X_i$).

Suppose the opposite. Then there exists some k_1 such that the corresponding inclusion is of the form $Y_{i_{k_1-1}+1} \cdots Y_{i_{k_1}} \subset X_{k_1}$ (the equality is impossible even if $i_{k_1} - i_{k_1-1} \ge 2$, since all the involved languages are indecomposable, and decompositions are minimal). In particular, none of the languages $Y_{i_{k_1-1}+1}, \ldots, Y_{i_{k_1}}$ is equal to X_{k_1}. But we know that the language X_{k_1} occurs in $\overline{X}$ and $\overline{Y}$ an equal number of times. So, X_{k_1} is equal to some Y_j, where $i_{k_2-1} + 1 \le j \le i_{k_2}$, and $X_{k_1} = Y_j \subset X_{k_2}$. Continuing this argument, we get an infinite sequence $X_{k_1} \subset X_{k_2} \subset \cdots \subset X_{k_m} \subset \cdots$. But there is only a finite number of entries in the canonical decomposition of a factorial language. A contradiction. $\square$

4 Simple Word Equations

Here we list several classical word equations and their solutions. Words are considered on an alphabet $\mathcal{A}$ which may be infinite since all considered words are finite anyway.

Lemma 15 (Commutation of words, see e.g. [12]) *Let words $x, y \in \mathcal{A}^*$ commute: $xy = yx$. Then $x = z^n$ and $y = z^m$ for some $z \in \mathcal{A}^*$ and $n, m \geq 0$.* □

Lemma 16 (Conjugacy of words, see, e. g., [5]) *Let $xz = zy$ for some $x, y, z \in \mathcal{A}^*$. Then either $x = y = \lambda$, or $z = \lambda$, or $x = rs$, $y = sr$, and $z = (rs)^k r$ for some $r, s \in \mathcal{A}^*$ with $r \neq \lambda$ and $k \geq 0$.* □

At last, the following lemma can be easily proved by a standard technique described, e. g., in [5].

Lemma 17 *Let $xay = yax$ for some $x, y \in \mathcal{A}^*$, $a \in \mathcal{A}$. Then $x = (za)^n z$ and $y = (za)^m z$ for some $z \in \mathcal{A}^*$ and $n, m \geq 0$.* □

5 Unary factorial languages

Before we pass to the main part of the paper, note that equations on unary factorial languages are in general easy to solve. Indeed, if the alphabet consists of one symbol a, then all possible factorial languages are a^* and $a^{\leq k} = \{a^i | 0 \leq i \leq k\}$ for all $k \geq 0$. We have $a^{\leq k} a^{\leq m} = a^{\leq (k+m)}$ and $a^* a^{\leq k} = a^{\leq k} a^* = a^*$ for all k and m. Thus, unary factorial languages equipped with catenation are equivalent to non-negative integers and infinity under addition, that is, to the Presburger arithmetic with infinity, which is decidable.

In particular, we easily see that $(a^{\leq k})^n = a^{\leq kn}$ and $(a^*)^n = a^*$, so that for unary factorial languages $X^n = Y^n$ if and only if $X = Y$; any two unary factorial languages commute; and $XZ = ZY$ if and only if $Z = a^*$ or $X = Y$.

So, from now on we may assume that both symbols do occur in at least one of the languages constituting the considered equations.

6 The equation $X^n = Y^n$

In general, the equality $X^n = Y^n$ for languages X and Y does not imply that $X = Y$: moreover, we may have $X \neq Y$ even for unary finite languages such that $X^2 = Y^2$ [3]. However, it cannot happen to factorial languages:

Theorem 2 *Let X and Y be factorial languages. Then for all $n \geq 2$ we have $X^n = Y^n$ if and only if $X = Y$.*

We shall give two proofs of this theorem: the first one is easy and is valid for an arbitrary alphabet, and the second one is longer and less general but uses the same technique that works for the other equations considered.

Proof 1 (S. V. Avgustinovich). Suppose that $X^n = Y^n$ but $X \neq Y$; then without loss of generality there exists a word $x \in X\backslash Y$. Then $x^n \in X^n = Y^n$; now consider all prefixes of x^n belonging to Y. The longest of them, denoted by y_1, is shorter than x: otherwise we would have $x \in Y$ since Y is factorial. So, $x = y_1 z_1$ for $z_1 \neq \lambda$, and $z_1 x^{n-1}$ belongs to Y^{n-1} which is a factorial language. Similarly, we see that the longest prefix y_2 of $z_1 x^{n-1}$ belonging to Y is shorter than $z_1 x$: $z_1 x = y_1 z_2$ for $z_2 \neq \lambda$ and $z_2 x^{n-2} \in Y^{n-2}$, etc.; at last we obtain that $z_{n-1} x \in Y$ and thus $x \in Y$, a contradiction. □

Proof 2. This proof is valid only if the alphabet Σ is binary, $\Sigma = \{a, b\}$. First of all, since $\{a, b\}^*$ is indecomposable, we have $X^n = \{a, b\}^*$ if and only if $X = \{a, b\}^*$. So, it remains to list all the possible forms of $\overline{X^n}$ and $\overline{Y^n}$ when $\Pi(X)$, $\Delta(X)$, $\Pi(Y)$, $\Delta(Y)$ are of cardinality 1 or empty. In fact, due to Lemma 9, the cases to be considered are: $\overline{XX} = \overline{X}\ \overline{X}$; or $\overline{XX} = \overline{X'}\ \overline{X}$, where $X' = R_x(X) \subset X$, $\#\Delta(X) = 1$; or $\overline{XX} = \overline{X}\ \overline{X''}$, where $X'' = L_x(X) \subset X$, $\#\Pi(X) = 1$; and these three cases may arbitrarily combine with the three analogous situations for $\overline{YY}$. Some of the combinations are symmetric to each other, so that the case study is not too long.

