The Complexity of Counting Solutions to Systems of Equations over Finite Semigroups

Gustav Nordh* and Peter Jonsson**

Department of Computer and Information Science
Linköpings Universitet
S-581 83 Linköping, Sweden
Fax: +46 13 28 44 99
{gusno, petej}@ida.liu.se

Abstract. We study the computational complexity of counting the number of solutions to systems of equations over a fixed finite semigroup. We show that if the semigroup is a group, the problem is tractable if the group is Abelian and #P-complete otherwise. If the semigroup is a monoid (that is not a group) the problem is #P-complete. In the case of semigroups where all elements have divisors we show that the problem is tractable if the semigroup is a direct product of an Abelian group and a rectangular band, and #P-complete otherwise. The class of semigroups where all elements have divisors contains most of the interesting semigroups e.g. regular semigroups. These results are proved by the use of powerful techniques from universal algebra.

1 Introduction

The computational complexity of deciding whether systems of equations over a fixed finite semigroup are solvable has been intensively studied in the past. In [3], it is proved that when the semigroup is a group, the problem is tractable if the group is Abelian and NP-complete otherwise. This line of research continued in [6, 7], where the corresponding problem for finite monoids was given a complete solution. Some partial results in the general case of finite semigroups have been proved in [7]. Note that even the restricted problem of determining the computational complexity of solving systems of equations over a fixed regular semigroup is still open.

In this paper we study the computational complexity of counting solutions to systems of equations over a fixed finite semigroup. This problem has not been given the same attention as the corresponding decision problem. A system of equations over a fixed finite semigroup $(S, \cdot)$ is a collection of equations of the form $w_1 \cdot w_2 \cdot \ldots \cdot w_k = y_1 \cdot y_2 \cdot \ldots \cdot y_j$ where each w_i and y_i is either a variable or a constant in S. We denote the problem of counting the number of solutions

* Supported by the *National Graduate School in Computer Science* (CUGS), Sweden.
** Partially supported by the Swedish Research Council (VR) under grant 221-2000-361.

to systems of equations over the semigroup $(S, \cdot)$ by $\#EQN_S^*$. The notation $\#EQN_S^*$ is used in order to comply with the notation in [3, 6, 7]. The presence of the * in $\#EQN_S^*$ is motivated by the need to distinguish this problem from the problem of counting the number of solutions to a single equation over $(S, \cdot)$ (denoted by $\#EQN_S$). The complexity of $\#EQN_S^*$ is measured in the size of the systems of equations (the size of $(S, \cdot)$ is fixed and does not matter).

We prove that $\#EQN_G^*$ is tractable when $(G, \cdot)$ is an Abelian group and #P-complete when $(G, \cdot)$ is a non-Abelian group. In the case of monoids, $\#EQN_M^*$ is #P-complete when $(M, \cdot)$ is a monoid that is not a group. Given a semigroup $(S, \cdot)$, we say that an element a in S is divisible if and only if there exists b, c in S such that $b \cdot c = a$. In the case of semigroups where all elements are divisible we show that $\#EQN_S^*$ is tractable if $(S, \cdot)$ is a direct product of an Abelian group and a rectangular band, and #P-complete otherwise. The class of semigroups where all elements have divisors contains most of the interesting semigroups, in particular regular semigroups. Moreover we prove that if $(S, \cdot)$ is a semigroup with zero, then $\#EQN_S^*$ is tractable if $(S, \cdot)$ is such that for all elements x, y in S, $x \cdot y = 0$, and #P-complete otherwise. Important to note is that all the conditions we impose on our semigroups to ensure the tractability (or #P-completeness) of $\#EQN_S^*$ can be checked in polynomial time (in the size of the semigroups).

Our approach for obtaining dichotomy theorems for $\#EQN_S^*$ relies heavily on the use of powerful algebraic techniques that have previously shown to be very useful in proving dichotomy theorems for Constraint Satisfaction Problems (CSPs) [1, 2]. It is our belief that similar algebraic techniques can also be used in a unified approach to determine the complexity of the decision problem.

The paper is organized as follows. In Section 2 we give the basic definitions and results needed in the rest of this paper. Section 3 contains all our tractability proofs for $\#EQN_S^*$. In Section 4 we prove the dichotomy for the computational complexity of $\#EQN_S^*$ when $(S, \cdot)$ is a group or monoid. In Section 5 we prove the dichotomy for the computational complexity of $\#EQN_S^*$ when $(S, \cdot)$ is a semigroup with zero or is in the class of semigroups where all elements are divisible.

