mathematics

MDPI

Article

On the Solutions of Linear Systems over Additively Idempotent Semirings

Álvaro Otero Sánchez †, **Daniel Camazón Portela** † **and Juan Antonio López-Ramos** *,†

Department of Mathematics, University of Almería, 04120 Almería, Spain; aos073@inlumine.ual.es (Á.O.S.); danielcp@ual.es (D.C.P.)

* Correspondence: jlopez@ual.es

† These authors contributed equally to this work.

Abstract: The aim of this article is to solve the system $XA = Y$, where $A = (a_{i,j}) \in M_{n\times m}(S)$, $Y \in S^m$ and X is an unknown vector of a size n, with S being an additively idempotent semiring. If the system has solutions, then we completely characterize its maximal one, and in the particular case where S is a generalized tropical semiring, a complete characterization of its solutions is provided as well as an explicit bound of the computational cost associated with its computation. Finally, we show how to apply this method to cryptanalyze two different key exchange protocols defined for a finite case and the tropical semiring, respectively.

Keywords: linear systems over semirings; maximal solution; generalized tropical semirings; cryptography

MSC: 16Y10; 15A06; 94A60

1. Introduction

A semiring $(S, +, \cdot, 0, 1)$ is an algebraic structure in which $(S, +)$ is a commutative monoid with an identity element 0 and $(S, \cdot)$ is a monoid with an identity element 1, with both being internal operations connected by ring-like distributivity. The additive identity 0 is multiplicatively absorbing, and $0 \neq 1$ (see, for example, the monograph [1] for an intensive treatment of this algebraic structure). Moreover, a semiring $(S, +, \cdot, 0, 1)$ is said to be additively idempotent if $x + x = x$ for all $x \in S$. Historically, the first notion of a semiring was from Vandiver [2] in 1934 , and interest in additively idempotent semirings arose in the 1950*s* through the observation that some problems in discrete optimization could be linearized over such structures (see, for example, [3]). The first work to make use of an algebra over an idempotent ring (apart from Boolean fields) was that of Kleene [4], where nerve nets were studied in the context of finite state machines. Since then, the study of additively idempotent semirings has led to multiple connections with such diverse fields as graph theory (path algebra), Hamilton–Jacobi theory, automata and language theory, discrete event system theory (where linear systems over additively idempotent semirings modelize discrete event systems of practical interest), and fuzzy logic. As some examples of connections with the latter, each fuzzy triangular norm (t-norm; see, for example, [5]) conducts an additively idempotent semiring, which is called a max-t semiring in the literature, and in [6–8], Nola et al. studied certain objects of algebra over semirings arising from fuzzy logic, such as MV-algebras or the Lukasiewicz transform. Moreover, there is currently vast research on matrices with idempotent coefficients and their applications (e.g., [3,9,10]).

As an example of an additively idempotent semiring, we will study the tropical semiring. Tropical algebra was the first section of tropical mathematics to appear, and although a systematic study of the tropical semiring began only after the works of Simon (see [11]), we should note that the $(\mathbb{R}, min, +)$ semiring had appeared before in optimization problems (see, for example, Floyd's algorithm for finding the shortest paths in a graph [12]).

Citation: Otero Sánchez, Á.; Camazón Portela, D.; López-Ramos, J.A. On the Solutions of Linear Systems over Additively Idempotent Semirings. *Mathematics* **2024**, *12*, 2904. https://doi.org/10.3390/math12182904

Academic Editor: Irina Cristea

Received: 31 August 2024
Revised: 14 September 2024
Accepted: 17 September 2024
Published: 18 September 2024

Although the problem of solving linear systems was formulated right after the definition of a root for a tropical polynomial and was given by Viro [13], the first paper [14] actually devoted to tropical linear algebra appeared only as late as 2005. Moreover, this problem has already proved to be quite interesting from the algorithmic point of view as it is known to be in $NP \cap coNP$. Some examples of algorithms proposed for solving tropical linear systems can be found in [15–17]. At present, there are numerous applications of linear systems over tropical semirings in various areas of mathematics, engineering, and computer science. For instance, Noel, Grigoriev, Vakulenko, and Radulescu recently proposed a way to use algorithms for solving tropical linear systems to study stable states of reaction networks in biology [18,19]. As an application in fuzzy set theory, Gavalec, Němcová et al. recently proposed a way to convert the problems of max-Lukasiewicz linear algebra (i.e., linear algebra over a max-Lukasiewicz semiring), to the problems of tropical (max-plus) linear algebra [20] and take advantage of the well-developed theory and algorithms of the latter in order to develop a theory of the matrix powers and the eigenproblem over a max-Lukasiewicz semiring. Thus, problems of tropical linear algebra and tropical linear systems in particular are important in terms of both theoretical and practical implications.

When letting $(S, +, \cdot)$ be an additively idempotent semiring, we want to solve the system $XA = Y$, where $A = (a_{i,j}) \in M_{n\times m}(S)$, $Y \in S^m$ and X is an unknown vector of a size n. We have to clarify that our notion of a solution differs from that of Viro in the sense that the maximum is achieved only once. If the system $XA = Y$ has solutions, then we can completely characterize its maximal one. Moreover, in the particular case where S is a generalized tropical semiring (see Definition 1.1.1), we are able to characterize completely its solutions and give an explicit bound of the computational cost associated with its computation. Finally, we give a cryptographic application by using our previous results in the case of S being finite and propose an attack to the key exchange protocol presented in [21] and, in the tropical semiring case, to cryptanalyze a quite recent protocol to key exchange in [22] as well.

2. Materials and Methods

In this section, we will introduce some basic background on semigroups and introduce some basic results which we will use throughout this paper.

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

$$a(b + c) = ab + ac,$$
$$(a + b)c = ac + bc,$$

where the symbol of the operation $\cdot$ is omitted.

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

Definition 2. *Let R be a semiring and $(M, +)$ be a commutative semigroup with the identity 0_M. M is a right semimodule over R if there is an external operation $\cdot : M \times R \to M$ such that*

$$(m \cdot a) \cdot b = m \cdot (a \cdot b),$$
$$m \cdot (a + b) = m \cdot a + m \cdot b,$$
$$(m + n) \cdot a = m \cdot a + n \cdot a,$$
$$0_M \cdot a = 0_M,$$

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

Let $(R, +, \cdot)$ be an additively idempotent semiring. Every such semiring is endowed with an order given by the first operation, which is defined as

$$a \leq b \text{ if and only if } a + b = b.$$

This order respects the operation in R and enables defining a partial order in R^n for every positive integer n:

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

If R is a semiring, then we will denote with $Mat_n(R)$ the semiring of square matrices of the order n for some positive integer n and whose entries are in R.

