Acta Cybernetica **19** (2009) 479–497.

Alphabetical Satisfiability Problem for Trace Equations*

L. Breveglieri[†], A. Cherubini[‡], C. Nuccio[‡], and E. Rodaro[§]

Abstract

It is known that the satisfiability problem for equations over free partially commutative monoids is decidable but computationally hard. In this paper we consider the satisfiability problem for equations over free partially commutative monoids under the constraint that the solution is a subset of the alphabet. We prove that this problem is NP-complete for quadratic equations and that its uniform version is NP-complete for linear equations.

Keywords: free partially commutative monoid, trace equation, NP-complete problem

1 Introduction

The theory of word equations is an important subfield of the combinatorics on words firstly introduced in 1954 by Markov [9] who, given an alphabet Σ of constants, a set of unknowns Ξ and a word equation $W_L = W_R$ with $W_L, W_R \in (\Sigma \cup \Xi)^*$ proposed the problem of stating whether an assignment $\varphi : \Xi \rightarrow \Sigma^*$ exists such that $\varphi(W_L) = \varphi(W_R)$. This problem was solved more than 20 years later by Makanin [8] who gave a very complicated algorithm to decide whether or not a word equation with constants has a solution. Later several authors considered the problem of satisfiability of equations by a solution $\{\varphi(x) |\ x \in \Xi\}$ satisfying some constraints. In particular Robson and Diekert considered in [12] the problem of determining whether equations on free monoids have or not a solution with fixed lengths and they gave a linear algorithm for solving this problem for quadratic equations.
In the second half of '90 attention was paid also to equations on free partially commutative monoids. Free partially commutative monoids, firstly introduced in

*This work was partially supported by INDAM group GNSAGA, PRIN "Aspetti matematici e applicazioni emergenti degli automi e dei linguaggi formali" and ESF project AutoMathA.
[†]Politecnico di Milano, Department of Electronics and Information, Piazza L. da Vinci, 32, 20133 Milano, Italy, E-mail: `luca.breveglieri@polimi.it`.
[‡]Politecnico di Milano, Department of Mathematics, Piazza L. da Vinci, 32, 20133 Milano, Italy, E-mail: {`alessandra.cherubini,claudia.nuccio`}`@polimi.it`.
[§]Universitá dell'Insubria, DSCPI, Via Valleggio 11, 22100 Como, Italy, E-mail: `emanuele.rodaro@gmail.com`.

combinatorics [3], became very important in computer science for the theory of concurrence in connection with the semantics of labelled Petri nets [11] and the investigation of parallel program schemata [7]. The decidability of the satisfiability problem for equations on free partially commutative monoids, trace equations for short, was proved by Matiyasevich in [10] and by Diekert and al. [4, 5].

In this paper we consider the *alphabetical satisfiability problem* for trace equations with constants and unknowns, i.e. we look for the existence of a solution $\{\varphi(x) \in \Sigma | x \in \Xi\}$. The alphabetical satisfiability problem for trace equations presents some motivations coming from molecular biology and from reconstruction of sentences in natural languages. For instance, recently much attention was paid to partial words in the sense of [2], with motivations coming from different areas. Several of these motivations suggest that also *partial traces*, i.e. the generalization of partial words to trace monoids, deserve some attention. The alphabetical satisfiability problem is the generalization of the compatibility problem of partial words to the case of partial traces.

Using an argument which closely follows the proof of Theorem 1 in [6], we prove that the general problem of alphabetical satisfiability for quadratic word equations over a given free partially commutative monoid is NP-complete. Then we look for the complexity class of the alphabetical satisfiability problem for linear trace equations and we prove that the general problem is polynomial under particular assumptions on the independence alphabet while the uniform problem (i.e. the problem where even the independence alphabet is considered as variable parameter) is NP-complete.

In Section 2 we start giving some necessary notations and definitions, Section 3 shows that the general problem of alphabetical satisfiability for quadratic trace equations is NP-complete, while Sections 4 and 5 deal with the alphabetical satisfiability for linear trace equations.

2 Preliminaries

Let Σ be a finite alphabet and let $I \subseteq \Sigma \times \Sigma$ be a binary irreflexive and symmetric relation, called *independence* relation. We denote by $D = (\Sigma \times \Sigma) \setminus I$ the *dependence* relation, and by $\sim_I$ the least congruence over Σ^* generated by the relations $ab = ba$, for all $(a, b) \in I$. The pairs (Σ, I) and (Σ, D) are called, respectively, *independence* and *dependence alphabet*. For a subset A of Σ, let $I_A = (A \times A) \cap I$. If $I_A = \emptyset$, then A is called a *clique* of the dependence alphabet, or a D-clique. If $I_A = A \times A$, then A is called a *clique* of the independence alphabet, or a I-clique. The *free partially commutative* monoid (or trace monoid) over (Σ, I), is the quotient $\mathbb{M}(\Sigma, I) = \Sigma^* / \sim_I$ and it can be also denoted by $\mathbb{M}$, when no confusion arises. The elements of $\mathbb{M}$ are called *traces* and the trace with representative $x \in \Sigma^*$ is denoted by $[x]$.

Let Ξ be a finite set of unknowns and $\Theta = \Sigma \cup \Xi$. A *trace equation* with constants over (Σ, I) has the form $W_L \equiv W_R$ with $W_L, W_R \in \Theta^+$. A trace equation

$W_L \equiv W_R$ is called *linear* if each unknown occurs at most once in $W_L W_R$ and it is called *quadratic* if each unknown occurs at most twice in $W_L W_R$.
An *assignment* is a map $\varphi : \Xi \to \Sigma^*$. It can be extended to the monoid homomorphism $\varphi^* : \Theta^* \to \Sigma^*$ by putting $\varphi(a) = a$ for all $a \in \Sigma$. We say that the trace equation $W_L \equiv W_R$ is *satisfiable* if $\varphi^*(W_L) \sim_I \varphi^*(W_R)$ for some assignment φ. In such case we say also that φ satisfies $W_L \equiv W_R$ and the set $\{\varphi(x) \mid x \in \Xi\}$ is called a *solution* of $W_L \equiv W_R$. In the sequel, for simplicity, φ^* is still denoted by φ.
We say that the trace equation $W_L \equiv W_R$ is *alphabetically satisfiable* if it is satisfied by an assignment $\varphi : \Xi \to \Sigma$, then φ is called an *alphabetical assignment* and $\{\varphi(x) \mid x \in \Xi\}$ an *alphabetical solution* of the trace equation.
We look for alphabetical solutions of $W_L \equiv W_R$. It is obvious that, if $|W_L| \neq |W_R|$, no assignment $\varphi : \Xi \to \Sigma$ satisfies $W_L \equiv W_R$, hence we always assume that $|W_L| = |W_R|$ and when we refer to an assignment, we always consider an alphabetical assignment, if it is not differently specified.

3 Alphabetical satisfiability for quadratic trace equations

In this section we prove that the general problem of checking whether a quadratic trace equation over a given trace monoid $\mathbb{M}(\Sigma, I)$ has an alphabetical solution is an NP-complete problem.
We recall the following well-known result:

Proposition 1. *Let $(\Sigma, D) = \bigcup_{i=1}^{k}(A_i, D_i)$ be a union of subalphabets with $I_i = (A_i \times A_i) \setminus D_i$, $\mathbb{M}_i = \mathbb{M}(A_i, I_i)$ and let $[\pi_i] : \mathbb{M}(\Sigma, I) \to \mathbb{M}_i$ be the canonical homomorphisms for all $i \in \{1, 2, \ldots k\}$.*
Then the map $\pi : \mathbb{M}(\Sigma, I) \to \mathbb{M}_1 \times \ldots \times \mathbb{M}_k, \qquad t \mapsto (\pi_1(t), \ldots, \pi_k(t))$
is an injective (canonical) homomorphism.

Remark 1. If the sets A_i are D-cliques, Proposition 1 says that two traces are equal if and only if their projections on the cliques A_i are equal.

