UNIVERSITY OF BIRMINGHAM

On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product

Muanalifah, Any; Sergeev, Sergei

Document Version
Peer reviewed version

[Link to publication on Research at Birmingham portal](#)

On the tropical discrete logarithm problem and security of a protocol based on tropical semidirect product

Any Muanalifah and Sergeĭ Sergeev[*][†]

Abstract

Tropical linear algebra has been recently put forward by Grigoriev and Shpilrain [9, 10] as a promising platform for implementation of protocols of Diffie-Hellman and Stickel type. Based on the CSR expansion of tropical matrix powers, we suggest a simple algorithm for the following tropical discrete logarithm problem: "Given that $A = V \otimes F^{\otimes t}$ for a unique t and matrices A, V, F of appropriate dimensions, find this t." We then use this algorithm to suggest a simple attack on a protocol based on the tropical semidirect product. The algorithm and the attack are guaranteed to work in some important special cases and are shown to be efficient in our numerical experiments.

Keywords: Tropical algebra, semidirect product, matrix powers, cryptanalysis.

MSC classification: 15A80, 94A60, 15A23.

1 Introduction

Tropical (max-plus) semiring is the set of real numbers with adjoined negative infinity $\mathbb{R}_{\max} = \mathbb{R} \cup \{-\infty\}$, equipped with tropical addition $a \oplus b := \max(a, b)$ and tropical multiplication $a \otimes b := a + b$. All the usual axioms hold (such as associativity, commutativity and distributivity), however there is a lack of genuine additive inverses: although the definition of $\ominus$ is possible via symmetrization (Baccelli et al. [1]), it is not straightforward and not easy to use. Instead of this,

---

[*]University of Birmingham, School of Mathematics, Edgbaston B15 2TT, UK.
[†]Corresponding Author: Sergeĭ Sergeev. E-mails: any.math13@gmail.com, sergiej@gmail.com

we have idempotency ($a \oplus a = a$), nonnegativity ($a \geq -\infty$, with $-\infty$ playing the role of additive zero) and close connection to the order: $a \oplus b = b \Leftrightarrow a \leq b$. Note that the multiplicative inverses in $\mathbb{R}_{\max}$ are well-defined for all elements except for $-\infty$: we have $a^- := -a$.

The semiring operations are easily extended to matrices and vectors: we have $(A \oplus B)_{ij} = a_{ij} \oplus b_{ij}$ for any two matrices $A = (a_{ij})$ and $B = (b_{ij})$ with entries in $\mathbb{R}_{\max}$ of same dimensions, and $(A \otimes B)_{ij} = \bigoplus_k a_{ik} \otimes b_{kj}$ for any two matrices A and B of appropriate dimensions. Using this product, we can also define the tropical matrix powers $A^{\otimes t} = \underbrace{A \otimes A \otimes \ldots \otimes A}_{t}$. We can define scalar tropical matrix powers not only for integer exponents but also for real exponents, as follows:

$$a^{\otimes k} = k \times a, \quad \forall a \in \mathbb{R} \quad \forall k \in \mathbb{R}; \quad (-\infty)^{\otimes k} = -\infty, \quad \forall k > 0; \quad (-\infty)^{\otimes 0} = 0.$$

Note that the kth power of $a \in \mathbb{R}$ in the semiring sense is a multiplied by k in the usual sense.

The behaviour of tropical matrix powers is in many ways similar to that of the nonnegative matrix powers (recall that any element of the tropical semiring is nonnegative) and can be considered as tropical counterpart of the classical Perron-Frobenius theory. To this end, we also have the tropical spectral problem, and a theorem that any matrix $F \in \mathbb{R}_{\max}^{d \times d}$ has at least one tropical eigenvalue, meaning $\lambda \in \mathbb{R}_{\max}$ such that there is at least one $x \in \mathbb{R}_{\max}^d$ with at least one component in $\mathbb{R}$ such that $F \otimes x = \lambda \otimes x$. This claim was originally proved by Vorobyev [21, 22], see also Butkovič [4] for a complete solution of this problem in all cases. Vector $x \in \mathbb{R}_{\max}^d$ with at least one component in $\mathbb{R}$ such that $F \otimes x = \lambda \otimes x$ is called a right eigenvector of F and vector $y \in \mathbb{R}_{\max}^d$ with at least one component in $\mathbb{R}$ such that $y \otimes F = \lambda \otimes y$ is called a left eigenvector of F. As usual, left eigenvectors of F are transposed right eigenvectors of F^T, and there is no need for a separate theory for them.

The largest tropical eigenvalue of $F \in \mathbb{R}_{\max}^{d \times d}$, denoted by $\lambda(F)$, can be computed explicitly as follows:

$$\lambda(F) = \bigoplus_{k=1}^{d} \bigoplus_{i_1, \ldots, i_k} (F_{i_1 i_2} \otimes \ldots \otimes F_{i_k i_1})^{\otimes 1/k} = \max_{1 \leq k \leq d} \max_{i_1, \ldots, i_k} \frac{F_{i_1 i_2} + \ldots + F_{i_k i_1}}{k}. \tag{1}$$

Observe that $\lambda(F) = \lambda(F^T)$. Formula (1) is best understood in terms of the associated weighted digraph $\mathcal{G}(F) = (N, E)$, where $N = \{1, \ldots, d\}$ is the set of nodes and $E = \{(i, j): F_{ij} \neq -\infty\}$ is

the set of arcs, weighted by the corresponding entries F_{ij}. In terms of this digraph, $\lambda(F)$ is the maximum mean weight of all cycles on $\mathcal{G}(F)$, also called the maximum cycle mean of $\mathcal{G}(F)$ (or of F). When $\mathcal{G}(F)$ is strongly connected we say that F is irreducible. In this case $\lambda(F)$ is the unique tropical eigenvalue of F.

This indicates an intimate connection between tropical linear algebra and combinatorial optimisation problems, for which many other examples were given by Butkovič [3]. Other important examples of such connection are the metric matrix F^+ and the Kleene star F^*, defined for $F \in \mathbb{R}_{\max}^{d \times d}$ in the case $\lambda(F) \leq 0$ as the matrix series

$$F^+ = F \oplus F^{\otimes 2} \oplus \ldots \oplus F^{\otimes d}, \tag{2}$$

$$F^* = I \oplus F \oplus \ldots \oplus F^{\otimes d-1}. \tag{3}$$

It is easy to see that 1) for arbitrary t, any entry $F_{ij}^{\otimes t}$ is the maximum weight of a walk on $\mathcal{G}(F)$ connecting i to j with length t, 2) any entry F_{ij}^+ of the metric matrix is the maximum weight of a walk on $\mathcal{G}(F)$ connecting i to j of arbitrary length.

Grigoriev and Shpilrain [9, 10] suggested a number of protocols based on the tropical linear algebra, which is briefly introduced above. In particular, they suggested a tropical version of Stickel's protocol, motivated by the lack of genuine additive inverses and by the lack of multiplicative inverses of generic tropical matrices: a tropical matrix cannot be inverted unless it is a generalised monomial matrix [4]. However, subsequently, an attack on their tropical implementation of Stickel's protocol was suggested by Kotov and Ushakov [13]. Furthermore, in a previous publication [16] we analysed a number of other tropical implementations of Stickel's protocol based on commuting matrices in tropical algebra and developed a generalization of the attack [13], which applies to all of them. Although this attack becomes inefficient as the number of monomials or generators of the domain of commuting matrices increases, it is quite successful and motivates the search of other protocols based on tropical algebra. To this end, Grigoriev and Shpilrain [10] suggested new protocols based on two different versions of tropical semidirect product. An attack on both protocols was more recently suggested by Rudy and Monico [19] and then another attack

(on Protocol 1) by Isaac and Kahrobei [12]. For discussion of these attacks, see Subsection 5.3 in the end of this paper.

Our first aim here to solve what we call the tropical discrete logarithm problem (see Problem 2.1 below), as we think that it can be quite important for the existing and future protocols in tropical cryptography. Thus we formulate a tropical discrete logarithm problem and suggest a solution of it based on the weak CSR expansion of Merlet et al. [15]. The solution is also very closely related to the quadratic bound on the ultimate periodicity of critical rows and columns of tropical matrix powers obtained by Nachtigall [17] and improved by Merlet et al. [14]. Theoretically, the solution is guaranteed to work in some special cases, but it also has 100% success in our numerical experiments.

We then show how our solution to the tropical discrete logarithm problem can be applied to suggest yet another attack on Protocol 1 of [10]. The attack is based on the ultimate periodicity of (the critical columns of) the tropical matrix powers, since, as we show in Proposition 3.2, the semidirect powers used in Protocol 1 of [10] can be expressed via the tropical matrix powers.

The rest of the paper is organised as follows. In Section 2 we give more background on the ultimate periodicity in tropical linear algebra, formulate the tropical discrete logarithm problem and give a solution to this problem. We then prove that the solution is guaranteed to work in some special cases. In Section 3 we revisit the tropical semidirect product used by Grigoriev and Shpilrain [10] to construct their Protocol 1. In particular, we show how the messages exchanged by Alice and Bob are related to tropical matrix powers. The protocol and attack on it are described in Section 4. This is followed by some toy examples, discussion of numerical experiments and attacks suggested by Issac and Kahrobaei [12] and Rudy and Monico [19].

2 Discrete logarithm problem and ultimate periodicity

In this section we will discuss the algorithmic solution of the following problem, which we call the tropical discrete logarithm.

Problem 2.1 (Tropical Discrete Logarithm). *Suppose that* $V \in \mathbb{R}_{\max}^{m \times d}$, $F \in \mathbb{R}_{\max}^{d \times d}$ *and secret key*

$t \geq 1$ are used to produce $A = V \otimes F^{\otimes t}$. Knowing A, V and F and that t is unique, find t.

There is an important special case, in which the tropical discrete logarithm is well defined.