The equality $\overline{XX} = \overline{X}\ \overline{X}$ due to Lemma 9 implies that $X = R_{\Delta(X)}(X) = L_{\Pi(X)}(X)$. By Lemma 3, we have $\Pi(X^2) = \Pi(X)$. Again using Lemma 9, we see that $\overline{X^3} \doteq \overline{R_{\Delta(X)}(X^2)}\overline{X}$ or $\overline{X^3} \doteq \overline{X^2}\,\overline{L_{\Pi(X^2)}(X)}$. In the first case, we due to Lemma 10 have $\overline{R_{\Delta(X)}(X^2)} \doteq \overline{R_{\Delta(R_{\Delta(X)}(X))}(X)}\ \overline{R_{\Delta(X)}(X)} \doteq \overline{R_{\Delta(X)}(X)}\overline{X} \doteq \overline{X}\ \overline{X}$; in the second case, we have $\overline{L_{\Pi(X^2)}(X)} \doteq \overline{L_{\Pi(X)}(X)} \doteq \overline{X}$. So, in any of the cases we see that $\overline{X^3} \doteq \overline{X}^3$. Continuing by induction, we see that $\overline{X^n} \doteq \overline{X}^n$.

If the equality $\overline{XX} = \overline{X'}\ \overline{X}$ holds, where $X' = R_x(X) \subset X$, then $\Delta(X) = \{x\}$ for some symbol x. If $X = x^*$, this is the case of the unary alphabet considered in the previous section. So, we may assume that X contains both letters; thus, $X' \neq \{\lambda\}$ and $\Delta(X') = \{x\}$ due to Lemma 12. Due to Lemma 4, $\Delta(X^2) = \Delta(X') = \{x\}$. Now we see that $\overline{X^3} \doteq \overline{R_x(X)}\ \overline{XX} \doteq \overline{X'}\ \overline{X'}\ \overline{X}$ due to Lemma 9. Continuing by induction, we obtain that $\overline{X^n} \doteq (\overline{X'})^{n-1}\overline{X}$ for all $n > 0$. Symmetrically, if $\overline{XX} = \overline{X}\ \overline{X''}$, then $\overline{X^n} \doteq \overline{X}(\overline{X''})^{n-1}$ for all $n > 0$.

Case 1. If the equality $X^n = Y^n$ is rewritten for the canonical decompositions as $\overline{X}^n \doteq \overline{Y}^n$, then clearly $X = Y$.

Case 2. Let only one of the canonical decompositions $\overline{X^n}$ and $\overline{Y^n}$ be not equal to $(\overline{X})^n$ (or $(\overline{Y})^n$), say, let the equation for canonical decompositions be

$$(\overline{X'})^{n-1}\overline{X} \doteq \overline{Y}^n \tag{1}$$

with $\Delta(X) = \{x\} = \Delta(X')$ and $X' = R_x(X)$. Note that due to the arguments above, equations analogous to (1) are valid for all degrees $n > 0$, not only for the fixed degree of the equation. Due to Lemma 3 applied to both sides of (1), we have $\Delta(Y) = \Delta(X') = \{x\}$. Since $\overline{YY} \doteq \overline{Y}\ \overline{Y}$, we see that Y does not change when we apply x to it from the right: $R_x(Y) = Y$. Note also that $\overline{R_x(X^n)} \doteq \overline{X'}^n$ as we can see from (1) (written for the degree $n+1$ instead of n) and Lemma 9. So, applying R_x to both parts of Equation (1), we obtain $(\overline{X'})^n \doteq \overline{Y}^n$ and thus clearly $X' = Y$. Substituting this to (1), we see that $X = Y = X'$, contradicting to the assumption that $X' \neq X$.

Case 3. Let the canonical decompositions of X^n and Y^n be biased in the same direction, say, let the equation for the canonical decompositions be

$$(\overline{X'})^{n-1}\overline{X} \doteq (\overline{Y'})^{n-1}\overline{Y} \tag{2}$$

with $X' \neq X$ and $Y' \neq Y$; clearly, on the binary alphabet it is possible only when $\Delta(X)$ and $\Delta(Y)$ are of cardinality 1. As above, after excluding the unary case, we use Lemma 12 to get $\Delta(X) = \Delta(X')$ and $\Delta(Y) = \Delta(Y')$; and also analogously to the previous case, we have $\Delta(X') = \Delta(Y')$ due to Lemma 3, so that $\Delta(X) = \Delta(Y) = \{x\}$ for some $x \in \{a, b\}$. Applying R_x to (2) as above, we obtain the "word" equation $(\overline{X'})^n \doteq (\overline{Y'})^n$ whose only solution is $X' = Y'$. Substituting it to (2), we obtain $X = Y$, which is what we needed.

Case 4. Let the canonical decompositions of X^n and Y^n be biased in opposite directions, that is, let the equation for the canonical decompositions be

$$(\overline{X'})^{n-1}\overline{X} \doteq \overline{Y}(\overline{Y''})^{n-1}. \tag{3}$$

Here $\Delta(X)$ and $\Pi(Y)$ cannot be empty since they change X and Y respectively; so, we have $\Delta(X) = \Delta(X') = \{x\}$ and $\Pi(Y) = \Pi(Y'') = \{y\}$ for $x, y \in \{a, b\}$. As usual, $X' = R_x(X)$ and $Y'' = L_y(Y)$. Let us apply to both parts of (3) the operators R_x and L_y: due to Lemma 13, the order of applying does not matter. We have $R_x((X')^{n-1}X) \doteq (\overline{X'})^n$ and $\Delta(X') = \{x\}$.

Suppose first that $x \neq y$, then X' does not change under L_y, and $L_y((X')^n) = (\overline{X'})^n$. Symmetrically, in this case we have $R_x(L_y(Y(Y'')^{n-1})) \doteq (\overline{Y''})^n$; since these canonical decompositions are equal, this means $X' = Y''$. Returning to (3), we see that $\overline{X}$ and $\overline{Y''} \doteq \overline{X'}$ are both suffixes of $\overline{X^n}$; clearly, $X \supset X'$, that is, the suffix corresponding to $\overline{X}$ is longer: $\overline{X} \doteq \overline{W}\ \overline{X'}$ for some $\overline{W} \in \mathcal{F}^*$. So, $R_x(X) = X' = R_x(WX')$, but due to Lemma 10, $\overline{R_x(WX')} \doteq \overline{W'}\ \overline{R_x(X')}$ for some W', and due to Lemma 6, $R_x(X') = X'$, so that $W' = \{\lambda\}$. Here $W' = R_{\Delta(X')}(W) = R_x(W)$; at the same time, we know that $\overline{W}\ \overline{X'} \doteq \overline{X}$, which means that $W' = R_{\Delta(X')}(W) = W$. So, $W = \{\lambda\}$ and $X' = X$, contradicting to our assumption.