In order to use the above Remark 1 in the case of trace equations and for all $A \subseteq \Sigma$ such that $A \times A \subseteq D$, we define the homomorphism $\overline{\pi}_A : (\Sigma \cup \Xi)^* \to (A \cup \Xi)^*$ such that, for all $x \in \Sigma \cup \Xi$,

$$\overline{\pi}_A(x) = \begin{cases} \epsilon & \text{if } x \notin A \cup \Xi \\ x & \text{otherwise} \end{cases}$$

For any $w \in (\Sigma \cup \Xi)^*$, the image $\overline{\pi}_A(w)$ is called *A-projection* of w.
As a direct consequence of Proposition 1 we get the following result:

Lemma 1. *Let $A_1, \ldots, A_k$ be cliques of the dependence alphabet of the trace monoid $\mathbb{M}(\Sigma, I)$. Then the trace equation $W_L \equiv W_R$ has a alphabetical solution if and only if there exists a family of assignments $\{\varphi_i : \Xi \to A_i \cup \{\epsilon\} | \, i = 1, \ldots, k\}$ such that:*

1. *for each $i \in \{1, \ldots, k\}$, φ_i satisfies the equation $\overline{\pi}_{A_i}(W_L) = \overline{\pi}_{A_i}(W_R)$;*

2. *for all $x \in \Xi$ there exists $i \in \{1,\ldots,k\}$ such that $\varphi_i(x) \in A_i$;*
3. *for all $i \in \{1,\ldots,k\}$, $x \in \Xi$, if $\varphi_i(x) \in A_i$ then, for all $l \in \{1,\ldots,k\} \setminus \{i\}$, $\varphi_l(x) = \epsilon$ if $\varphi_i(x) \notin A_i \cap A_l$ or $\varphi_i(x) = \varphi_l(x)$ if $\varphi_i(x) \in A_i \cap A_l$.*

We recall that a system of word equations is quadratic if each unknown occurs at most twice in the system. We use the following lemma whose proof is very close to the proof of Theorem 1 in [6]:

Lemma 2. *Let $|\Sigma| \geq 2$. The following problem is NP-complete.*
INSTANCE *A system of quadratic word equations.*
QUESTION *Is there an assignment $\varphi : \Xi \to \Sigma \cup \{\epsilon\}$ that satisfies the system?*

Proof. It is easy to verify that the problem is in NP. To prove that it is NP-hard we give a reduction from 3-SAT. Let $\mathcal{F} = C_0 \wedge C_1 \wedge \ldots \wedge C_{M-1}$ be a Boolean formula in 3-CNF over a finite set of variables Γ. Each clause has the form $C_i = l_{3i} \vee l_{3i+1} \vee l_{3i+2}$ where l_{3i+h} denotes a literal. We can assume that each variable has both positive and negative occurrences.
We associate the formula $\mathcal{F}$ with the following quadratic system $S(F,\Xi)$ of word equations with constants $a, b, a \neq b$ and the following set Ξ of unknowns:

- $y_i,\ t_i,\ 0 \leq i \leq M-1$,
- $x_j,\ 0 \leq j \leq 3M-1$,
- $z_X,\ u_X$, for all $X \in \Gamma$,
- $v_{X,s}$, for all $X \in \Gamma$, $0 < s \leq M-1$.

For each clause C_i we consider the equation

$$x_{3i}x_{3i+1}x_{3i+2} = ay_it_i \qquad (1)$$

Now let $X \in \Gamma$ and consider the set of positions $D(X) = \{i_1, i_2, \ldots, i_r\}$ of the literal X in $\mathcal{F}$ and the set of positions $C(X) = \{j_1, j_2, \ldots, j_k\}$ of the literal $\neg X$ in $\mathcal{F}$. For each $X \in \Gamma$ we introduce another equation

$$L(X) = R(X) \qquad (2)$$

where, if $r \leq k$,

$$L(X) = x_{i_1}x_{i_2}\ldots x_{i_r}v_{X,1}v_{X,2}\ldots v_{X,k-r}u_Xa^kbx_{j_1}x_{j_2}\ldots x_{j_k}z_X$$

and

$$R(X) = a^kba^kb$$

or, if $r > k$,

$$L(X) = x_{i_1}x_{i_2}\ldots x_{i_r}u_Xa^rbx_{j_1}x_{j_2}\ldots x_{j_k}v_{X,1}v_{X,2}\ldots v_{X,r-k}z_X$$

and

$$R(X) = a^rba^rb.$$

It is easy to see that $\mathcal{F}$ is satisfiable if and only if the system $S(F, \Xi)$, formed by the above equations (1),(2), has a solution whose lengths are not greater than 1. In fact if $\varphi : \Xi \to \Sigma \cup \{\epsilon\}$ is a possible assignment which satisfies the system then, encoding the value TRUE for the variable X of $\mathcal{F}$ in the fact that $\varphi(x_i) = a$ for all $i \in D(X)$, $\varphi(x_j) = \epsilon$ for all $j \in C(X)$ and the value FALSE in the fact that $\varphi(x_j) = a$ for all $j \in C(X)$, $\varphi(x_i) = \epsilon$ for all $i \in D(X)$, the equations of the form (1) guarantee that at least one literal in each clause assumes the value TRUE, while the equations of type (2) guarantee that the values of the literals are given in a coherent way. □

The next example illustrates the construction done in the proof of Lemma 1.

Example 1. Let us consider the following Boolean formula in 3-CNF over the set of variable $\Gamma = \{X_1, X_2, X_3\}$:

$$\mathcal{F} = (X_1 \vee \neg X_2 \vee X_3) \wedge (X_1 \vee \neg X_2 \vee \neg X_3) \wedge (\neg X_1 \vee X_2 \vee X_3).$$

We build the quadratic system $S(F, \Xi)$ of word equations with constants a, b, $a \neq b$ and this set Ξ of unknowns:

- y_i, t_i, $0 \leq i \leq 2$
- x_j, $0 \leq j \leq 8$
- $v_{X_1,1}, v_{X_2,1}, v_{X_3,1}$, $v_{X_1,2}, v_{X_2,2}, v_{X_3,2}$
- u_{X_1}, z_{X_1}, u_{X_2}, z_{X_2}, u_{X_3}, z_{X_3}

where the unknowns y_i, t_i are associated with the i-th clause C_i, the unknown x_i to the i-th literal in $\mathcal{F}$ and the unknowns $u_{X_i}, z_{X_i}, v_{X_i,s}$ to the variable X_i.
We associate with the three clauses of $\mathcal{F}$ these three word equations:

$$\begin{aligned} x_0x_1x_2 &= ay_0t_0 \\ x_3x_4x_5 &= ay_1t_1 \\ x_6x_7x_8 &= ay_2t_2 \end{aligned}$$

Then we introduce a word equation for each variable X_i. For example, for the variable X_1 we build the following word equation:

$$x_0x_3u_{X_1}a^2bx_6v_{X_1,1}z_{X_1} = a^2ba^2b. \tag{3}$$

The left side of the equation is built as follows. The variable X_1 occurs in the first, forth and seventh literal so in the equation we use the unknowns x_0, x_3, x_6. The factor $u_{X_1}a^2b$, where the exponent of a is the maximum between the numbers of positive and negative occurrences of X_1, is a separator between the unknowns that encode the positive and negative occurrences of X_1. After the unknown x_6 (that corresponds to the negative occurrence of X_1) we put a number of unknowns $v_{X_1,s}$ equal to the difference between the number of positive and negative occurrences of X_1 and at the end we put the variable z_{X_1}. The right side of the word equation

is a^2ba^2b where again the exponent of a is the maximum between the number of positive and negative occurrences of X_1.
Similarly, we proceed for the variable X_2 but, since the number of positive occurrences of X_2 is smaller than the number of its negative occurrences, after the unknown x_7 (encoding the positive occurrence of X_2 in the eighth literal) we put a number of unknowns $v_{X_2,s}$ equal to the difference between the number of negative and positive occurrences of X_2. We obtain the following equation:

$$x_7 v_{X_2,1} u_{X_2} a^2 b x_1 x_4 z_{X_2} \quad = \quad a^2ba^2b$$

Analogously we build the word equation relative to X_3 and we obtain this quadratic system of word equations:

$$\begin{cases} x_0x_1x_2 = ay_0t_0 \\ x_3x_4x_5 = ay_1t_1 \\ x_6x_7x_8 = ay_2t_2 \\ x_0x_3u_{X_1}a^2bx_6v_{X_1,1}u_{X_1} = a^2ba^2b \qquad (3) \\ x_7v_{X_2,1}u_{X_2}a^2bx_1x_4z_{X_2} = a^2ba^2b \\ x_2x_8u_{X_3}a^2bx_5v_{X_3,1}z_{X_3} = a^2ba^2b \end{cases}$$

