On the solutions of linear systems over additively idempotent semirings*

Álvaro Otero Sánchez†1, Daniel Camazón Portela‡1, and Juan Antonio López Ramos§1

1Department of Mathematics, University of Almería

Abstract

The aim of this paper is to address the system $AX = Y$, where $A = (a_{ij}) \in M_{m\times n}(S)$, $Y \in S^m$, and X represents an unknown vector of size n, with S being an additively idempotent semiring. Should the system possess solutions, we aim to comprehensively characterize a particular solution as it is the so-called maximal solution with respect to an order that is induced by the addition of the semiring. Additionally, in the specific scenario where S is what we call a generalized tropical semiring, we offer a thorough characterization of its solutions along with an explicit estimation of the computational cost involved in its computation.

1 Introduction

A semiring $(S, +, \cdot)$ is a set S with two internal operations, $+, \cdot$ where $(S, +)$ is a commutative monoid, and $(S, \cdot)$ is a monoid, being both internal operations connected by a ring-like distributivity. We also assume that for both operations, there exists an identity element; 0 for $+$ and 1 for $\cdot$. In addition, a semiring $(S, +, \cdot, 0, 1)$ is said to be additively idempotent if $x + x = x$ for all $x \in S$.

One of the most important examples of semirings are the tropical semirings. The semiring $(\mathbb{R}, min, +)$ appeared in optimization problems such as Floyd's algorithm for finding shortest paths in a graph [5]. However, a systematic study of the tropical semiring began only after the Simon's work (see [3]) and since then the study has significantly increased due to the huge number of applications.

The first paper [4] about linear algebra on such a semirings appeared in 2005. However, solving linear systems was a major task from the beginning of tropical algebras, but it was not until the work of Viro [6] that the problem actually took a most present role in mathematics. Moreover, this problem has already proved to be very interesting from the algorithmic point of view as it is known to be in $NP \cap coNP$ [7].

Letting $(S, +, \cdot)$ be an additively idempotent semiring, we want to solve the system $AX = Y$, where $A = (a_{ij}) \in M_{m\times n}(S)$, $Y \in S^m$ and X is an unknown vector of size n. In the context where the system $AX = Y$ admits solutions, we can compute the maximal one. Moreover, within the specific framework where S is a generalized tropical semiring (see Definition 1.1.1), we present a complete characterization of all its solutions, with an explicit polynomial computational cost.

2 Preliminars

We will recall some basic background and introduce the notation we will use through this work.

[*] The full version of this work can be found in [10] and has been submited to Funzy set and Systems. This research is supported by the Department of Mathematics, University of Almería.

[†] Email: aos073@inlumine.ual.es. Research of supported by Department of Mathematics, University of Almería.

[‡] Email: danielcp@ual.es. Research supported by Ministerio de Ciencia e Innovación PID2022-138906NB-C21..

[§] Email: jlopez@ual.es. Research supported by Ministerio de Ciencia e Innovación PID2020-113552GB-I00 and FQM 0211 Junta de Andalucía..

Definition 1. *A semiring $(R,+,\cdot)$ is a non-empty set R together with two operations $+$ and $\cdot$ such that $(R,+)$ is a commutative monoid, $(R,\cdot)$ is a monoid and the distributive laws hold:*

$$\begin{aligned} a(b+c) &= ab+ac \\ (a+b)c &= ac+bc \end{aligned} \tag{1}$$

We say that $(R,+,\cdot)$ is additively idempotent if $a+a=a$ for all $a \in R$.

Example 2. *From the work of J. Zumbrägel [13], the following additively idempotent semiring with 5 elements can be obtained:*

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	1	1	1	1	5
2	2	1	2	1	2	5
3	3	1	1	3	3	5
4	4	1	2	3	4	5
5	5	5	5	5	5	5

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	2	0	0	5
3	0	3	4	3	4	3
4	0	4	4	0	0	3
5	0	5	2	5	2	5

Example 3. *In [14], a classification of all additively commutative semirings with two elements is presented. In that article, we can see that the set $\{0,1\}$ endowed with the following operations results in an additively idempotent semiring:*

$+$	0	1
0	0	0
1	0	1

$\cdot$	0	1
0	0	1
1	1	1

Definition 4. *Let R be a semiring and $(M,+)$ be a commutative semigroup with identity 0_M. M is a right semimodule over R if there is an external operation $\cdot\ : M \times R \to M$ such that*

$$\begin{aligned} (m\cdot a)\cdot b &= m\cdot(a\cdot b) \\ m\cdot(a+b) &= m\cdot a + m\cdot b \\ (m+n)\cdot a &= m\cdot a + n\cdot a \\ 0_M \cdot a &= 0_M \end{aligned} \tag{2}$$

for all $a,b \in R$ and $m,n \in M$. We will denote $m \cdot a$ by the concatenation ma.