Lemma 1. *The previous order is compatible with the operations in R^n as a right $Mat_n(R)$ semimodule.*

Proof. On one hand, if $X = (x_1, \dots, x_n)$, $Y = (y_1, \dots, y_n) \in R^n$ are such that $X \geq Y$ and $C = (c_1, \dots c_n) \in R^n$, then we have $X \geq Y$ implying that $x_i \geq y_i \ \forall i \in \{1, \dots, n\}$ and therefore $x_i + c_i \geq y_i + c_i \ \forall i \in \{1, \dots, n\}$. Thus, $X + C \geq Y + C$.

On the other hand, if $A = (a_{i,j}) \in Mat_n(R)$, and $X \geq Y$ (i.e., $x_i \geq y_i \ \forall i = 1, \dots, n$), then $x_i a_{i,j} \geq y_i a_{i,j} \ \forall i, j \in \{1, \dots, n\}$ and thus $\sum_i x_i a_{i,j} \geq \sum_i y_i a_{i,j} \ \forall i, j \in \{1, \dots, n\}$. Therefore, $XA \geq YA$. □

Let $XA = Y$ be the system of linear equations in R with indeterminates $x_1, \dots, x_n$:

$$x_1 \begin{pmatrix} a_{1,1} \\ a_{1,2} \\ \vdots \\ a_{1,m-1} \\ a_{1,m} \end{pmatrix} + x_2 \begin{pmatrix} a_{2,1} \\ a_{2,2} \\ \vdots \\ a_{2,m-1} \\ a_{2,m} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{n,1} \\ a_{n,2} \\ \vdots \\ a_{n,m-1} \\ a_{n,m} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{m-1} \\ y_m \end{pmatrix},$$

with $a_{i,j}, y_j \in R$ for all $i = 1, \dots, n$ $j = 1, \dots, m$. If we denote A_i as the ith row of A, where $A_i = (a_{i,1}, a_{i,2}, \dots, a_{i,m})$, then the system can be written as

$$x_1 A_1 + x_2 A_2 + \cdots + x_n A_n = Y.$$

Definition 3. *Let R be an additively idempotent semiring, and let $XA = Y$ be a linear system of equations. We say that $\hat{X}$ is the maximal solution of the system if the two following conditions are satisfied:*

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

Note that the last condition is equivalent to $Z \leq \hat{X}$.

3. Results

3.1. The Maximal Solution of a Linear System

Our aim in this section is to provide a characterization of the maximal solution of a linear system on certain additively idempotent semirings which will allow us to characterize every solution of these types or systems, and then we will be able to derive an algorithm to compute them.

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

$$C_i = \max W_i.$$

If $XA = Y$ has a solution, then $Z = (C_1, \dots C_n)$ is the maximal solution of the system.

Proof. If there is a solution $\hat{X} = (\hat{x}_1, \ldots, \hat{x}_n)$, then for all $k = 1, \ldots, n$ we have that

$$\hat{X}A = Y \Rightarrow \hat{x}_1A_1 + \hat{x}_2A_2 + \ldots \hat{x}_kA_k + \cdots + \hat{x}_nA_n = Y \Rightarrow \hat{x}_kA_k + Y = Y \Rightarrow \hat{x}_k \in W_k, \quad (1)$$

where we used the following relation:

$$\begin{aligned} Y &= Y + Y, \\ &= \hat{x}_1 \cdot A_1 + \hat{x}_2 \cdot A_2 + \cdots + \hat{x}_k \cdot A_k + \cdots + \hat{x}_n \cdot A_n + Y, \\ &= \hat{x}_1 \cdot A_1 + \hat{x}_2 \cdot A_2 + \cdots + \hat{x}_k \cdot A_k + \hat{x}_k \cdot A_k + \cdots + \hat{x}_n \cdot A_n + Y, \\ &= \hat{x}_k \cdot A_k + \hat{x}_1 \cdot A_1 + \hat{x}_2 \cdot A_2 + \cdots + \hat{x}_n \cdot A_n + Y, \\ &= \hat{x}_k \cdot A_k + Y. \end{aligned}$$

Since $\hat{x}_k \in W_k$ in Equation (1), we have $C_k \geq \hat{x}_k \ \forall k = 1, \ldots, n$. Hence, under the proof of Lemma 1, we have

$$Z \geq \hat{X} \Rightarrow ZA \geq \hat{X}A = Y. \quad (2)$$

In addition, as $maxW_i \in W_i$, by the definition of W_i, we find that

$$C_i \in W_i \Rightarrow ZA \leq Y,$$

and thus, $ZA = Y$ (i.e., Z is a solution). Furthermore, under the definition of the order in R^n, we find that this solution is maximal. □

In the finite case, where both the existence of a solution for the linear system and the computation of the maximal solution are guaranteed precisely by the finiteness condition, we have the following result.

Theorem 2. *Let R be an additively idempotent finite semiring, and let $XA = Y$ be a system of equations with $Y \in R^m$ and $A = (a_{i,j}) \in Mat_{n\times m}(R)$. If the system has a solution, then $W_i = \{x \in R : x \cdot A_i + Y = Y\}$ is finite and*

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

is the maximal solution of the system.

Proof. To show this, it is enough to prove that the set $W_i = \{x \in R : xA_i + Y = Y\}$ has a maximum, which is

$$x_i = \max_{x \in W_i} x = \sum_{x \in W_i} x$$

and then apply Theorem 1.

Given that W_i is finite for every $i = 1, \ldots, n$, we can assert that $x_i = \sum_{x \in W_i} x$ for every $i = 1, \ldots, n$ is well defined.

Now, if $h \in W_i$, then $h \leq x_i$ for every $i = 1, \ldots, n$, given that

$$x_i + h = \sum_{x \in W_i} x + h = \sum_{x \in W_i, x \neq h} x + h + h = \sum_{x \in W_i, x \neq h} x + h = \sum_{x \in W_i} x = x_i$$

Finally, if $a + y = b + y = y$, then $(a + b) + y = y$, which shows that W_i is additively closed, and hence $x_i = \sum_{x \in W_i} \in W_i$. □

3.2. Linear Systems on Tropical Semirings

As we showed in Theorem 1, we can characterize the maximal solution of a linear system over an additively idempotent semiring under some circumstances. Our aim in this section is to study the existence of solutions in the particular case of tropical semirings.