Now suppose that $x = y$. If X' does not change under L_x and Y'' does not change under R_x, we repeat the arguments above and obtain a contradiction. Suppose that X' changes under L_x; due to Lemma 8, this is possible only if $X' \doteq x^*\overline{X''}$ for some $X'' = L_x(X')$. Then $L_x((X')^n) = (\overline{X''}x^*)^{n-1}\overline{X''}$; we see that the number of elements of $\mathcal{F}$ in this canonical decomposition modulo n is equal to $n-1$, so that we cannot have $R_x(L_x(Y(Y'')^{n-1})) \doteq (\overline{Y''})^n$. Thus, Y'' must change under R_x, $\overline{Y''} \doteq \overline{Y'''}x^*$. So, after applying R_x and L_x to both parts of (3) we obtain

$$(\overline{X''}x^*)^{n-1}\overline{X''} \doteq (\overline{Y'''}x^*)^{n-1}\overline{Y'''}$$

and thus $X'' = Y'''$. Denote that language by Z; then $\overline{X'} \doteq x^*\overline{Z}$ and $\overline{Y''} \doteq \overline{Z}x^*$, and (3) can be rewritten as $(x^*\overline{Z})^{n-1}\overline{X} \doteq \overline{Y}(\overline{Z}x^*)^{n-1}$. We see that $\overline{X}$ ends with x^*, which means that $\overline{X} \doteq \overline{R_x(X)}x^* \doteq \overline{X'}x^* \doteq x^*\overline{Z}x^*$. Symmetrically, we obtain $\overline{Y} \doteq x^*\overline{Z}x^*$, that is, $X = Y$, which was to be proved.

We have listed all the cases and thus proved the theorem. □

Of course this second proof is much more complicated and less general than the first one, but its technique works also for other equations on binary factorial languages, and we show it in the subsequent sections.

7 Commutation

In this section, we completely solve the equation $XY = YX$, where X and Y are binary factorial languages.

Clearly, if factorial languages (in fact, languages in general) are powers of the same language, they commute. We call it word type commutation:

Word type commutation: $XY = YX$ if $X = Z^m$ and $Y = Z^n$ for some factorial language Z and non-negative integers n and m.

However, it is easy to see that binary factorial languages may commute also in other situations. The simplest of them is absorption:

Commutation by absorption: Let Σ_X be the subalphabet of all letters occurring in a factorial language X. Then $XY = YX = Y$ if $Y\Sigma_X \subseteq Y$, $\Sigma_X Y \subseteq Y$, and thus $Y = Y\Sigma_X^* = \Sigma_X^* Y$: the language Y *absorbs* X.

In the binary case, absorption means that either $X = \{\lambda\}$, or $X \subseteq x^*$ for some letter x and $\Pi(Y) = \Delta(Y) = \{x\}$, or $Y = \{a, b\}^*$.

There are also less obvious examples of commutation. Let us list them:

Unexpected commutation I. Let Z be a binary factorial language with $\Delta(Z) = \{x\}$ and $\Pi(Z) = \{y\}$, $x \neq y$. Then for all $r, p > 0$ the language Z^p commutes with any language X satisfying the inclusions

$$Z^r \subseteq X \subseteq Z^r x^* \cap y^* Z^r.$$

Such a language not equal to Z^r exists if and only if there exists a word v such that $yv \in Z^r$, $vx \in Z^r$, but $yvx \notin Z^r$.

Example 6 Consider the languages $F_a = \mathrm{Fac}(\{a, ab\}^*)$ and $F_b = \mathrm{Fac}(\{b, ab\}^*)$: the language F_a contains all words avoiding two successive bs, and the language F_b contains all words avoiding two successive as. Consider $Z = F_b \cdot F_a$; then $\Pi(Z) = \{a\}$ and $\Delta(Z) = \{b\}$. Let us fix $r = 1$. Then any language $X = Z + S$, where S is a factorial subset of a^*b^*, commutes with any power Z^p of Z.

The word v satisfying the condition above is equal to ab since $aab \in Z$, $abb \in Z$, but $aabb \notin Z$.

Unexpected commutation II. Let $x \in \Sigma_2$ be a symbol and Q be a binary factorial language with $L_x(Q) = R_x(Q) = Q$ and $\Delta(Q), \Pi(Q)$ equal to $\emptyset$ or $\{y\}$, $y \neq x$. Then for all $p \geq 0$ and $r \geq 1$ the language $(x^*Q)^p x^*$ commutes with any language X satisfying the inclusions

$$(x^*Q)^r + (Qx^*)^r \subseteq X \subseteq (x^*Q)^r x^*. \tag{4}$$

Example 7 The languages $X = a^*b^* + b^*a^*$ and $Y = a^*$ commute since $XY = YX = a^*b^*a^*$. Here $x = a$ and $Q = b^*$, so, in fact Y commutes with any factorial language which includes $a^*b^* + b^*a^*$ and is included into $a^*b^*a^*$.

The following example based on the same idea is a bit more sophisticated.

Example 8 For each $p, n, m, k \geq 0$, the language $(a^*b^*)^p a^*$ commutes with the language $X = a^*b^*a^*b^*a^{\leq n} + a^{\leq m}b^*a^*b^*a^* + a^*b^*a^{\leq k}b^*a^*$, since $a^*b^*a^*b^* + b^*a^*b^*a^* \subset X \subset a^*b^*a^*b^*a^*$.

Unexpected commutation III. Let Z be a binary factorial language such that $\overline{ZZ} \doteq \overline{Z}\ \overline{Z}$ and $\Delta(Z) = \{x\}$. Let Y be a factorial language satisfying $Z^n \subseteq Y \subseteq Z^n x^*$, $n > 0$. Then Y commutes with $Z^m Y$ for all $m > 0$.

Symmetrically, if Z is a binary factorial language with $\overline{ZZ} \doteq \overline{Z}\ \overline{Z}$ and $\Pi(Z) = \{x\}$, and if Y is a factorial language satisfying $Z^n \subseteq Y \subseteq x^* Z^n$, then Y commutes with YZ^m for all $n, m > 0$.