Lemma 2.2. *Suppose that V has finite entries and F is irreducible. Then $V \otimes F^{\otimes t_1} \neq V \otimes F^{\otimes t_2}$ for any t_1 and t_2 with $t_1 \neq t_2$ if and only if $\lambda(F) \neq 0$.*

Proof. Suppose that we have $V \otimes F^{\otimes t_1} = V \otimes F^{\otimes t_2}$ for some $t_1 < t_2$. However, then each row $V \otimes F^{\otimes t_1}$ with some finite entries (which has some finite entries since so does V and since F is irreducible) is a left eigenvector of $F^{\otimes(t_2-t_1)}$ with eigenvalue 0. However, since F is irreducible, by [4, Theorem 4.4.8] $\lambda(F) \neq 0$ is the only eigenvalue of F (both for left and for right eigenvectors) and by [5, Corollary 5.5] the set of eigenvalues of $F^{\otimes(t_2-t_1)}$ consists only of the value $(t_2-t_1) \times \lambda(F) \neq 0$, thus it is the unique eigenvalue of $F^{\otimes(t_2-t_1)}$ (both for left and for right eigenvectors). This contradiction shows that $V \otimes F^{\otimes t_1} = V \otimes F^{\otimes t_2}$ implies $t_1 = t_2$, so the tropical discrete logarithm is well-defined.

If $\lambda(F) = 0$, then the sequence $(V \otimes F^{\otimes t})_{t \geq 1}$ is ultimately periodic [7, 8] (see also [1, 4, 11]), implying that the tropical discrete logarithm is not well-defined. $\square$

Now consider $F \in \mathbb{R}_{\max}^{d \times d}$ with $\lambda(F) \neq -\infty$. The critical graph of F, denoted by $\mathcal{G}^c(F)$, is the subgraph of $\mathcal{G}(F)$, which consists of all nodes and arcs of the cycles where the maximum cycle mean $\lambda(F)$ is attained. It is easy to see that the critical graph in general consists of several strongly connected components (abbreviated as s.c.c.), which do not have any connection to one another.

Cyclicity of each component of $\mathcal{G}^c(F)$ is defined as g.c.d. of the lengths of all cycles of that component . Now, suppose that the critical graph $\mathcal{G}^c(F)$ has l s.c.c. $\mathcal{G}_1^c, \ldots, \mathcal{G}_l^c$ with corresponding cyclicities $\sigma_1, \ldots, \sigma_l$. For all $\nu \in \{1, ..., l\}$, each νth component gives rise to a CSR term via the following procedure.

Let $\lambda = \lambda(F)$. Denote $U_\nu = ((\lambda^- \otimes F)^{\otimes \sigma_\nu})^+$ (using the metric matrix defined in (2)). Then,

let matrices C_ν, R_ν and S_ν be defined by:

$$
(C_\nu)_{ij} = \begin{cases} (U_\nu)_{ij} & \text{if } j \text{ is in } \mathcal{G}_\nu^c \\ -\infty & \text{otherwise,} \end{cases} \qquad (R_\nu)_{ij} = \begin{cases} (U_\nu)_{ij} & \text{if } i \text{ is in } \mathcal{G}_\nu^c \\ -\infty & \text{otherwise,} \end{cases}
$$

$$
(S_\nu)_{ij} = \begin{cases} \lambda^- \otimes F_{ij} & \text{if } (i,j) \in \mathcal{G}_\nu^c \\ -\infty & \text{otherwise.} \end{cases} \tag{4}
$$

Define also matrices $B_\nu[F]$ and $B[F]$ by

$$
(B_\nu[F])_{ij} = \begin{cases} -\infty, & \text{if } i \in \mathcal{G}_\nu^c \text{ or } j \in \mathcal{G}_\nu^c, \\ F_{ij}, & \text{otherwise,} \end{cases} \qquad (B[F])_{ij} = \begin{cases} -\infty, & \text{if } i \in \mathcal{G}^c(F) \text{ or } j \in \mathcal{G}^c(F), \\ F_{ij}, & \text{otherwise.} \end{cases} \tag{5}
$$

Denote by $t(\operatorname{rem}\sigma)$ the remainder of t modulo σ (i.e., $r \in \{0,\ldots,\sigma-1\}$) such that $t = k\sigma + r$ for some k. Denote $C_\nu S_\nu^k R_\nu[F] = C_\nu \otimes S_\nu^k \otimes R_\nu$ and $C_\nu S_\nu^k[F] = C_\nu \otimes S_\nu^{\otimes k}$ for more brevity and to indicate the matrix (F) from which C_ν, S_ν and R_ν are defined.

The following claims can be derived from certain results of [15], see Appendix.

Proposition 2.3 (Coro. of [15], Theorem 4.1 and Corollary 4.3). *Let $F \in \mathbb{R}_{\max}^{d\times d}$ with $\lambda = \lambda(F) \neq -\infty$ and suppose that $\mathcal{G}^c(F)$ has components $\mathcal{G}_1^c, \ldots, \mathcal{G}_l^c$ and σ_ν for $1 \leq \nu \leq l$ are their cyclicities. Then for any $\nu \in \{1,\ldots,l\}$*

$$
F^{\otimes t} = \lambda^{\otimes t} \otimes C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \oplus (B_\nu[F])^{\otimes t}, \qquad \forall t \geq (d-1)^2 + 1. \tag{6}
$$

Proposition 2.4. *Under the conditions of Proposition 2.3, we also have*

$$
F^{\otimes t} = \lambda^{\otimes t} \otimes \left(\bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \right) \oplus (B[F])^{\otimes t} \qquad \forall t \geq (d-1)^2 + 1, \tag{7}
$$

Furthermore, if F is irreducible then there exists $T(F)$ such that

$$
F^{\otimes t} = \lambda^{\otimes t} \otimes \left(\bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\operatorname{rem}\sigma_\nu)} R_\nu[F] \right), \qquad \forall t \geq T(F). \tag{8}
$$

6

Equation (8) implies that after $T(F)$ the sequence of powers $(\lambda(F)^- \otimes F)^{\otimes t}$ is periodic, with period equal to the least common multiple of σ_ν for $\nu = 1, \ldots, l$, a well-known fact established by Cohen et. al. [7, 8].

It is not too difficult to compute the CSR terms. In particular, one needs to find λ, for which one can exploit Karp's method with complexity $O(d^3)$ [1, 4] or the policy iteration algorithm of Cochet-Terrasson et al. [6, 11], which works in general case and is very efficient in practice. The usual technique for powering up a matrix is to use repeated squaring, and this yields the addition of an $O(d^3 \log d)$ term (observing that $\sigma_\nu \leq d$). Further, the metric matrix can be computed by shortest path algorithms such as Floyd-Warshall [1, 4, 11]. The complexity of finding the components of $\mathcal{G}^c(F)$ does not exceed $O(d^3)$ [1]. We also need to know the cyclicity of the components, which can be computed in $O(d^2)$ by Balcer and Veinott's digraph condensation [2]. However, below we are going to show how some of these problems can be avoided, as instead of the whole critical component we can use one critical cycle from that component, following an idea of Merlet et al. [15, Theorem 6.1]. The resulting complexity of computing CSR remains of the order $O(d^3 \log d)$, but we avoid the need for identifying the whole components of $\mathcal{G}^c(V)$ and the use of Balcer-Veinott digraph condensation.

Let us first give yet another definition of a CSR term, as below. Suppose that Z is a critical cycle, with length $l(Z)$. Denote $U_Z = ((\lambda^- \otimes F)^{\otimes l(Z)})^+$. Then, let matrices C_Z, R_Z and S_Z and $B_Z[F]$ be defined by:

$$
(C_Z)_{ij} = \begin{cases} (U_Z)_{ij} & \text{if } j \text{ is in } Z \\ -\infty & \text{otherwise,} \end{cases} \qquad (R_Z)_{ij} = \begin{cases} (U_Z)_{ij} & \text{if } i \text{ is in } Z \\ -\infty & \text{otherwise,} \end{cases}
$$
$$
(S_Z)_{ij} = \begin{cases} \lambda^- \otimes F_{ij} & \text{if } (i,j) \in Z \\ -\infty & \text{otherwise,} \end{cases}
$$

(9)

Proof of the following statement is deferred to Appendix. However, it can be also seen as a corollary of [15, Theorem 6.1].

Proposition 2.5 (Coro. of [15], Theorem 6.1)**.** *Let Z be a cycle belonging to a component $\mathcal{G}^c_\nu$ of*

the critical graph of a square matrix F with $\lambda(F) \neq -\infty$. Then $C_\nu S_\nu^t R_\nu[F] = C_Z S_Z^t R_Z[F]$ for any natural t, and therefore:

$$F^{\otimes t} = \lambda^{\otimes t} \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F] \oplus (B_\nu[F])^{\otimes t}, \qquad \forall t \geq (d-1)^2 + 1. \tag{10}$$

for any critical cycle Z and component $\mathcal{G}_\nu^c$ in which it lies.

Here, equation (10) follows from (6) and the first part of the claim since σ_ν divides $l(Z)$ and $\{C_\nu S_\nu^t R_\nu[F]\}_{t \geq 0}$ is periodic with period σ_ν by [20, Prop. 3.2].

The next immediate corollary of above results will be used in practice, for solving the tropical discrete logarithm problem. It is closely related to an observation by Nachtigall [17] that critical rows and columns of matrix powers become periodic after $O(d^2)$, and the further more refined results of Merlet et al. [14].

Corollary 2.6. *Let $V \in \mathbb{R}_{\max}^{m \times d}$ and $F \in \mathbb{R}_{\max}^{d \times d}$ with $\lambda = \lambda(F) \neq -\infty$, and let Z be a cycle of $\mathcal{G}^c(F)$. Then for any $t \geq (d-1)^2 + 1$, the columns of $V \otimes F^{\otimes t}$ with indices in Z are equal to the corresponding columns in $\lambda^{\otimes t} \otimes V \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F]$.*

Proof. Equation (10) implies that the columns of $F^{\otimes t}$ with indices in Z are equal to the corresponding columns of $\lambda^{\otimes t} \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F]$. The claim now follows as we premultiply the columns of $F^{\otimes t}$ and $\lambda^{\otimes t} \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))} R_Z[F]$ with indices in Z by V. $\qquad \square$

Corollary 2.6 suggests the following algorithm for finding t such that $A = V \otimes F^{\otimes t}$, that is, for solving Problem 2.1. In this algorithm, E will denote a matrix of appropriate dimensions consisting of all zeros.