The formula $\mathcal{F}$ is satisfiable if and only if there exists an assignment $\varphi : \Xi \rightarrow \{a,b\} \cup \{\epsilon\}$ that satisfies the previous system. Suppose that such an assignment exists and consider the word equation (3). Since its right side is a^2ba^2b and the left side contains the factor a^2b, it follows that

$$\varphi(x_0) = \varphi(x_3) = a,\ \varphi(u_{X_1}) = b \quad \text{and} \quad \varphi(x_6 v_{X_1,1} z_{X_1}) = \epsilon \tag{4}$$

or

$$\varphi(x_0 x_3 u_{X_1}) = \epsilon \quad \text{and} \quad \varphi(x_6) = \varphi(v_{X_1,1}) = a,\ \varphi(z_{X_1}) = b \tag{5}$$

Notice that if we encode the value TRUE (resp. FALSE) for the variable X in the fact that $\varphi(x_i) = a$ (resp. $\varphi(x_i) = \epsilon$) for all indices $i \in D(X)$ and $\varphi(x_j) = \epsilon$ (resp. $\varphi(x_j) = a$) for all indices $j \in C(X)$, conditions (4) and (5) mean that the assignment of truth value to X_1 is coherent. A similar argument applies for the coherence in the truth assignments to X_2 and X_3.
Now consider the first three word equations of the system relative to the three clauses of $\mathcal{F}$. The presence of the letter a in the right side encodes that at least one literal in each clause takes the value TRUE and so each clause is satisfied. Hence a truth assignment satisfying $\mathcal{F}$ corresponds to the assignment φ satisfying the system.
Viceversa, it is easy to verify that to each truth assignment that satisfies $\mathcal{F}$, corresponds an assignment $\varphi : \Xi \rightarrow \{a,b\} \cup \{\epsilon\}$ satisfying the systems.

As a consequence of Lemma 2 we can prove the following result:

Theorem 1. *The general problem of alphabetical satisfiability of a quadratic trace equation is NP-complete.*

Proof. It is quite obvious that this problem is in NP. Then to check that it is NP-hard we consider an alphabet $\Sigma = \{a, b, c, \sharp\}$ with the dependence relation D whose maximal D-cliques are $\{a, b, \sharp\}, \{c, \sharp\}$ and the set of unknowns Ξ defined in Lemma 2 and we give a reduction from 3-SAT. Using the notation introduced in the proof of Lemma 2 we consider the following equation:

$$\prod_{i=0}^{M-1} (x_{3i}x_{3i+1}x_{3i+2}\sharp) \prod_{X\in\Gamma} (L(X)\sharp) = \prod_{i=0}^{M-1} (ay_it_i\sharp) \prod_{X\in\Gamma} (R(X)c^{l_X}\sharp) \tag{6}$$

Let $I = (\Sigma^* \times \Sigma^*) \setminus D$. By Lemma 1, this equation has an alphabetical solution in $\mathbb{M}(\Sigma, I)$ if and only if its projections on the D-cliques $A_1 = \{a, b, \sharp\}$ and $A_2 = \{c, \sharp\}$ are satisfied respectively by the assignments φ_1 and φ_2 as in Lemma 1. Moreover such an assignment φ_1 exists if and only if there exists an assignment $\varphi : \Xi \to \{a, b\} \cup \{\epsilon\}$ which satisfies the system $S(F, \Xi)$. Indeed, notice that, for each assignment φ_1 satisfying the A_1-projection of equation (6) that assigns $\sharp$ to the unknowns of a subset $\Upsilon \subseteq \Xi$, there exists an assignment $\varphi : \Xi \to \{a, b\} \cup \{\epsilon\}$ which satisfies the system $S(F, \Xi)$ and such that

$$\forall z \in \Xi \qquad \varphi(z) = \begin{cases} \epsilon & \text{if } z \in \Upsilon \\ \varphi_1(z) & \text{otherwise} \end{cases}$$

Finally notice that, for each assignment φ_1 satisfying the A_1-projection of equation (6), there always exists an assignment φ_2 satisfying the A_2-projection of equation (6) such that φ_1 and φ_2 fulfill conditions in Lemma 1. Whence to decide whether equation (6) has an alphabetical solution is equivalent to decide whether the system $S(F, \Xi)$ has a solution whose lengths are not greater than 1. Then the problem is NP-complete. □

Remark 2. If in the proof of Theorem 1 we replace each occurrence of the symbol $\sharp$ with the string $ba^{2M+1}b$ where M is the number of clauses in the formula $\mathcal{F}$, we obtain a new equation having $(\{a, b, c\}, \{(a, a), (b, b), (a, b), (b, a), (c, c)\})$ as dependence alphabet. With some minor changes we can prove that such equation is satisfiable if and only if the system $S(F, \Xi)$ has a solution whose lengths are not greater than 1. Then the general problem of the alphabetical satisfiability of a quadratic trace equation is NP-complete even when $|\Sigma| = 3$.

4 The uniform problem of alphabetical satisfiability for linear trace equations

Let $w \in (\Sigma \cup \Xi)^+$, the sets $\mathcal{L}(w) = \{\varphi(w) | \ \varphi : \Xi \to \Sigma\}$ and $[\mathcal{L}](w) = \{[v] | v \in \mathcal{L}(w)\}$ are called respectively the *language associated with* w and the *trace language associated with* w.

Let $W_L \equiv W_R$ be a linear trace equation on the free partially commutative monoid $\mathbb{M}(\Sigma, I)$. The equation is satisfied by an alphabetical assignment $\varphi : \Xi \to \Sigma$ if and only if the finite trace languages associated with W_L and W_R have non empty

intersection. Since the membership problem for a regular trace language (i.e. for a trace language $T = \{[v] |\, v \in R\}$, where R is a regular language) can be solved in polynomial time with respect to the length of the input word [1], there is a naive algorithm for checking whether a trace equation has or not an alphabetical solution. Obviously this algorithm has exponential time complexity because, for all $w \in (\Sigma \cup \Xi)^+$, the number of words in $[\mathcal{L}](w)$ is exponential with respect to the number of unknowns occurring in w.
It is natural to ask whether the alphabetical satisfiability problem is or not NP-complete. In particular, we obtained the following result:

Theorem 2. *The uniform problem of the alphabetical satisfiability for linear trace equations is NP-complete.*