Definition 4. *Let $(R, +, \cdot)$ be a semiring. We say that R is a generalized tropical semiring if*

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

The following lemma is immediate from the preceding definition.

Lemma 2. *Every generalized tropical semiring is totally ordered with respect to the order induced by the addition.*

Example 1. *$(\mathbb{N}, \max, \cdot)$ is a semiring where $a + b = \max\{a, b\} = a$ or b, and thus it is a generalized tropical semiring. Analogously, $(\mathbb{R}, \max, +)$, $(\mathbb{Z}, \max, +)$ and $(\mathbb{Q}, \max, +)$ are also generalized tropical semirings, and they verify being a group with respect to the second operation.*

The semiring $(\mathbb{N}, +, \cdot)$, where $+$ and $\cdot$ denote the usual addition and product of natural numbers, respectively, is an example of a semiring which is not a generalized tropical semiring.

The previous example induces the following definition.

Definition 5. *Let $(S, +)$ be a semigroup with a total order which is compatible with the operation $+$. We define the tropicalized semiring of S as the semiring $Trop(S) = S \cup \{-\infty\}$, with the inner addition defined by* max*, given by the order in S, and the inner product defined by $+$, the inner operation of S, and extend these to ∞ in the following way:*

1. $a + (-\infty) = -\infty + a = -\infty \ \forall a \in Trop(S)$.
2. $\max\{a, -\infty\} = \max\{-\infty, a\} = a \ \forall a \in Trop(S)$.

Example 2. *Let us consider the semiring with two elements $T = \{0, 1\}$ whose addition is given by $0 + 0 = 1 + 0 = 0 + 1 = 0$ and $1 + 1 = 1$ and the product defined by $a \cdot b = 0$ for $a, b \in T$. Then, $(T, +, \cdot)$ is a generalized tropical semiring, but it is not a tropical semiring nor the tropicalized semiring of an ordered semigroup.*

The following result is straightforward.

Lemma 3. *Let $(S, +)$ be a totally ordered semigroup, and let $(Trop(S), \max, +)$ be its tropicalized semiring. Then, $(Trop(S), \max, +)$ is a generalized tropical semiring.*

Let us recall from [17] that the tropical semiring is given by the semiring $(\mathbb{R} \cup \{-\infty\}, \max, +)$. It can immediately be found that the tropical semiring is the tropicalized version of $\mathbb{R}$ with the usual operations.

Theorem 3. *Let $(R, +, \cdot)$ be a generalized tropical semiring where $(R, \cdot)$ is a group. If the linear system $X \cdot A = Y$ has a solution $X = (x_1, \ldots, x_n)$, then it is of the form $x_i = maxW_i$.*

Proof. Firstly, we will prove that the sets $W_i = \{x \in R : x \cdot A_i + Y = Y\}$ with $A_i = (a_{i,j})_{j=1\ldots,m}$, $i = 1, \ldots, n$ have a maximum, and thus we can use Theorem 1.

If $x \in W_i$, then we have that $x \cdot A_i + Y = Y$, where if we see the jth row, then we can obtain $x \cdot a_{i,j} + y_j = y_j$. Therefore, we have

$$\max\{x \cdot a_{i,j}, y_j\} = y_j \Rightarrow x \cdot a_{i,j} \leq y_j \Rightarrow x \leq y_j \cdot a_{i,j}^{-1},$$

and thus $x \in W_i$ if and only if $x \leq y_j \cdot a_{i,j}^{-1}$ for all $j \in \{1, \ldots, m\}$. This condition is verified if $x \leq \min_j\{y_j \cdot a_{i,j}^{-1}\}$.

Now, if we denote $C_i = \min_j\{y_j \cdot a_{i,j}^{-1}\}$, then we find that C_i is an upper bound of W_i because $x \in W_i \Rightarrow x \leq C_i$. In addition, it belongs to the set W_i due to the following identity:

$$C_i a_{i,j} = \min_j \{y_j \cdot a_{i,j}^{-1}\} a_{i,j} \leq y_j a_{i,j}^{-1} a_{i,j} = y_j,$$

which holds for all $j \in \{1, \ldots, m\}$, where $C_i a_{i,j} + y_j = y_j$. We can conclude that $\max W_i = C_i$. □

Moreover, as a consequence of the previous result, we obtain the following corollary.

Corollary 1. *Let $(R, +, \cdot)$ be a generalized tropical semiring where $(R, \cdot)$ is a group, $A = (a_{i,j}) \in Mat_{n\times m}(R)$, and the column vector $Y = (y_1, \ldots, y_m) \in R^m$. If the linear system $XA = Y$ has at least one solution, then its maximal solution is of the form $(M_1, \ldots, M_n)$, where $M_i = \min_j \{y_j a_{i,j}^{-1}\} = \max W_i$ for $i = 1, \ldots, n$.*

We can also point out that in case the semiring $(R, +, \cdot)$ is such that $(R, \cdot)$ is not a group, we can use the following theorem from [23].

Theorem 4. *A commutative semigroup can be embedded in a group if and only if it is cancellative.*

Theorem 5. *Every generalized tropical semiring $(R, +, \cdot)$ such that $(R, \cdot)$ is cancellative can be embedded into a generalized tropical semiring having inverses with respect to $\cdot$.*

Proof. Let $(R, +, \cdot)$ be a generalized tropical semiring such that $(R, \cdot)$ is cancellative. Then, under the preceding, it can be embedded into a group, which we will denote as $Q(R)$. Note that the elements of $Q(R)$ are of the form $a/b := ab^{-1}$ with $a, b \in R$. Now, given that R is totally ordered, we can endow $Q(R)$ with a total order as follows:

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bd \; \forall a, b, c, d \in R. \tag{3}$$

Now, we can define the addition in $Q(R)$ as

$$\frac{a}{b} +_Q \frac{c}{d} = \max\{\frac{a}{b}, \frac{c}{d}\}. \tag{4}$$

Then, the properties which the operation max satisfy give us that $(Q(R), +_Q, \cdot)$ is a generalized tropical semiring. Inverses exist with respect to the second operation, and the embedding $R \hookrightarrow Q(R)$ is a semiring homomorphism. □

Example 3. *We have that $(\mathbb{N} \cup \{-\infty\}, \max, \cdot)$ is a generalized tropical semiring. Furthermore, $(\mathbb{N}, \cdot)$ is cancellative. With the previous result, we can embed $(\mathbb{N} \cup \{-\infty\}, \max, \cdot)$ into a generalized tropical semiring with inverses which, under the preceding construction, can be $(\mathbb{Q}_{>0} \cup \{-\infty\}, \max, \cdot)$.*

Now, we will show how to find every solution of the previous system.