2 Preliminaries

2.1 CSPs

In this section we introduce the notation and basic results on CSPs that we will use in the rest of this paper.

Let D be a finite set. The set of all n-tuples of elements of D is denoted by D^n. Any subset of D^n is called an n-ary relation on D. The set of all finitary relations over D is denoted by R_D.

Definition 1. *A constraint language over a finite set, D, is an arbitrary set $\Gamma \subseteq R_D$.*

Definition 2. *The counting constraint satisfaction problem over the constraint language Γ, denoted $\#CSP(\Gamma)$, is defined to be the counting problem with instance (V, D, C), where*

- *V is a finite set of variables,*
- *D is a set of values (sometimes called a domain), and*
- *C is a set of constraints $\{C_1, \ldots, C_q\}$, in which each constraint C_i is a pair (s_i, ϱ_i) with s_i a list of variables of length m_i, called the constraint scope, and ϱ_i an m_i-ary relation over the set D, belonging to Γ, called the constraint relation.*

We ask for the number of solutions to (V, D, C), that is, the number of functions from V to D such that, for each constraint in C, the image of the constraint scope is a member of the constraint relation.

The corresponding decision problem where we are interested in the existence of a solution is denoted $CSP(\Gamma)$. In the context of this paper D is the elements of a finite semigroup $(S, \cdot)$ and Γ is the set of relations expressible as equations over $(S, \cdot)$ (denoted by Γ_S). For example the equation $x \cdot y = c$ where x, y are variables and c is a constant gives rise to the following relation $R = \{(x, y) | x \cdot y = c\}$.

Next we consider operations on the domain D. Any operation on D can be extended in a standard way to an operation on tuples over D, as follows.

Definition 3. *Let f be a k-ary operation on D and let R be an n-ary relation over D. For any collection of k tuples, $t_1, t_2, \ldots, t_k \in R$, the n-tuple $f(t_1, t_2, \ldots, t_k)$ is defined as follows: $f(t_1, t_2, \ldots, t_k) =$*

$$(f(t_1[1], t_2[1], \ldots, t_k[1]), f(t_1[2], t_2[2], \ldots, t_k[2]), \ldots, f(t_1[n], t_2[n], \ldots, t_k[n]))$$

where $t_j[i]$ is the i:th component in tuple t_j.

A technique that has shown to be useful in determining the computational complexity of $CSP(\Gamma)$ is that of investigating whether Γ is closed under certain families of operations [5].

Definition 4. *For any constraint relation $\varrho_i \in \Gamma$ if f is an operation such that for all $t_1, t_2, \ldots, t_k \in \varrho_i$: $f(t_1, t_2, \ldots, t_k) \in \varrho_i$, then ϱ_i is closed under f. If all constraint relations in Γ are closed under f then Γ is closed under f. An operation f such that Γ is closed under f is called a polymorphism of Γ. The set of all polymorphisms of Γ is denoted $Pol(\Gamma)$.*

In this paper we will only be concerned with a particular family of ternary operations called Mal'tsev operations. An operation M is a *Mal'tsev operation* if and only if for all x, y, $M(x, y, y) = M(y, y, x) = x$.

The following result provides us with the key to prove the #P-completeness of constraint languages.

Theorem 1 ([2]). *If Γ is a finite constraint language that is closed under no Mal'tsev operation then $\#CSP(\Gamma)$ is #P-complete.*

Throughout this paper we will use the following notation for the application of an arbitrary Mal'tsev operation M on tuples in a relation R.

$$\begin{array}{rc} & (a,b) \in R \\ & (b,b) \in R \\ & (b,a) \in R \\ M & \\ \hline & (a,a) \end{array}$$

In the example above $(a,b),(b,b)$ and (b,a) are three tuples in a relation R. If $(a,a) \notin R$ we have shown that R is closed under no Mal'tsev operation, since $(M(a,b,b),\, M(b,b,a)) = (a,a)$ for *any* Mal'tsev operation M.

