On the Characterization of Saddle Point Equilibrium for Security Games with Additive Utility*

Hamid Emadi[1][0000−0002−6707−9679] and Sourabh Bhattacharya[1][0000−0002−1306−2775]

Iowa State University, Ames, IA 50011 USA
{emadi,sbhattac}@iastate.edu

Abstract. In this work, we investigate a security game between an attacker and a defender, originally proposed in [6]. As is well known, the combinatorial nature of security games leads to a large cost matrix. Therefore, computing the value and optimal strategy for the players becomes computationally expensive. In this work, we analyze a special class of zero-sum games in which the payoff matrix has a special structure which results from the *additive property* of the utility function. Based on variational principles, we present structural properties of optimal attacker as well as defender's strategy. We propose a linear-time algorithm to compute the value based on the structural properties, which is an improvement from our previous result in [6], especially in the context of large-scale zero-sum games.

Keywords: Security Game, Zero-Sum Game, Nash Equilibrium and Computational Complexity.

1 Introduction

Game theory [2] is a useful tool to model adversarial scenarios. *Security games* model attack scenarios wherein an attacker attacks a number of targets while the defender allocates its resources to protect them to minimize the impact. The payoff for the attacker and the defender is based on the successfully attacked and protected targets, respectively. Traditionally, attacker-defender games have been modeled as zero-sum games, and the resulting saddle-point strategies are assumed to be optimal for both players. In general, two-player zero-sum game can be formulated as an linear programming problem [2], and therefore saddle-point equilibrium can be computed in polynomial time. The most efficient running time of solver for a general LP problem is $\mathcal{O}(n^{2.055})$ [9]. However, solving security games with more than 2 resources for attacker and defender with a general LP solver is computationally expensive due to the combinatorial nature of the problem.

* This work was supported in part by NSF CPS grant ECCS 1739969.

In the past two decades, game theory has played an important role in quantifying and anlyzing security in large-scale networked systems. Here, we mention some of these efforts across several applications. In [4], authors propose an evolutionary game framework that models integrity attacks and defenses in an Advanced Metering Infrastructure in a smart grid. In [18], a game-theoretic defense strategy is developed to protect sensor nodes from attacks and to guarantee a high level of trustworthiness for sensed data. In [17], authors consider a security game in power grid in which the utility functions are defined based on the defender's net loss, and players' action set are defined based on different scenarios such as false data injection to electronic monitoring systems. In [23], authors provide a game theoretic approach to modeling attack and defense of smart grid in different layers of power plant, transmission and distribution network. In [8],[5], authors propose a game-theoretic model for the adaptive security policy and the power consumption in the Internet of Things. In [22], authors propose a zero-sum game for security-aware sensor placement in which the attacker minimizes its visibility by attacking certain number of nodes, and the detector maximizes the visibility of the attack signals by placement of sensors. In [20], authors consider a cyber-security problem in a networked system as a resilient graph problem. They use backward induction to obtain optimal strategies for both players which try to disrupt the communication and maintain the connectivity, respectively. In [20], authors propose a stochastic game-based model to provide a control synthesis method to minimize deviations from the desired specification due to adversaries, who has limited capability of observing the controller's strategy. In [7], authors focus on notions of self-protection (e.g., patching system vulnerabilities) and self insurance (e.g., having good backups) rather than only security investments in information security games. [10] introduces a method for resolving uncertainty in interdependent security scenarios in computer network and information security. In [24], authors examine security game in which each player collectively minimize the cost of virus spread, and assuring connectivity. In [11], authors propose a game theoretic framework for picking vs guessing attacks in the presence of preferences over the secret space, and they analyse the trade-off between usability and security. In [16], authors introduce a game-theoretic framework for optimal stochastic message authentication, and they provide guarantees for resource-bounded systems. For a comprehensive survey of game-theoretic approaches in security and privacy in computer and communication, a reader could refer to [19].