Example 9 Consider $Z = a^*b^*$ and $Y = \mathrm{Fac}(a^*(bb)^*a^*b^* + a^*b(bb)^*a^*b^*a^*)$. Here $\Delta(Z) = \{a\}$ and $Z^2 = a^*b^*a^*b^* \subset Y \subset a^*b^*a^*b^*a^* = Z^2a^*$. We see that Y commutes with all sets X of the form $X = Z^m Y$: $XY = YX = Z^{m+2}Y$.

The following theorem states that in fact we have listed all possible situations of commutation:

Theorem 3 *Two binary factorial languages commute if and only if one of the situations above is realized: either word type commutation, or absorption, or unexpected commutation I, II, or III.*

Proof. Let $XY = YX$ for binary factorial languages X and Y. Due to Lemma 9, there are only three possibilities of how the equality for canonical decompositions looks like: either

$$\overline{X'} \cdot \overline{Y} \doteq \overline{Y} \cdot \overline{X''}, \tag{5}$$

where $X' = R_{\Delta(Y)}(X)$ and $X'' = L_{\Pi(Y)}(X)$ (or $\overline{X}\ \overline{Y'} \doteq \overline{Y''}\ \overline{X}$, which is the same up to renaming X and Y); or

$$\overline{X'} \cdot \overline{Y} \doteq \overline{Y'} \cdot \overline{X}, \tag{6}$$

where $X' = R_{\Delta(Y)}(X)$ and $Y' = R_{\Delta(X)}(Y)$; or $\overline{X}\ \overline{Y''} \doteq \overline{Y}\ \overline{X''}$, and this case is completely symmetric to (6).

These cases intersect: for example, the situation when $L_{\Pi(Y)}(X) = X$ and $R_{\Delta(X)}(Y) = Y$ falls into both (5) and (6). However, to get a classification of the cases of commutation, we consider the cases (5) and (6) separately.

Suppose first that (5) holds. It is a conjugacy equation on the alphabet $\mathcal{F}$, and it can be solved according to Lemma 16. Since the unit element of the semigroup $\mathcal{F}^*$ is the language $\{\lambda\}$, the equation has the following solutions:

(1) Either $Y = \{\lambda\}$; then $X' = X'' = X$ and this is a particular case of absorption.
(2) Or $X' = X'' = \{\lambda\}$, and this is again absorption, since $XY = YX = Y$.
(3) Or $\overline{X'} \doteq \overline{R}\ \overline{S}$, $\overline{X''} \doteq \overline{S}\ \overline{R}$, and $\overline{Y} \doteq (\overline{R}\ \overline{S})^k \overline{R}$ for some $\overline{R}, \overline{S} \in \mathcal{F}^*$, where $R \neq \{\lambda\}$, $k \geq 0$.

Let us consider this third situation in detail.

Due to Lemma 3 (applied several times), we have

$$\Delta(Y) = \Delta(R) = \Delta(X') \text{ and } \Pi(Y) = \Pi(R) = \Pi(X''); \tag{7}$$

in what follows we denote these subalphabets just by Δ and Π.

Suppose first that one of the subalphabets Δ and Π is empty: say, $\Delta = \emptyset$. Then $\overline{X'} \doteq \overline{R_\emptyset(X)} \doteq \overline{X} \doteq \overline{R}\ \overline{S}$ and $\overline{X''} \doteq \overline{L_\Pi(X)} \doteq \overline{S}\ \overline{R}$; due to Lemma 14, $X'' = X$, and the commutation equation (5) is just $\overline{X}\ \overline{Y} \doteq \overline{Y}\ \overline{X}$. Due to Lemma 15, we have $\overline{X} \doteq \overline{Z}^n$ and $\overline{Y} \doteq \overline{Z}^m$ for some $\overline{Z} \in \mathcal{F}^*$, and this is word type commutation.

Note that if $Y = \{a,b\}^*$, then $X' = X'' = \{\lambda\}$, and this is absorption. So, the only non-trivial situation is $\#\Delta = \#\Pi = 1$, that is, either $\Delta = \{x\}$ and $\Pi = \{y\}$, $y \neq x$, or $\Delta = \Pi = \{x\}$. We shall consider these two situations in succession, but before that, note that in both cases we have

$$L_\Pi(X') = R_\Delta(X'') \tag{8}$$

due to Lemma 13, and $X' + X'' \subseteq X \subseteq X'\Delta^* \cap \Pi^* X''$ by the definitions of $X' = R_\Delta(X)$ and $X'' = L_\Pi(X)$; that is,

$$RS + SR \subseteq X \subseteq RS\Delta^* \cap \Pi^* SR. \tag{9}$$

Suppose first that $\Delta = \{x\}$ and $\Pi = \{y\}$, $x \neq y$. Then it can be easily seen that $L_y(X') = X'$ and $R_x(X'') = X''$. By (8) we see that $X' = X''$, that is, $\overline{R}\ \overline{S} \doteq \overline{S}\ \overline{R}$, and due to Lemma 15, we have $\overline{R} \doteq \overline{Z}^n$ and $\overline{S} \doteq \overline{Z}^m$ for some $\overline{Z} \in \mathcal{F}^+$; here $m \geq 0$ and $n > 0$ since $R \neq \{\lambda\}$. So, $\overline{X'} \doteq \overline{X''} \doteq \overline{Z}^{n+m}$ and $\overline{Y} \doteq \overline{Z}^{k(n+m)+n}$. After renaming variables we can write $\overline{X'} \doteq \overline{X''} \doteq \overline{Z}^r$ and $\overline{Y} \doteq \overline{Z}^p$ for some $r, p > 0$.

Now (9) can be rewritten as

$$Z^r \subseteq X \subseteq Z^r x^* \cap y^* Z^r. \tag{10}$$

It can be easily checked that any language X satisfying (10) commutes with $Y = Z^p$, and this is exactly **Unexpected commutation I** described above. Note that in particular we may have $X = Z^r$ which corresponds to the word-type commutation.

