Systems of Equations Satisfied in All Commutative Finite Semigroups

Paweł Parys, Warsaw University (parys@mimuw.edu.pl)

May 7, 2007

Abstract

The following problem is considered: check if a system of equations has a solution in every commutative finite semigroup. It is shown that the problem is decidable, and NP-complete.

1 Introduction

There are at least two problems connected with solving systems of equations in semigroups. The first is solving a system of equations in a given free semigroup [6]. The second is solving a system of equations in a given finite semigroup [5].

Another interesting problem is to check if a system of equations is satisfied in all semigroups simultaneously. However, it can be easily shown that a system of equations having a solution in the free semigroup, also has a solution in every other semigroup. In a sense, for equations the free semigroup is the most difficult of semigroups. This argument, however, fails for finite semigroups. There are systems, which have solutions in all finite semigroups, but not in the free semigroup. For instance in a finite semigroup, when we add an element to itself several times, we always start looping, which can cause the existence of a solution. It's easy to show that in every finite semigroup there exists an idempotent element (i.e. a solution of an equation $x + x = x$). It is enough to take any element and to add it to itself appropriate number of times. This fails in the free semigroup (no empty words). Solving of other equations will be a generalisation of this observation.

Exactly the following problem may be considered: Given a system of equations (with variables and coefficients), decide if the system has a solution in every finite semigroup and for every evaluation of the coefficients in this semigroups.

The problem of checking if a system have a solution in every finite semigroup is interesting itself, but it has also some motivation. There is a correspondence between finite semigroups and regular languages, so questions about semigroups are also questions about regular languages. Solving equations in finite semigroups can be seen as generalisation of pumping. What does it mean that a system of equations has a solution in every finite

semigroup? For any finite semigroup (finite automaton) we choose, there would exist such values of variables such that in this semigroup left and right sides will evaluate to the same element. So using these values of variables we will deceive any semigroup: it cannot distinguish between the left and right side. For example in recent work over tree-walking automata, standard pumping lemmas proved to inadequate, and nonexpressiveness results were shown by using equations in semigroups. For example in [1] for every semigroup and for every a and b they need to have u and v such that $u = u + a + u = u + b + v$ and $v = v + a + u = v + b + v$.

In this paper I concentrate on commutative semigroups and on a problem if a system has a solution in every commutative finite semigroup.

Theorem 1.1 *The following problem is NP-complete: Given a system of word equations, decide if the system has a solution in every finite commutative semigroup.*

The non-commutative case is left open.

2 Notations and Definitions

Vectors of letters like $c_1, \ldots, c_m$ or $X_1, \ldots, X_n$ etc. will be denoted by $\bar{c}, \bar{X}, \ldots$ When I need to consider simultaneously several vectors of the same type, I use superscripts: $\bar{X}^{(1)}, \ldots, \bar{X}^{(h)}, \ldots$

For a in a semigroup and $k \geq 1$ I write $k \cdot a$ for a added to itself k times.

I fix the following finite nonempty alphabets:

$\Sigma_0 = \{X_1, \ldots, X_\gamma\}$ — the alphabet of *variables*,

$\Sigma_1 = \{C_1, \ldots, C_\omega\}$ — the alphabet of *coefficients*.

An *interpretation of coefficients* in a semigroup S is a vector $\bar{c} = (c_1, \ldots, c_\omega)$ of elements of S (an element c_i corresponds to a coefficient C_i). It is easier to treat an interpretation of coefficients as a part of a semigroup. A pair $(S, \bar{c})$ of a semigroup and an interpretation of coefficients in it will be called a *semigroup with coefficients*. Since now as a semigroup I will understand a semigroup with coefficients and sometimes I will simply write S for $(S, \bar{c})$.