Security games pose computational challenges in analysis and synthesis of optimal strategies due to exponential increase in the size of the strategy set for each player. A class of security games which renders tractable computational analysis is that of Stackelberg games [1]. In Stackelberg models, the leader moves first, and the follower observes the leaders strategy before acting. Efforts involving randomized strategies [12] and approximation algorithms [3] for Stackelberg game formulation of security games have been proposed to efficiently allocate multiple resources across multiple assets/targets. In order to extend the efficient computational techniques for simultaneous move games, efforts have been made

to characterize conditions under which any Stackelberg strategy is also a NE strategy [15]. An extensive review of various efforts to characterize and reduce the computational complexity of Stackelberg games with application in security can be found in [6], and references therein. Here, we mention a few that are relevant to the problem under consideration. [13] shows that computing the optimal Stackelberg strategy in security resource allocation game, when attacker attacks one target, is NP-hard in general. However, when resources are homogeneous and cardinality of protection set is at most 2, polynomial-time algorithms have been proposed by the authors. [13] propose an LP formulation similar to Kiekintveld's formulation, and presents a technique to compute the mixed strategies in polynomial time.

In [14], a security game between an attacker and a defender is modeled as a non-zero game with multiple attacker resources. The authors analyze the scenario in which the payoff matrix has an *additive structure*. They propose an $\mathcal{O}(m^2)$ iterative algorithm for computing the mixed-strategy Nash Equilibrium where m is the size of the parameter set. Motivated from [14], in [6], we analyzed a zero-sum security game with multiple resources for attacker and defender in which the payoff matrix has an additive structure. Based on combinatorial arguments, we presented structural properties of the saddle-point strategy of the attacker, and proposed an $\mathcal{O}(m^2)$ algorithm to compute the saddle-point equilibrium and the value of the game, and provided closed-form expressions for both. In this paper, we show that a zero-sum security game can be reduced to the problem of minimizing the sum of the k-largest functions over a polyhedral set which can be computed in linear time [21]. Based on this insight, we use a variational approach to propose an $\mathcal{O}(m)$ algorithm which is the best possible in terms of the complexity. Moreover, we present structural properties of the saddle-point strategy of both players, and an explicit expression for the value of the game.

The rest of the paper is organized as follows. In Section 2, we present the problem formulation. In Section 3, we present structural properties of the optimal attacker strategy. In Section 4, we present a linear time algorithm to compute the value of a large-scale zero-sum game. In Section 5, we present structural properties of the defender's optimal strategy, and a dual algorithm to compute the value and equilibrium. In section 6, we present our conclusions along with some future work.

2 Problem Formulation: Security Game

Consider a two-person zero-sum game, and let $\mathcal{I} = \{1, \dots m\}$ denotes a set of targets. We assume an attacker (player 1) chooses k_a-targets to attack. So, there are $n_a = \binom{m}{k_a}$ actions for player 1. On the other hand, protection budget of targets is limited, and we assume that only k_d targets will be protected by the defender (player 2). So, there are $n_d = \binom{m}{k_d}$ actions for player 2. The defender has no knowledge about the targets chosen by player 1. In order to find the optimal strategy for the players, we formulate a strategic security game $(\mathcal{X}, \mathcal{Y}, A)$, where $\mathcal{X}$ and $\mathcal{Y}$ denote the action sets for attacker and defender, respectively, and

$\text{card}(\mathcal{X}) = n_a, \text{card}(\mathcal{Y}) = n_d$. Every element $x_i \in \mathcal{X}$ represents a set of targets that are attacked. Similarly, $y_i \in \mathcal{Y}$ represents a protected targets. Each $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$ is a k_a-tuple, and k_d-tuple subset of $\mathcal{I}$, respectively.

The attacker has no information about the targets that are protected by the defender. Let ϕ_i denote the cost associated to target i. Moreover, without loss of generality, we assume that targets are labeled such that $\phi_i \geq \phi_j \geq 0$ for $i > j$.

We consider an additive property for the utility function i.e., entries of the cost matrix A are defined as follows:

$$A_{ij} = \sum_{\{l | l \in x_i \cap y_j^c\}} \phi_l. \tag{1}$$

A represents the game matrix or payoff matrix for player 1. Since we consider a zero-sum game, the payoff matrix for player 2 is $-A$. Note that we assume both players have the complete information of the target costs.