All of our #P-completeness proofs for $\#EQN^*_S$ follows this outline: First we choose a relation R in Γ_S i.e., R is expressed by a specific equation E over $(S,\cdot)$. Then we show that R is closed under no Mal'tsev operation, thus proving the #P-completeness of $\#CSP(\Gamma_S)$. It should be clear that this implies the #P-completeness of $\#EQN^*_S$. It is also easy to realize that any system of equations over a finite semigroup $(S,\cdot)$ can be (parsimoniously) reduced in polynomial time to a system of equations over $(S,\cdot)$ such that no equation in this system of equations contains more than three variables. Equations containing more that three variables can be split into smaller parts by introducing new variables. Hence we can safely assume that all constraint languages we consider are finite.

The following theorem is very useful when it comes to proving tractability results for $\#CSP(\Gamma)$.

Theorem 2 ([2]). *A Mal'tsev operation $M(x,y,z) = x * y^{-1} * z$ where $*$ and $^{-1}$ are the operations of an Abelian group is called an affine operation. If $M \in Pol(\Gamma)$ then $\#CSP(\Gamma)$ is tractable.*

2.2 Definitions and Results from Semigroup Theory

For the convenience of the reader we here give the definitions and results from semigroup theory that we use in the rest of this paper. The proofs are available in (or easily deducible from) any standard reference on semigroup theory such as [4].

A *semigroup* $(S,\cdot)$ is a set S with an associative binary operation $\cdot$. A *semigroup with zero* is a semigroup that contains an element 0 such that for all x in S, $0 \cdot x = x \cdot 0 = 0$. A *monoid* is a semigroup that has an identity element. A *band* is a semigroup where all elements are idempotent (that is for all x in S, $x \cdot x = x$). A *rectangular band* is a band where for all a,b in S, $a \cdot b \cdot a = a$. A *regular semigroup* is a semigroup where for all a in S there exists an element b in S such that $a \cdot b \cdot a = a$. A *right zero semigroup* is a semigroup where for all a,b in S, $a \cdot b = b$ (*left zero semigroups* are defined in an analogous way). If two semigroups $(S,\cdot_s)$ and $(T,\cdot_t)$ are *isomorphic* we denote this by $(S,\cdot_s) \cong (T,\cdot_t)$. If $(S,\cdot_s)$ and $(T,\cdot_t)$ are semigroups, then the Cartesian product $(S,\cdot_s) \times (T,\cdot_t)$ becomes a semigroup if we define $(s,t) \cdot (s',t') = (s \cdot_s s', t \cdot_t t')$. We refer to this semigroup as the *direct product* of $(S,\cdot_s)$ and $(T,\cdot_t)$. Let $Div(S)$ denote the set of divisible elements in S where $(S, \cdot)$ is a finite semigroup (a is divisible if and only if there exists b, c in S such that $b \cdot c = a$).

Theorem 3. *If $(S, \cdot)$ is a finite semigroup and a an arbitrary element in S, then a^m is idempotent for some m.*

Theorem 4. *If $(M, \cdot)$ is a finite monoid with the identity element as the only idempotent then $(M, \cdot)$ is a group.*

Theorem 5. *Let $(S, \cdot)$ be a rectangular band, then there exist a left zero semigroup $(L, \cdot_l)$ and a right zero semigroup $(R, \cdot_r)$ such that $(S, \cdot) \cong (L, \cdot_l) \times (R, \cdot_r)$.*

The following theorem is folklore.

Theorem 6. *A regular semigroup $(S, \cdot)$ whose idempotents form a rectangular band is isomorphic to a direct product of a group and a rectangular band.*

We give some hints on how to prove this theorem. By using Green's relations it can be proved that $(S, \cdot)$ is a completely simple semigroup, and since $(S, \cdot)$ is orthodox it follows from the Rees-Suschkewitch Theorem [4] that $(S, \cdot)$ is a direct product of a group and the rectangular band of its idempotents.

3 Tractability Results

Due to the similar structure of the tractability proofs for the tractable cases of $\#EQN_S^*$ we have gathered all of these proofs in this section to make a unified approach possible. In the rest of this section assume that all equations in the systems of equations are of the following two types: equations only containing variables, $x_1 \cdot \ldots \cdot x_n = \hat{x}_1 \cdot \ldots \cdot \hat{x}_m$ or equations with a single variable on the left hand side and a constant on the right hand side, $x = a$. We can make this assumption because it is easy to reduce (parsimoniously and in polynomial time) any system of equations over a finite semigroup into a system of equations of this form.