A *system of equations* $\bar{\phi}$ is a system of equalities of the form

$$\begin{cases} \phi_{11} = \phi_{12} \\ \quad \ldots \\ \phi_{m1} = \phi_{m2} \end{cases}$$

where $\phi_{11}, \ldots, \phi_{m1}, \phi_{12}, \ldots, \phi_{m2}$ are nonempty words over $\Sigma_0 \cup \Sigma_1$. Sometimes I will write plus signs between symbols in the equations (just for convenience). For a given semigroup with coefficients $(S, \bar{c})$ and vector $\bar{x}$ of elements of S, by $\phi_{js}(\bar{x})$ I denote evaluation of ϕ_{js} in semigroup S with c_i (and x_i) substituted for C_i (and X_i). For a given semigroup with coefficients $(S, \bar{c})$, a *solution* of the system $\bar{\phi}$ is a vector $\bar{x} \in S$ such that $\phi_{i1}(\bar{x}) = \phi_{i2}(\bar{x})$ for all $1 \leq i \leq m$.

A *homomorphism* of semigroups with coefficients from $(S, \bar{c})$ to $(S', \bar{c}')$ is a homomorphism of semigroups $f\colon S \to S'$ such that $f(c_i) = c'_i$ for every i. See that if a system $\bar{\phi}$ has a solution $\bar{x}$ in $(S, \bar{c})$ and we have any homomorphism $f\colon (S, \bar{c}) \to (S', \bar{c}')$, then image of $\bar{x}$ is obviously a solution in $(S', \bar{c}')$.

We will shortly say that a system *has a solution in the class FinComm* if for every commutative finite semigroup with coefficients there exists a solution of the system. Note the quantifier alternation: for all semigroups and all values of the coefficients, one must be able to find a values of the variables that yield a solution. In the article I present an algorithm for solving the following problem:

> Input: a system of equations.
> Output: Has the system a solution in every commutative finite semigroup with coefficients?

What would happen if we've skipped the word "finite"? When a system has a solution in every commutative semigroup it also has in a free commutative semigroup. There is a homomorphism from the free commutative semigroup to any other, so from a solution in free commutative semigroup we get a solution in any other commutative semigroup. Therefore the problem would reduce to finding solutions in the free commutative semigroup, which is easy.

3 Special form of equations: variables on both sides

Definition 3.1 *I will say that an equation is* balanced *if on its every side there is at least one variable. I will say that a system of equations is* balanced *if every equation is balanced.*

The problem is somehow easier if we consider only balanced systems. At the beginning I will solve the problem in this special case. The results from this section will be used later for solving the general case.

3.1 One coefficient

At the very beginning we will consider an even simpler form of systems, where at most one coefficient is used in the system. A general balanced system will be later reduced to several such systems. The following two theorems tell us that it sufficient to solve such systems over $\mathbb{Z}$.

Theorem 3.2 *Let C be a coefficient and let $\bar{\phi}$ be a balanced system where no coefficients other than C appear in the system. Then the following statements are equivalent:*

1. *the system $\bar{\phi}$ has a solution in FinComm;*
2. *for every $n \geq 2$ the system $\bar{\phi}$ has a solution in the group $\mathbb{Z}_n$ (integers modulo n) with an interpretation $C \mapsto 1$.*

Interpretation of coefficients other than C doesn't matter, as they do not appear in the system, but for completeness we should fix it somehow.

In a proof of the theorem I will use the following fact:

Fact 3.3 *For a given element c of a finite semigroup S there exists N such that $2N \cdot c = N \cdot c$.*

Proof Look at all multiples of c. As there is only finite number of elements in S, there have to be $k \cdot c = (k+l) \cdot c$ for some $k, l \geq 1$. Adding to this equation $l \cdot c$ several times we get

$$k \cdot c = (k+l) \cdot c = (k+2l) \cdot c = \ldots = (k+kl) \cdot c.$$

Then adding $(l-1)k \cdot c$ to it we get $kl \cdot c = 2kl \cdot c$. So taking $N = kl$ we are done. ■

Proof of Theorem 3.2 $1 \Rightarrow 2$. Obvious, because 2 is a special case of 1.

$1 \Leftarrow 2$. Fix a commutative finite semigroup S with an interpretation $c \in S$ of the coefficient C, for which the system should have a solution. Let N be such that $2N \cdot c = N \cdot c$ (from fact 3.3). We have the following two properties for every $k, l \geq 0$:

- there is $(N+k) \cdot c + (N+l) \cdot c = (N+k+l) \cdot c$;
- if additionally $k \equiv l \pmod{N}$ there is $(N+k) \cdot c = (N+l) \cdot c$.