Let p, q be the probability vectors representing the mixed strategies for player 1 and player 2, respectively. The expected utility function is

$$v = p^T A q.$$

According to the minimax theorem, every finite two-person zero-sum game has a saddle point with the value, v^*, in mixed strategy $p^* = \left[p_1^*, \ldots, p_{n_a}^*\right]^T$ for player 1, and mixed strategy $q^* = \left[q_1^*, \ldots, q_{n_d}^*\right]^T$ for player 2, such that player 1's average gain is at least v^* no matter what player 2 does. And player 2's average loss is at most v^* regardless of player 1's strategy, that is

$$p^T A q^* \leq p^{*T} A q^* \leq p^{*T} A q.$$

In order to solve every finite matrix game, we can reduce the game to the following LP problem,

$$\begin{aligned} \underset{p_i}{\text{maximize}} \quad & v \\ \text{subject to} \quad & v \leq \sum_{i=1}^{n_a} p_i a_{ij}, \quad j = 1, \ldots, n_d \\ & p_1 + \cdots + p_{n_a} = 1 \\ & p_i \geq 0 \quad \text{for} \quad i = 1, \ldots, n_a. \end{aligned} \tag{2}$$

However, the dimension of the decision variables in the above formulation is $(n_a + 1)$ which is exponential in terms of m. In the next section, we present an equivalent LP formulation with dimension m to compute v^*.

3 Structural Properties of the Attacker's Strategy

In this section, we investigate the structural properties of the optimal attacker's strategy. The value of the game (v^*) can be defined as follows based on the

attacker's mixed strategy p:

$$v^* = \max_{p} \min_{1 \le i \le n_d} (p^T A)_i,$$

where $(p^T A)_i$ denote the i^{th} element of $p^T A$. From (1), $(p^T A)_i$ can be written in the following form,

$$(p^T A)_i = \sum_{j=1}^{n_a} p_j a_{ji} = \sum_{j=1}^{n_a} p_j \sum_{l \in x_j \cap {y_i}^c} \phi_l = \sum_{l \in y_i^c} \alpha_l \phi_l,$$

where,

$$\alpha_j = \sum_{\{i | j \in x_i\}} p_i \implies M_{[m,k_a]} p = \alpha, \tag{3}$$

where $\alpha = [\alpha_1, \ldots, \alpha_m]^T$, and $M_{[m,k_a]} \in \mathbb{R}^{m \times n_a}$ is a *combinatorial matrix* [1].

Since $M_{[m,k_a]}$ is a combinatorial matrix, $\sum_{i=1}^{m} \alpha_i = k_a$. Moreover, in the following lemma we show that for any feasible α there exists a feasible p. Hence, the problem reduces to computing α^*.

Lemma 1. *$M_{[m,k_a]}$ is a surjective mapping.*

Proof. Please refer to the Appendix for the proof.

Based on the above lemma, the problem reduces to computing α^*.

Lemma 2. *α^* satisfies the following property:*

$$\alpha_i^* \phi_i \ge \alpha_j^* \phi_j \quad \textit{for} \quad i > j \tag{4}$$

where α_j^* is defined in (3) *for p^*.*

Proof. Assume the following holds for α^*:

$$\alpha_{i_m}^* \phi_{i_m} \ge \cdots \ge \alpha_{i_1}^* \phi_{i_1}. \tag{5}$$

Note that v^* is $(m-k_d)$-sum of smallest $\alpha_l \phi_l$, that is $v^* = \sum_{l=i_1}^{i_{m-k_d}} \alpha_l^* \phi_l$. Assume that there exist i and j such that $\alpha_i^* \phi_i < \alpha_j^* \phi_j$ for $i > j$. $\phi_i \ge \phi_j \Rightarrow \alpha_j^* > \alpha_i^*$. $\alpha_i^* < 1, \alpha_j^* > 0 \Rightarrow (e_i - e_j)^T \nabla_\alpha v|_{v^*} \le 0$. Since v^* is the maximum value of the $(m-k_d)$-sum of smallest $\alpha_l \phi_l$, we arrive at a contradiction. Therefore, $\alpha_i^* \phi_i \ge \alpha_j^* \phi_j$ for $i > j$. □