Let A be finite set and let $f : A^n \to A$ and $g : A^m \to A$ be two operations. If $f(a, \ldots, a) = a$ for all $a \in A$, then f is *idempotent*. We say that g *commutes* with f if for all $a_{11}, \ldots, a_{1m}, \ldots, a_{nm} \in A$,

$$g(f(a_{11}, \ldots, a_{n1}), \ldots, f(a_{1m}, \ldots, a_{nm})) = f(g(a_{11}, \ldots, a_{1m}), \ldots, g(a_{n1}, \ldots, a_{nm}))$$

The following lemma is the foundation for our tractability results.

Lemma 1. *Let $(S, \cdot)$ be a finite semigroup. If $f : S^k \to S$ is an idempotent operation and $\cdot$ commutes with f, then $f \in Pol(\Gamma_S)$.*

Proof. Arbitrarily choose a relation $R \in \Gamma_S$. If R is a unary relation (i.e. $R(x)$ holds if and only if $x = a$ for some $a \in S$), then R is closed under f since f is idempotent. Otherwise, $R = \{(x_1, \ldots, x_n, \hat{x}_1, \ldots, \hat{x}_m) \mid x_1 \cdot \ldots \cdot x_n = \hat{x}_1 \cdot \ldots \cdot \hat{x}_m\}$

and we arbitrarily choose k tuples $t_1, \ldots, t_k$ in R. Now, R is closed under f if the following holds:

$$\prod_{i=1}^{n} f(t_1[i], \ldots, t_k[i]) = \prod_{i=n+1}^{n+m} f(t_1[i], \ldots, t_k[i]) \qquad (*)$$

We know that $\cdot$ commutes with f so

$$\prod_{i=1}^{n} f(t_1[i], \ldots, t_k[i]) = f\left(\prod_{i=1}^{n} t_1[i], \ldots, \prod_{i=1}^{n} t_k[i]\right)$$

and

$$\prod_{i=n+1}^{n+m} f(t_1[i], \ldots, t_k[i]) = f\left(\prod_{i=n+1}^{n+m} t_1[i], \ldots, \prod_{i=n+1}^{n+m} t_k[i]\right).$$

Since $t_1, \ldots, t_k$ are tuples in R, it follows that $\prod_{i=1}^{n} t_j[i] = \prod_{i=n+1}^{n+m} t_j[i]$ for all j and $(*)$ holds. $\square$

Lemma 2. *Let $(S, \cdot)$ be a finite semigroup. If f is an affine operation and $\cdot$ commutes with f, then $\#EQN_S^*$ is tractable.*

Proof. We see that f is idempotent since $f(a, a, a) = a * a^{-1} * a = a$ so $f \in Pol(\Gamma_S)$ by Lemma 1. Consequently, Theorem 2 implies that $\#EQN_S^*$ is tractable. $\square$

Our tractability results for $\#EQN_S^*$ are contained in the following theorem.

Theorem 7. *$\#EQN_S^*$ is tractable when*

1. *$(S, \cdot)$ is an Abelian group.*
2. *$(S, \cdot)$ is a left zero or right zero semigroup.*
3. *$(S, \cdot)$ is a semigroup with zero such that for all x, y in S, $x \cdot y = 0$.*
4. *$(S, \cdot) \cong (T, *) \times (T', *')$ and $\#EQN_T^*$, $\#EQN_{T'}^*$ are tractable.*

Proof. If $(S, \cdot)$ is an Abelian group, then let $M(x, y, z) = x \cdot y^{-1} \cdot z$. We show that $\cdot$ commutes with M and tractability follows from Lemma 2. Let a, b, c be arbitrary tuples in S^2, then $M(a[1], b[1], c[1]) \cdot M(a[2], b[2], c[2]) = a[1] \cdot b[1]^{-1} \cdot c[1] \cdot a[2] \cdot b[2]^{-1} \cdot c[2] = a[1] \cdot a[2] \cdot (b[1] \cdot b[2])^{-1} \cdot c[1] \cdot c[2] = M(a[1] \cdot a[2], b[1] \cdot b[2], c[1] \cdot c[2])$.

If $(S, \cdot)$ is a right-zero group (the proof for left-zero groups is analogous), then let $M(x, y, z) = x * y^{-1} * z$ where the operation $*$ is chosen such that $(S, *)$ is an Abelian group (such a choice is always possible). Let a, b, c be arbitrary tuples in S^2, then $M(a[1], b[1], c[1]) \cdot M(a[2], b[2], c[2]) = M(a[2], b[2], c[2]) = M(a[1] \cdot a[2], b[1] \cdot b[2], c[1] \cdot c[2])$ and tractability follows from Lemma 2.