Let $\bar{y}$ will be a solution of the system in $\mathbb{Z}_n$ (understood as numbers from 0 to $N-1$), which exists from point 2. We take $x_j = (N + y_j) \cdot c$ for all $1 \leq j \leq \gamma$. Then for every $1 \leq i \leq m$, $s = 1, 2$ we have $\phi_{is}(\bar{x}) = (N + \phi_{is}(\bar{y})) \cdot c$. Since $\bar{y}$ is a solution in $\mathbb{Z}_n$, we have $\phi_{i1}(\bar{y}) \equiv \phi_{i2}(\bar{y}) \pmod{N}$, so $(N + \phi_{i1}(\bar{y})) \cdot c = (N + \phi_{i2}(\bar{y})) \cdot c$, which means that $\bar{x}$ is a solution in S. ■

Theorem 3.4 *Let C be a coefficient and let $\bar{\phi}$ be a balanced system where no coefficients other than C appear in the system. Then the following statements are equivalent:*

1. *for every $n \geq 2$ the system $\bar{\phi}$ has a solution in the group $\mathbb{Z}_n$ with an interpretation $C \mapsto 1$;*
2. *the system $\bar{\phi}$ has a solution in the group $\mathbb{Z}$ with an interpretation $C \mapsto 1$.*

Proof $1 \Leftarrow 2$. This implication is almost obvious. For every n there is a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$ (taking numbers modulo n), so if we have a solution in $\mathbb{Z}$, we also have it in $\mathbb{Z}_n$.

$1 \Rightarrow 2$. In this theorem in fact we deal with classical systems of number equations in $\mathbb{Z}$ or $\mathbb{Z}_n$. The system can be written in the form of $\bar{\bar{a}} \cdot \bar{X} = \bar{b}$ where $\bar{\bar{a}}$ and $\bar{b}$ are a matrix and a vector of integer numbers and $\bar{X}$ is a vector of variables. For solving this system in $\mathbb{Z}$ we can perform a Gauss elimination on the pair $(\bar{\bar{a}}, \bar{b})$. To keep all the constants in $\mathbb{Z}$ we cannot divide a equation by a number, we can only multiply, but it is enough. The only difference from normal Gauss elimination (with division allowed) is that we are not

able to get ones "on the diagonal", we get there arbitrary nonzero numbers. After possibly changing numeration of variables (order of columns in $\bar{\bar{a}}$) we get the following equivalent system

$$\begin{bmatrix} a_{11} & 0 & 0 & \dots & 0 & a_{1,k+1} & a_{1,k+2} & \dots & a_{1\gamma} \\ 0 & a_{22} & 0 & \dots & 0 & a_{2,k+1} & a_{2,k+2} & \dots & a_{2\gamma} \\ 0 & 0 & a_{33} & \dots & 0 & a_{3,k+1} & a_{3,k+2} & \dots & a_{3\gamma} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & a_{kk} & a_{k,k+1} & a_{k,k+2} & \dots & a_{k\gamma} \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{bmatrix} \begin{bmatrix} X_1 \\ X_2 \\ X_3 \\ \vdots \\ X_k \\ X_{k+1} \\ X_{k+2} \\ \vdots \\ X_\gamma \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \\ b_k \\ b_{k+1} \\ \vdots \\ b_m \end{bmatrix}$$

where $a_{11}, \dots, a_{kk}$ are nonzero.

The same operations we can do, when we are considering the system over $\mathbb{Z}_n$, and we get the same system (with the exception that all numbers are treated modulo n). Here the system we get is not necessarily equivalent to the original one (when multiplying by a number which has common divisors with n, a equality may become true, when it wasn't). But if the original system had a solution, then this also has (for every $\mathbb{Z}_n$).

Firstly see that $b_{k+1} = b_{k+2} = \ldots = b_m = 0$. Otherwise for $b_i \neq 0$ we have a equation $0 = b_i$ which should be satisfied in all semigroups $\mathbb{Z}_n$, but is not satisfied in almost all of them, e.g. for any $n > b_i$.