Algorithm 2.7 (Finding the tropical discrete logarithm)**.**
 Input: $A, V \in \mathbb{R}_{\max}^{m \times d}$, $F \in \mathbb{R}_{\max}^{d \times d}$.
Output: t such that $A = V \otimes F^{\otimes t}$.

   0. Find $\lambda = \lambda(F)$ and a critical cycle Z. Compute C_Z and S_Z according to (9).

   1. For $t = 0, 1, \ldots, (d-1)^2$ check if $A = V \otimes F^{\otimes t}$ and return t if it is found;

8

2. For $k = 0, \ldots, l-1$, where $l = l(Z)$, check if $A_{\cdot i} - V \otimes (C_Z S_Z^k R_Z[F])_{\cdot i} = \mu + E_{\cdot i}$ for all $i \in Z$ and some μ such that $t = \mu / \lambda(F)$ is a natural number and return the first such t that is found.

Proposition 2.8. *Part 0., part 1. and part 2. of Algorithm 2.7 require at most $O(d^3 \log l(Z))$, $O(md^4)$ and $O(ml(Z)(d + l(Z)))$ operations, respectively.*

Proof. Complexity bounds:

0. Finding $\lambda(F)$ and a critical cycle Z needs at most $O(d^3)$ operations (Karp's algorithm and the methods described in [11, 18]. After this, C_Z can be found in $O(d^3 \log l(Z))$ operations (dominated by the repeated matrix squaring).

1. At step 1, the outer loop has size $(d-1)^2$, and the computationally dominant operation is that of repeated multiplication of an $m \times d$ matrix by an $d \times d$ matrix F, taking md^2 operations. Thus, the overall complexity is $O(md^4)$.

2. At step 2, the computational complexity can be decreased using the observation that the columns of $C_Z S_Z^{t(\mathrm{rem}\, l(Z))} R_Z[F]$ with indices in Z are equal to the corresponding columns $C_Z S_Z^{t(\mathrm{rem}\, l(Z))}[F]$ by [20, Corollary 3.7], and therefore we actually check if $A_{\cdot i} - (V \otimes C_Z \otimes S_Z^{\otimes k})_{\cdot i} = \mu + E_{\cdot i}$ for all $i \in Z$ and some μ such that $t = \mu / \lambda(F)$ is a natural number (the same for all i). The outer loop has size $l(Z)$ and we precompute the columns of $V \otimes C_Z$ with indices in Z, which gives $O(mdl(Z))$ operations. The computationally dominant operation at each step is that of multiplying an $m \times l$ matrix by S_Z (done by a permutation of and adding some scalar values to the columns of that matrix), which is $O(ml(Z))$. Overall it gives $O(ml(Z)(d + l(Z)))$.

$\square$

Remark 2.9. Using [20, Corollary 3.7], $C_Z S_Z^{t\,\mathrm{rem}(l(Z))} R_Z[F]$ can be replaced with $C_Z S_Z^{t\,\mathrm{rem}(l(Z))}[F]$ in Corollary 2.6 and Algorithm 2.7.

Remark 2.10. We can also suggest a lighter but less reliable version of Algorithm 2.7 where $A_{\cdot i} - (V \otimes C_Z S_Z^{t(\mathrm{rem}\, l(Z))}[F])_{\cdot i} = \mu + E_{\cdot i}$ is checked just for one $i \in Z$. Then the complexity of Step 2. drops further.

9

Theorem 2.11. *Suppose that matrices $V \in \mathbb{R}_{\max}^{m \times d}$, $F \in \mathbb{R}_{\max}^{d \times d}$ and critical cycle Z are such that any of the following equivalent conditions holds:*

1. *For any $t_1 \neq t_2$, we have $V \otimes \lambda^{\otimes t_1} \otimes C_Z S_Z^{t_1 \operatorname{rem} l(Z)}[F] \neq V \otimes \lambda^{\otimes t_2} \otimes C_Z S_Z^{t_2 \operatorname{rem} l(Z)}[F]$,*

2. *For no $t_1, t_2 \geq (d-1)^2 + 1$, $t_1 \neq t_2$ we have that all columns of $V \otimes F^{\otimes t_1}$ with indices in Z are equal to the corresponding columns of $V \otimes F^{\otimes t_2}$.*

Then, for any $A = V \otimes F^{\otimes t}$ with $t \geq (d-1)^2 + 1$, part 2. of Algorithm 2.7 finds this t and it is unique.

Proof. The equivalence between 1. and 2. follows by Corollary 2.6 and Remark 2.9, which also imply that if $t \geq (d-1)^2 + 1$, then $A_{\cdot i} = t \times \lambda + V \otimes (C_Z S_Z^{t(\operatorname{rem} l(Z)}[F])_{\cdot i}$ and hence for $k = t \operatorname{rem}(l(Z)$ we have $A_{\cdot i} - V \otimes (C_Z S_Z^{k}[F])_{\cdot i} = \mu + E_{\cdot i}$ for all $i \in Z$, where μ is such that $t = \mu / \lambda(F)$ is natural. Furthermore, if this holds for $t \geq (d-1)^2 + 1$, then we have $A_{\cdot i} = \lambda^{\otimes t} \otimes V \otimes (C_Z S_Z^{t(\operatorname{rem} l(Z))}[F])_{\cdot i}$ for all $i \in Z$, and hence $A_{\cdot i} = (V \otimes F^{\otimes t})_{\cdot i}$ for all such i by Proposition 2.5 and (6). Condition 2. of the theorem then implies that such t is unique and hence correct. $\qquad\square$

Remark 2.12. The algorithm cannot work when $\lambda(F) = 0$. In this case, obviously, the sequence of columns $\{(V \otimes F^{\otimes t})_{\cdot i}\}_{t > (d-1)^2}$ is periodic for any $i \in Z$ with the same period, and there are infinitely many t such that $A_{\cdot i} = (V \otimes F^{\otimes t})_{\cdot i}$, if one such t exists. However, if F is irreducible with $\lambda(F) = 0$, then the tropical discrete logarithm problem is not well-defined, either.

The following corollary gives a simplification of above conditions in an important special case.

Corollary 2.13. *Suppose that V has finite entries, F is irreducible, $\mathcal{G}^c(F)$ is strongly connected and $\lambda(F) \neq 0$. Then, if $A = V \otimes F^{\otimes t}$ then Algorithm 2.7 finds this t.*

Proof. Lemma 2.2 shows that the tropical discrete logarithm is well-defined in this case.

For $t \leq (d-1)^2$, Algorithm checks the equality $A = V \otimes F^{\otimes t}$ in a straightforward way, and there is nothing to prove. Assume that $t \geq (d-1)^2 + 1$. For the validity of Algorithm, it suffices to show that the condition of this corollary implies the condition of Theorem 2.11. For this, suppose that by the contrary that condition 1. of Theorem 2.11 is violated. Then we have

$V \otimes \lambda^{\otimes t_1} \otimes C_Z S_Z^{t_1 \operatorname{rem} l(Z)}[F] = V \otimes \lambda^{\otimes t_2} \otimes C_Z S_Z^{t_2 \operatorname{rem} l(Z)}[F]$ for some $t_1 \neq t_2$. Postmultiplying it by R_Z and multiplying it by $\lambda^{\otimes k l(Z)}$ for big enough k (if necessary), we obtain

$$V \otimes \lambda^{\otimes t_1} \otimes C_Z S_Z^{t_1 (\operatorname{rem} l(Z))} R_Z[F] = V \otimes \lambda^{\otimes t_2} \otimes C_Z S_Z^{t_2 (\operatorname{rem} l(Z))} R_Z[F], \tag{11}$$

for some $t_1 \neq t_2$, $t_1, t_2 \geq T(F)$. Now let σ be the cyclicity of the critical graph. As the critical graph is strongly connected, there is a unique CSR term (with C, S and R defined using $\mathcal{G}_1^c = \mathcal{G}^c(F)$). Using Proposition 2.5 and that $l(Z)$ is a multiple of σ we rewrite (11) as

$$V \otimes \lambda^{\otimes t_1} \otimes CS^{t_1 (\operatorname{rem} \sigma)} R[F] = V \otimes \lambda^{\otimes t_2} \otimes CS^{t_2 (\operatorname{rem} \sigma)} R[F],$$

for some $t_1 \neq t_2$, $t_1, t_2 \geq T(F)$. Now recall that we have $F^{\otimes t} = \lambda^{\otimes t} \otimes CS^{t (\operatorname{rem} \sigma)} R[F]$ for all $t \geq T(F)$ by Proposition 2.4, hence $V \otimes F^{\otimes t_1} = V \otimes F^{\otimes t_2}$ for some $t_1, t_2 \geq T(F)$ and $t_1 \neq t_2$, violating the result of Lemma 2.2. So the condition of this theorem implies any of the equivalent conditions of Theorem 2.11, and the claim follows. $\qquad \square$

3 Semidirect products and powers

Grigoriev and Shpilrain [10] consider the following *semidirect product* of the pairs of matrices over tropical semiring

$$(M, G)(A, H) = ((M \circ H) \oplus A, G \circ H) \tag{12}$$

We will consider one of the protocols in [10], where $\circ$ is defined as the *adjoint product:*

$$A \circ B = A \oplus B \oplus A \otimes B, \tag{13}$$

defined for any square matrices A and B of the same size. It has the following properties:

- $(A \circ B) \circ C = A \circ (B \circ C)$ (associativity),

- $A \circ (B \oplus C) = A \circ B \oplus A \circ C$ and $(B \oplus C) \circ A = B \circ C \oplus B \circ A$ (distributivity).