If $(S, \cdot)$ is a semigroup with zero such that for all x, y in S, $x \cdot y = 0$, then let $M(x, y, z) = x * y^{-1} * z$ where the operation $*$ is chosen such that $(S, *)$ is an Abelian group. Let a, b, c be arbitrary tuples in S^2, then $M(a[1], b[1], c[1]) \cdot$

$M(a[2], b[2], c[2]) = 0 = M(a[1] \cdot a[2], b[1] \cdot b[2], c[1] \cdot c[2])$ and tractability follows from Lemma 2.

If $(S, \cdot) \cong (T, *) \times (T', *')$, then a system of equations over $(S, \cdot)$ can be split into two independent systems of equations, one over $(T, *)$ and one over $(T', *')$. The number of solutions to the system of equations over $(S, \cdot)$ equals the product of the number of solutions to the systems of equations over $(T, *)$ and $(T', *')$ respectively. Hence if $\#EQN_T^*$ and $\#EQN_{T'}^*$ are tractable, then so is $\#EQN_S^*$. □

4 Finite Groups and Monoids

In this section we prove our dichotomies for the complexity of the counting problem over finite groups and monoids. Note that the decision dichotomy proved in [6] and the counting dichotomy we prove differs in the case of monoids, for example it is tractable to decide whether systems of equations over a commutative band are solvable, but to count the number of solutions is #P-complete.

Theorem 8. *Let $(G, \cdot)$ be a finite group, then $\#EQN_G^*$ is tractable if $(G, \cdot)$ is Abelian, and #P-complete otherwise.*

Proof. We begin by proving the #P-completeness of $\#EQN_G^*$ when $(G, \cdot)$ is a non-Abelian group. Because $(G, \cdot)$ is a non-Abelian group there exists two elements a, b in G such that $a \cdot b \neq b \cdot a$. Consider the following relation $R = \{(x, y) | x \cdot y = y \cdot x\}$. It is easy to see that R is closed under no Mal'tsev operation.

$$\begin{array}{lll} & (a,1) \in R & a \cdot 1 = 1 \cdot a \\ & (1,1) \in R & 1 \cdot 1 = 1 \cdot 1 \\ & (1,b) \in R & 1 \cdot b = b \cdot 1 \\ M & & \\ \hline & (a,b) \notin R & a \cdot b \neq b \cdot a \end{array}$$

Hence $\#EQN_G^*$ is #P-complete for non-Abelian groups. The tractability part is proved in Theorem 7. □

Next we consider the case where the semigroup is a finite monoid.

Theorem 9. *Let $(M, \cdot)$ be a finite monoid that is not a group, then $\#EQN_M^*$ is #P-complete.*

Proof. According to Theorem 4 we know that there exist an element a in M such that $a \neq 1$ and $aa = a$. Consider the relation $R = \{(x, y) | x \cdot y = a\}$. It is easy to see that R is closed under no Mal'tsev operation.

$$\begin{array}{lll} & (1,a) \in R & 1 \cdot a = a \\ & (a,a) \in R & a \cdot a = a \\ & (a,1) \in R & a \cdot 1 = a \\ M & & \\ \hline & (1,1) \notin R & 1 \cdot 1 = 1 \neq a \end{array}$$

Thus, $\#EQN_M^*$ is #P-complete. □

5 Finite Semigroups

The computational complexity of deciding whether systems of equations over a fixed finite semigroup are solvable has been studied in [7], where some evidence is given that a dichotomy in the decision case would be very hard to prove. Even the restricted problem of proving a dichotomy for regular semigroups is open. We prove that for semigroups where all elements have divisors the counting problem is tractable if the semigroup is a direct product of an Abelian group and a rectangular band, and #P-complete otherwise. Moreover we prove that for semigroups with zero, the problem is tractable if the semigroup is such that for all elements x, y $x \cdot y = 0$, and #P-complete otherwise.

The following lemma will be very useful in the proofs that follows.