Proof. Again, the difficult part is to prove that the problem is NP-hard. We give a reduction from 3-SAT. Let $\mathcal{F} = C_0 \wedge C_1 \wedge \ldots \wedge C_{M-1}$ be a Boolean formula in 3-CNF over a set of n variables $\Gamma = \{X_1, \ldots, X_n\}$, where

$$\forall\, j \in \{0, 1, \ldots, M-1\} \qquad C_j = l_{3j} \vee l_{3j+1} \vee l_{3j+2}$$

and l_{3j+h}, with $0 \leq h \leq 2$, are literals. We define the alphabet $\Sigma_{\mathcal{F}}$ and the independence relation $I_{\mathcal{F}}$ in the following way:

$$\Sigma_{\mathcal{F}} = \bigcup_{\substack{i \in \{1,\ldots,n\} \\ j \in \{0,1,\ldots,M-1\}}} \{\, d_i^j,\, c_i^j,\, z_i^j,\, u_i^j,\, e,\, \perp_j,\, \sharp_j,\, t_j \,\}$$

$$\begin{aligned} I_{\mathcal{F}} = \Bigg(& \bigcup_{\substack{i,j \in \{1,\ldots,n\} \\ h,k \in \{0,1,\ldots,M-1\}}} \Bigg(\bigcup_{\substack{k \geq h \\ i \neq j}} \{(z_i^h, d_j^k), (u_i^h, c_j^k), \} \cup \\ & \bigcup_{k \geq h} \{(u_i^h, t_k), (u_i^h, d_j^k), (z_i^h, c_j^k), (z_i^h, t_k)\} \cup \\ & \bigcup_{h > k} \{(u_i^h, \perp_k), (u_i^h, \sharp_k), (z_i^h, \perp_k), (z_i^h, \sharp_k), (\perp_k, d_j^h), (\sharp_k, d_j^h), (\perp_k, c_j^h), (\sharp_k, c_j^h)\} \cup \\ & \bigcup_{h \neq k} \{(u_i^h, u_j^k), (z_i^h, z_j^k)\} \cup \{(u_i^h, z_j^k) \,|\, h \neq k, i \neq j\} \cup \{(\perp_h, t_k), (\sharp_h, t_k)\} \cup \\ & \{(u_i^h, e), (z_i^h, e), (\perp_k, e), (\sharp_k, e)\} \Bigg)\Bigg)^{sym} \end{aligned}$$

where, for a binary relation R on an alphabet Σ, R^{sym} denotes the least symmetric relation on Σ containing R. Now, starting from the formula $\mathcal{F}$, we build a trace equation with constants in $\Sigma_{\mathcal{F}}$ and set of unknowns $\Xi = \{y_i |\, i = 0, 1, \ldots, 4M-1\}$ such that its subsets $\{y_i |\, i = 0, 1, \ldots, 3M\}$ and $\{y_i |\, i = 3M+1, \ldots, 4M-1\}$ are in one to one correspondence respectively with the set of literals and with the set of clauses. In this equation the letters d_i^j and c_i^j encode the fact that the variable X_i

has respectively a positive or negative occurrence in the clause C_j. The letters z_i^j and u_i^j mean that the variable X_i assumes respectively the value FALSE or TRUE in the clause C_j. The letters e encode the fact that the truth values of some variables occurring in a clause C are not relevant in order to satisfy the formula $\mathcal{F}$. In the sequel these variables of C and the unknowns associated with the literals of C where they occur are called *irrelevant variables* of C and *irrelevant unknowns* associated with C. The other variables and the unknowns associated with the literals where they occur are call *relevant variables* of C and *relevant unknowns* associated with C. Finally the letters $\perp_j, \sharp_j, t_j$ act like filters with the aim of assuring two conditions:

1. there is exactly one relevant unknown associated with each clause;
2. if y, y' are unknowns associated respectively with literals of two different clauses C_h and C_k where the same variable X_i occurs, then no assignment φ such that either $\varphi(y) = z_i^h$ and $\varphi(y') = u_i^k$ or $\varphi(y) = u_i^h$ and $\varphi(y') = z_i^k$ satisfies the equation.

This last condition corresponds to the fact that if a variable X_i is relevant in different clauses of $\mathcal{F}$ then the truth values assigned with X_i are coherent, i.e. X_i cannot assume the value TRUE in a clause and the value FALSE in another clause.
For each $j \in \{0, 1, \ldots, M-1\}$ and $0 \leq h \leq 2$, we associate with the literal l_{3j+h} the unknown $y_{3j+h} \in \Xi$ and a letter $a_h^j \in \Sigma_{\mathcal{F}}$ where

$$a_h^j = \begin{cases} d_r^j & \text{if } l_{3j+h} = X_r \\ c_r^j & \text{if } l_{3j+h} = \neg X_r \end{cases}$$

In this way, each $C_j = l_{3j} \vee l_{3j+1} \vee l_{3j+2}$ is associated with the following word

$$w_j = y_{3j}\, y_{3j+1}\, y_{3j+2}\, a_0^j\, a_1^j\, a_2^j \in (\Sigma_{\mathcal{F}} \cup \Xi)^+.$$

Finally, we associate the formula $\mathcal{F}$ with the following words $w_{\mathcal{F}}, w'_{\mathcal{F}} \in (\Sigma_{\mathcal{F}} \cup \Xi)^+$:

$$w_{\mathcal{F}} = w_0 \sharp_0 \perp_0 w_1 \sharp_1 \perp_1 \ldots \sharp_{M-2} \perp_{M-2} w_{M-1} \sharp_{M-1} \perp_{M-1} t_{M-1} t_{M-2} \ldots t_1 t_0,$$

$$w'_{\mathcal{F}} = e^2 a_0 e^2 a_1 \ldots e^2 a_{M-1} t_{M-1} y_{3M} t_{M-2} y_{3M+1} \ldots t_0 y_{4M-1} \sharp\perp,$$

where, for all $j \in \{0, 1, \ldots, M-1\}$, $a_j = a_0^j a_1^j a_2^j$ and $\sharp\perp = \sharp_0 \perp_0 \sharp_1 \perp_1 \ldots \sharp_{M-1} \perp_{M-1}$.
Then the formula $\mathcal{F}$ is satisfiable if and only if the trace equation $w_{\mathcal{F}} \equiv w'_{\mathcal{F}}$ has a solution.
We note that this equation is linear by the definition of the indices of the unknowns y and that it has polynomial size with respect to $\mathcal{F}$.
First, assume that the Boolean formula $\mathcal{F}$ is satisfiable, that is for each C_j there is at least one literal assuming the value TRUE. Pick for each C_j an $h_j \in \{0, 1, 2\}$ such that the literal l_{3j+h_j} assumes the value TRUE. Then consider the assignment $\varphi : \Xi \to \Sigma_{\mathcal{F}}$ defined in the following way: $\varphi(y_{3j+h_j}) = u_r^j$ if $l_{3j+h_j} = X_r$, $\varphi(y_{3j+h_j}) = z_r^j$ if $l_{3j+h_j} = \neg X_r$ and $\varphi(y_{3j+h}) = e$, for all $h \neq h_j$. For each $j = 0, 1, \ldots M-1$, put $\varphi(y_{4M-1-j}) = \varphi(y_{3j+h_j})$. Then from the definition of the independence relation it easily follows that

$$\varphi(w_{\mathcal{F}}) \sim_{I_{\mathcal{F}}} e^2 a_0 \ldots e^2 a_{M-1} t_{M-1} \varphi(y_{3M}) t_{M-2} \varphi(y_{3M+1}) \ldots t_0 \varphi(y_{4M-1}) \sharp\perp$$

and so the equation $w_{\mathcal{F}} \equiv w'_{\mathcal{F}}$ is satisfied by the assignment φ.
Conversely, assume that the equation $w_{\mathcal{F}} \equiv w'_{\mathcal{F}}$ is satisfied by an alphabetical assignment $\varphi : \Xi \to \Sigma_{\mathcal{F}}$ and prove that there exists an assignment of truth values to the variables of $\mathcal{F}$ which satisfies the formula.

Claim 1. The assignment φ has to assign the value e to at least $2M$ unknowns occurring in $w_{\mathcal{F}}$. Moreover, for each $j = 0, 1, \ldots, M-1$, two unknowns assigned to e have to occur in the words w_j, since the constants e are dependent on all the elements in the set $\{d_r^i, c_r^i |\ 0 \le i \le M-1, 1 \le r \le n\}$.

Claim 2. The remaining unknown occurring in w_j not assigned to e, say ξ_j, is such that $\varphi(\xi_j) \in \{z_r^s, u_r^s |\ 0 \le s \le j, 1 \le r \le n\}$. Indeed, $\varphi(\xi_j)$ has to take a value independent of e and of all the constants occurring in a_t for all $t \ge j$. But if $\varphi(\xi_j) \in \{\perp_s, \sharp_s |\ 0 \le s < j\}$ then $j > 0$ and so it is impossible to get the equivalence of $\varphi(w_{\mathcal{F}})$ with a word whose suffix is $\sharp\perp$.