Lemma 4. *Let R be a generalized tropical semiring, where $(R, \cdot)$ is cancellative and $XA = Y$ is a linear system of equations which has a solution, for which $A = (a_{i,j}) \in Mat_{n\times m}(R)$ and $Y = (y_1, \ldots, y_m) \in R^m$. Let $C_i = \max W_i$. Then, $x \in W_i$ if and only if $x \leq C_i$.*

Proof. Let $x \leq C_i$, and let A_i be the ith row of A for $i = 1, \ldots, n$. Then, $xA_i \leq C_i A_i$, and thus $xA_i + Y \leq C_i A_i + Y = Y$ Moreover, $Y \leq xA_i + Y$, since

$$Y + (xA_i + Y) = (xA_i + Y) + Y = xA_i + (Y + Y) = xA_i + Y$$

and hence $xA_i + Y = Y$ and $x \in W_i$. □

Let R be a generalized tropical semiring, and let $XA = Y$ be a linear system of equations with $Y = (y_i) \in R^m$ and $A = (a_{i,j}) \in Mat_{n\times m}(R)$. Let $W_i = \{x \in R :$

$x \cdot A_i + Y = Y\}$. Then, under the proof of Theorem 3, W_i has a maximum which will be denoted by C_i for all $i = 1, \ldots, n$.

Theorem 6. *Let R be a generalized tropical semiring, and let $XA = Y$ be a system of equations with $Y = (y_i) \in R^m$ and $A = (a_{i,j}) \in Mat_{n\times m}(R)$. $X = (x_1, x_2, \ldots, x_n)$ is a solution of the system if and only if*

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

Proof. Let us assume first that $X = (x_1, x_2, \ldots, x_n)$ is a solution of the system. Then, the first condition was already proven in Equation 1. Let us now show the second condition. We have that

$$x_1 \cdot A_1 + x_2 \cdot A_2 + \cdots + x_n \cdot A_n = Y.$$

For a fixed value j, we find that

$$x_1 \cdot a_{1,j} + x_2 \cdot a_{2,j} + \cdots + x_n \cdot a_{n,j} = y_j.$$

Using the definition of generalized tropical semiring, we have that there exists $h \in \{1, \ldots, n\}$ such that $x_h a_{h,j} = y_j$.

Conversely, let us suppose now that X verifies both conditions. Then, we have

$$\sum_i x_i \cdot a_{i,j} = x_1 \cdot a_{1,j} + \cdots + x_{h-1} \cdot a_{h-1,j} + x_h \cdot a_{h,j} + x_{h+1} \cdot a_{h+1,j} + \cdots + x_n \cdot a_{n,j}$$

Now, under condition 2, there exists $h \in \{1, \ldots, n\}$ such that $x_h a_{h,j} = y_j$, and thus we can rewrite the equation as

$$\sum_i x_i \cdot a_{i,j} = \sum_{i \neq h} x_i \cdot a_{i,j} + y_j$$

As $x_i a_{i,j} + y_j = y_j$ for all j, and as the semiring is additively idempotent, we finally obtain

$$\sum_i x_i \cdot a_{i,j} = y_j$$

for all $j \in \{1, \ldots, m\}$. Thus, X is a solution of the system. □

Corollary 2. *Let $(R, +, \cdot)$ be a generalized tropical semiring such that $(R, \cdot)$ is a group. If the system $XA = Y$ has a solution, then $X = (x_1, x_2, \ldots, x_n)$ is a solution if and only if*

1. $x_i \in W_i\ \forall i = 1, \ldots, n$.
2. $\forall j = 1, \ldots, m\ \exists h \in \{1, \ldots, n\}$ *such that* $x_h = C_h = y_j a_{h,j}^{-1}$

where $a_{h,j}^{-1}$ is the inverse of $a_{h,j}$ in a generalized tropical semiring having inverses with respect to $\cdot$ and which contains R.

Proof. It is enough to show that the conditions are equivalent to those of Theorem 6.

Firstly, note that the first condition and condition 1 of Theorem 6 are equivalent.

We will show now that if condition 1 is true, then condition 2 is equivalent to condition 2 of Theorem 6.

If 1 is satisfied, then $x_i \leq C_i = max\ W_i$. In addition, if condition 2 of Theorem 6 is verified, then

$$x_h = y_j a_{h,j}^{-1} \geq \min_p \{y_p a_{h,p}^{-1}\} = C_h \geq x_h.$$

using Corollary 1, and thus $x_h = C_h$. The converse is trivial. □

Remark 1. *Let R be a generalized tropical semiring as illustrated above, and let us consider the system $AX = Y$. $X = (x_1, x_2, \ldots, x_n)$ to be a solution of the system if and only if, for every equation, $j \in \{1, \ldots, m\}$ in the system:*

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

Then, under the previous corollary, for every $j = 1, \ldots, m$, there exists $h \in \{1, \ldots, n\}$ such that $C_h = y_j a_{h,j}^{-1}$, and in addition, $x_h = C_h$. As a result, there exits a non-empty set $Index(j) = \{i \in \{1, \ldots, n\} : C_i = y_i a_{i,j}^{-1}\}$. This induces the following result, which provides an algorithm to solve linear equations systems.

Theorem 7. *Let $(R, +, \cdot)$ be a generalized tropical semiring such that $(R, \cdot)$ is a group, and let $XA = Y$ be a system of equations with $Y \in R^m$ and $A = (a_{i,j}) \in Mat_{n \times m}(R)$. Determining all of the solutions of the system has a computational cost of $o(nm)$.*

Proof. We observe that the solution of the system is given by the vectors $X = (x_1, x_2, \ldots, x_n)$ with the following designations.

For every j, we can choose $h \in Index(j)$ such that $x_h = C_h$. The rest of the conditions (x_p $p = 1, \ldots, n$, $p \neq h$) verify that $x_p \leq C_p$.

To prove this, note that every $X = (x_1, \ldots, x_n)$ with this designation verifies that $x_i \leq C_i$, and from Lemma 4, we have $x_i \in W_i$. Moreover, we observe that for every j, we have some $h \in Index(j)$ with $x_h = C_h = y_j a_{h,j}^{-1}$. Thus, under the preceding corollary, it is a solution.

On the other hand, if $X = (x_1, \ldots, x_n)$ is a solution, then it satisfies the conditions of the preceding corollary. Then, $x_i \in W_i$, and thus $x_i \leq C_i = \max W_h$. Moreover, for every $j = 1, \ldots, m$, there exists h such that $x_h = C_h$. But then $x_h = y_h a_{h,j}^{-1}$, and hence $h \in Index(j)$.