Corollary 1. *α^* and v^* satisfy the following property:*

(a) $v^* = \sum_{l=1}^{m-k_d} \alpha_l^* \phi_l$,

[1] A combinatorial matrix $M_{[m,k]} \in \mathbb{R}^{m \times \binom{m}{k}}$ is a boolean matrix containing all combinations of k 1's. Each column of M has k entries equal to 1 and rest of the entries equal to 0. In other words, M is a matrix constructed from $\binom{m}{k}$ combinations of k one in an m dimensional vector

(b) $\alpha^*_m\phi_m = \cdots = \alpha^*_s\phi_s > \alpha^*_{s-1}\phi_{s-1} \geq \cdots \geq \alpha^*_{s-r}\phi_{s-r}$, $\alpha^*_{s-r-1} = \cdots = \alpha^*_1 = 0$ *for* $1 \leq s \leq \max(k_a, m-k_d)$ *and* $0 \leq r \leq s-1$.

Proof. (a) Since v^* is $(m-k_d)$-sum of smallest $\alpha_l\phi_l$, This property can be concluded directly from Lemma 2.

(b) Let k denotes $\max(k_a, m-k_d)$. First, we show that there is an optimal solution such that $\alpha^*_m\phi_m = \cdots = \alpha^*_k\phi_k$. We proceed the proof by contradiction. We assume that $\exists i \in \{k+1, \ldots, m\}$ such that $\alpha^*_i\phi_i > \alpha^*_{i-1}\phi_{i-1}$. Since $\sum_{l=1}^{m}\alpha_l = k_a$, there is $j \in \{1, \ldots k\}$ such that $\alpha^*_j < 1$. Therefore, $(e_j - e_i)^T\nabla_\alpha v|_{v^*} \leq 0$. Note that if $(e_i - e_j)^T\nabla_\alpha v|_{v^*} < 0$ is a contradiction with the fact that v^* is the optimal value, and if $(e_i - e_j)^T\nabla_\alpha v|_{v^*} = 0$ then it means there are multiple solutions which at least one satisfy the property. Moreover, from Lemma 2, if $\alpha^*_m\phi_m = \alpha^*_s\phi_s$ then $\alpha^*_m\phi_m = \cdots = \alpha^*_s\phi_s$, which completes the proof. □

Let s^*, r^* denote the indices for optimal structure expressed in Corollary 1 . Let $\mathcal{U}_a$ and $\mathcal{U}_d$, called active sets of attacker and defender, denote the union of x_i's and y_i's corresponding to the support sets of p^* and q^*, respectively.

Corollary 2. *In a security game* $(\mathcal{X}, \mathcal{Y}, A)$, $\mathcal{U}_a = \{s^* - r^*, \ldots, m\}$. *When* $s^* > m - k_d$, *the defender has a pure strategy with* $\mathcal{U}_d = \{m - k_d + 1, \ldots, m\}$, *else* $\mathcal{U}_d = \{s^*, \ldots, m\}$ *(for* $s^* \leq m - k_d$*).*

Proof. The proof of first part directly follows from the fact that $\alpha_m, \ldots, \alpha_{s^*-r^*} > 0$ and $\alpha_{s^*-r^*-1} = \cdots = \alpha_1 = 0$.

For second part, consider $({p^*}^T A)_j$. The following condition holds for U_{i^*, i^*+r^*}:

$$\alpha_m\phi_m = \cdots = \alpha_{s^*}\phi_{s^*} > \alpha_{s^*-1}\phi_{s^*-1} \geq \cdots \geq \alpha_{s^*-r^*}\phi_{s^*-r^*}$$
$$\alpha_{s^*-r^*-1} = \cdots = \alpha_1 = 0.$$

When $k_a + k_d \leq m$, $({p^*}^T A)_j > v^*$ for all j such that $\{1, \ldots, s-1\} \not\subseteq y^c_j$. Consequently,

$$q^*_j = 0 \quad \forall j \quad \text{s.t.} \quad \{1, \ldots, s-1\} \not\subseteq y^c_j,$$

else ${p^*}^T A q^* > v^*$, which is a contradiction. Therefore, any q^*_j corresponding to y_j such that $y_j \cap \{1, \ldots, s-1\} \neq \emptyset$ is zero. In other words, $\mathcal{U}_d = \{s^*, \ldots, m\}$.