Adjoint product (16) can be used to define *adjoint powers* inductively: $A^{\circ(k+1)} = A^{\circ k} \circ A$ for all k. Moreover, the associativity implies that for any nonzero numbers $m_1, \ldots, m_s \in \mathbb{N}$ such that $m_1 + \ldots + m_s = k$ we have

$$A^{\circ k} = A^{\circ m_1} \circ A^{\circ m_2} \circ \ldots \circ A^{\circ m_s}. \tag{14}$$

Thus the adjoint powers $A^{\circ n} = \underbrace{A \circ \ldots \circ A}_{n}$ are well-defined and can be quickly computed using (14). Alternatively, the following identity for them can be offered:

$$A^{\circ n} = A \oplus A^{\otimes 2} \oplus \ldots \oplus A^{\otimes n}. \tag{15}$$

Indeed, $A^{\circ 2} = A \oplus A^{\otimes 2}$ is obvious, and for general n we can use a simple induction:

$$A^{\circ n} = A^{\circ(n-1)} \circ A = A \oplus A^{\circ(n-1)} \oplus (A^{\circ(n-1)} \otimes A)$$
$$= A \oplus (A \oplus A^{\otimes 2} \oplus \ldots \oplus A^{\otimes(n-1)}) \oplus (A^{\otimes 2} \oplus \ldots \oplus A^{\otimes n})$$
$$= A \oplus A^{\otimes 2} \oplus \ldots \oplus A^{\otimes n}.$$

Using (15) we also observe the following:

Proposition 3.1. *Let* $A \in \mathbb{R}_{\max}^{d \times d}$ *have* $\lambda(A) \leq 0$ *and* $n \geq d$. *Then* $A^{\circ n} = A^+$.

Here A^+ is the *metric matrix* of A defined in (2).

With $\circ$ being the adjoint multiplication, the semidirect product of (M, G) and (A, H) given by (12) becomes

$$(M, G)(A, H) = (M \oplus A \oplus H \oplus M \otimes H, G \otimes H \oplus G \oplus H). \tag{16}$$

The semidirect product is associative: we have

$$[(M, G) \cdot (A, H)] \cdot (B, J) = (M, G) \cdot [(A, H) \cdot (B, J)] \tag{17}$$

For the proof of this property, see Appendix.

Semidirect product (16) can be used to define semidirect powers of matrix pairs inductively:

12

$(M, H)^{k+1} = (M, H)^k \cdot (M, H)$ for all k. Moreover, associativity (17) implies that for any nonzero numbers $m_1, \ldots, m_s \in \mathbb{N}$ such that $m_1 + \ldots + m_s = k$ we have

$$(M, H)^k = (M, H)^{m_1}(M, H)^{m_2} \ldots (M, H)^{m_s}. \tag{18}$$

This property assures that the semidirect powers $(M, H)^k = \underbrace{(M, H) \cdot \ldots \cdot (M, H)}_{k}$ are well-defined. We now express the semidirect powers in terms of the tropical matrix powers.

Proposition 3.2. *Let $M, H \in \mathbb{R}_{\max}^{d \times d}$. Then*

$$(M, H)^k = ((M \otimes \bigoplus_{i=0}^{k-1} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{k-2} H^{\otimes i}), H^{\circ k})$$

for all $k \geq 2$.

Proof. We first consider $k = 2$ to check the base of induction. We obtain:

$$(M, H)(M, H) = (M \oplus H \oplus M \oplus M \otimes H, \ H^{\circ 2}) = (M \otimes (I \oplus H) \oplus H, \ H^{\circ 2}).$$

We now assume that the statement holds for $k = t$ and prove it for $k = t + 1$. Indeed:

$$(M, H)^{t+1} = (M, H)^t \cdot (M, H) = ((M \otimes \bigoplus_{i=0}^{t-1} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{t-2} H^{\otimes i}), H^{\circ t}) \cdot (M, H)$$

$$= ((M \otimes \bigoplus_{i=0}^{t-1} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{t-2} H^{\otimes i}) \oplus M \oplus H \oplus (M \otimes \bigoplus_{i=1}^{t} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=1}^{t-1} H^{\otimes i}), H^{\circ(t+1)})$$

$$= ((M \otimes \bigoplus_{i=0}^{t} H^{\otimes i}) \oplus (H \otimes \bigoplus_{i=0}^{t-1} H^{\otimes i}), H^{\circ(t+1)}).$$

The induction is complete. $\qquad\square$

Note that we can also use that $\bigoplus_{i=0}^{k} H^{\otimes i} = (I \oplus H)^{\otimes k}$ for any k, and then the result of the previous proposition can be reformulated as follows:

$$(M, H)^k = (M \otimes (I \oplus H)^{\otimes(k-1)} \oplus H \otimes (I \oplus H)^{\otimes(k-2)}, H^{\circ k})$$

$$= ((M \otimes (I \oplus H) \oplus H) \otimes (I \oplus H)^{\otimes(k-2)}, H^{\circ k}). \tag{19}$$

4 The protocol and its cryptanalysis

In this section we will use the following order relations between matrices $A, B \in \mathbb{R}_{\max}^{m \times n}$ of same dimensions. We write:

- $A \leq B$ (resp. $A \geq B$), if $a_{ij} \leq b_{ij}$ (resp. $a_{ij} \geq b_{ij}$) for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots n\}$;

- $A < B$, if $A \leq B$ and $A \neq B$;

- $A > B$, if $A \geq B$ and $A \neq B$.

4.1 The protocol under question

Based on the property (18), Grigoriev and Shpilrain [10] suggested the following protocol using tropical semidirect powers:

Protocol 4.1 (Grigoriev and Shpilrain [10])**.**

1. Alice and Bob agree on public matrices $M, H \in \mathbb{Z}_{\max}^{d \times d}$ (that is, $d \times d$ matrices M and H whose entries are integer numbers or $-\infty$);

2. Alice selects a private positive integer m and Bob selects a private positive integer n;

3. Alice computes $(M, H)^m = (A, H^{\circ m})$ and sends A to Bob;

4. Bob computes $(M, H)^n = (B, H^{\circ n})$ and sends B to Alice;

5. Alice computes $K_a = A \oplus B \oplus H^{\circ m} \oplus (B \otimes H^{\circ m})$;

6. Bob computes $K_b = A \oplus B \oplus H^{\circ n} \oplus (A \otimes H^{\circ n})$.

Property (18) implies that $K_a = K_b$, since both of them are the first component of $(M, H)^{m+n}$. For the protocol recalled above, we immediately obtain using (19)

$$
\begin{aligned}
A &= \left(M \otimes \bigoplus_{i=0}^{m-1} H^{\otimes i} \right) \oplus \left(H \otimes \bigoplus_{i=0}^{m-2} H^{\otimes i} \right) = (M \otimes (I \oplus H) \oplus H) \otimes (I \oplus H)^{\otimes(m-2)}, \\
B &= \left(M \otimes \bigoplus_{i=0}^{n-1} H^{\otimes i} \right) \oplus \left(H \otimes \bigoplus_{i=0}^{n-2} H^{\otimes i} \right) = (M \otimes (I \oplus H) \oplus H) \otimes (I \oplus H)^{\otimes(n-2)},
\end{aligned}
\tag{20}
$$

14

for the messages exchanged between Alice and Bob ($m \geq 2$ and $n \geq 2$), using Proposition 3.2.

We have the following immediate corollary of these expressions.

Corollary 4.2. *We have the following implications:*

(i) $m > n \Rightarrow A \geq B$, $n > m \Rightarrow B \geq A$;

(ii) $A > B \Rightarrow m > n$, $B > A \Rightarrow n > m$.

In the next sections we describe the attack on the Grigoriev-Shpilrain protocol, which depends on the sign of $\lambda(H)$.

Let us denote

$$V = M \otimes (I \oplus H) \oplus H.$$

The messages sent by Alice and Bob can be expressed as

$$A = V \otimes (I \oplus H)^{\otimes(m-2)}, \quad B = V \otimes (I \oplus H)^{\otimes(n-2)},$$

as it follows from (20). Hence, under the assumptions of Theorem 2.11 or Corollary 2.13, we can apply Algorithm 2.7 to A, B, V and $F = I \oplus H$ to find $m - 2$ and $n - 2$ (unless $m = 1$ or $n = 1$). Notice, however, that this algorithm cannot be applied when $\lambda(H) \leq 0$, and this motivates a separate treatment of this case.

4.2 Case $\lambda(H) \leq 0$

Recall that if $\lambda(H) \leq 0$ for $H \in \mathbb{R}_{\max}^{d \times d}$, then we have

$$H^* = I \oplus H \oplus \ldots H^{\otimes(d-1)} \tag{21}$$

We then immediately obtain the following corollary of (20).

Corollary 4.3. *Let $M, H \in \mathbb{R}_{\max}^{d \times d}$ and $\lambda(H) \leq 0$. If $m \geq d+1$ then $A = (M \oplus H) \otimes H^*$, and if $n \geq d+1$ then $B = (M \oplus H) \otimes H^*$.*

Using this corollary and (15), if $m \geq d+1$ or if $A = (M \oplus H) \otimes H^*$ we also obtain

$$A \otimes H^{\circ n} = (M \oplus H) \otimes (H^* \otimes H^{\circ n})$$

$$= (M \oplus H) \otimes \left(H^* \otimes \bigoplus_{i=1}^{n} H^{\otimes i} \right) \leq (M \oplus H) \otimes H^* = A,$$

$$H^{\circ n} = \bigoplus_{i=1}^{n} H^{\otimes i} \leq A,$$

and also $B \leq A$, using (20). If $n \geq d+1$ or if $B = (M \oplus H) \otimes H^*$ then we have

$$B \otimes H^{\circ m} = (M \oplus H) \otimes (H^* \otimes H^{\circ m})$$

$$= (M \oplus H) \otimes \left(H^* \otimes \bigoplus_{i=1}^{m} H^{\otimes i} \right) \leq (M \oplus H) \otimes H^* = B,$$

$$H^{\circ m} = \bigoplus_{i=1}^{m} H^{\otimes i} \leq B$$

and $A \leq B$. Therefore, we have

$$K_a = B \oplus A \oplus H^{\circ m} \oplus B \otimes H^{\circ m} = A \oplus B = B, \quad \text{if } n \geq d+1$$

$$K_b = A \oplus B \oplus H^{\circ n} \oplus A \otimes H^{\circ n} = A \oplus B = A, \quad \text{if } m \geq d+1.$$

Thus we arrive at the following result.