In an additively idempotent semiring $(R,+,\cdot)$, an order can be induced by the addition operation, by:

$$a \le b \text{ if and only if } a+b=b. \tag{3}$$

This order respects the operation in R and enables us to define a partial order in R^n for every positive integer n.

$$X=(x_1,\ldots x_n) \ge Y=(y_1,\ldots,y_n) \text{ if and only if } x_i \ge y_i \ \forall i=1,\ldots,n. \tag{4}$$

In addition, note that this order also respect the multiplication by a square matrices of order n whose entries are in R.

Let $AX=Y$ be the system of linear equations in R with indeterminates $x_1,\ldots,x_n$,

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{(m-1)1} \\ a_{m1} \end{pmatrix} x_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{(m-1)2} \\ a_{m2} \end{pmatrix} x_2 + \cdots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{(m-1)n} \\ a_{mn} \end{pmatrix} x_n = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{m-1} \\ y_m \end{pmatrix}, \tag{5}$$

with $a_{i,j}, y_j \in R$ for all $i = 1, \ldots, n$ $j = 1, \ldots, m$. Let A_j be the $j - th$ column of A, $A_j = (a_{1j}, a_{2j}, \ldots, a_{mj})$, then, the previous system can be written as

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = Y. \tag{6}$$

Definition 5. *Let R be an additively idempotent semiring, and let $AX = Y$ be a linear system of equations. We say that $\hat{X}$ is the maximal solution of the system if and only if the two following conditions are satisfied*

1. *$\hat{X} \in R^n$ is a solution of the system, i.e. $A\hat{X} = Y$,*
2. *if $Z \in R^n$ is any other solution of the system, then $Z \leq \hat{X}$*

The following result depicts a method to compute the maximal solution of such a system of equations.

Theorem 6. *Given $(R, +, \cdot)$ an additively idempotent semiring, let $W_i = \{x \in R : xA_i + Y = Y\}$ $\forall i = 1, \ldots, n$. Suppose that these subsets have a maximum with respect to the order induced in R*

$$C_i = \max W_i. \tag{7}$$

If $XA = Y$ has as a solution, then $\hat{X} = (C_1, \ldots C_n)$ is the maximal solution of the system.

Proof. If there is a solution $Z = (z_1, \ldots, z_n)$, then, it is enough to proof that $z_k \cdot A_k + Y = Y$ for all $k = 1, \ldots, n$, and therefore we can show that $z_k \in W_k$. As a consequence, $\hat{X} \geq Z$. Finally, we show that $\hat{X}$ is a solution, and therefore, it is the maximal solution. □

In [10, example 3.19], an example of a direct application of this theorem can be found.

3 Particular cases

An important example of the considered semirings is the so-called tropical semiring, which is the semiring given by $(\mathbb{R} \cup \{\infty\}, \max, +)$. The following definition is a generalization of this concept.

Definition 7. *Let $(R, +, \cdot)$ be a semiring. We say that R is a generalized tropical semiring if*

$$a + b = a \text{ or } a + b = b \text{ of all } a, b \in R.$$

It is straightforward that the tropical semiring is the tropicalized of $\mathbb{R}$ with the usual operations.

Using the argument given in the proof of the preceding theorem to this specific case, allows us to provide the following result. A complete proof of theorems 8 and 9 can be found in [10, Theorem 3.6] and [10, Theorem 3.12] respectively.

Theorem 8. *Let $(R, +, \cdot)$ be a generalized tropical semiring where $(R, \cdot)$ is a group. Then the linear system $A \cdot X = Y$ has at least one solution.*

Tropical lineal algebra over tropical semirings appears naturally in several problems of graph theory (c.f. [12] or [11]). The following result shows a characterization of all solutions of the linear system $AX = Y$.