Based on similar arguments, we can conclude that $\mathcal{U}_d = \{s^*, \ldots, m\}$ for $k_a + k_d > m$ and $s^* \leq m - k_d$. When $k_a + k_d > m$ and $s^* > m - k_d$, $({p^*}^T A)_j > v^*$ for all j such that $\{s, \ldots, m\} \cap y^c_j \neq \emptyset$, and consequently $q^*_j = 0$. Therefore,

$$q^*_j = 0 \quad \forall j \quad \text{s.t.} \quad \{s, \ldots, m\} \not\subseteq y_j$$

Since the defender has k_d resources, it has a pure strategy to allocate it to targets $\{m - k_d + 1, \ldots, m\}$. □

Remark 1. According to Corollary 2, both players choose mixed strategies that involve targets with highest impacts (ϕ_i).

4 Computation of v^*

Based on Lemma 2, we can solve the following LP to compute v^*:

$$\begin{aligned} \underset{\alpha_1,\ldots,\alpha_m}{\text{maximize}} \quad & \sum_{l=1}^{m-k_d} \alpha_l \phi_l \\ \text{subject to} \quad & \alpha_i \phi_i \geq \alpha_j \phi_j \quad \text{for all} \quad i > j \\ & \sum_{i=1}^{m} \alpha_i = k_a \\ & \alpha_i \leq 1 \quad i = 1, \ldots, m. \end{aligned} \tag{6}$$

Note that from Lemma 1, we show that for any α which satisfies the conditions in (6), there exists a p on a simplex such that $Mp = \alpha$, which satisfy the feasibility condition of (6).

From Corollary 1, v^* and α^* can be computed by examining all feasible solutions for $1 \leq s \leq k$ ($k = \max(k_a, m - k_d)$), and $0 \leq r \leq s-1$ which satisfy the condition in Corollary 1 (b). Let U denote a square matrix of dimension k. The $(i, i+r)^{\text{th}}$ entry of U (denoted by $U_{i,i+r}$) is the solution to the following problem:

$$\begin{aligned} \underset{\alpha_1,\ldots,\alpha_m}{\text{maximize}} \quad & \sum_{l=1}^{m-k_d} \alpha_l \phi_l \\ \text{subject to} \quad & \alpha_m \phi_m = \cdots = \alpha_s \phi_s > \alpha_{s-1}\phi_{s-1} \geq \cdots \geq \alpha_{s-r}\phi_{s-r} \\ & \alpha_{s-r-1} = \cdots = \alpha_1 = 0, \qquad s = k - i + 1 \\ & 0 \leq \alpha_l \leq 1, \forall l \in \mathcal{I}. \end{aligned}$$

The following theorem relates v^* to the elements of U.

Theorem 1. *$v^* = \max\limits_{i,j}\{U_{i,j}\}$, and the entries of U are as follows:*

For $i \leq k_a + k_d - m$:

$$\begin{cases} U_{i,i} = 0, \\ U_{i,i+r} = \sum_{l=s-r}^{m-k_d} \phi_l \quad \textit{when} \quad c_i\phi_s \geq k_a - r > c_i\phi_{s-1} \end{cases}$$

For $i > k_a + k_d - m$:

$$\begin{cases} U_{i,i} = \frac{k_a(i-k-k_d+m)}{c_i} \quad \textit{when} \quad c_i\phi_s \geq k_a \\ U_{i,i+r} = \sum_{l=s-r}^{s-1} \phi_l + \frac{(k_a-r)(i-k-k_d+m)}{c_i}, \\ \qquad \textit{when} \quad c_i\phi_{s-r} > (i-k-k_d+m), \quad \textit{and} \quad c_i\phi_s \geq k_a - r > c_i\phi_{s-1}, \\ U_{i,i+r} = (k_a - r - c_{i-1}\phi_s)\phi_{s-r} + \sum_{l=s-r+1}^{s-1} \phi_l + (i-k-k_d+m)\phi_s \\ \qquad \textit{when} \quad c_i\phi_{s-r} \leq (i-k-k_d+m) \quad \textit{and} \quad c_i\phi_s \geq k_a - r > c_i\phi_s - 1 \\ U_{i,i+r} = 0 \quad \textit{otherwise} \end{cases}$$

where $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$.