Lemma 3. *Let $(S, \cdot)$ be a semigroup and I be the set of idempotents in S. A necessary condition for $\#EQN^*_S$ to be tractable is that the following holds: for all a in I and for all b, c in S, $b \cdot c = b \cdot a \cdot c$. Otherwise $\#EQN^*_S$ is #P-complete.*

Proof. Assume that there exists a in I and that there exists b, c in S and $b \cdot c \neq b \cdot a \cdot c$. Consider the relation $R = \{(x, y) | x \cdot y = b \cdot a \cdot c\}$. R is closed under no Mal'tsev operation.

$$\begin{array}{l r l r}
 & (b, a \cdot c) & \in R & b \cdot a \cdot c = b \cdot a \cdot c \\
 & (b \cdot a, a \cdot c) & \in R & b \cdot a \cdot a \cdot c = b \cdot a \cdot c \\
 & (b \cdot a, c) & \in R & b \cdot a \cdot c = b \cdot a \cdot c \\
M & & & \\
\hline
 & (b, c) & \notin R & b \cdot c \neq b \cdot a \cdot c
\end{array}$$

Hence $\#EQN^*_S$ is #P-complete. □

We continue by proving a dichotomy in the case where the semigroup is a band.

Theorem 10. *If $(S, \cdot)$ is a band, then $\#EQN^*_S$ is tractable if $(S, \cdot)$ is a rectangular band and #P-complete otherwise.*

Proof. It follows directly from Lemma 3 that if S is a band that is not a rectangular band then $\#EQN^*_S$ is #P-complete. If $(S, \cdot)$ is a rectangular band we know from Theorem 5 that there exist a left zero semigroup $(L, \cdot_l)$ and a right zero semigroup $(R, \cdot_r)$ such that $(S, \cdot) \cong (L, \cdot_l) \times (R, \cdot_r)$. Thus the tractability of $\#EQN^*_S$ when $(S, \cdot)$ is a rectangular band follows from Theorem 7. □

The following lemma gives us an important necessary condition for the tractability of $\#EQN^*_S$.

Lemma 4. *Given a semigroup $(S, \cdot)$, it is a necessary condition for $\#EQN^*_S$ to be tractable that $(Div(S), \cdot)$ form a regular semigroup. Otherwise $\#EQN^*_S$ is #P-complete.*

Proof. Arbitrarily choose $a \in Div(S)$ and assume that $a = b \cdot c$ for some b, c. Since S is finite, we know from Theorem 3 that b^n and c^m are idempotent for some m, n. From Lemma 3 we know that $a = b \cdot c = b \cdot c^m \cdot b^n \cdot c = a \cdot c^{m-1} \cdot b^{n-1} \cdot a$, otherwise $\#EQN_S^*$ is #P-complete. Thus it is a necessary condition for $\#EQN_S^*$ to be tractable that all elements in $Div(S)$ are regular. □

Now we can prove a dichotomy $\#EQN_S^*$ when $(S, \cdot)$ is a regular semigroup.

Theorem 11. *Let $(S, \cdot)$ be a finite regular semigroup. Then $\#EQN_S^*$ is tractable if $(S, \cdot)$ is a direct product of an Abelian group and a rectangular band. Otherwise $\#EQN_S^*$ is #P-complete.*

Proof. If the idempotents in $(S, \cdot)$ do not form a rectangular band then by Lemma 3, $\#EQN_S^*$ is #P-complete. If the idempotents in $(S, \cdot)$ do form a rectangular band then by Theorem 6, $(S, \cdot)$ is a direct product of a group and a rectangular band. We conclude from Theorem 7 that $\#EQN_S^*$ is tractable if $(S, \cdot)$ is a direct product of an Abelian group and a rectangular band.

Now assume that $(S, \cdot)$ is isomorphic to the direct product of a non-Abelian group by a rectangular band i.e. $(S, \cdot) \cong (G, \cdot_g) \times (RB, \cdot_b)$ where $(G, \cdot_g)$ is a non-Abelian group and $(RB, \cdot_b)$ is a rectangular band. Consider the following relation $R = \{(x, y) | x \cdot y = y \cdot x\}$. We show that R is closed under no Mal'tsev operation. The elements below are chosen as follows, 1 is the identity in $(G, \cdot_g)$, since $(G, \cdot_g)$ is non-Abelian we know that there exists elements a, b in G such that $a \cdot_g b \neq b \cdot_g a$, and c is an arbitrary element in $(RB, \cdot_b)$.

$$\begin{array}{lll} & ((a,c),(1,c)) \in R & (a,c)\cdot(1,c) = (1,c)\cdot(a,c) \\ & ((1,c),(1,c)) \in R & (1,c)\cdot(1,c) = (1,c)\cdot(1,c) \\ & ((1,c),(b,c)) \in R & (1,c)\cdot(b,c) = (b,c)\cdot(1,c) \\ M & & \\ \hline & ((a,c),(b,c)) \notin R & (a,c)\cdot(b,c) \neq (b,c)\cdot(a,c) \end{array}$$

Hence $\#EQN_S^*$ is #P-complete when $(S, \cdot)$ is isomorphic to the direct product of a non-Abelian group by a rectangular band. □

The following corollary follows directly from Lemma 4 and Theorem 11.