Claim 3. Either $\varphi(\xi_j) = z_r^j$ when c_r^j occurs in a_j or $\varphi(\xi_j) = u_r^j$ when d_r^j occurs in a_j for some $r \in \{1, \ldots, n\}$. Indeed, if $s < j$ then $\varphi(\xi_j)$ and $\perp_{j-1}$ are dependent, hence $\sharp\perp$ cannot be the suffix of a word equivalent to $\varphi(w_{\mathcal{F}})$.

The occurrences of d_r^j or c_r^j in a_j indicate respectively that the literals X_r or $\neg X_r$ occur in C_j, then encoding with the letter u_r^j the value TRUE and with the letter z_r^j the value FALSE for the variable X_r in C_j, the assignment $\varphi(\xi_j)$ guarantees that at least one literal in C_j assumes the value TRUE. It remains to prove that each assignment satisfying the equation $w_{\mathcal{F}} \equiv w'_{\mathcal{F}}$ corresponds to a coherent way of assigning truth values to the variables in $\mathcal{F}$.

Claim 4. No $j, s \in \{0, 1, \ldots, M-1\}$ exist such that $\varphi(\xi_j) = u_r^j$ and $\varphi(\xi_s) = z_r^s$. Indeed for each φ satisfying the equation we get

$$\varphi(w_{\mathcal{F}}) \sim_{I_{\mathcal{F}}} e^2 a_0 e^2 a_1 \ldots e^2 a_{M-1} \varphi(\xi_0)\varphi(\xi_1) \ldots \varphi(\xi_{M-1}) t_{M-1} \ldots t_1 t_0 \sharp\perp.$$

Then the assignment φ has to satisfy the trace equation

$$\xi_0 \xi_1 \ldots \xi_{M-1} t_{M-1} \ldots t_1 t_0 \equiv t_{M-1} y_{3M} t_{M-2} y_{3M+1} \ldots t_0 y_{4M-1},$$

and this assures the claim 4. In fact suppose by contradiction that such j and s exist and that $j > s$. Then, since u_r^j and z_r^s are dependent and z_r^s depends on t_{s-1}, it follows that the assignment φ does not satisfy the last equation. So either the unknowns $\xi_j,\ j = 0, 1, \ldots, M-1$, which are not assigned to e correspond to different variables of $\mathcal{F}$, or if some of them correspond to the same variable X_r, φ gives them either the values u_r^j and u_r^s or the values z_r^j and z_r^s.
We can conclude that each assignment satisfying the equation encodes a truth assignment to the variables of $\mathcal{F}$ which satisfies the formula. □

The following example illustrates the construction done in the proof of Theorem 2 and also explains the rationale behind the definition of the alphabet and the independence relation.

Example 2. Let us consider the formula $\mathcal{F} = (X_1 \vee X_2 \vee \neg X_3) \wedge (\neg X_1 \vee \neg X_2 \vee \neg X_4)$.

Then we have:

$$\Sigma_{\mathcal{F}} = \bigcup_{\substack{i\in\{1,2,3,4\}\\ j\in\{0,1\}}} \{\, d_i^j,\, c_i^j,\, z_i^j,\, u_i^j,\, \perp_j,\, \sharp_j,\, t_j\ e\} \qquad \Xi = \{y_0, y_1, \ldots, y_7\}.$$

The left side and the right side of the trace equation associated with $\mathcal{F}$ are respectively:

$$w_{\mathcal{F}} = y_0\, y_1\, y_2\, d_1^0\, d_2^0\, c_3^0\, \sharp_0 \perp_0 y_3\, y_4\, y_5\, c_1^1\, c_2^1\, c_4^1\, \sharp_1 \perp_1 t_1\, t_0$$
$$w'_{\mathcal{F}} = e^2\, d_1^0\, d_2^0\, c_3^0\, e^2\, c_1^1\, c_2^1\, c_4^1\, t_1\, y_6\, t_0\, y_7\, \sharp_0 \perp_0 \sharp_1 \perp_1 .$$

We can associate with each coherent assignment of truth values the variables satisfying the formula $\mathcal{F}$ with an alphabetical assignment φ that satisfies the trace equation associated with $\mathcal{F}$. For instance, the formula $\mathcal{F}$ is satisfied giving the value TRUE to X_1 and the value FALSE to X_2, independently from the truth values assigned to the remaining variables. Then the relevant unknown associated with the first clause is y_0 and the relevant unknown associated with the second clause is y_4. It is easy to see that the assignment $\varphi : \Xi \to \Sigma_{\mathcal{F}}$ such that $\varphi(y_0) = \varphi(y_7) = u_1^0$, $\varphi(y_4) = \varphi(y_6) = z_2^1$, $\varphi(y_1) = \varphi(y_2) = \varphi(y_3) = \varphi(y_5) = e$ satisfies the trace equation $w_{\mathcal{F}} \equiv w'_{\mathcal{F}}$.
Conversely assume that there exists an alphabetical assignment φ that satisfies the trace equation $w_{\mathcal{F}} \equiv w'_{\mathcal{F}}$. Then at least four unknowns of $w_{\mathcal{F}}$ have to assume the value e. Only two unknowns in each set $\{y_0, y_1, y_2\}, \{y_3, y_4, y_5\}$ can take the value e because $(e, d_1^0), (e, c_1^1) \notin I_{\mathcal{F}}$. Then assume, for instance, $\varphi(y_1) = \varphi(y_2) = \varphi(y_4) = \varphi(y_5) = e$. Since $e^2\, d_1^0\, d_2^0\, c_3^0$ is a prefix of $\varphi(w'_{\mathcal{F}})$, $\varphi(y_0)$ has to be independent from the letters of that prefix, hence $\varphi(y_0) \in \{u_1^0, u_2^0, z_3^0\}$. In such case, by cancellativity, the assignment φ has to satisfy the following trace equation

$$\varphi(y_0)\sharp_0\perp_0 y_3\, e^2\, c_1^1\, c_2^1\, c_4^1\, \sharp_1 \perp_1 t_1\, t_0 \equiv e^2\, c_1^1\, c_2^1\, c_4^1\, t_1\, y_6\, t_0\, y_7\, \sharp_0 \perp_0 \sharp_1 \perp_1$$

whence $\varphi(y_3) \in \{z_1^1, z_2^1, z_4^1\} \cup \{\sharp_0, \perp_0\} \cup \{z_i^0, u_i^0 |\ 1 \le i \le 4\}$ and so

$$\varphi(y_0)\sharp_0\perp_0 \varphi(y_3)\, e^2\, c_1^1\, c_2^1\, c_4^1\, \sharp_1 \perp_1 t_1\, t_0 \sim_{I_{\mathcal{F}}}\ e^2\, c_1^1\, c_2^1\, c_4^1\, \varphi(y_0)\sharp_0\perp_0 \varphi(y_3) t_1\, t_0 \sharp_1 \perp_1 .$$

Using again cancellativity we obtain that the assignment φ has to satisfy the trace equation

$$\varphi(y_0)\sharp_0\perp_0 \varphi(y_3)\, t_1\, t_0 \equiv t_1\, y_6\, t_0\, y_7\, \sharp_0 \perp_0 \qquad (7)$$

It is easy to deduce that $\{\varphi(y_6), \varphi(y_7)\} = \{\varphi(y_0), \varphi(y_3)\}$, i.e. the unknowns of the right side of the trace equation have always to assume the same values taken by the relevant unknowns of the left side.
Now we want to show that actually $\varphi(y_3) \in \{z_1^1, z_2^1, z_4^1\}$. By contradiction, let for instance $\varphi(y_3) = \sharp_0$, then we have $\varphi(y_0)\sharp_0\perp_0 \varphi(y_3)\, t_1\, t_0 \sim_{I_{\mathcal{F}}} t_1 \varphi(y_0)\, t_0 \sharp_0 \perp_0 \sharp_0$. So the trace equation (7) is not satisfied by φ because the word $\varphi(t_1\, y_6\, t_0\, y_7\, \sharp_0 \perp_0)$ cannot be equivalent to a word whose suffix is $\perp_0\sharp_0$. Analogously we can prove that $\varphi(y_3) \neq \perp_0$.
Now suppose that $\varphi(y_3) \in \{z_i^0, u_i^0 |\ 1 \le i \le 4\}$ and, for instance, let $\varphi(y_3) = z_1^0$.