Now suppose that $\Delta = \Pi = \{x\}$. First consider the case when $\overline{R}$ does not start with x^*. Then we have $L_x(X') = L_x(RS) = RS$ due to Lemma 8, and thus $\overline{R}\ \overline{S} \doteq \overline{R_x(SR)}$ due to (8). So, due to Lemma 14 we have $\overline{R}\ \overline{S} \doteq \overline{S}\ \overline{R}$, and due to Lemma 15, $\overline{R}\ \overline{S} \doteq \overline{S}\ \overline{R} \doteq \overline{X'} \doteq \overline{X''} \doteq \overline{Z}^{n+m}$ for some factorial language Z with $\overline{R} \doteq \overline{Z}^n$ and $\overline{S} \doteq \overline{Z}^m$. Now (9) can be rewritten as

$$Z^r \subseteq X \subseteq Z^r x^* \cap x^* Z^r,$$

where $r = n + m$; but in fact, both inclusions here are equalities: $Z^r x^* = x^* Z^r = Z^r$ since $\Delta(Z) = \Delta(R) = \{x\}$ and $\Pi(Z) = \Pi(R) = \{x\}$ due to Lemma 3. So, $\overline{X} \doteq \overline{Z}^r$, $\overline{Y} \doteq (\overline{R}\ \overline{S})^k \overline{R} \doteq \overline{Z}^{kr+n}$, and this is word type commutation. Symmetrically, the same holds if $\overline{R}$ does not end with x^*.

So, anything non-trivial can appear only when $\overline{R} \doteq x^*$ or $\overline{R} \doteq x^* \overline{T} x^*$ for some $\overline{T} \in \mathcal{F}^+$ (note that $T \neq \{\lambda\}$ since $\overline{x^* x^*} \doteq x^*$).

Suppose first that $R = x^*$. Then (9) can be rewritten as

$$x^* S + S x^* \subseteq X \subseteq x^* S x^*. \tag{11}$$

Any language X satisfying these inclusions commutes with all languages of the form $(x^*S)^p x^*$, $p \geq 0$. Here S is an arbitrary language which can precede and follow x^* in a canonical decomposition: that is, an arbitrary language such that $L_x(S) = R_x(S) = S$ and $x \notin \Delta(S), \Pi(S)$ (which means that $\Delta(S)$ and $\Pi(S)$ are equal to $\{y\}$ or to $\emptyset$). Note that if X is the maximal possible, $X = x^*Sx^*$, this is again a word type commutation since $X^k = (x^*Sx^*)^k = (x^*S)^k x^* = Y$. If $X \neq x^*Sx^*$, this is a particular case of Unexpected commutation II.

Now suppose that $\overline{R} \doteq x^*\overline{T}x^*$, $\overline{T} \in \mathcal{F}^+$. Then $\overline{L_x(RS)} \doteq \overline{T}x^*\overline{S}$ and $\overline{R_x(SR)} \doteq \overline{S}x^*\overline{T}$ due to Lemma 8; due to (8), we have the following word equation on $\mathcal{F}^*$:

$$\overline{T}x^*\overline{S} \doteq \overline{S}x^*\overline{T}.$$

Due to Lemma 17, the general solution of this equation is $\overline{S} \doteq (\overline{Q}x^*)^n\overline{Q}$ and $\overline{T} \doteq (\overline{Q}x^*)^m\overline{Q}$ for some $\overline{Q} \in \mathcal{F}^*$ such that $L_x(Q) = R_x(Q) = Q$ and $x \notin \Delta(Q), \Pi(Q)$, and for $n, m \geq 0$. So, $RS = (x^*Q)^{n+m+2}$, $SR = (Qx^*)^{n+m+2}$, and $Y = (x^*Q)^{k(n+m+2)+m+1}x^*$. After renaming variables, we get $RS = (x^*Q)^r$, $SR = (Qx^*)^r$, and $Y = (x^*Q)^p x^*$ for some $r \geq 2$ and $p \geq 1$; and (9) takes the form (4) (with $r \geq 2$ and $p \geq 1$). The cases of $r = 1$ and of $p = 0$ are covered in the previous paragraph (to get the general case of $p = 0$, we must take $\overline{S} \doteq (\overline{Q}x^*)^{r-1}\overline{Q}$ for some Q). So, we get exactly **Unexpected commutation II**.

We have considered all situations possible if (5) holds. Now suppose that (6) holds, that is, the canonical decompositions for the commutation equation $XY = YX$ are $\overline{X'}\,\overline{Y} \doteq \overline{Y'}\,\overline{X}$.

Suppose first that $X' = \{\lambda\}$ or $Y' = \{\lambda\}$. Then $XY = Y$ or $XY = X$, and this is commutation by absorption. So, in what follows we assume that X' and Y' are not equal to $\{\lambda\}$.

Suppose that $\Delta(X) = \emptyset$. Then $\overline{Y'} \doteq \overline{Y}$ due to Lemma 5, and we have $\overline{X'}\,\overline{Y} \doteq \overline{Y}\,\overline{X}$. This case has been considered above (where it has been shown that this is inevitably word type commutation).

Thus we have $\Delta(X) = \{x\}$ and $\Delta(Y) = \{y\}$ for some $x, y \in \{a, b\}$. But $\{y\} = \Delta(Y') = \Delta(XY) = \Delta(X') = \{x\}$ due to Lemmas 12 and 3 since X' and Y' are not equal to $\{\lambda\}$. So, $x = y$. Note that this is the main critical point in this theorem where we require the alphabet to be binary: all the previous arguments in this section could be extended to the general alphabet.

Note that if $X' = Y'$, then $X = Y$, and this is word type commutation. So, we may assume that one of the "words" $\overline{X'}, \overline{Y'}$ on the alphabet $\mathcal{F}$ is a proper prefix of the other: say, $\overline{X'} \doteq \overline{Y'}\,\overline{C}$ for some $\overline{C} \in \mathcal{F}^+$. Then $\overline{X} \doteq \overline{C}\,\overline{Y}$ because of (6), and $\overline{Y'}\,\overline{C} \doteq \overline{X'} \doteq \overline{R_x(X)} \doteq \overline{R_x(CY)} \doteq \overline{C'}\overline{R_x(Y)} \doteq \overline{C'}\,\overline{Y'}$ because of Lemma 10; here $C' = R_x(C)$ since $\Delta(Y') = \Delta(Y) = \{x\}$. Clearly, $C' = C$

since C precedes Y in the canonical decomposition of XY, and $\Delta(Y) = \{x\}$. Thus, we have $\overline{Y'}\,\overline{C} \doteq \overline{C}\,\overline{Y'}$, so that $\overline{Y'} \doteq \overline{Z}^n$, $\overline{C} \doteq \overline{Z}^m$ for some $n, m > 0$ due to Lemma 15. Here Z is an arbitrary factorial language with $\Delta(Z) = \{x\}$ and $\overline{ZZ} \doteq \overline{Z}\,\overline{Z}$.