Proposition 4.4. *Let* $M, H \in \mathbb{R}_{\max}^{d \times d}$ *and* $\lambda(H) \leq 0$ *and let* $m \geq d+1$, $n \geq d+1$, $A = (M \oplus H) \otimes H^*$ *or* $B = (M \oplus H) \otimes H^*$. *Then*

$$K_a = K_b = A \oplus B = (M \oplus H) \otimes H^*.$$

Thus in this case the key can be computed simply as $A \oplus B$.

4.3 Computing the key with known m and n

If we have m and n then the key can be obviously computed as

$$K_a = K_b = A \oplus B \oplus H^{\circ m} \oplus (B \otimes H^{\circ m}) = A \oplus B \oplus H^{\circ n} \oplus (A \otimes H^{\circ n}), \tag{22}$$

where $H^{\circ m}$ and $H^{\circ n}$ can be computed as adjoint powers, using (14) or (15).

Let us also consider how to simplify expression (22). Assume first that $m > n$. Then $A \geq B$ and $A \geq H^{\circ n}$, since any power $H^{\otimes i}$ for $1 \leq i \leq n$ appears as one of the terms in

$$A = (M \otimes (I \oplus H) \oplus H)(I \oplus H \oplus \ldots \oplus H^{\otimes(m-2)}),$$

when we multiply it out. Then the key simplifies to

$$K_a = K_b = A \otimes (I \oplus H^{\circ n}) = A \otimes (I \oplus H \oplus \ldots \oplus H^{\otimes n}) = A \otimes (I \oplus H)^{\otimes n}. \tag{23}$$

In the case $n > m$ we similarly obtain

$$K_a = K_b = B \otimes (I \oplus H \oplus \ldots \oplus H^{\otimes m}) = B \otimes (I \oplus H)^{\otimes m}. \tag{24}$$

In the case $m = n$ we have $B = A$ and therefore

$$K_a = K_b = A \otimes (I \oplus H)^{\otimes n} \oplus H \otimes (I \oplus H)^{\otimes(n-1)}. \tag{25}$$

4.4 Attacking the protocol

Let us now give a more formal description of the attack on Protocol 4.1, in the form of an algorithm.

Algorithm 4.5 (Attacking Protocol 4.1)**.**

 Input: public matrices $M, H \in \mathbb{Z}_{\max}^{d \times d}$ and messages $A, B \in \mathbb{Z}_{\max}^{d \times d}$ of Alice and Bob.

Output: common key $K_a = K_b$.

   0. Compute $\lambda(H)$, $F = I \oplus H$ and $V = (M \otimes (I \oplus H) \oplus H)$.

1. If $\lambda(H) \leq 0$ then check if $A = (M \oplus H) \otimes H^*$ or $B = (M \oplus H) \otimes H^*$. If any of these two conditions is true then return $K = (M \oplus H) \otimes H^*$.

   If none of these conditions are true, check if $A = M$ or $B = M$ or find $l_1, l_2 = 0, \ldots d-2$ such that $A = V \otimes F^{\otimes l_1}$ and $B = V \otimes F^{l_2}$. Then set $m = l_1 + 2$ or $m = 1$ if $A = M$, and $n = l_2 + 2$ or $n = 1$ if $B = M$, and go to 3.

2. If $\lambda(H) > 0$ then check $A = M$ or $B = M$ or find l_1 and l_2 satisfying $A = V \otimes F^{\otimes l_1}$ and $B = V \otimes F^{\otimes l_2}$ using Algorithm 2.7. Then set $m = l_1 + 2$ or $m = 1$ if $A = M$, and $n = l_2 + 2$ or $n = 1$ if $B = M$, and go to 3.

3. Compute the key using (23), (24) or (25).

The increasing property of $F = I \oplus H$ means that the sequence of matrices $\{M,\ V,\ V \otimes F,\ V \otimes F^2 \ldots\}$ is non-decreasing, and it either stabilises so that $V \otimes F^{\otimes t} = (M \oplus H) \otimes H^*$ for $t \geq T$ for some $T \leq d - 1$, or it grows in such a way that

$$M < V < V \otimes F^{\otimes t_1} < V \otimes F^{\otimes t_2} < \ldots$$

In particular, we have $V \otimes F^{\otimes t_1} \neq V \otimes F^{\otimes t_2}$ for $t_1 \neq t_2$, unless both are equal to $(M \oplus H) \otimes H^*$. These observations, together with the validity of Algorithm 2.7, imply the following claim, where by $\mathcal{E}$ we define a matrix of arbitrary dimensions with all entries equal to $-\infty$.

Proposition 4.6. *Suppose that F is irreducible with strongly connected $\mathcal{G}^c(F)$, and that $V = (M \otimes (I \oplus H) \oplus H) \neq \mathcal{E}$. Then the attacker can compute the key using Algorithm 4.5.*

Let us analyse how many operations the algorithm requires.

0. Computation of $\lambda(H)$ and V requires no more than $O(d^3)$ operations.

1. Checking if $A = (M \oplus H) \otimes H^*$ or $B = (M \oplus H) \otimes H^*$ requires $O(d^3)$ operations. Straightforward checking for powers less than $d - 1$ requires $O(d^4)$ operations.

2. Here we apply Algorithm 2.7, whose complexity is analysed in Proposition 2.8. However, see also the discussion in Subsection 5.3.

18

3. Computation of the key (unless it has been computed at step 1) requires no more than $O(d^3 \log \min(m, n))$. This is done using repeated tropical matrix squaring.

5 Examples, numerical experiments and discussion

5.1 Toy examples

We first give a couple of toy examples to demonstrate how the attack on the protocol works in the cases $\lambda(H) \leq 0$ and $\lambda(H) > 0$.

Example 5.1 $((\lambda(H) \leq 0))$. Let

$$
M = \begin{pmatrix} 8 & 7 & 2 \\ 10 & 3 & 6 \\ -10 & -1 & 3 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & -3 & -5 \\ -1 & -2 & 2 \\ 1 & -3 & -4 \end{pmatrix}.
$$

Bob and Alice pick two random integer numbers $m = 5$ and $n = 8$ respectively. Alice and Bob compute

$$
A = B = \begin{pmatrix} 10 & 7 & 9 \\ 10 & 7 & 9 \\ 4 & 1 & 3 \end{pmatrix} = K_a = K_b.
$$

Since $\lambda(H) = 0$, we cannot use tropical discrete logarithm method to find m and n. However, Eve can check that $A = B = (M \oplus H) \otimes H^*$, hence she concludes that $K_a = K_b = (M \oplus H) \otimes H^*$.

Example 5.2 $((\lambda(H) > 0))$. Alice and Bob agree on public matrices

$$
M = \begin{pmatrix} -75 & -45 & -69 & 60 \\ 83 & 52 & 9 & -72 \\ 27 & 92 & 92 & -16 \\ 87 & 93 & -3 & 84 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 7 & 2 & 5 \\ -1 & -2 & 2 & 4 \\ 3 & 4 & 2 & 2 \\ -5 & -10 & 10 & 0 \end{pmatrix}.
$$

Then they follow the protocol as follows

- Alice and Bob pick two random integer numbers $m = 15$ and $n = 16$ respectively.

- Alice computes $(M, H)^m = (A, H^{\circ m})$ and Bob computes $(M, H)^n = (B, H^{\circ n})$. They exchange the following messages:

$$
A = \begin{pmatrix} 145 & 146 & 148 & 144 \\ 176 & 177 & 179 & 175 \\ 175 & 176 & 178 & 174 \\ 176 & 177 & 179 & 175 \end{pmatrix}, \quad B = \begin{pmatrix} 151 & 152 & 154 & 150 \\ 182 & 183 & 185 & 181 \\ 181 & 182 & 184 & 180 \\ 182 & 183 & 185 & 181 \end{pmatrix}.
$$

- Alice computes $K_a = A \oplus B \oplus H^{\circ m} \oplus (B \otimes H^{\circ m})$ and $K_b = B \oplus A \oplus H^{\circ n} \oplus (A \otimes H^{\circ n})$. They thus obtain the common secret key:

$$
K_a = K_b = \begin{pmatrix} 241 & 242 & 244 & 240 \\ 272 & 273 & 275 & 271 \\ 271 & 272 & 274 & 270 \\ 272 & 273 & 275 & 271 \end{pmatrix}.
$$

Attacking the protocol

Eve as an attacker only knows public matrices M and H and public keys A and B. To attack the protocol Eve needs to find m and n and compute K_a or K_b. Using Algorithm 5.3, Eve obtains Alice's private key by the following:

1. Eve computes $\lambda(H) = 6$ and

$$
F = I \oplus H = \begin{pmatrix} 1 & 7 & 2 & 5 \\ -1 & 0 & 2 & 4 \\ 3 & 4 & 2 & 2 \\ -5 & -10 & 10 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 55 & 50 & 70 & 60 \\ 98 & 99 & 97 & 97 \\ 95 & 96 & 94 & 96 \\ 92 & 93 & 95 & 97 \end{pmatrix}.
$$

2. Since $\lambda(H) > 0$, Eve needs to find m_a satisfying $A = V \otimes F^{\otimes (m_a - 2)}$. For this Eve finds a

critical cycle $Z = (1\ 2\ 4\ 3)$ and computes

$$
C_Z = R_Z = \begin{pmatrix} 0 & 1 & 3 & -1 \\ -5 & 0 & 2 & -2 \\ -1 & -2 & 0 & -4 \\ 1 & 2 & 4 & 0 \end{pmatrix}, \quad
S_Z = \begin{pmatrix} -\infty & 1 & -\infty & -\infty \\ -\infty & -\infty & -\infty & -2 \\ -3 & -\infty & -\infty & -\infty \\ -\infty & -\infty & 4 & -\infty \end{pmatrix}.
$$

3. The dimension is $d = 4$, hence for $t = 0, \ldots, (4-1)^2 = 9$, Eve first tries to find t such that $A = V \otimes F^{\otimes t}$. Here we cannot find t satisfying $A = V \otimes F^{\otimes t}$ for these low exponents.