Let $n = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{kk}$. Let $x_1, \dots, x_\gamma$ be a solution in this $\mathbb{Z}_n$. The i-th equation $(1 \leq i \leq k)$ says that

$$a_{ii}x_i + a_{i,k+1}x_{k+1} + a_{i,k+2}x_{k+2} + \ldots + a_{i\gamma}x_\gamma \equiv b_i \pmod{a_{11} \cdot a_{22} \cdot \ldots \cdot a_{kk}}$$

from which we have

$$a_{ii}x_i + a_{i,k+1}x_{k+1} + a_{i,k+2}x_{k+2} + \ldots + a_{i\gamma}x_\gamma \equiv b_i \pmod{a_{ii}}$$

which means that

$$a_{ii} | b_i - a_{i,k+1}x_{k+1} - a_{i,k+2}x_{k+2} - \ldots - a_{i\gamma}x_\gamma \tag{1}$$

As a solution for $\mathbb{Z}$ we will take:

$$x'_i = \begin{cases} (b_i - a_{i,k+1}x_{k+1} - a_{i,k+2}x_{k+2} - \ldots - a_{i\gamma}x_\gamma) \cdot \frac{1}{a_{ii}} & \text{for } 1 \leq i \leq k \\ x_i & \text{for } k+1 \leq i \leq \gamma \end{cases}$$

Condition (1) guaranties that x'_i is integer. It's easy to see that it is really a solution. ■

3.2 Many coefficients

Definition 3.5 *For a given balanced system $\bar{\phi}$ and a coefficient $C \in \Sigma_1$ we define a projection $\bar{\phi}^{(C)}$ as a system obtained from $\bar{\phi}$ by erasing all coefficients other than C.*

Notice that the assumption that $\bar{\phi}$ has a variable on every side (is balanced) guarantees that $\bar{\phi}^{(C)}$ also has a variable on every side. In particular the sides are nonempty, so we get an well defined system.

Lemma 3.6 *Let $\bar{\phi}$ be a balanced system. Then the following statements are equivalent:*

1. *the system $\bar{\phi}$ has a solution in FinComm;*
2. *for every coefficient $C \in \Sigma_1$ and $n \geq 2$ the system $\bar{\phi}^{(C)}$ has a solution in the group $\mathbb{Z}_n$ with an interpretation $C \mapsto 1$.*

Proof $1 \Rightarrow 2$. Almost obvious. Fix C and n. As a special case of 1 we get that the system $\bar{\phi}$ has a solution in $\mathbb{Z}_n$ with interpretation $C \mapsto 1$ and $D \mapsto 0$ for all $D \in \Sigma_1$, $D \neq C$. But this solution is also a solution of $\bar{\phi}^{(C)}$, because evaluation of sides of $\bar{\phi}$ and $\bar{\phi}^{(C)}$ are the same (the only difference is that in $\bar{\phi}$ we add 0 several times).

$1 \Leftarrow 2$. Fix a commutative finite semigroup S with coefficients $\bar{c}$. From 2 and Theorem 3.2 for every $C_i \in \Sigma_1$ we have a solution $\bar{x}^{(C_i)}$ of the projection $\bar{\phi}^{(C_i)}$ in S. As our solution of the whole system we take the sum of these solutions: $x_j = x_j^{(C_1)} + x_j^{(C_2)} + \ldots + x_j^{(C_\omega)}$ for every $1 \leq j \leq \gamma$. Then the evaluation of a side of an equation will be the sum of evaluations of sides of equations for one coefficient: $\phi_{ks}(\bar{x}) = \phi_{ks}^{(C_1)}(\bar{x}^{(C_1)}) + \phi_{ks}^{(C_2)}(\bar{x}^{(C_2)}) + \ldots + \phi_{ks}^{(C_\omega)}(\bar{x}^{(C_\omega)})$. This is because every c_i or $x_j^{(C_i)}$ appears the same number of times in $\phi_{ks}(\bar{x})$ as in $\phi_{ks}^{(C_i)}(\bar{x}^{(C_i)})$ and does not appear in any other element. Of course we've used the assumption that the semigroup is commutative. ■

As an immediate corollary of Lemma 3.6 and Theorem 3.4 we get the following theorem:

Theorem 3.7 *Let $\bar{\phi}$ be a balanced system. Then the following statements are equivalent:*

1. *the system $\bar{\phi}$ has a solution in FinComm;*
2. *for every coefficient $C \in \Sigma_1$ the system $\bar{\phi}^{(C)}$ has a solution in the group $\mathbb{Z}$ with an interpretation $C \mapsto 1$.*

So we've got an easy to check criterion for testing if such system has a solution in the class *FinComm*.