By the definition of Y', we have $Y' = Z^n \subseteq Y \subseteq Z^n x^*$, and Y can be equal to any set satisfying these inclusions. Note that Y can be not equal to Y' only if $\Pi(Z)$ is equal to $\emptyset$ or $\{z\}$, $z \neq x$.

Now we can just return to $X = Z^m Y$ and observe that X and Y really commute: $XY = YX = Z^{n+m}Y$. So, this is the "right-to-left" version of **Unexpected commutation III**.

The symmetric "left-to-right" version of unexpected commutation III can be found and stated symmetrically starting from the equation $\overline{X}\,\overline{Y''} \doteq \overline{Y}\,\overline{X''}$.

Of course, unexpected commutation III includes some cases of word type commutation: in particular, if $Y = Z^{n-1}D$ for some $Z \subseteq D \subseteq Zx^*$, where $\{x\} = \Delta(Z)$, then $Y = D^n$ and $X = D^{m+n}$. But situations when it is not word type commutation also exist, as Example 9 shows.

We have studied all possible cases when binary factorial languages commute. Theorem 3 is proved. □

8 Conjugacy

The conjugacy equation is $XZ = ZY$, and its solutions on words have been described in Lemma 16. Clearly, for factorial languages, all the "word" solutions are also admitted:

Word type conjugacy: either $X = Y = \{\lambda\}$; or $Z = \{\lambda\}$ and $X = Y$; or $X = RS$, $Y = SR$, $Z = (RS)^k R$ for some $R, S \in \mathcal{F}^*$ such that $R \neq \{\lambda\}$, $k \geq 0$, and if $S \neq \{\lambda\}$, then $\overline{RS} \doteq \overline{R}\,\overline{S}$, $\overline{SR} \doteq \overline{S}\,\overline{R}$, otherwise $\overline{RR} \doteq \overline{R}\,\overline{R}$.

On the other hand, it is easy to list all cases when $XZ = ZY = \{a, b\}^*$: we call them *trivial absorption*.

Trivial absorption: We have $XZ = ZY = \{a, b\}^*$ if and only if $X = Y = \{a, b\}^*$ or $Z = \{a, b\}^*$.

So, in all other cases on the binary alphabet, the subalphabets Δ and Π of X, Y, and Z are either empty or of cardinality one. To list all solutions, we should consider all possible cases. Like above, we shall group them according to the form of the canonical decompositions of XZ and ZY, assuming that

X, Y, Z are not equal to $\{\lambda\}$. Basically, there are only four possible cases:

$$\overline{X'}\,\overline{Z} \doteq \overline{Z}\,\overline{Y'},\ \text{ where } X' = R_{\Delta(Z)}(X), Y' = L_{\Pi(Z)}(Y); \tag{12}$$

$$\overline{X}\,\overline{Z'} \doteq \overline{Z''}\,\overline{Y},\ \text{ where } Z' = L_{\Pi(X)}(Z), Z'' = R_{\Delta(Y)}(Z);\ \text{ or} \tag{13}$$

$$\overline{X}\,\overline{Z'} \doteq \overline{Z}\,\overline{Y'}, \tag{14}$$

or, symmetrically, $\overline{X'}\,\overline{Z} \doteq \overline{Z''}\,\overline{Y}$, where X', Y', Z', Z'' are defined as above. Of course, each of the reduced languages (with primes) can be equal to the initial language, in particular when the respective subalphabet is empty.

We could consider these cases successively, but the resulting list of cases is long and too awkward to form a nice-looking theorem. So, let us show how the technique works on an example.

In what follows we consider $X = F_aF_b$, where F_a and F_b are defined as in Example 6. In particular, F_a and F_b are the two components of the canonical decomposition of X, and we have $\Delta(F_a) = \Pi(F_a) = \Delta(X) = \{a\}$, $\Delta(F_b) = \Pi(F_b) = \Pi(X) = \{b\}$. Also we have $L_a(X) = L_b(X) = R_a(X) = R_b(X) = X$, so that X remains unchanged under any of these operators. So, we should eliminate the situation when $XZ = \{a, b\}^*$, and after that due to Lemma 9 it is sufficient to consider equalities (13) and (14).

First of all, clearly, $XZ = ZY = \{a, b\}^*$ if and only if $Z = \{a, b\}^*$; here Y is arbitrary. This gives us

Solution 1. $Z = \{a, b\}^*$ and $Y \subseteq \{a, b\}^*$ is arbitrary.

Suppose first that (14) holds: $F_aF_bZ' \doteq ZY'$, where $Z' = L_b(Z)$ and $Y' = L_{\Pi(Z)}(Y)$. If $Z = \{\lambda\}$, we have $Y = X$, which gives

Solution 2. $Z = \{\lambda\}$ and $Y = X = F_aF_b$.

Now suppose that $Z \neq \{\lambda\}$. Then due to (14) the canonical decomposition $\overline{Z}$ starts with F_a. So, $Z' = L_b(Z) = Z$, and (14) is in fact a conjugacy equation for words on $\mathcal{F}$: $F_aF_b\overline{Z} \doteq \overline{Z}\,\overline{Y'}$. Excluding the solution with $Z = \{\lambda\}$ which has been mentioned above, we get that

$$F_aF_b \doteq \overline{R}\,\overline{S}, \text{ where } R \neq \{\lambda\},\ Y' \doteq \overline{S}\,\overline{R}, \text{ and } \overline{Z} \doteq (\overline{R}\,\overline{S})^k\overline{R} \text{ for some } k \geq 0.$$

We must consider two possibilities: $R = F_a$, $S = F_b$, or $R = F_aF_b$, $S = \{\lambda\}$.