Proof. First, we consider the case $s \leq m - k_d$. Let the optimal solution be $\alpha^* = (\alpha_1^*, \ldots, \alpha_m^*)$. Since $\alpha_i = \alpha_s(\phi_s/\phi_i)$ for $i \geq s$, $\delta\alpha_i = \delta\alpha_s(\phi_s/\phi_i)$ for any perturbation $\delta\alpha_s$. Since $\sum \alpha_i = k_a$, any allowable perturbation around α^* satisfies the following condition:

$$\sum_{j=1}^{m} \delta\alpha_j = 0 \implies \sum_{j=1}^{s-1} \delta\alpha_j + c_i\phi_s\delta\alpha_s = 0, \tag{7}$$

where $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$. Consider a perturbation that involves perturbing α_l for $l < s$ and $\alpha_s, \ldots, \alpha_m$. From (7), we obtain the following:

$$\delta\alpha_l = -c_i\phi_s\delta\alpha_s \tag{8}$$

Based on the first order necessary conditions for maxima, we obtain the following:

$$\delta v|_{v^*} < 0 \implies \phi_l\delta\alpha_l + \sum_{j=s}^{m-k_d} \phi_s\delta\alpha_s = \phi_l\delta\alpha_l + \phi_s(m - k_d - s + 1)\delta\alpha_s < 0 \tag{9}$$

Let $g(\phi) = -c_i\phi + (m - k_d - s + 1)$. Substituting (8) in (9) leads to the condition $g(\phi_l)\delta\alpha_s < 0$. $g(\phi_l) > 0 \Rightarrow \delta\alpha_s < 0 \Rightarrow \forall j < s, \alpha_j^* = 1$. If for any $l < s$, $g(\phi_l) < 0 \Rightarrow \delta\alpha_s > 0 \Rightarrow \alpha_s^* = 1$.

As a result, we obtain the following conditions:

$$\begin{aligned} &\alpha_j^* = 1 \quad \text{if} \quad g(\phi_j) > 0 \\ &\alpha_s^* = 1 \quad \text{if} \quad \exists j \quad \text{such that} \quad \alpha_j g(\phi_j) < 0, \end{aligned} \tag{10}$$

From (10), we conclude that α^* and v^* can have the following forms:

1.

$$\alpha_j = \begin{cases} 0 & j = 1, \ldots, s - r - 1 \\ 1 & j = s - r, \ldots, s - 1 \\ \frac{k_a - r}{c_i\phi_j} & j = s, \ldots, m \end{cases} \tag{11}$$

From feasibility conditions in (6) (i.e. $\sum_{l=1}^{m} \alpha_l = k_a, \alpha_j \leq 1$ and $\alpha_s\phi_s > \alpha_{s-1}\phi_{s-1}$), we conclude that at $(i, i + r)^{th}$ entry of U, feasibility conditions are satisfied if $c_i\phi_s \geq k_a - r > c_i\phi_{s-1}$. Substituting (11) in $U_{i,i+r} = \sum_{j=1}^{m-k_d} \alpha_j\phi_j$ leads to the following expression for $U_{i,i+r}$:

$$U_{i,i+r} = \sum_{l=s-r}^{s-1} \phi_l + \frac{(k_a - r)(i - k - k_d + m)}{c_i} \tag{12}$$

2.