As a result, to determine all of the solutions of the system, it is enough to compute $C_i = \max W_i$ for every $i = 1, \ldots, n$ and $Index(j) = \{i \in \{1, \ldots, n\} : C_i = y_i a_{i,j}^{-1}\}$ for every $j = 1, \ldots, m$.

To calculate these, we can use the following algorithm.

We first compute the matrix $M \in Mat(R)_{n \times m}$, whose ith column M_i is of the form

$$M_i = (y_j a_{i,j}^{-1})_{j=1,\ldots,m} = \begin{pmatrix} y_1 a_{i,1}^{-1} \\ y_2 a_{i,2}^{-1} \\ \vdots \\ y_m a_{i,m}^{-1} \end{pmatrix}$$

for every $i = 1, \ldots, n$

This results in the computation of nm being inverse and nm operations in the set R.

Then, we calculate $C_i = \min M_i = \min_{j=1,\ldots,m} y_j a_{i,j}^{-1}$ for every $i = 1, \ldots, n$, and simultaneously, we compute the set $Row(i) = \{j \in \{1, \ldots, m\}; C_i = y_j a_{i,j}^{-1}\}$, which gives m comparisons for each column and thus nm operations.

Next, we build $Index(j) = \{i \in \{1, \ldots, n\} : C_i = y_i a_{i,j}^{-1}\}$ using $Row(i)$ with the following process:

1. Take $Index(j)$ to be empty for every $j = 1, \ldots, m$.
2. Examine $Row(i)$ for $i = 1, \ldots, n$, and if $j \in Row(i)$, then add i to $Index(j)$.

This process requires examining $Row(i)$, and since $Row(i) \subseteq \{1, \ldots, m\}$, this procedure requires $o(m)$ comparisons for every $i = 1, \ldots, n$. Hence, the cost is $o(nm)$.

Taking into account that the comparison of two elements is made through the addition of both elements in R, the total cost is $o(nm)$ basic operations in the ring $(R, +, \cdot)$. □

Remark 2. *We recall that when the generalized tropical semiring R is such that $(R, \cdot)$ is cancellative, which is less restrictive than being a group. Using Theorem 5, we can embed this semiring into a generalized tropical semiring S in the conditions of Corollary 2, and then we can solve any linear system as previously shown, obtaining each solution in S and then checking if any of them are in fact contained in R.*

4. Discussion

Within the references, in [17], a method for solving a system of equations through normalization is presented. In [24], the structure of the solution of a system of equations over a tropical semiring was studied by using the rank over rows and columns, and subsequently, a generalized Cramer method was used to find the maximal solution over a tropical semiring.

Examples of systems of equations appear in both papers. In [17], a solution (though not necessarily maximal) was computed, and in [24], the authors provided the range of freedom of the solution. Now, using the preceding, we can show the complete set of solutions of those systems of equations.

To avoid misreading the operation over R as a usual ring and rather as a tropical semiring, the operation $(R, \max, +)$ will be denoted as $(R, +_T, \cdot_T)$.

Example 4. *In [24] , the authors computed a solution of the system*

$$\begin{bmatrix} -4 & 7 & 12 & -3 & 0 \\ 3 & 2 & 8 & 3 & -1 \\ -9 & 1 & 6 & 0 & 2 \\ 2 & 8 & -5 & 1 & -3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 14 \\ 10 \\ 8 \\ 11 \end{bmatrix}.$$

Let us determine the complete set of solutions of the system as well as the maximal solution. Firstly, we calculate $y_j \cdot_T a_{i,j}^{-1} = y_j - a_{i,j}$, obtaining the matrix

$$(y_j - a_{i,j})_{i,j} = \begin{bmatrix} 18 & 7 & 2 & 17 & 14 \\ 7 & 8 & 2 & 7 & 11 \\ 17 & 7 & 2 & 8 & 6 \\ 8 & 3 & 16 & 12 & 14 \end{bmatrix}.$$

Then, we have $C_i = \min_j\{y_j - a_{i,j}\}$ and the rows where these minima are reached.

$\max W_i$	Value	Row
C_1	7	$\{2\}$
C_2	3	$\{4\}$
C_3	2	$\{1,2,3\}$
C_4	7	$\{2\}$
C_5	6	$\{3\}$

Now, let us compute $Index(j)$.

	Columns
$Index(1)$	$\{3\}$
$Index(2)$	$\{1,3,4\}$
$Index(3)$	$\{3,5\}$
$Index(4)$	$\{2\}$

Thus, the solutions are

$$\begin{aligned} v_1 &= (7,3,2,7,h_5)\\ v_1 &= (7,3,2,h_4,6)\\ v_1 &= (h_1,3,2,7,h_5)\\ v_1 &= (h_1,3,2,h_4,6)\\ v_1 &= (h_1,3,2,7,h_5)\\ v_1 &= (h_1,3,2,7,6) \end{aligned}$$

with $h_i \leq C_i$.

Moreover, we can observe that the maximal solution was $(7,3,2,7,6)$.

Example 5. *In [17], the authors computed the maximal solution of*

$$\begin{bmatrix} 165 & 57 & 72 & -7 & 0\\ 141 & 64 & 48 & 3 & -1\\ 137 & 101 & 46 & 0 & 2\\ -243 & 98 & -206 & 156 & -5 \end{bmatrix} \begin{bmatrix} x_1\\ x_2\\ x_3\\ x_4\\ x_5 \end{bmatrix} = \begin{bmatrix} 102\\ 78\\ 76\\ 160 \end{bmatrix}$$

Using our proposed method, we will compute all of the solutions, including the maximal one:

$$(y_j - a_{i,j})_{i,j} = \begin{bmatrix} -63 & 45 & 30 & 109 & 102\\ -63 & 14 & 30 & 75 & 79\\ -61 & -25 & 30 & 76 & 74\\ 403 & 62 & 366 & 4 & 165 \end{bmatrix}$$

Then, we have $C_i = \min_j\{y_j - a_{i,j}\}$ *and the rows where those minima were reached.*

$\max W_i$	Value	Row
C_1	-63	$\{3\}$
C_2	-25	$\{3\}$
C_3	30	$\{1,2,3\}$
C_4	4	$\{4\}$
C_5	74	$\{3\}$

Now, we compute $Index(j)$.