If $R = F_a$, we have $Z = (F_aF_b)^kF_a$ for some $k \geq 0$, $\Pi(Z) = \{a\}$, and $Y' = F_bF_a$; so, $F_bF_a \subseteq Y \subseteq a^*F_bF_a$. It is easy to check that Z and any Y satisfying this double inclusion fit the conjugacy equation: $XZ = ZY = (F_aF_b)^{k+1}F_a$. This is

Solution 3. $Z = (F_aF_b)^kF_a$ for some $k \geq 0$ and Y is an arbitrary factorial language satisfying $F_bF_a \subseteq Y \subseteq a^*F_bF_a$.

If $R = F_aF_b$, we have $Z = (F_aF_b)^{k+1}$ for some $k \geq 0$, $\Pi(Z) = \{b\}$, and $Y' = F_aF_b$. So, $F_aF_b \subseteq Y \subseteq b^*F_aF_b$. Clearly, Z and any Y satisfying this double inclusion fit the conjugacy equation: $XZ = ZY = (F_aF_b)^{k+2}$. This is

Solution 4. $Z = (F_aF_b)^k$ for some $k \geq 1$ and Y is an arbitrary factorial language satisfying $F_aF_b \subseteq Y \subseteq b^*F_aF_b$.

Now suppose that (13) holds. Here we may suppose that $Z'' \neq Z$ since otherwise the situation falls also into the previous case and has been considered. So, $\Delta(Y) = \{y\}$ for some $y \in \{a, b\}$.

If $Z'' = \{\lambda\}$, we have $Y = XZ' = F_aF_bZ'$, which means that $\Delta(Y) = \{a\}$ and thus $Z \subseteq a^*$. Consequently, $Z' = Z$, and we get

Solution 5. $Z \subseteq a^*$ (that is, $Z = a^*$ or $Z = a^{\leq k}$ for some $k \geq 0$) and $Y = F_aF_bZ$.

If $Z' = \{\lambda\}$, then $Z \subseteq b^*$ and thus $Z'' = Z$ or $Z'' = \{\lambda\}$. Both cases have been considered above.

Now suppose that $Z' \neq \{\lambda\}$, $Z'' \neq \{\lambda\}$. Due to Lemma 13, we have $R_y(Z') = L_b(Z'')$. Note that $L_b(Z'') = Z''$ since Z'' is not equal to $\{\lambda\}$ and thus its canonical decomposition starts with F_a; so, $Z'' = R_y(Z')$. Let us apply R_y to both parts of (13). If $Y = y^*$, we get $F_aF_b\overline{Z''} \doteq \overline{Z''}$ which is impossible since $\overline{Z''}$ is a finite word on $\mathcal{F}$. So, $Y \neq y^*$ and we obtain $F_aF_b\overline{Z''} \doteq \overline{Z''}\,\overline{Y_1}$, where $Y_1 = R_y(Y)$; here the right part of the equality holds since due to Lemma 12 we have $\Delta(Y_1) = \Delta(Y) = \{y\}$. This equality is the conjugacy equation for words on $\mathcal{F}$; since we have already considered the case when $Z'' = \{\lambda\}$, the only new situation is $F_aF_b \doteq \overline{R}\,\overline{S}$, where $R \neq \{\lambda\}$, $\overline{Y_1} \doteq \overline{S}\,\overline{R}$, and $\overline{Z''} \doteq (\overline{R}\,\overline{S})^k\overline{R}$ for some $k \geq 0$.

As above, there are two cases: either $R = F_a$, $S = F_b$, or $R = F_aF_b$, $S = \{\lambda\}$.

If $R = F_a$, we have $Z'' = (F_aF_b)^kF_a$ and $Y_1 = F_bF_a$, so that $y = b$. Since $Z'' = R_y(Z)$, we have $(F_aF_b)^kF_a \subseteq Z \subseteq (F_aF_b)^kF_ab^*$, and since $Y_1 = R_b(Y)$, we have $F_bF_a \subseteq Y \subseteq F_bF_ab^*$. Note also that $Z' = L_b(Z) \supseteq (F_aF_b)^kF_a$ by the definition of L_b, so that $(F_aF_b)^kF_a \subseteq Z' \subseteq Z \subseteq (F_aF_b)^kF_ab^*$.

If we return to (13), we see that the cases when $k = 0$ and $k > 0$ give different solutions. If $k = 0$, we have $F_aF_b\overline{Z'} \doteq F_a\overline{Y}$, so that $\overline{Y} \doteq F_b\overline{Z'}$. Here Z is an arbitrary factorial language such that $F_a \subseteq Z \subseteq F_ab^*$, and $Z' = L_b(Z)$. Note also that $Y = F_bZ$, and any Z satisfying the inclusions gives such a solution. This is

Solution 6. Z is an arbitrary factorial language such that $F_a \subseteq Z \subseteq F_a b^*$, and $Y = F_b Z$. (For example we can take $Z = F_a + b^*$, and then $Y = F_b F_a$; or $Z = F_a +$ Fac(bab^*), and then $Y = F_b a^{\leq 1}(F_a + b^*)$.)

If $k > 0$, we have $F_a F_b \overline{Z'} \doteq (F_a F_b)^k F_a \overline{Y}$, so that Y is an arbitrary factorial language such that $F_b F_a \subseteq Y \subseteq F_b F_a b^*$ and $\Delta(Y) = \{b\}$ (then automatically Y can follow F_a in a canonical decomposition). Then $\overline{Z'} \doteq (F_a F_b)^{k-1} F_a \overline{Y}$. Here Z is an arbitrary language such that $L_b(Z) = Z'$ and $R_b(Z) = Z''$, that is, an arbitrary language such that $Z' + Z'' \subseteq Z \subseteq b^* Z' \cap Z'' b^*$. Note also that $Z'' = (F_a F_b)^k F_a \subseteq Z'$, so it is not necessary to mention Z'' in the left part of the previous inclusion.

Solution 7. Y is an arbitrary factorial language such that $F_b F_a \subseteq Y \subseteq F_b F_a b^*$ and $\Delta(Y) = \{b\}$; and Z is an arbitrary factorial language satisfying $(F_a F_b)^k F_a Y \subseteq Z \subseteq b^*(F_a F_b)^k F_a Y \cap (F_a F_b)^{k+1} F_a b^*$, $k \geq 0$.