Then $\varphi(y_0)\sharp_0\bot_0\,\varphi(y_3)\,t_1\,t_0 \sim_{I_{\mathcal{F}}} t_1\,\varphi(y_0)\,t_0\sharp_0\,\bot_0 z_1^0$ and $(z_1^0, \bot_0) \notin I_{\mathcal{F}}$. It follows that the trace equation (7) is not satisfied by φ because $\varphi(t_1\,y_6\,t_0\,y_7\,\sharp_0\,\bot_0)$ cannot be equivalent to a word whose suffix is $\bot_0 z_1^0$.
We can deduce that $\varphi(y_3) \in \{z_1^1, z_2^1, z_4^1\}$ but notice that the choice of the values of $\varphi(y_0)$ and $\varphi(y_3)$ is tied, as required in the condition 2 in the proof of Theorem 2. If, for instance, $\varphi(y_0) = u_1^0$ then it is necessary that $\varphi(y_3) \neq z_1^1$. Indeed, if $\varphi(y_3) = z_1^1$ then $\varphi(y_0)\sharp_0\bot_0\,\varphi(y_3)\,t_1\,t_0 \sim_{I_{\mathcal{F}}} u_1^0 z_1^1 t_1\,t_0\sharp_0\,\bot_0$ hence, using cancellativity, by the equation (7) it follows that φ has to satisfy the trace equation $u_1^0 z_1^1 t_1\,t_0 \equiv t_1 y_6 t_0 y_7$. But this is impossible since $(u_1^0, z_1^1), (t_0, z_1^1) \notin I_{\mathcal{F}}$. This last fact allows to control the coherent assignment of the truth values to the relevant variables in $\mathcal{F}$. Indeed $\varphi(y_0) = u_1^0$ and $\varphi(y_3) = z_1^1$ would encode that X_1 is a relevant variable for both the first and the second clause and also that X_1 assumes in an incoherent way the value TRUE in the first clause and the value FALSE in the second one.
We can conclude that the assignment φ satisfying the trace equation encodes a coherent assignment of truth values to the variables of $\mathcal{F}$ which satisfies the formula.

5 Linear trace equations on free products of free commutative monoids

In this section we consider a linear trace equation $W_L \equiv W_R$ on a trace monoid $\mathbb{M}(\Sigma, I)$ that is a free product of free commutative monoids. This conditions means that the maximal I-cliques $C_1, \ldots, C_r$ of the independence alphabet (Σ, I) are disjoint. We give a polynomial time algorithm to solve the alphabetical satisfiability problem for such equation.

Remark 3. Let $[u], [v] \in \mathbb{M}$, and let $u = u_1 \ldots u_m$ be a decomposition of u such that, for each $i \in \{1, \ldots, m\}$, $u_i \in C_{j_i}^+$ for some $j_i \in \{1, \ldots, r\}$ and $j_i \neq j_{i+1}$. Then $[v] = [u]$ if and only if $v = v_1 \ldots v_m$ and, for each $i \in \{1, \ldots, m\}$, $v_i \sim_I u_i$.

In the sequel, for each word W we denote by $W(i)$ the i-th letter of W and by $W[i,k]$, $i \leq k$ the factor $W(i)W(i+1)\ldots W(k)$ of W.
As an immediate consequence of Remark 3, we obtain the following lemma:

Lemma 3. *Let φ be an alphabetical assignment that satisfies the trace equation $W_L \equiv W_R$ and let $i \in \{1, \ldots, |W_L|\}$, $k \in \{1, \ldots, r\}$ such that $W_L(i) = c \in C_k$ and $W_R(i) = x \in \Xi$ (resp. $W_L(i) = x \in \Xi$ and $W_R(i) = c \in C_k$). Then $\varphi(x) \in C_k$. Moreover there exist $1 = j_0 < j_1 < \ldots < j_s = |W_L| + 1$, such that $\varphi(W_L) = \prod_{i=0}^{s-1} \varphi(W_L[j_i, j_{i+1} - 1])$, $\varphi(W_R) = \prod_{i=0}^{s-1} \varphi(W_R[j_i, j_{i+1} - 1])$, with $\varphi(W_L[j_i, j_{i+1} - 1]) \in C_{k_i}^+$ for some $k_i \in \{1, \ldots, r\}$, $k_i \neq k_{i+1}$ and, for each $i \in \{0, \ldots, s-1\}$, $\varphi(W_L[j_i, j_{i+1} - 1]) \sim_I \varphi(W_R[j_i, j_{i+1} - 1])$.*

Now we introduce a function $\psi : \{0, 1, \ldots, |W_L| + 1\} \to \{-2, -1, 0, 1, \ldots, r\}$ to express when $W_L(i)$ and $W_R(i)$ belong to the same or to different maximal I-cliques or if they are unknowns. This function is defined in the following way:

$$\forall i \in \{0, 1, \ldots, |W_L| + 1\} \qquad \psi(i) = \begin{cases} -2 & \text{if } i \in \{0, |W_L| + 1\} \\ -1 & \text{if } W_L(i) \in C_h,\ W_R(i) \in C_k \\ & \text{with } h \neq k \\ 0 & \text{if } W_L(i), W_R(i) \in \Xi \\ h & \text{if } W_L(i), W_R(i) \in C_h \\ & \text{or } W_L(i) \in C_h \text{ and } W_R(i) \in \Xi \\ & \text{or } W_L(i) \in \Xi \text{ and } W_R(i) \in C_h \end{cases}$$

Definition 1. *A* microblock *associated with the trace equation $W_L \equiv W_R$ is a couple (i, j) of indices of $\{1, 2, \ldots, n\}$ with $i \leq j$ such that*

1. $\forall k \in \{i, \ldots, j-1\} \qquad \psi(k) = \psi(k+1) \notin \{-1, -2\}$;
2. $\psi(i-1) \neq \psi(i)$ *and* $\psi(j) \neq \psi(j+1)$.

A microblock (i, j) is called microblock of unknowns *if $\psi(i) = 0$ and* microblock of type h *if $\psi(i) = h$.*

Notice that if a microblock (j, k) of unknowns is preceded and followed by two microblocks of the same type h then, without loss of generality, we can suppose that an alphabetical assignment that satisfies the trace equation assigns the unknowns of $W_L[j, k]$ and of $W_R[j, k]$ in the same I-clique C_h. An analog argument holds if the first or the final microblock are microblocks of unknowns. This fact is stated in the following lemma:

Lemma 4. *Let $(i, j-1), (j, k-1), (k, l)$ with $1 \leq i < j < k \leq l \leq |W_L|$ be microblocks associated with the linear trace equation $W_L \equiv W_R$ such that $(j, k-1)$ is a microblock of unknowns and $(i, j-1), (k, l)$ are microblocks of type h. Then the trace equation $W_L \equiv W_R$ is alphabetically satisfiable if and only if there exists an alphabetical assignment φ satisfying $W_L \equiv W_R$ such that $\varphi(W_L[j, k-1]), \varphi(W_R[j, k-1]) \in C_h^+$.*
Analogously, let $(1, k-1), (k, l)$ with $1 < k \leq l \leq |W_L|$ (resp. $(j, k-1), (k, |W_L|)$ with $1 \leq j < k \leq |W_L|$) be the first two (resp. the last two) microblocks associated with the linear trace equation $W_L \equiv W_R$ such that $(1, k-1)$, (resp. $(k, |W_L|)$) is a microblock of unknowns and (k, l), (resp. $(j, k-1)$) is a microblock of type h. Then the trace equation $W_L \equiv W_R$ is alphabetically satisfiable if and only if there exists an alphabetical assignment φ satisfying $W_L \equiv W_R$ such that $\varphi(W_L[1, k-1]) \in C_h^+$, (resp. $\varphi(W_L[k, |W_L|]) \in C_h^+$).