$Index(j)$	Columns
$Index(1)$	$\{3\}$
$Index(2)$	$\{3\}$
$Index(3)$	$\{1,2,3,5\}$
$Index(4)$	$\{4\}$

Thus the solutions are

$$\begin{aligned} v_1 &= (-63,h_2,30,4,h_5)\\ v_1 &= (h_1,-25,30,4,h_5)\\ v_1 &= (h_1,h_2,30,4,h_5)\\ v_1 &= (h_1,h_2,30,4,74) \end{aligned}$$

where $h_i \leq C_i$.

In addition, the maximal solution was $(-63,-25,30,4,74)$*, which matched the one obtained in the original paper.*

Cryptographic Applications

In [21], the authors introduced a key exchange protocol over semirings and proposed the use of a finite additively idempotent semiring. Quite recently, and using a similar construction to find the shared key, in [22], the authors proposed the tropical semiring to obtain another group key exchange. We now show a general strategy which reduces the cryptanalysis to solve a linear system of equations, and in the case of additively idempotent semirings, the method which we introduced in this paper can then be used to find the keys used by both proposals rather easily from just the information which the parties make public.

In both cases, they used an additively idempotent semiring R and $M, T, N \in Mat_n(R)$. Each party had a pair of polynomials over the center of R, (p_a, q_a), $(p_b.q_b)$. In the case of the protocol introduced in [21], the parties agreed on a finite additively idempotent semiring. Then, they had $p_a(M)Tq_a(N)$ and $p_b(M)Tq_b(N)$, and the common shared key was $p_a(M)p_b(M)Tq_b(N)q_a(N)$. In the case of [22], the parties agreed on the tropical semiring, and they used two private numbers $h_a, h_b \in \mathbb{N}$ and had $T_a = \sum_{n=0}^{h_a-1} p_a(M)^{h_a-1-n}Tq_a(N)^n$ and $T_b = \sum_{n=0}^{h_b-1} p_b(M)^{h_b-1-n}Tq_b(N)^n$, respectively. In this case, the shared key was $\sum_{n=0}^{h_b-1}\sum_{m=0}^{h_a-1} p_b(M)^{b-1-n}p_a(M)^{a-1-m}Tq_a(N)^m p_b(N)^n$.

Notice that the protocol appearing in [22] is an extension of that given in [21], if we consider that $h_a = h_b = 1$. Therefore, it is enough to simply study the second case.

Let us fix h to an upper bound for the degrees of p_a, q_a, and let u be a bound for the integer h_a, h_b. This is chosen by the attacker at the moment of starting the activity and depends on the computational capabilities. Then, we can rewrite T_a as

$$T_a = \sum_{n=0}^{h_a-1} p_a(M)^{h_a-1-n}Tq_a(N)^n = \sum_{n=0}^{h_a-1}(\sum_{i=0}^{h} p_i M^i)^{h_a-1-n}T(\sum_{j=0}^{h} q_i N^j)^n = \sum_{i,j=0}^{(h_a-1)\cdot h} c_{ij}M^iTN^j \tag{5}$$

for certain values of c_{ij}, where p_i, q_j are elements of the center of R. Note that these coefficients constitute a particular solution of the system

$$T_a = \sum_{i,j=0}^{(h_a-1)\cdot h} d_{ij}M^iTN^j \tag{6}$$

Using the algorithm previously described, we can find a particular solution of the system $d_{i,j} \in Z[R]$. Then, we can build the function $F[X, Y, Z] = \sum_{i,j=0}^{(u-1)h} d_{i,j}X^iYZ^j$, which verifies that

$$F[M, T, N] = \sum_{i,j=0}^{(u-1)h} d_{i,j}M^iTN^j = A.$$

Then, we have

$$\begin{aligned} F[M, T_b, N] = \sum_{i,j=0}^{(u-1)h} d_{i,j}M^iT_bN^j = \sum_{i,j=0}^{(u-1)h} d_{i,j}M^i\left(\sum_{n=0}^{(u-1)h} C^{u-1-n}TD^n\right)N^j = \\ \sum_{i,j=0}^{(u-1)h}\sum_{n=0}^{(u-1)h} d_{i,j}M^iC^{u-1-n}TD^nN^j = \sum_{i,j=0}^{(u-1)h}\sum_{n=0}^{(u-1)h} C^{u-1-n}d_{i,j}M^iTN^jD^n = \\ \sum_{n=0}^{(u-1)h}\sum_{i,j=0}^{(u-1)h} C^{u-1-n}d_{i,j}M^iTN^jD^n = \sum_{n=0}^{(u-1)h} C^{u-1-n}\left(\sum_{i,j=0}^{(u-1)h} d_{i,j}M^iTN^j\right)D^n = \\ \sum_{n=0}^{(u-1)h} C^{u-1-n}T_aD^n = K \end{aligned} \tag{7}$$

which is the shared key after the parties run the protocol.

Now, let us check how this reasoning applies to the example proposed in [22], revealing the common key agreed upon by the parties. In this case, we make use of the following matrices:

$$M = \begin{pmatrix} 1012 & 1011 \\ 2 \times 1011 & 3 \times 1012 \end{pmatrix}$$

$$N = \begin{pmatrix} 4 \times 1012 & 3 \times 1011 \\ 8 \times 1011 & 1012 \end{pmatrix}$$

$$T = \begin{pmatrix} 0 & 5 \times 1011 \\ -\infty & 0 \end{pmatrix}$$

and one of the values that is made public by one of the parties is

$$T_a = \begin{pmatrix} 4 \times 10^{12} & 3.6 \times 10^{12} \\ 3.2 \times 10^{12} & 6 \times 10^{12} \end{pmatrix}$$

Using the previous algorithm, we can find the polynomial:

$$\begin{aligned} F[X,Y,Z] = {} & 3.1 \times 10^{12} \oplus X^0YZ^0 \otimes 2.1 \times 10^{12} \oplus X^0YZ^1 \otimes \\ & -3 \times 10^{12} \oplus X^0YZ^3 \otimes -6 \times 10^{12} \oplus X^0YZ^4 \otimes \\ & -1.2 \times 10^{13} \oplus X^0YZ^6 \otimes -1.5 \times 10^{13} \oplus X^0YZ^7 \otimes \\ & 0 \oplus X^1YZ^0 \otimes -1 \times 10^{12} \oplus X^1YZ^1 \otimes \\ & -7 \times 10^{12} \oplus X^1YZ^3 \otimes -1 \times 10^{13} \oplus X^1YZ^4 \otimes \\ & -1.6 \times 10^{13} \oplus X^1YZ^6 \otimes -1.9 \times 10^{13} \oplus X^1YZ^7 \otimes \\ & -4 \times 10^{12} \oplus X^2YZ^0 \otimes -5 \times 10^{12} \oplus X^2YZ^1 \otimes \\ & -1.1 \times 10^{13} \oplus X^2YZ^3 \otimes -1.4 \times 10^{13} \oplus X^2YZ^4 \otimes \\ & -2 \times 10^{13} \oplus X^2YZ^6 \otimes -2.3 \times 10^{13} \oplus X^2YZ^7 \otimes \\ & -8 \times 10^{12} \oplus X^3YZ^0 \otimes -9 \times 10^{12} \oplus X^3YZ^1 \otimes \\ & -1.5 \times 10^{13} \oplus X^3YZ^3 \otimes -1.8 \times 10^{13} \oplus X^3YZ^4 \otimes \\ & -2.4 \times 10^{13} \oplus X^3YZ^6 \otimes -2.7 \times 10^{13} \oplus X^3YZ^7 \otimes \\ & -1.2 \times 10^{13} \oplus X^4YZ^0 \otimes -1.3 \times 10^{13} \oplus X^4YZ^1 \otimes \\ & -1.9 \times 10^{13} \oplus X^4YZ^3 \otimes -2.2 \times 10^{13} \oplus X^4YZ^4 \otimes \\ & -2.8 \times 10^{13} \oplus X^4YZ^6 \otimes -3.1 \times 10^{13} \oplus X^4YZ^7 \otimes \\ & -1.6 \times 10^{13} \oplus X^5YZ^0 \otimes -1.7 \times 10^{13} \oplus X^5YZ^1 \otimes \\ & -2.3 \times 10^{13} \oplus X^5YZ^3 \otimes -2.6 \times 10^{13} \oplus X^5YZ^4 \otimes \\ & -3.2 \times 10^{13} \oplus X^5YZ^6 \otimes -3.5 \times 10^{13} \oplus X^5YZ^7 \otimes \\ & -2 \times 10^{13} \oplus X^6YZ^0 \otimes -2.1 \times 10^{13} \oplus X^6YZ^1 \otimes \\ & -2.7 \times 10^{13} \oplus X^6YZ^3 \otimes -3 \times 10^{13} \oplus X^6YZ^4 \otimes \\ & -3.6 \times 10^{13} \oplus X^6YZ^6 \otimes -3.9 \times 10^{13} \oplus X^6YZ^7 \otimes \\ & -2.4 \times 10^{13} \oplus X^7YZ^0 \otimes -2.5 \times 10^{13} \oplus X^7YZ^1 \otimes \\ & -3.1 \times 10^{13} \oplus X^7YZ^3 \otimes -3.4 \times 10^{13} \oplus X^7YZ^4 \otimes \\ & -4 \times 10^{13} \oplus X^7YZ^6 \otimes -4.3 \times 10^{13} \oplus X^7YZ^7 \otimes \\ & -2.8 \times 10^{13} \oplus X^8YZ^0 \otimes -2.9 \times 10^{13} \oplus X^8YZ^1 \otimes \\ & -3.5 \times 10^{13} \oplus X^8YZ^3 \otimes -3.8 \times 10^{13} \oplus X^8YZ^4 \otimes \\ & -4.4 \times 10^{13} \oplus X^8YZ^6 \otimes -4.7 \times 10^{13} \oplus X^8YZ^7 \otimes \end{aligned}$$

$$\begin{aligned} & 0 \oplus X^0YZ^2 \otimes \\ & -9 \times 10^{12} \oplus X^0YZ^5 \otimes \\ & -1.8 \times 10^{13} \oplus X^0YZ^8 \otimes \\ & -4 \times 10^{12} \oplus X^1YZ^2 \otimes \\ & -1.3 \times 10^{13} \oplus X^1YZ^5 \otimes \\ & -2.2 \times 10^{13} \oplus X^1YZ^8 \otimes \\ & -8 \times 10^{12} \oplus X^2YZ^2 \otimes \\ & -1.7 \times 10^{13} \oplus X^2YZ^5 \otimes \\ & -2.6 \times 10^{13} \oplus X^2YZ^8 \otimes \\ & -1.2 \times 10^{13} \oplus X^3YZ^2 \otimes \\ & -2.1 \times 10^{13} \oplus X^3YZ^5 \otimes \\ & -3 \times 10^{13} \oplus X^3YZ^8 \otimes \\ & -1.6 \times 10^{13} \oplus X^4YZ^2 \otimes \\ & -2.5 \times 10^{13} \oplus X^4YZ^5 \otimes \\ & -3.4 \times 10^{13} \oplus X^4YZ^8 \otimes \\ & -2 \times 10^{13} \oplus X^5YZ^2 \otimes \\ & -2.9 \times 10^{13} \oplus X^5YZ^5 \otimes \\ & -3.8 \times 10^{13} \oplus X^5YZ^8 \otimes \\ & -2.4 \times 10^{13} \oplus X^6YZ^2 \otimes \\ & -3.3 \times 10^{13} \oplus X^6YZ^5 \otimes \\ & -4.2 \times 10^{13} \oplus X^6YZ^8 \otimes \\ & -2.8 \times 10^{13} \oplus X^7YZ^2 \otimes \\ & -3.7 \times 10^{13} \oplus X^7YZ^5 \otimes \\ & -4.6 \times 10^{13} \oplus X^7YZ^8 \otimes \\ & -3.2 \times 10^{13} \oplus X^8YZ^2 \otimes \\ & -4.1 \times 10^{13} \oplus X^8YZ^5 \otimes \\ & -5 \times 10^{13} \oplus X^8YZ^8 \end{aligned}$$

which satisfies $F[M,T,N] = T_a$, and $F[M,T_b,N] = K$ with K as the shared key.

In the use case proposed in [21], using a particular method, the authors of [25] were able to obtain a polynomial as demonstrated above, whose evaluation in the appropriate values provided the common key. Now, by using the above reasoning and the general

algorithm to solve linear equation systems, for the finite case proposed in [21], we were able to obtain precisely the same polynomial provided in [25], which shows the cryptanalysis of this case.

We determined that finding an appropriate setting to give a key exchange protocol for the post-quantum era is currently an open problem. In 2017, NIST called for a contest to select new cryptographic primitives which allowed obtaining secure algorithms against the attack of a quantum computer. In 2023, four algorithms were selected: one for key encapsulation and three others for digital signatures. Extremely recently, two digital signatures and a key encapsulation method were officially standardized, but the problem of exchanging a secret collaboratively among two communicating parties through an insecure channel remains open. Thus, the alternatives presented in the two previously discussed cases are not appropriate.