Theorem 9. *Let R be a generalized tropical semiring, and let $AX = Y$ be a system of equations with $Y = (y_i) \in R^m$ and $A = (a_{i,j}) \in Mat_{n\times m}(R)$. $X = (x_1, x_2, ..., x_n)$ is solution of the system if and only if*

1. $a_{j,i} \cdot x_i + y_j = y_j \ ,\forall j = 1, \dots, m,$
2. $\forall j = 1, \dots, m \ \exists h \in \{1, \dots, n\}$ *such that* $a_{j,h} \cdot x_h = y_j$ *.*

Another significant case is that of finite idempotent semirings, which has garnered renewed interest in the scientific community due to its potential applications in cryptography. As an example, [8] provides a characterization of all finite commutative simple semirings, among which one of the five possible cases is the additively idempotent semiring.

Then, due to the finiteness of the semiring we get that

Theorem 10. *Let R be an additively idempotent finite semiring, and let $AX = Y$ be a system of equations, with $Y \in R^m$ and $A = (a_{i,j}) \in Mat_{n\times m}(R)$. Then, the system is compatible, $W_i = \{x \in R : x \cdot A_i + Y = Y\}$ is finite and*

$$X = (x_1, \dots, x_n) \text{ such that } x_i = \sum_{x \in W_i} x \tag{8}$$

is the maximal solution of the system.

An important consequence of this result is that we are able to provide a cryptanalysis of the key exchange over finite semirings that are congruence simple and that is introduced in [2] and that it is published in [9].

References

[1] J. S. Golan, Semirings and their applications, Kluwer Academic Publishers, Dordrecht, 1999, xii+381.

[2] G. Maze, C. Monico, J. Rosenthal, Public key cryptography based on semigroup actions, *Adv. Math. Commun.* **1** (2007), 489–507.

[3] I. Simon, Limited subsets of a free monoid, in: *19th Annual Symposium on Foundations of Computer Science (Ann Arbor, Mich., 1978)*, IEEE, Long Beach, CA, 1978, pp. 143–150.

[4] M. Develin, F. Santos, B. Sturmfels, On the rank of a tropical matrix, in: *Combinatorial and computational geometry*, Math. Sci. Res. Inst. Publ., vol. 52, Cambridge Univ. Press, Cambridge, 2005, pp. 213–242.

[5] R. W. Floyd, Algorithm 97: Shortest Path, *Commun. ACM* **5(6)** (1962), 345. https://doi.org/10.1145/367766.368168

[6] O. Viro, Dequantization of Real Algebraic Geometry on Logarithmic Paper, in: *European Congress of Mathematics*, eds. Carles Casacuberta, Rosa Maria Miró-Roig, Joan Verdera, Sebastià Xambó-Descamps, Birkhäuser Basel, Basel, 2001, pp. 135–146. ISBN: 978-3-0348-8268-2.

[7] D. Grigoriev, Complexity of solving tropical linear systems, *comput. complex.* **22** (2013), 71–88, DOI 10.1007/s00037-012-0053-5.

[8] C. Monico, On finite congruence-simple semirings, *J. Algebra* **271** (2004) 846-854.

[9] A. Otero Sánchez and J. A. López Ramos, Cryptanalysis of a key exchange protocol based on a congruence-simple semiring action, Journal of Algebra and Its Applications, Online Ready No Access, https://doi.org/10.1142/S0219498825502299

[10] A. Otero Sánchez, D. Camazón, J. A. López Ramos, "On the solutions of linear systems over additively idempotent semirings", arXiv:2404.03294 [cs.IT], https://doi.org/10.48550/arXiv.2404.03294

[11] B. M. E. Moret and H. D. Shapiro, An Empirical Assessment of Algorithms for Constructing a Minimum Spanning Tree, Computational Support for Discrete Mathematics, 15(1):99–117, 1992.

[12] D. Speyer and B. Sturmfels, Tropical Mathematics, Mathematics Magazine, 82(2):163–173, April 2009.

[13] J. Zumbrägel, Classification of finite congruence-simple semirings with zero, Journal of Algebra and Its Applications, 7:363–377, 2008.

[14] R. El Bashir, J. Hurt, A. Jančařík, and T. Kepka, Simple commutative semirings, Journal of Algebra, 236:277–306, 2001.