Corollary 1. *If $(S, \cdot)$ is a finite semigroup where all elements have divisors, then $\#EQN_S^*$ is tractable if $(S, \cdot)$ is a direct product of an Abelian group and a rectangular band, and #P-complete otherwise.*

The following theorem proves a dichotomy for $\#EQN_S^*$ when $(S, \cdot)$ is a semigroup with zero.

Theorem 12. *Let $(S, \cdot)$ be a finite semigroup with zero, then $\#EQN_S^*$ is tractable if for all x, y in S, $x \cdot y = 0$, and #P-complete otherwise.*

Proof. The tractability part is proved in Theorem 7. We continue by proving the #P-completeness of $\#EQN_S^*$ when $(S, \cdot)$ is a semigroup with zero and there exist two elements a, b in S such that $a \cdot b \neq 0$. Consider the following relation

$R = \{(x,y)|x \cdot y = 0\}$. It is easy to see that R is closed under no Mal'tsev operation.

$$\begin{array}{lll} & (a,0) \in R & a \cdot 0 = 0 \\ & (0,0) \in R & 0 \cdot 0 = 0 \\ & (0,b) \in R & 0 \cdot b = 0 \\ M & & \\ \hline & (a,b) \notin R & a \cdot b \neq 0 \end{array}$$

Hence $\#EQN_S^*$ is #P-complete when $(S, \cdot)$ is a semigroup with zero and there exist two elements x, y in S such that $x \cdot y \neq 0$. □

It is easy to realize that all the conditions we impose on our semigroups to ensure the tractability (or #P-completeness) of $\#EQN_S^*$ can be checked in polynomial time (in the size of the semigroups), except maybe for the condition in Theorem 11. To check whether a semigroup, isomorphic to a direct product of a group and a rectangular band, is in fact isomorphic to a direct product of an Abelian group and a rectangular band, we need a way to extract the group part from the semigroup. Choose an idempotent x in $(S, \cdot)$. Then we know that x is of the form $(1, x')$ where 1 is the identity in $(G, \cdot_g)$. Consider the set xSx, elements in this set is of the form $(1, x') \cdot (a, y) \cdot (1, x') = (a, x')$. This implies that $(xSx, \cdot) \cong (G, \cdot_g)$. Now it is easy to check whether $(G, \cdot_g)$ is Abelian.

Acknowledgments

The authors want to thank Pascal Tesson for interesting discussions and remarks on the topics in this paper, Andrei Bulatov for many valuable remarks on an earlier version of this paper and Jorge Almeida for his explanations of some topics in the realm of semigroups.

References

1. A. Bulatov. A dichotomy theorem for constraints on a three-element set. In *Proc. 43rd IEEE Symposium on Foundations of Computer Science, FOCS'02*, pages 649–658, 2002.
2. A. Bulatov and V. Dalmau. Towards a dichotomy theorem for the counting constraint satisfaction problem. In *Proc. 44th IEEE Symposium on Foundations of Computer Science, FOCS'03*, 2003.
3. M. Goldmann and A. Russel. The complexity of solving equations over finite groups. *Inform. and Comput.*, 178(1):253–262, 2002.
4. J.M. Howie. *Fundamentals of Semigroup Theory.* Claredon Press, Oxford, 1995.
5. P. Jeavons, D. Cohen, and M. Gyssens. Closure properties of constraints. *Journal of the ACM*, 44:527–548, 1997.
6. C. Moore, P. Tesson, and D.Thérien. Satisfiability of systems of equations over finite monoids. In *Proc. 26th International Symposium on Mathematical Foundations of Computer Science, MFCS'01*, pages 537–547, 2001.
7. P. Tesson. *Computational Complexity Questions Related to Finite Monoids and Semigroups.* PhD thesis, School of Computer Science, McGill University, Montreal, 2003.