4. Now Eve uses the CSR method. The length of critical cycle is $l = 4$, but it turns out that

$$
C_Z S_Z^k R_Z[F] = \begin{pmatrix} 0 & 1 & 3 & -1 \\ -1 & 0 & 2 & -2 \\ -3 & -2 & 0 & -4 \\ 1 & 2 & 4 & 0 \end{pmatrix} \quad \text{for all } k.
$$

For $k = 0$ Eve finds that $A = V \otimes (C_Z R_Z[F]) = \mu + E$ with $\mu = 78$. Eve then finds that $m_a = \mu/\lambda(F) + 2 = \frac{78}{6} + 2 = 15$.

5. Eve computes $K_a = B \otimes (I \otimes H)^{\otimes 15} = \begin{pmatrix} 241 & 242 & 244 & 240 \\ 272 & 273 & 275 & 271 \\ 271 & 272 & 274 & 270 \\ 272 & 273 & 275 & 271 \end{pmatrix}.$

5.2   Numerical experiments

In this section we will describe the numerical experiments which we performed with the tropical discrete logarithm and attack on [10, Protocol 1].

We first discuss how we generated matrix F, which gets powered up in the discrete logarithm problem, or matrix H for [10, Protocol 1]. If we generate matrix F by random and all of its entries are real, then it will be irreducible and generically we will have only one critical cycle.

This case is the same as the one described in Corollary 2.13, in which our solution of the tropical discrete logarithm problem and our attack on Protocol 4.1 ([10, Protocol 1]) are guaranteed to work. Therefore, in part of our experiments, we generate matrices F (and H) in such a way that the critical graph is guaranteed to have at least three components.

In more detail, we are doing it as follows:

(a) We determine two random integer numbers k_1 and k_2, where k_1 is approximately $\frac{1}{3}$ of the dimension of matrix d and k_2 is a random integer number between k_1 and d. Then we generate three random matrices with entries 0 and $-\infty$. Each matrix has dimension k_1, $k_2 - k_1$ and $d - k_2$ respectively. The frequency of 0 entries is approximately $\frac{1}{3}$ and we make sure that each of these matrices contains a cycle and there is $-\infty$ on the diagonal.

(b) We compose a $d \times d$ matrix with entries in $\{0, -\infty\}$, which has the three matrices generated above as as its principal submatrices. The rest of entries in this matrix are set to $-\infty$.

(c) We substitute all $-\infty$ entries in step (b) with a random negative number in the interval $[-100, -1]$ and add to the whole matrix a nonzero random number $\lambda \in [1, 100]$.

(d) We apply a diagonal similarity scaling $A \mapsto D^{-1} \otimes A \otimes D$ where D is a diagonal matrix with all diagonal entries equal to d_i for $i \in \{1, \ldots, n\}$ and all off-diagonal entries equal to $-\infty$. We write $D = \mathrm{diag}(d_1, \ldots, d_n)$ for such matrix, and the max-algebraic inverse of it can be written as $D^{-1} = \mathrm{diag}(-d_1, \ldots, -d_n)$. In our case, the diagonal entries d_i are randomly selected in the interval $[-100, 100]$.

The resulting matrix can be then used as matrix H in [10, Protocol 1], however here we also need to make sure that $\lambda(H) > 0$, otherwise we are in the very easy case, treated in Subsection 4.2. Note that this is guaranteed by taking $\lambda > 0$ at step c), as this is the maximum cycle mean of the matrix generated following (a), (b), (c) and (d).

For the tropical discrete logarithm problem as well as for the protocol, we run similar experiments using the following parameters:

- Dimension d is in the interval $[6, 500]$;

- The entries of matrix M are random integer numbers in the interval $[-100, 100]$;

- Exponents m, n used by Alice and Bob, and the secret key t in the tropical discrete logarithm are random integer numbers in the interval $[(d-1)^2 + 1, d^2]$.

We coded all our attacks in MATLAB and performed experiments using MATLAB R2019/b, also using supercomputer Bluebear system (University of Birmingham) for dimensions between 400 and 500. We run 100 experiments for each dimension d:

1. We solved the tropical discrete logarithm by Algorithm 2.7 where we skipped step (1): straightforward "catching" powers up to $(d-1)^2$. In this experiment we found 100% success rate.

2. We attacked [10, Protocol 1] using Algorithm 4.5. In this experiment we also found 100% success rate.

For the dimensions up to 100, the average computation times are given on Figure 1. We distinguish between the cases where H is randomly generated and where $F = I \oplus H$ is guaranteed to have three critical components. However, the average time that it takes is similar (being slightly less for the case of special matrices), and it does not exceed 6 seconds for dimensions up to 100 in both cases.

5.3 Discussion

To our knowledge, the first attack on [10, Protocol 1] was suggested by Rudy and Monico [19]. The attack is based on the property that the sequence $(A^{(k)})_{k \geq 1}$, where $A^{(k)}$ is defined by $(M, H)^k = (A^{(k)}, H^{\circ k})$, is nondecreasing (if viewed in max-plus algebra). This allows Eve to apply a binary search to find the secret keys of Alice and Bob. This attack is guaranteed to work and can be efficiently implemented [19]. However, its worst-case computational complexity is $O(K^2)$, where K is an upper bound on the logarithm of the secret keys of Alice and Bob.

Isaac and Kahrobaei [12] take a different approach. They find the secret keys of Alice and Bob based on the assumption that the sequence $(A^{(k)})_{k \geq 1}$ is ultimately periodic, which means
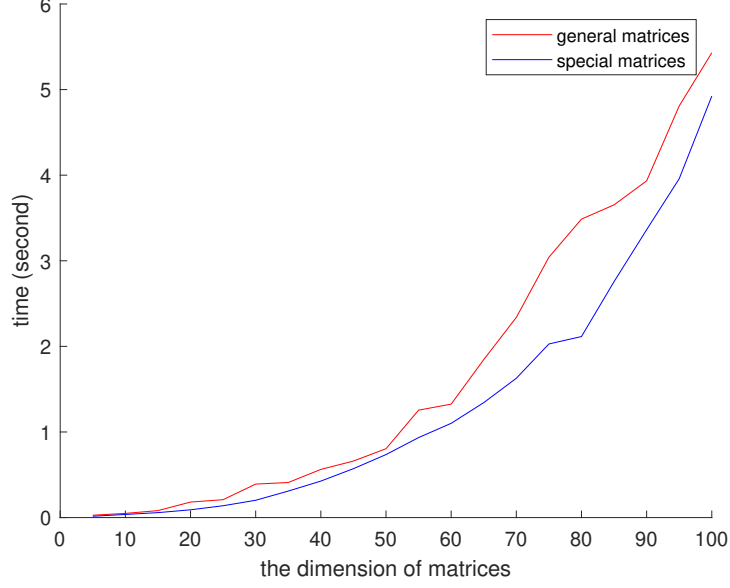
Figure 1: Time required by Algorithm 4.5 in the case where H is randomly generated ("general matrices") and in the case where $\mathcal{G}^c(F)$ is guaranteed to have at least three critical components and $\lambda(F) > 0$ ("special matrices)"

that $A_{ij}^{(k+p)} = \xi + A_{ij}^{(k)}$ for all $k \geq D$, all indices i and j , some real ξ and some D, $p \geq 1$. Not being dependent on the magnitude of the secret keys of Alice and Bob, this attack is more efficient in practice. In view of Proposition 3.2 and (19) of the present paper, the ultimate periodicity assumption holds when H is irreducible (i.e., when graph associated with H is strongly connected). However, it generally fails when Alice and Bob choose H to be reducible, in which case the attack of [12] would not apply. Another implicit assumption for the efficiency of this attack is that the defect (i.e., the periodicity transient) D is rather small. But the magnitude of D can be arbitrarily large for a sequence of tropical matrix powers, which can pose a problem when Alice and Bob are allowed choose M and H (even if with real entries only) to force a large D.

Clearly, our attack on Protocol 4.1, which is based on the ultimate periodicity of the critical columns of $\left((I \oplus H)^{\otimes k}\right)_{k \geq 1}$ (and, therefore, the same columns of $A^{(k)}$) can be applied in the general case. As in [12] and unlike the attack of [19], the computation of secret keys of Alice and Bob in our attack does not depend on the magnitude of these secret keys. Furthermore, our attack is directly based on the solution of the tropical discrete logarithm problem in the case $\lambda(H) > 0$ and is reduced to the optimal paths problem (i.e., computation of the Kleene star) for $\lambda(H) \leq 0$.

Although the statement of the tropical discrete logarithm problem is quite obvious, the authors are unaware of works in tropical algebra literature, where this problem was posed and solved. As for Algorithm 2.7, which we are suggesting, there is clearly some room for improvement. Firstly, the most inefficient part of this algorithm is the straightforward "catching powers" up to $(d-1)^2$ in part 1., and here we see the potential in using the ideas of [19] and [12]. In the case of $F = I \oplus H$, where the tropical matrix powers are nondecreasing, we can use the binary search as in [19]. Note that this decreases the complexity of Step 1 to $O((m+d)d^2(\log d)^2)$ (similar to the estimate of [19] but with $(\log d)^2$ instead of K^2). This holds for the application of Algorithm 2.7 to our attack. Secondly, as noticed in Remark 2.10, we could try to check $A_{\cdot i} - (V \otimes C_Z S_Z^{t(\operatorname{rem} l(Z))}[F])_{\cdot i} = \mu + E_{\cdot i}$ just for one $i \in Z$. Thirdly, our theoretical claims can guarantee that Algorithm 2.7 works in some special cases, which includes the generic case encountered when F has randomly chosen real entries. However, we have not found any counterexample to Algorithm 2.7 in the case where the critical graph has several components, indicating that its performance and hence the performance of Algorithm 4.5 could be guaranteed in a more general case. Such counterexamples, as well as more refined and more efficient versions of Algorithm 2.7 and Algorithm 4.5, guaranteed in more general cases, will be sought in the future.