4 General case

4.1 Everywhere something is one everywhere

Now I will prove an important technical lemma, which simplifies further argumentation. Here we need a version of the lemma for commutative finite semigroups, but the same lemma is true for general finite semigroups.

Lemma 4.1 *Let $\{\bar{\phi}^{(1)}, \ldots, \bar{\phi}^{(N)}\}$ be systems of equations such that in every commutative finite semigroup with coefficients some $\bar{\phi}^{(i)}$ has a solution. Then some of the systems $\bar{\phi}^{(i)}$ has a solution in every of these semigroups.*

Proof Assume that for every system $\bar{\phi}^{(i)}$ there exists a semigroup S_i in which there is no solution of $\bar{\phi}^{(i)}$. Look at the product semigroup $S = S_1 \times \ldots \times S_N$ (naturally interpretation of coefficient in the product is a sequence of its interpretations in every S_i). Some system $\bar{\phi}^{(i)}$ has to have a solution in S. But we have a homomorphism from S to S_i (a projection), so $\bar{\phi}^{(i)}$ has a solution in S_i too. But we've assumed that it hasn't, we've got contradiction, so the theorem is true. ■

4.2 Removing "wrong" variables

Let $\bar{\phi}$ be a system in which in some equations on one side there are only coefficients and on the other side there are also variables. We will replace the system by a number of simpler systems. For notational simplicity, assume that this happened in the first equation: that on the right side of this equation (ϕ_{12}) there are only coefficients, and that on its left side (ϕ_{11}) there is at least the variable X_1. For a word of coefficients $w \in \Sigma_1^*$ we define a system $\bar{\phi}^{(w)}$. It will be $\bar{\phi}$ in which we replace every occurrence of X_1 in every equation by the word w. We will be considering these systems for all nonempty subsequences of the right side of the first equation (in fact the order of coefficients in w doesn't matter, as we have only commutative semigroups, so we can also think about all submultisets of the ϕ_{12}). Obviously there are only finitely many of these subsequences.

Theorem 4.2 *For a system $\bar{\phi}$ as above, the system has a solution in FinComm if and only if for some w — subsequence of ϕ_{12}, the system $\bar{\phi}^{(w)}$ has a solution in FinComm.*

Proof $\Leftarrow$. Let w be this subsequence of ϕ_{12}, for which $\phi^{(w)}$ has a solution in *FinComm*. Fix a commutative finite semigroup with coefficients S, for which we need a solution of $\bar{\phi}$. Let $\bar{x}$ be a solution of $\bar{\phi}^{(w)}$ there. As a solution of $\bar{\phi}$ we can take an evaluation of w as x_1 and values from $\bar{x}$ as the other variables. Then the evaluation of sides of $\bar{\phi}$ and $\bar{\phi}^{(w)}$ are the same, so this is a solution of $\bar{\phi}$ (the only difference between $\bar{\phi}$ and $\bar{\phi}^{(w)}$ is that on the places of X_1 we have w, but they both evaluates to the same value).

$\Rightarrow$. According to Lemma 4.1 it is enough to show that in every commutative finite semigroup for every interpretation of coefficients at least one of these systems has a solution.

Then the lemma would say that one of the systems would have a solution in every of these semigroups.

Fix a commutative finite semigroup with coefficients S, for which we need a solution of some system $\bar{\phi}^{(w)}$. We will construct a semigroup S' and basing on a solution of $\bar{\phi}$ in it, we will construct a solution of some $\bar{\phi}^{(w)}$ in S. Let N be the length of ϕ_{12} (the right side of the first equation, which contains only coefficients). The semigroup S' will contain two disjoint parts:

1. all the elements of S;
2. all commutative words (multisets) of coefficients from Σ_1 up to length N.

Now we need to define an operation. Inside S we just add in S. When adding between the parts, we evaluate the word of coefficients in S and then add in S. When adding two words of coefficients, we concatenate it. If the result fits into second part (has length $\leq N$), we just take it. When it is longer, we evaluate it in S. The idea is that S' for short words simulates free commutative semigroup. Words no longer than N we remember as they are, for longer words we remember only their value in S.