Proof. Let $W_L \equiv W_R$ be a satisfiable linear equation and let φ be an alphabetical assignment satisfying $W_L \equiv W_R$ such that $\varphi(W_L[j, k-1]) \notin C_h^+$ and $\varphi(W_L[j, k-1])$ contains the minimum number f of factors in C_t^+ for any $t \in \{1, \ldots, r\} \setminus \{h\}$. Suppose that $f \geq 1$ and let $s \in \{j, \ldots, k-1\}$ be the first index such that $\varphi(W_L[s, s+p]) \in C_t^+$ and $\varphi(W(s+p+1)) \notin C_t$ for some $t \in \{1, \ldots, r\}$, $t \neq h$ and for some natural number p with $s+p \leq k-1$. Then, by Lemma 3, $\varphi(W_R[s, s+p]) \in C_t^+$ and $\varphi(W_L[s, s+p]) \sim_I \varphi(W_R[s, s+p])$. Let ϕ be an alphabetical assignment such that

$\phi(W_L(q)) = \phi(W_R(q)) = z \in C_h$ for all $q \in \{s, \dots, s+p\}$ and $\phi(x) = \varphi(x)$ for all $x \in \Xi$ that do not occur in $W_L[s, s+p]$ and $W_R[s, s+p]$. Then ϕ is an alphabetical assignment that satisfies $W_L \equiv W_R$ such that $\phi(W_L[j, k-1])$ contains less factors in C_t^+ for any $t \in \{1, \dots, r\} \setminus \{h\}$ than $\varphi(W_L[j, k-1])$. This is a contradiction, hence $f = 0$. □

The previous lemma justifies the following definition:

Definition 2. *Let $h \in \{1, \dots, r\}$. A* block of type h *associated with the linear trace equation $W_L \equiv W_R$ is a couple of indices (i, j), $i, j \in \{1, 2, \dots, |W_L|\}$, $i \le j$ such that there exist $i = i_1 < i_2 < \dots < i_s = j+1$ satisfying the following properties:*

1.
$$W_L[i, j] = \prod_{1 \le k < s} W_L[i_k, i_{k+1} - 1]$$

2. there exists $h \in \{1, \dots, r\}$ such that $(i, i_2 - 1), (i_{s-1}, i_s - 1)$ are microblocks of type h and, for all $k \in \{i, \dots, j\}$, $\psi(k) \in \{0, h\}$.

The factors $W_L[i, j]$ and $W_R[i, j]$ are called respectively left factor and right factor associated with the block (i, j). *Obviously each microblock is a block.*
A macroblock of type h *associated with the trace equation $W_L \equiv W_R$ is a couple of indices $i, j \in \{1, 2, \dots, |W_L|\}$ with $i \le j$ such that there exists a block (i', j') of type h satisfying the following properties:*

1. $i \le i' \le j' \le j$;

2. if $i \ne i'$ (resp. $j \ne j'$) then, for all $k \in \{i, \dots, i'\}$ (resp. $k \in \{j', \dots, j\}$), $\psi(k) = 0$.

Now we describe a linear algorithm to state whether the linear trace equation $W_L \equiv W_R$ on the trace monoid on $\mathbb{M}(\Sigma, I)$ is satisfiable when the maximal I-cliques $C_1, \dots, C_r$ of the independence alphabet (Σ, I) are disjoint. Roughly speaking, the algorithm works in the following way. It identifies the blocks associated with $W_L \equiv W_R$ and checks if $W_L[i, j] \equiv W_R[i, j]$ in each block (i, j). If so the equation is satisfiable. If for some block (i, j) the trace equation $W_L[i, j] \equiv W_R[i, j]$ is not satisfied and no block of unknowns is adjacent to (i, j), the algorithm exits and outputs "NO". Otherwise it extends the block (i, j) to a macroblock (i', j') including also these new unknowns and it checks whether $W_L[i', j'] \equiv W_R[i', j']$ is satisfiable. The procedure is described in Algorithm 1.
Now we check the correctness of the Algorithm 1. The procedure from line 1 to line 13 identifies the blocks associated with the trace equation by building an array η whose odd and even cells contain respectively the beginning and the end of a block of a certain type h with $h \ne 0$. The initial and final blocks identified by the previous procedure can be macroblocks. In fact if the trace equation begins or finishes with microblocks of unknowns, thanks to Lemma 4 we can assume without loss of generality that an alphabetical assignment satisfying the trace equation gives to the unknowns of these microblocks values in the same I-cliques of the adjacent

Algorithm 1 Equation satisfiability with disjoint maximal I-cliques

```
η(1) ← 1, k ← 2,c ← 1
for i = 1 to |W_L| do
    if ψ(i) = −1 then
        Exit and write "NO"
    end if
    if ψ(i) ≠ 0 then
        if ψ(c) ∉ {ψ(i), 0} then
            η(k) ← c, η(k + 1) ← i, k ← k + 2
        end if
        c ← i
    end if
end for
η(k) ← |W_L|
in ← 1
for t = 1 to k/2 do
    out ← η(2t)
    for i = 1 to |Σ| do
        K_R(i) ← 0
        K_L(i) ← 0
    end for
    for i = in to out do
        for j = 1 to |Σ| do
            if W_L(i) = a(j) then
                K_L(j) ← K_L(j) + 1
            end if
            if W_R(i) = a(j) then
                K_R(j) ← K_R(j) + 1
            end if
        end for
    end for
    θ ← 0
    for j = 1 to |Σ| do
        H(j) ← K_R(j) − K_L(j)
        if H(j) > 0 then
            θ ← θ + H(j)
        end if
    end for
    λ ← out − in + 1 − \sum_{s=1}^{|Σ|} K_L(s)
    if λ − θ ≤ 0 then
        if η(2t + 1) − out − 1 < |λ − θ| then
            Exit and write "NO"
        else
            in ← out + |λ − θ| + 1
        end if
    else
        in ← out + 1
    end if
end for
Exit and write "YES"
```

block. Hence we can directly consider the initial and final macroblocks.
Let (in, out) with $in = 1$ be the first block associated with the trace equation and suppose that it is of type l. By Lemmas 3 and 4 we can assume, without loss of generality, that an alphabetical assignment satisfying the trace equation gives to the unknowns some values in the same maximal I-clique C_l. So we can check if such an assignment exists just counting the number of occurrences of a letter $a(i) \in \Sigma$ in the left and right factors associated with (in, out). Hence the procedure from line 17 to line 30 defines two arrays K_L and K_R whose i-th cell contains respectively $|W_L[in, out]|_{a(i)}$ and $|W_R[in, out]|_{a(i)}$, i.e. the number of the occurrences of the letter $a(i)$ respectively in the left and in the right factor associated with the block (in, out). If $K_R(j) - K_L(j) > 0$ (resp. $K_R(j) - K_L(j) < 0$) for some j, it means that $a(j)$ is a *right surplus constant* (resp. *left surplus constant*), i.e. $a(j)$ has a number of occurrences in the right (resp. left) factor associated with (in, out) greater than in the left (resp. right) factor. Hence a suitable number of unknowns of $W_L[in, out]$ (resp. $W_R[in, out]$) has to be assigned to $a(j)$. Obviously if $K_R(j) - K_L(j) = 0$ we have no constraints on the assignments to the unknowns.
Now we have to check if the number of unknowns in the left (resp. right) factor associated with (in, out) is sufficient to match with the right (resp. left) surplus constants. Therefore we introduce the following notations:

- λ: number of unknowns in the left factor associated with (in, out);
- β: number of unknowns in the right factor associated with (in, out);
- θ: number of the right surplus constants of (in, out);
- ρ: number of the left surplus constants of (in, out).