Acknowledgement

References

[1] François Baccelli, Guy Cohen, Geert Jan Olsder, and Jean Pierre Quadrat. *Synchronization and linearity: an algebra for discrete event systems.* John Wiley & Sons Ltd, 1992.

[2] Yves Balcer and A.F. Veinott. Computing a graph's period quadratically by node condensation. *Discrete Mathematics*, 4:295–303, 1973.

[3] Peter Butkovič. Max algebra: the linear algebra of combinatorics? *Linear Algebra and its Applications*, 367:313–335, 2003.

[4] Peter Butkovič. *Max-linear systems: theory and algorithms.* Springer Science & Business Media, 2010.

[5] Peter Butkovič, Hans Schneider, Sergeĭ Sergeev, and Bit-Shun Tam. Two cores of a nonnegative matrix. *Linear Algebra and its Applications*, 439:1929–1954, 2013.

[6] Jean Cochet-Terrasson, Guy Cohen, Stéphane Gaubert, Michael M. Gettrick, and Jean-Pierre Quadrat. Numerical computation of spectral elements in max-plus algebra. In *Proceedings of the IFAC conference on systems structure and control*, pages 699–706, IRCT, Nantes, France, 1998.

[7] Guy Cohen, Didier Dubois, Jean-Pierre Quadrat, and Michel Viot. A linear system theoretic view of discrete event processes and its use for performance evaluation in manufacturing. *IEEE Transactions on Automatic Control*, AC–30:210–220, 1985.

[8] Guy Cohen, Didier Dubois, Jean-Pierre Quadrat, and Michel Viot. Analyse du comportement périodique de systèmes de production par la théorie des dioïdes. Technical report, INRIA, Février 1983. Rapport de Recherche no. 191.

[9] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography. *Communications in Algebra*, 42(6):2624–2632, 2014.

[10] Dima Grigoriev and Vladimir Shpilrain. Tropical cryptography II. extensions by homomorphisms. *Communications in Algebra*, 47:4224–4229, 2018.

[11] Bernd Heidergott, Geert Jan Olsder, and Jacob Van der Woude. *Max Plus at Work.* Princeton University Press, 2006.

[12] Steve Isaac and Delaram Kahrobaei. A closer look at the tropical cryptography. *International Journal of Computer Mathematics: Computer Systems Theory* 6(2):137–142, 2021.

[13] Matvei Kotov and Alexander Ushakov. Analysis of a key exchange protocol based on tropical matrix algebra. *Journal of Mathematical Cryptology*, 12(3):137–141, 2018.

[14] Glenn Merlet, Thomas Nowak, Hans Schneider, and Sergeĭ Sergeev. Generalizations of bounds on the index of convergence to weighted digraphs. *Discrete Applied Mathematics*, 178:121–134, 2014.

[15] Glenn Merlet, Thomas Nowak, and Sergeĭ Sergeev. Weak CSR expansions and transience bounds in max-plus algebra. *Linear Algebra and its Applications*, 461:163–199, 2014.

[16] Any Muanalifah and Sergeĭ Sergeev. Modifying the tropical version of stickel's key exchange protocol. *Applications of Mathematics*, 65(6):727–753, 2020.

[17] Karl Nachtigall. Powers of matrices over an extremal algebra with applications to periodic graphs. *Mathematical Methods of Operations Research*, 46:87–102, 1997.

[18] Geert-Jan Olsder, Kees Roos, and R.J. van Egmond. An efficient algorithm for critical circuits and finite eigenvectors in the max-plus algebra. *Linear Algebra and its Applications*, 295(1):231–240, 1999.

[19] Dylan Rudy and Chris Monico. Remarks on a tropical key exchange system. *Journal of Mathematical Cryptology* 15(1): 280-283, 2020.

[20] Sergeĭ Sergeev and Hans Schneider. CSR expansions of matrix powers in max algebra. *Transactions of the American Mathematical Society*, 364(11):5969–5994, 2012.

[21] N.N. Vorobyev. Extremal algebra of positive matrices. *Elektronische Informationsverarbeitung und Kybernetik*, 3:39–71, 1967.

[22] N.N. Vorobyev. Extremal algebra of non-negative matrices. *Elektronische Informationsverarbeitung und Kybernetik*, 6:303–311, 1970.

A Associativity of the semidirect product

In this appendix we show that the semidirect product, which we are considering, is indeed associative. We need to prove:

$$[(M, G) \cdot (A, H)] \cdot (B, J) = (M, G) \cdot [(A, H) \cdot (B, J)]$$

Indeed, on the left-hand side we have:

$$
\begin{aligned}
[(M, G) \cdot (A, H)] \cdot (B, J) &= (M \circ H \oplus A, \ G \circ H) \cdot (B, J) \\
&= ((M \oplus H \oplus (M \otimes H) \oplus A) \circ J \oplus B, \ G \circ H \circ J) \\
&= (M \circ J \oplus H \circ J \oplus (M \otimes H) \circ J \oplus A \circ J \oplus B, G \circ H \circ J) \\
&= (M \oplus J \oplus (M \otimes J) \oplus H \oplus J \oplus (H \otimes J) \oplus (M \otimes H) \oplus J \\
&\quad \oplus (M \otimes H \otimes J) \oplus A \oplus J \oplus (A \otimes J) \oplus B, G \circ H \circ J) \\
&= (M \oplus H \oplus J \oplus A \oplus B \oplus (M \otimes J) \oplus (M \otimes H) \oplus (H \otimes J) \oplus (A \otimes J) \\
&\quad \oplus (M \otimes H \otimes J), \ G \circ H \circ J)
\end{aligned}
$$

On the right-hand side:

$$
\begin{aligned}
(M, G) \cdot [(A, H) \cdot (B, J)] &= (M, G) \cdot (A \circ J \oplus B, H \circ J) \\
&= (M, G) \cdot (A \oplus J \oplus A \otimes J \oplus B, H \oplus J \oplus H \otimes J) \\
&= (M \circ (H \oplus J \oplus H \otimes J) \oplus A \oplus J \oplus A \otimes J \oplus B, G \circ H \circ J) \\
&= (M \circ H \oplus M \circ J \oplus M \circ (H \otimes J) \oplus A \oplus J \oplus A \otimes J \oplus B, G \circ H \circ J) \\
&= (M \oplus H \oplus (M \otimes H) \oplus M \oplus J \oplus (M \otimes J) \oplus M \oplus (H \otimes J) \oplus \\
&\quad (M \otimes H \otimes J) \oplus A \oplus J \oplus (A \otimes J) \oplus B, G \circ H \circ J) \\
&= (M \oplus H \oplus J \oplus A \oplus B \oplus (M \otimes J) \oplus (M \otimes H) \oplus (H \otimes J) \\
&\quad \oplus (A \otimes J) \oplus (M \otimes H \otimes J), G \circ H \circ J),
\end{aligned}
$$

which is identical with what we obtained for the left-hand side.

B   CSR proofs

B.1   Proofs of Proposition 2.3 and Proposition 2.4

Here we deduce these propositions from results of Merlet et al. [15]. To do this, we need to introduce other versions of CSR decomposition and expansion, which appeared in that work. First of all, we can define the "big" CSR terms by considering the whole critical graph instead of individual components. For this, let σ be the l.c.m. of all $\sigma_1, \ldots, \sigma_l$ and define $U = ((\lambda^- \otimes F)^{\otimes \sigma})^+$. Then let matrices C, R and S be defined by

$$C_{ij} = \begin{cases} U_{ij} & \text{if } j \text{ is in } \mathcal{G}^c(F) \\ -\infty & \text{otherwise,} \end{cases} \qquad R_{ij} = \begin{cases} U_{ij} & \text{if } i \text{ is in } \mathcal{G}^c(F) \\ -\infty & \text{otherwise,} \end{cases}$$

$$S_{ij} = \begin{cases} \lambda^- \otimes F_{ij} & \text{if } (i,j) \in \mathcal{G}^c(F) \\ -\infty & \text{otherwise.} \end{cases}$$

We will denote $CS^t R[F] = C \otimes S^{\otimes t} \otimes R$. By Wielandt's bound (15) in [15, Theorem 4.1], we have

$$F^{\otimes t} = \lambda^{\otimes t} \otimes CS^t R[F] \oplus (B[F])^{\otimes t} = \lambda^{\otimes t} \otimes CS^{t(\mathrm{rem}\,\sigma)} R[F] \oplus (B[F])^{\otimes t}, \quad t \geq (d-1)^2 + 1 \quad (26)$$

Let us now discuss how the CSR term appearing in (26) can be decomposed into smaller CSR terms. For this, assume some numbering of the critical components and for $\mu: 1 \leq \mu \leq l-1$, define matrix $F_{\mu+1}$ by

$$(F_{\mu+1})_{ij} = \begin{cases} -\infty, & \text{if } i \in \mathcal{G}_\mu^c \text{ or } j \in \mathcal{G}_\mu^c, \\ (F_\mu)_{ij}, & \text{otherwise,} \end{cases}$$

with $F_1 = F$. Observe that $\lambda(F_\mu) = \lambda$ for any such μ, and that the critical graph of F_μ consists of components $\mathcal{G}_\mu^c, \ldots, \mathcal{G}_l^c$. Denote $U_\mu' = ((\lambda^- \otimes F_\mu)^{\otimes \sigma_\mu})^+$. Then, let matrices C_μ', R_μ' and S_μ' for

$\mu = 1, \dots, l$ be defined by:

$$
(C'_\mu)_{ij} = \begin{cases} (U'_\mu)_{ij} & \text{if } j \text{ is in } \mathcal{G}^c_\nu \\ -\infty & \text{otherwise,} \end{cases} \qquad (R'_\mu)_{ij} = \begin{cases} (U'_\mu)_{ij} & \text{if } i \text{ is in } \mathcal{G}^c_\nu \\ -\infty & \text{otherwise,} \end{cases}
$$

$$
(S'_\mu)_{ij} = (S_\mu)_{ij} = \begin{cases} \lambda^- \otimes (F_\mu)_{ij} & \text{if } (i,j) \in \mathcal{G}^c_\nu \\ -\infty & \text{otherwise.} \end{cases}
$$