5. Conclusions

In this paper, we characterized the maximal solution of a linear equation system defined over an additively idempotent semiring. This characterization gave us the possibility of obtaining general algorithms which could be run in polynomial time to obtain the complete set of solutions of such systems (in case there is at least one) in both the finite case and the tropical semiring case. In the latter case, we extending the existing results to find not only the maximal solution of a linear system but also every solution of the system. Moreover, we have shown how to apply these algorithms to cryptography and show how possible alternatives for a group key exchange protocol for the post-quantum era are vulnerable.

Author Contributions: All authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Junta de Andalucía FQM 0211; Ministerio de Ciencia, Innovación y Universidades, Agencia Estatal de Investigación, Grant number MICIU/AEI/ 10.13039/501100011033; and European Regional Development Fund, European Union, Grant number ERDF/EU PID2022-138906NB-C21.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Golan, J.S. *Semirings and Their Applications*; Kluwer Academic Publishers: Dordrecht, Netherlands, 1999.
2. Vandiver, H.S. Note on a simple type of algebra in which the cancellation law of addition does not hold. *Bull. Am. Math. Soc.* **1934**, *40*, 914–920. [CrossRef]
3. Cuninghame-Green, R. Minimax Algebra. In *Lecture Notes in Economics and Mathematical Systems*; Springer: Berlin, Germany; New York, NY, USA, 1979; Volume 166, p. 258.
4. Kleene, S.C. Representation of events in nerve nets and finite automata. In *Automata Studies*; Annals of Mathematics Studies; Princeton University Press: Princeton, NJ, USA, 1956; Volume 34, pp. 3–41.
5. Klement, E.P.; Mesiar, R.; Pap, E. *Triangular Norms*; Springer: Dordrecht, The Netherlands, 2013; Volume 8.
6. Di Nola, A.; Gerla, B. Algebras of Lukasiewicz's logic and their semiring reducts. In *Idempotent Mathematics and Mathematical Physics*; Contemporary Mathematics; The American Mathematical Society: Providence, RI, USA, 2005; Volume 377, pp. 131–144
7. Di Nola, A.; Lettieri, A.; Perfilieva, I.; Novák, V. Algebraic analysis of fuzzy systems. *Fuzzy Sets Syst.* **2007**, *158*, 1–22. [CrossRef]
8. Di Nola, A.; Russo, C. Semiring and semimodule issues in MV-algebras. *Commun. Algebra* **2013**, *41*, 1017–1048. [CrossRef]
9. Krivulin, N. *Idempotent Algebra Methods for Problems in Modeling and Analysis of Complex Systems*; St. Petersburg University: St. Petersburg, Russia, 2009.
10. Litvinov, G.L.; Maslov, V.P.; Rodionov, A.Y.; Sobolevski, A.N. Universal algorithms, mathematics of semirings and parallel computations. In *Coping with Complexity: Model Reduction and Data Analysis*; Lecture Notes in Engineering and Computer Science; Springer: Berlin, Germany, 2011; Volume 75, pp. 63–89.
11. Simon, I. Limited subsets of a free monoid. In Proceedings of the 19th Annual Symposium on Foundations of Computer Science, Ann Arbor, MI, USA, 16–18 October 1978; IEEE: Long Beach, CA, USA, 1978; pp. 143–150.
12. Floyd, R.W. Algorithm 97: Shortest path. *Commun. ACM* **1962**, *5*, 345. [CrossRef]

13. Viro, O. Dequantization of real algebraic geometry on logarithmic paper. In *European Congress of Mathematics*; Casacuberta, C., Miró-Roig, R.M., Verdera, J., Xambó-Descamps, S., Eds.; Birkhauser Basel: Basel, Switzerland, 2001; pp. 135–146
14. Develin, M.; Santos, F.; Sturmfels, B. On the rank of a tropical matrix. In *Combinatorial and Computational Geometry*; Publications of the Math Sciences Research Institute ; Cambridge Univercity Press: Cambridge, UK, 2005; Volume 52, pp. 213–242.
15. Grigoriev, D. Complexity of solving tropical linear systems. *Comput. Complex.* **2013**, *22*, 71–88. [CrossRef]
16. Davydow, A. New algorithms for solving tropical linear systems. *Algebra i Anal.* **2016**, *28*, 1–19. [CrossRef]
17. Olia, F.; Ghalandarzadeh, S.; Amiraslani, A.; Jamshidvand, S. Solving linear systems over tropical semirings through normalization method and its applications. *J. Algebra Appl.* **2021**, *20*, 2150159. [CrossRef]
18. Noel, V.; Grigoriev, D.; Vakulenko, S.; Radulescu, O. Tropical geometries and dynamics of biochemical networks application to hybrid cell cycle models. In *Electronic Notes in Theoretical Computer Science, Proceedings of the 2nd International Workshop on Static Analysis and Systems Biology (SASB 2011), Venice, Italy, 13 September 2011*; Elsevier Science B.V.: Amsterdam, The Netherlands, 2012; Volume 284, pp. 75–91.
19. Noel, V.; Grigoriev, D.; Vakulenko, S.; Radulescu, O. Hybrid Models of the Cell Cycle Molecular Machinery. In International Workshop on Hybrid Systems Biology Newcastle. 2012. Available online: https://api.semanticscholar.org/CorpusID:12521148 (accessed on 9 August 2024).
20. Gavalec, M.; Němcová, Z.; Storage, S. Tropical linear algebra with the Lukasiewicz T-norm. *Fuzzy Sets Syst.* **2015**, *276*, 131–148. [CrossRef]
21. Maze, G.; Monico, C.; Rosenthal, J. Public key cryptography based on semi- group actions. *Adv. Math. Commun.* **2007**, *1*, 489–507. [CrossRef]
22. Durcheva, M.; Danilchenko, K. Secure Key Exchange in Tropical Cryptography: Leveraging Efficiency with Advanced Block Matrix Protocols. *Mathematics* **2024**, *12*, 1429. [CrossRef]
23. Clifford, A.H.; Preston, G.B. *The Algebraic Theory of Semigroups*; American Mathematical Society: Providence, RI, USA, 1961; p. 34.
24. Jamshidvand, S.; Ghalandarzadeh, S.; Amiraslani, A.; Olia, F. On the maximal solution of a linear system over tropical semirings. *Math. Sci.* **2020**, *14*, 147–157. [CrossRef]
25. Otero Sánchez, A.; López Ramos, J.A. Cryptanalysis of a key exchange protocol based on a congruence-simple semiring action. *J. Algebra Appl.* **2024**, *2024*, 2550229. [CrossRef]