So we have to consider the differences $\lambda - \theta$ and $\beta - \rho$. Using the arrays K_L and K_R we have:

$$\lambda = out - in + 1 - \sum_{s=1}^{|\Sigma|} K_L(s) \qquad \beta = out - in + 1 - \sum_{s=1}^{|\Sigma|} K_R(s)$$

$$\theta = \sum_{\substack{i \in \{1,\dots,|\Sigma|\}, \\ K_R(i) > K_L(i)}} (K_R(i) - K_L(i)) \qquad \rho = \sum_{\substack{i \in \{1,\dots,|\Sigma|\}, \\ K_L(i) > K_R(i)}} (K_L(i) - K_R(i))$$

A trivial verification shows that $\lambda - \theta = \beta - \rho$, hence the procedure from line 31 to 38 determines θ and λ. If $\lambda - \theta \leq 0$, it means that the number of unknowns in the left factor are not sufficient to match with the right surplus constants, hence the trace equation $W_L[in, out] \equiv W_R[in, out]$ is not alphabetically satisfiable. It follows that the initial trace equation $W_L \equiv W_R$ can be satisfied only if there exists a block $(out + 1, out + s)$ of unknowns such that $s \geq |\lambda - \theta|$. In that case the trace equation $W_L[in, out + |\lambda - \theta|] \equiv W_R[in, out + |\lambda - \theta|]$ is alphabetically satisfiable. If $|\lambda - \theta| < s$, the procedure from line 39 to line 47 adds the remaining $s - |\lambda - \theta|$ unknowns of the factors associated with $(out + 1, out + s)$ to the factors associated

with the block following $(out+1, out+s)$ obtaining a new macroblock. Then the entire process is iterated considering the successive macroblock (in, out).
Notice that the algorithm works in linear time. Clearly the procedure 1-14 require a linear time, hence let us consider the cycle of lines 15-48. It runs on the number $k/2$ of macroblocks associated with the trace equation. Let us denote by $(in(i), out(i))$ the macroblock in the i^{th} iteration and put $l_i = out(i) - in(i)$. Since the cycle of lines 21-30 scans the macroblock $(in(i), out(i))$ and $[in(i), out(i)] \cap [in(i+1), out(i+1)] = \emptyset$ (where, for all $p, q \in \mathbb{N}$ such that $p \leq q$, $[p, q]$ is the subset of natural numbers $\{p, p+1, \ldots, q\}$), we obtain that

$$\sum_{i=1}^{k/2} l_i \leq n.$$

Hence, an easy calculation allow to conclude that the number of steps in the cycle 15-48 is $O(n)$.

Example 3. Let $\Sigma = \{a, b, c, d\}$ and let $I = \{(a, b), (b, a), (c, d), (d, c)\}$ be the independence relation. Hence $C_1 = \{a, b\}$, $C_2 = \{c, d\}$ are the maximal I-cliques. Let us consider the trace equation $W_L \equiv W_R$, where

$$W_L = ax_1adx_2x_3ddcdddx_4x_5x_6a$$

and

$$W_R = bay_1cy_2y_3cdcy_4ccy_5y_6y_7b.$$

The division of the equation in blocks is the following:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a	x_1	a	d	x_2	x_3	d	d	c	d	d	d	x_4	x_5	x_6	a
b	a	y_1	c	y_2	y_3	c	d	c	y_4	c	c	y_5	y_6	y_7	b

The array η relative to the beginning and the end of each block of type 1 or 2 is $\eta = (1, 3, 4, 12, 16, 16)$.
It is easy to see that $W_L[1, 3] \equiv W_R[1, 3]$ is alphabetically satisfiable.
In the next block $(4, 12)$ we have

$$K_L = (0, 0, 1, 6),\ K_R = (0, 0, 5, 1),\ H = (0, 0, 4, -5),\ \theta = 4,\ \lambda = 2$$

so $\lambda - \theta < 0$ and the trace equation $W_L[4, 12] \equiv W_R[4, 12]$ is not alphabetically satisfiable. But $\eta(5) - 12 - 1 \geq |\lambda - \theta|$ hence we can extend the block $(4, 12)$ to the macroblock $(4, 14)$ obtaining a trace equation $W_L[4, 14] \equiv W_R[4, 14]$ that is alphabetically satisfiable.
We include the remaining unknowns in position 15 to the factors associated with the next block $(16, 16)$ that therefore becomes the macroblock $(15, 16)$. It is evident that $W_L[15, 16] \equiv W_R[15, 16]$ is alphabetically satisfiable, so we can conclude that the initial trace equation $W_L \equiv W_R$ is alphabetically satisfiable too.

6 Conclusion

It is still an open problem to determine the complexity class of the general alphabetical satisfiability problem for a linear trace equation. The problem is polynomial when the number of unknowns in one side of the equation is logarithmic with respect the length of a member of the equation.
In Section 5 we proved that there is a polynomial time algorithm to check the alphabetical satisfiability problem on free products of free commutative monoids. We also have a (not yet published) polynomial time algorithm to solve the satisfiability problem for linear trace equations on free products with amalgamation of free commutative monoids, i.e. partially free commutative monoids whose maximal I-cliques $C_1, \ldots, C_r$ satisfy the condition $C_i \cap C_j = \bigcap_{k=1}^{r} C_k$ for all $i, j \in \{1, \ldots, r\}$. Previous monoids are both particular cases of free partially commutative monoids that are free products of free products with amalgamation of free commutative monoids, i.e. monoids whose independence alphabet (Σ, I) fulfils the following conditions: Σ is a disjoint union of Σ_i such that each I-clique of (Σ, I) is contained in some Σ_i and for each pair of I-cliques C_h,C_k contained in Σ_i for some i, $C_h \cap C_k$ is equal to the intersection of all the I-cliques contained in Σ_i. So we strongly conjecture that also in this case there is a polynomial algorithm for the alphabetical satisfiability problem for linear trace equations.
It would be interesting to consider in the future the complexity class of the alphabetical satisfiability problem for linear equations under some other constraints on the independence alphabet in order to have some hint for the general case.

References

[1] A. Bertoni, G. Mauri, N. Sabadini, *Equivalence and membership problems trace languages*, LNCS 140, 1982, 61-71.

[2] F. Blanchet-Sadri, *Algorithmic Combinatorics on Partial Words*, Chapman and Hall/CRC Press, Boca Raton, FL, 2008.

[3] P. Cartier and D. Foata, *Problèmes combinatoires de commutation and réarrangements*, LNM 85, 1969.

[4] V. Diekert, Yu. Matiyasevich and A. Muscholl, *Solving trace equations using lexicographical normal forms*, LNCS 1256, 1997, 336-347.

[5] V. Diekert, Yu. Matiyasevich and A. Muscholl, *Solving word equations modulo partial commutations*, TCS 224, 1999, 224-215.

[6] V. Diekert and J. Robson, *Quadratic word equations*, Jewels are Forever, 1999, 314-326.

[7] R. M. Keller, *Parallel program schemata and maximal parallelism I. Fundamental results*, Journal of A. C. M. 20 3, 1973, 514-537.

[8] G. S. Makanin, *The problem of solvability of equations in a free semigroup*, Math. Sbornik 103, 1977, 147-236, English transl. in Math. URSS Sbornik 32 (1977).

[9] A. A. Markov, *The theory of algorithms*, Trudy Math. Inst. Steklov. 42, (1954).

[10] Yu. Matiyasevich, *Some decision problems for traces*, LNCS 1234, 1997, 248-257.

[11] A. A. Mazurkiewicz, *Trace theory*, LNCS 255, 1987, 279-324.

[12] J. M. Robson and V. Diekert, *On quadratic word equations*, LNCS 1563, 1999, 217-226.

[13] V. Diekert and G. Rozenberg editors, *The book of traces*, World Scientific, 1995.

Received 12th October 2008