Let us also compare C'_μ, S'_μ and R'_μ with the matrices introduced in (4). Notice that $S'_\mu = S_\mu$, for all μ and also $C'_1 = C_1$ and $R'_1 = R_1$, but in general only $C'_\mu \leq C_\mu$ and $R'_\mu \leq R_\mu$. We further denote $C'_\mu S_\mu^{t(\mathrm{rem}\, \sigma_\nu)} R'_\mu[F] = C'_\mu \otimes S_\mu^{t(\mathrm{rem}\, \sigma_\mu)} \otimes R'_\mu$, similarly to the CSR notation before. According to [15, Corollary 4.3], the following decomposition holds:

$$
CS^{t(\mathrm{rem}\, \sigma)} R[F] = \bigoplus_{\mu=1}^{l} C'_\mu S_\mu^{t(\mathrm{rem}\, \sigma_\mu)} R'_\mu[F], \qquad \forall t. \tag{27}
$$

Combining (26) and (27), we obtain

$$
F^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\mu=1}^{l} C'_\mu S_\mu^{t(\mathrm{rem}\, \sigma_\mu)} R'_\mu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geq (d-1)^2 + 1. \tag{28}
$$

Observing that $C'_1 S_1^{t(\mathrm{rem}\, \sigma_1)} R'_1[F] = C_1 S_1^{t\, \mathrm{rem}\, \sigma_1} R_1[F]$ we can also write:

$$
F^{\otimes t} = \lambda^{\otimes t} \otimes C_1 S_1^{t(\mathrm{rem}\, \sigma_1)} R_1[F] \oplus \lambda^{\otimes t} \otimes \bigoplus_{\mu=2}^{l} C'_\mu S_\mu^{t(\mathrm{rem}\, \sigma_\mu)} R'_\mu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geq (d-1)^2 + 1. \tag{29}
$$

But by a similar combination of [15] Theorem 4.1 and Corollary 4.3, we also have:

$$
(B_1[F])^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\mu=2}^{l} C'_\mu S_\mu^{t(\mathrm{rem}\, \sigma_\mu)} R'_\mu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geq (d-1)^2 + 1, \tag{30}
$$

where $B_1[F]$ is defined as in (5) with $\nu = 1$. Substituting (30) into (29) we obtain

$$
F^{\otimes t} = \lambda^{\otimes t} \otimes C_1 S_1^{t(\mathrm{rem}\, \sigma_1)} R_1[F] \oplus (B_1[F])^{\otimes t},
$$

30

which is the same as (6) for $\nu = 1$, thus establishing Proposition 2.3.

To explain (7) (Proposition 2.4), observe that (28) holds for any numbering of critical components. In other words, for any numbering of critical components we get the corresponding CSR decomposition of the form (28). Depending on which of these components is the first one, the first term in (28) can be equal to any of the terms $C_\nu S_\nu^{t(\mathrm{rem}\,\sigma_\nu)} R_\nu[F]$, while any other term in (28) is less than or equal to one of these $C_\nu S_\nu^{t(\mathrm{rem}\,\sigma_\nu)} R_\nu[F]$. This implies that taking the tropical sum of all CSR decompositions (28) written for all possible numberings of the critical components we obtain (7):

$$F^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\mathrm{rem}\,\sigma_\nu)} R_\nu[F] \oplus (B[F])^{\otimes t}, \quad \forall t \geq (d-1)^2 + 1, \tag{31}$$

For the irreducible matrices, the existence of $T(F)$ such that

$$F^{\otimes t} = \lambda^{\otimes t} \otimes C S^{t(\mathrm{rem}\,\sigma)} R[F], \qquad \forall t \geq T(F) \tag{32}$$

follows from [20, Theorem 5.6], and a number of upper bounds on $T(F)$ have been established in [15]. Recall also that

$$C S^t R[F] = \bigoplus_{\mu=1}^{l} C'_\mu S_\mu^{t(\mathrm{rem}\,\sigma_\mu)} R'_\mu[F] \leq \bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\mathrm{rem}\,\sigma_\nu)} R_\nu[F], \quad \forall t. \tag{33}$$

It follows from (31) and (32) that

$$\bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\mathrm{rem}\,\sigma_\nu)} R_\nu[F] \leq C S^{t(\mathrm{rem}\,\sigma)} R[F], \quad \forall t \geq \max(T(F), (d-1)^2 + 1). \tag{34}$$

Combining (33), (34) and the periodicity of CSR terms, we can replace inequalities in (33) and (34) with equalities, and we can write (32) as

$$F^{\otimes t} = \lambda^{\otimes t} \otimes \bigoplus_{\nu=1}^{l} C_\nu S_\nu^{t(\mathrm{rem}\,\sigma_\nu)} R_\nu[F],$$

establishing (8) and completing the proof of Proposition 2.4.

B.2 Proof of Proposition 2.5

The proof given below is a simplified version of the proof of [15, Theorem 6.1]

In the beginning of this proof let us introduce some extra notation, following [15]. For walk W denote by $p(W)$ its weight, and for a set of walks $\mathcal{W}$, denote by $p(\mathcal{W})$ the maximal weight of a walk in $\mathcal{W}$. Below we are going to use the following sets of walks:

- $\mathcal{W}(i \to j)$: set of walks connecting node i to node j;

- $\mathcal{W}^t(i \to j)$: set of walks connecting node i to node j and having length t;

- $\mathcal{W}^{t,l}(i \to j)$: set of walks connecting node i to node j and having length $t(\operatorname{rem} l)$;

- $\mathcal{W}^{t,l}(i \xrightarrow{\mathcal{G}} j)$: set of walks connecting node i to node j, going through a node in subgraph $\mathcal{G}$ and having length $t(\operatorname{rem} l)$.

In particular, we have the following optimal walk interpretation of the entries of a matrix power and a metric matrix [4]:

$$(A^{\otimes t})_{ij} = p(\mathcal{W}^t(i \to j)), \qquad (A^+)_{ij} = p(\mathcal{W}(i \to j)). \tag{35}$$

The proof given below is a simplified version of the proof of [15, Theorem 6.1]. For the sake of this proof we assume without loss of generality that the critical graph is strongly connected, i.e., it consists of one component, and let C, S and R be defined from it. We will show that for arbitrary i and j

$$(C \otimes S^{\otimes t} \otimes R)_{ij} = (C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} = p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)). \tag{36}$$

We first show

$$(C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} \le p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)), \quad (C \otimes S^{\otimes t} \otimes R)_{ij} \le p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)). \tag{37}$$

For the first inequality, we have $(C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} = (C_Z)_{is_1} \otimes (S_Z^{\otimes t})_{s_1 s_2} \otimes (R_Z)_{s_2 j}$, for some $s_1, s_2 \in Z$, which means that in terms of walks, there is a walk V such that $p(V) = (C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij}$ and

decomposed as $V = V_1 V_2 V_3$, where $V_1 \in \mathcal{W}^{0,l(Z)}(i \to s_1)$, $V_2 \in \mathcal{W}^t(s_1 \to s_2)$ and $V_3 \in \mathcal{W}^{0,l(Z)}(s_2 \to j)$. It is then obvious that $V \in \mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)$, and the first inequality of (37) follows.

As for the second inequality, $(C \otimes S^{\otimes t} \otimes R)_{ij}$ is the weight of a walk W that can be decomposed as $W = W_1 W_2 W_3$, where $W_1 \in \mathcal{W}^{0,\sigma}(i \to k_1)$, $W_2 \in \mathcal{W}^t(k_1 \to k_2)$ and $W_3 \in \mathcal{W}^{0,\sigma}(k_2 \to j)$ and $k_1, k_2 \in \mathcal{G}_1^c$. We now introduce a walk W_4 connecting k_1 to a node $k_3 \in Z$ on $\mathcal{G}^c(F)$ and a walk W_5 going back to k_1 on $\mathcal{G}^c(F)$. The composition $W_4 W_5$ forms a closed walk on $\mathcal{G}^c(F)$, and its length is a multiple of σ. In k_3, we insert a closed walk W_6 of a big enough length, whose all arcs belong to $\mathcal{G}^c(F)$ and whose length is such that the sum of lengths of W_1, W_3, W_4, W_5 and W_6 is a multiple of $l(Z)$. Then for the walk $\tilde{W} = W_1 W_4 W_6 W_5 W_2 W_3$, we have $\tilde{W} \in \mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)$. We thus have $p(W) = p(\tilde{W}) \le p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j))$, hence the second inequality of (37).

We now prove:

$$(C_Z \otimes S_Z^{\otimes t} \otimes R_Z)_{ij} \ge p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)), \quad (C \otimes S^{\otimes t} \otimes R)_{ij} \ge p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)). \quad (38)$$

For this, consider a walk W such that $p(W) = p(\mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j))$. Then we decompose it as $W = V_1 V_2$, where V_1 connects i to a node $k \in Z \subseteq \mathcal{G}^c(F)$, and V_2 connects k to j. At node k we insert mZ: a number of copies of Z such that $ml(Z) \ge t + l(Z)$. We then find V_3, W_2 and V_4 such that $mZ = V_3 W_2 V_4$, W_2 has length t and both $l(V_1) + l(V_3)$ and $l(V_4) + l(V_2)$ are multiples of $l(Z)$. Since $\tilde{W} = V_1 V_3 W_2 V_4 V_2 \in \mathcal{W}^{t,l(Z)}(i \xrightarrow{Z} j)$ and m is big enough, such walks V_3, W_2 and V_4 can be found. Denoting by k_1 the end of walk V_3 and by k_2 the beginning of walk V_4, we see that

$$p(V_1) + p(V_3) \le (C_Z)_{ik_1}, \quad p(V_1) + p(V_3) \le C_{ik_1}, \quad p(W_2) \le (S_Z^{\otimes t})_{k_1 k_2}, \quad p(W_2) \le S_{k_1 k_2}^{\otimes t},$$

$$p(V_4) + p(V_2) \le (R_Z)_{k_2 j}, \quad p(V_4) + p(V_2) \le R_{k_2 j},$$

and this implies both inequalities of (38).