Example 10 We can take $Y = F_b F_a + b^* a^* b^*$ and $Z = F_a F_b F_a + F_a b^* a^* b^* + b^* F_a b^*$ and will have $F_a F_b Z = ZY$.

It remains to consider the case of $R = F_a F_b$, that is, $Z'' = (F_a F_b)^k$, $k \geq 1$, and $Y_1 = F_a F_b$. Here $y = a$ and thus $F_a F_b \subseteq Y \subseteq F_a F_b a^*$; the subalphabet $\Delta(Y)$ must be equal to $\{a\}$. Equation (13) gives $F_a F_b \overline{Z'} \doteq (F_a F_b)^k \overline{Y}$, so that $Z' = (F_a F_b)^{k-1} Y$ and thus $(F_a F_b)^{k-1} Y \subseteq Z \subseteq b^*(F_a F_b)^{k-1} Y \cap (F_a F_b)^k a^*$. This is

Solution 8. Y is an arbitrary factorial language such that $F_a F_b \subseteq Y \subseteq F_a F_b a^*$ and $\Delta(Y) = \{a\}$; and Z is an arbitrary factorial language such that $(F_a F_b)^{k-1} Y \subseteq Z \subseteq b^*(F_a F_b)^{k-1} Y \cap (F_a F_b)^k a^*$ for some $k \geq 1$.

Example 11 We can take $Y = F_a F_b + a^* F_b a^*$ and $Z = F_a F_b +$Fac$(ba^* F_b a^*)$ and will have $F_a F_b Z = ZY$.

We have listed all the possible cases and can state

Lemma 18 *Define $X = F_a F_b$. Then $XZ = ZY$ for some binary factorial languages Z and Y if and only if Y and Z are defined according to one of Solutions 1–8.*

A general theorem describing when binary factorial languages conjugate can be stated as well, but will contain an intricate list of cases.

9 Further problems

Two natural questions arise after several equations have been solved over binary factorial languages.

First, is it possible to generalize our results to larger alphabets? In fact, we know that the theorem concerning the equation $X^n = Y^n$ holds for an arbitrary alphabet; and it is not a problem to solve the conjugacy equation on a larger alphabet, but the situation with commutation is less clear. The case study of subalphabets Δ occurring when we consider the case of (6) grows rapidly with the alphabet and instantly becomes very complicated.

The second question concerns equations other than the considered ones: Is there a way to standardize solving general equations on binary factorial languages and to describe something like the Makanin algorithm for them?

Clearly, solving equations on factorial languages by our technique cannot be easier than solving word equations: every time we have to list all possible forms of the equation for the canonical decompositions, and one of them just repeats the initial equation (but holds for words on $\mathcal{F}$). We should solve it, as well as all the other possible equations for the canonical decompositions. Note that the number of the "word" equations to study increases rapidly with the cardinality of the alphabet considered and the length of the (left and right parts of the) initial equation: for each language variable X, we should consider all possible values of the subalphabets $\Delta(X)$ and $\Pi(X)$ and can meet the "word" variables $L_\Pi(X)$, $R_\Delta(X)$ and $L_\Pi(R_\Delta(X))$ for all possible subalphabets Δ and Π. As it is shown above, the case study is far from trivial even if the alphabet is binary and the initial equation is very short.

In fact, if we consider a longer equation, the following problem arises. A particular equation involving, e. g., variables X, $L_a(X)$ and $L_b(X)$ can admit a solution in terms of some new variable factorial languages (above they have been denoted for instance by R, S, and Q). We must have $L_a(X) + L_b(X) \subseteq X \subseteq a^*L_a(X) \cap b^*L_b(X)$: a solution of the "word" equation gives a solution of the initial language equation if and only if these inclusions hold. However, it is not even clear if satisfiability of such inclusions on factorial languages is decidable. In the considered examples, it was every time clear that a solution exists, but it was just some luck.

So, it is not clear if generalizing the described technique to larger alphabets or longer equations is possible.

Acknowledgements

I am deeply grateful to both anonymous referees for careful reading of the initial text and important corrections and suggestions.

References

[1] S. V. Avgustinovich, A. E. Frid, A unique decomposition theorem for factorial languages, Internat. J. Algebra Comput. 15 (2005), 149–160.

[2] S. V. Avgustinovich, A. E. Frid, Canonical decomposition of a regular factorial language, in: CSR 2006, LNCS 3967, Springer, 2006, 18–22.

[3] C. Choffrut, J.Karhumäki, On Fatou properties of rational languages, in: C. Martin-Vide and V. Mitrana, Eds., *Where Mathematics, Computer Science, Linguistics and Biology Meet*, Kluwer, Dordrecht, 2000, 227–235.

[4] J. H. Conway, Regular Algebra and Finite Machines, Chapman & Hall, London, 1971.

[5] V. Diekert, Makanin's Algorithm, in: M. Lothaire, Algebraic combinatorics on words, Cambridge Univ. Press, 2002. Pp. 387–442.

[6] A. E. Frid, Canonical decomposition of a catenation of factorial languages, Siberian Electronic Mathematical Reports 4 (2007) 14–22, `http://semr.math.nsc.ru/2007/V4/p12-19.pdf`.

[7] A. E. Frid, Commutation of binary factorial languages, in: DLT 2007, LNCS 4588, Springer, 2007, 193–204.

[8] J. Karhumäki, M. Latteux, I. Petre, Commutation with codes, Theoret. Comput. Sci. 340 (2005) 322–333.

[9] J. Karhumäki, M. Latteux, I. Petre, The commutation with ternary sets of words, Theory Comput. Systems 38 (2005) 161–169.

[10] M. Kunc, The power of commuting with finite sets of words, Theory of Computing Systems 40 (2007), 521–551.

[11] M. Kunc, What do we know about language equations?, in: DLT 2007, LNCS 4588, Springer, 2007, 23–27.

[12] M. Lothaire, Combinatorics on words, Addison-Wesley, 1983.

[13] B. Ratoandromanana, Codes et motifs, RAIRO Inform. Theor. 23 (1989) 425–444.

[14] A. Salomaa, S. Yu, On the decomposition of finite languages, in: Developments in Language Theory. Foundations, Applications, Perspectives, World Scientific, 2000, 22–31.