We take an interpretation of coefficients in S' such that a coefficient is interpreted as an one-letter word containing it. S' is a commutative finite semigroup, so $\bar{\phi}$ has a solution $\bar{x}'$ in it. See that when something is in the first part, then after adding anything it will remain in this part. The right side of the first equation, which contains just N coefficients, in S' will evaluate to itself in the second part. This means that x'_1 (and the whole left side) is also in the second part. Moreover, x'_1 is a submultiset of the right side. We will take x'_1 as the word w. Now we need to have a solution of $\bar{\phi}^{(w)}$ in S. As x_i (for $2 \leq i \leq \gamma$) we will take x'_i when it is in the first part or evaluation of x'_i in S, when it is in the second part. It's easy to see that $\bar{\phi}^{(w)}$ gives now the same equalities, as $\bar{\phi}$ before (when an equation from $\bar{\phi}$ in S' has given an equality on words, then it also holds after evaluation to S). So it's a solution in S and we're done. ■

4.3 The algorithm

Theorem 4.2 almost gives us an algorithm. In every moment we will have a set of systems, about which we'd like to know if at least one of the systems has a solution in *FinComm*. At the very beginning the set contains only the original system. Then we repeatedly replace a system, in which in some equations variables are only on one side, by a number of systems, as described above. See that after such step, we get systems containing less variables, so the process has to finish. At the end we get a set of systems, in which every equation contains at least one variable on both sides or no variables at any side.

Now see what happens, if in an equation there are only coefficients. If the number of coefficients of every kind is equal on both sides (the sides are equal as multisets), then the equation is always satisfied, because our semigroups are commutative. In this case we can just remove this equation and we get equivalent system. Otherwise there is an coefficient

C, which on left side appears k times and on the right side l times, where $k \neq l$. Consider an additive group $\mathbb{Z}_{k+l+1}$ with interpretation $C \mapsto 1$ and $D \mapsto 0$ for all $D \in \Sigma_1$, $D \neq C$. Here left side evaluates to k and right side to l, which aren't equal, so the equality isn't satisfied. This means that we can immediately say that system containing such equation cannot have a solution in *FinComm*.

Finally we get a set of balanced systems; we want to say if any of them has a solution in *FinComm*. But for such systems it can be determined by the algorithm from section 3.

5 Complexity

In this section I will show that the problem is NP-complete. To talk about the complexity we need to know how we represent the system and how is its size defined. The easiest (but not good enough) way is to remember an equation as it is, as a list of coefficients and variables. When we use this representation, then during the operation of our algorithm the size of the system can grow exponentially, so it wouldn't work in NP. But we can do better: a side of a equation will be described by numbers of occurrences of every symbol (coefficient or variable). So when a symbol repeats N times, the binary representation of N will be remembered, which has a length of $\Theta(\log N)$.

Firstly I will show that the problem is in NP. Of course I will use the algorithm described above in the paper. Essentially the algorithm consists of two parts. In the first part we remove a variable from unbalanced equation several times and substitute for it some subsequence of the other side of the equation (see subsection 4.2). Note that in nondeterministic model we can just guess the correct substitution instead of checking all the possibilities. In the second part we solve a balanced system of equations over $\mathbb{Z}$. This can be done in NP (see [2], the solution will have polynomial size, so we can just guess it).

The only question is what is the length of the system after the first part. We need to show that it will grow at most polynomially. Let V_i and B_i be a total number of occurrences of variables and of coefficients in the system after the i-th step of the algorithm (in particular V_0 and B_0 are these numbers in the initial system). Note that the length of the initial system is at least $\Omega(\log |V_0 + B_0|)$. In i-th step we substitute for a variable at most B_{i-1} coefficients, and the variable occurs at most V_{i-1} times, so

$$B_i \leq B_{i-1} + V_{i-1}B_{i-1} = (V_{i-1} + 1)B_{i-1}$$

The number of occurrences of variables even decrease, so $V_i \leq V_{i-1}$. After k steps we have: $V_k \leq V_0$ and $B_k \leq (V_0 + 1)^k B_0$. Let N be the length of the initial system, $\gamma \leq N$ — number of different variables and $\omega \leq N$ — number of different coefficients. In each step we remove one variable, so there are at most $k \leq \gamma \leq N$ steps. The length of the resulting system will be at most:

$$\begin{aligned} 2m(\gamma \log V_k + \omega \log B_k) &\leq 2N^2(\log V_0 + \log((V_0 + 1)^N B_0)) = \\ &= 2N^2(\log V_0 + N \log(V_0 + 1) + \log B_0) \leq \\ &\leq O(N^3)O(\log |V_0 + B_0|) \leq O(N^4) \end{aligned}$$

so it's polynomial.

Now I will show that the problem is NP-hard. To do that I will reduce to it the NP-complete clique problem (defined in [3]). Assume that we are looking for a clique of size k in a graph $G = (V, E)$. Assume that $V = \{1, 2, \ldots, |V|\}$. We will have only one coefficient C. We will have a variable X_i for each vertex and helper variables X'_i and X''_{ij} for each vertex and each pair of vertices. The equations are:

$$\begin{cases} X_1 + X_2 + \ldots + X_{|V|} = (|V| + k) \cdot C & \\ X_i + X'_i = 3 \cdot C & \text{for every } i \in V \\ X_i + X_j + X''_{ij} = 4 \cdot C & \text{for every } (i,j) \notin E \end{cases}$$

If there is a clique of size k, then we will have a solution in every commutative finite semigroup (and even in the free commutative semigroup). We take $X_i = 2 \cdot C$ if the vertex i is in the clique or $X_i = C$ if it isn't. First equation is satisfied, because there are exactly k vertices in the clique. The equations of the second and third type can be satisfied by taking X'_i and X''_{ij} equal to C or $2 \cdot C$. When there is no edge (i, j), then at most one of vertices i and j is in the clique, so it's possible to satisfy the equations of the third type.

When there is a solution in every commutative finite semigroup, then there is also some solution $\bar{x}$ in the following semigroup S: Elements of S are $\{1, 2, \ldots, M\}$ for large enough $M = \max(5, |V| + k + 1)$. The operation $a + b$ is defined as $\min(M, a + b)$. The coefficient C evaluates to 1. From equations of the second type we see that $x_i = 1$ or 2. We take vertex i to a clique iff $x_i = 2$. The equations of the third type guaranties that two vertices cannot be in the clique if there is no edge between them. First equation says that the clique has size k.

6 Other questions

It may be interesting to check if a system has a solution in other classes of semigroups, for example all finite semigroups or all idempotent finite semigroups.

For idempotent finite semigroups this question is easy, as we know that there are only finitely many idempotent semigroups with a given number of generators (see [4]). Moreover all these semigroups can be listed, because there is a formula for maximum number of elements in such semigroup. It is enough to check if a system has a solution in all semigroups generated by our coefficients, which we can do one semigroup after another. For any semigroup, when there is a solution in a subsemigroup generated by coefficients, it is also a solution in whole semigroup.

It remains open how to check that in class of all finite semigroups.

References

[1] M. Bojańczyk, T. Colcombet, *Tree-walking automata cannot be determinized* Theoretical Computer Science, Volume 350, Issues 2-3, (Feb., 2006), pages 164-173

[2] I. Borosh, L.B. Trebig, *Bounds on positive integral solutions of linear Diophantine equations* Proc. Amer. Math. Soc. 55 (1976), 299304

[3] R.M. Karp, *Reducibility Among Combinatorial Problems* Complexity of Computer Computations, Proc. Sympos. IBM Thomas J. Watson Res. Center, Yorktown Heights, New York (1972), pages 85-103

[4] D. McLean, *Idempotent semigroups*, The American Mathematical Monthly, Volume 61, Number 2 (Feb., 1954), pages 110-113

[5] O. Klíma, P. Tesson, D. Thérien, *Dichotomies in the Complexity of Solving Systems of Equations over Finite Semigroups* Electronic Colloquium on Computational Complexity, Report 091 (2004)

[6] G.S. Makanin, *The problem of solvability of equations in a free semigroup* Mathematics of the USSR – Sbornik, Volume 32 (1977), pages 129-198