$$\alpha_j = \begin{cases} 0 & j = 1, \ldots, s - r - 1 \\ \delta & j = s - r \\ 1 & j = s - r + 1, \ldots, s \\ \frac{\phi_s}{\phi_j} & j = s + 1, \ldots, m, \end{cases} \tag{13}$$

where $\delta = (k_a - r - c_{i-1}\phi_s)$, which results from $\sum_{j=1}^{m} \alpha_j = k_a$. Since $0 < \delta \leq 1$, $0 < k_a - r - c_{i-1}\phi_s \leq 1$, which is equivalent to $c_i\phi_s \geq k_a - r > c_i\phi_s - 1$. Moreover, substituting (13) in $U_{i,i+r} = \sum_{l=1}^{m-k_d} \alpha_l\phi_l$ leads to the following expression for v:

$$U_{i,i+r} = \delta\phi_{s-r} + (i - k - k_d + m)\phi_s + \sum_{l=s-r+1}^{s-1} \phi_l. \tag{14}$$

3.

$$\alpha_m\phi_m = \cdots = \alpha_s\phi_s, \quad \alpha_s \neq 0, \quad \alpha_j = 0 \quad \text{for} \quad j \in \{1, \ldots, s-1\}$$

Substituting the above condition in $U_{i,i+r} = \sum_{l=1}^{m-k_d} \alpha_l\phi_l$, we obtain the following:

$$U_{i,i+r} = \sum_{l=s}^{m-k_d} \alpha_l\phi_l = (i - k - k_d + m)\alpha_j\phi_j \tag{15}$$

$$\implies \alpha_j = \frac{U_{i,i+r}}{(i - k - k_d + m)\phi_j}, \quad j \in \{s, \ldots, m\} \tag{16}$$

By substituting (16) into $U_{i,i+r} = \sum_{l=1}^{m-k_d} \alpha_l v_l$, we obtain the following:

$$\sum_{j=s}^{m} \frac{U_{i,i+r}}{(i - k - k_d + m)\phi_j} = k_a \implies U_{i,i+r} = \frac{k_a(i - k - k_d + m)}{\sum_{j=s}^{m} \frac{1}{\phi_j}} \tag{17}$$

Let $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$. Next, we have to check whether α satisfies the feasibility conditions of (6). Substituting $U_{i,i+r}$ in (16) leads to the following:

$$\alpha_j = \begin{cases} \frac{k_a}{\phi_j c_i} & j \in \{s, \ldots, m\} \\ 0 & j \in \{1, \ldots, s-1\} \end{cases}$$

Finally, we consider the case when $k_a + k_d > m$. Since $U_{i,i+r} = \sum_{l=s-r}^{m-k_d} \alpha_l\phi_l$ and $\alpha_j = 0$ for $j = 1, \ldots, m - k_d$, for $i = 1, \ldots, k_a + k_d - m$, $U_{i,i} = 0$. Moreover, $U_{i,i+r}$ can be written as $U_{i,i+r} = \sum_{l=s-r}^{m-k_d} \alpha_l\phi_l$, and the feasible α's are given as follows:

$$\alpha_j = \begin{cases} 0 & j = 1, \ldots, s-r-1 \\ 1 & j = s-r, \ldots, s-1 \\ \frac{k_a - r}{c_i\phi_j} & j = s, \ldots, m \end{cases} \tag{18}$$

If $c_i\phi_s \geq k_a - r > c_i\phi_{s-1}$, then $(i, i+r)^{\text{th}}$ entry of U is feasible. For all $i > k_a + k_d - m$, the arguments are same as for the case $k_a \leq m - k_d$.

Since v^* is the maximum value which satisfies all feasibility conditions, v^* is the maximum entry of U. □

Next, we show that U is a sparse matrix, which leads to a linear time algorithm for computing v^*. Let U^I and U^{II} be square matrices of dimension k defined as follows:

$$U^I_{i,i+r} = \begin{cases} U_{i,i+r} & c_i\phi_{s-r} > (i-k-k_d+m), c_i\phi_s \geq k_a - r > c_i\phi_{s-1}, \\ 0 & \text{otherwise} \end{cases}, \quad (19)$$

$$U^{II}_{i,i+r} = \begin{cases} U_{i,i+r} & c_i\phi_{s-r} \leq (i-k-k_d+m), c_i\phi_s \geq k_a - r > c_i\phi_s - 1 \\ 0 & \text{otherwise} \end{cases} \quad (20)$$

Lemma 3. *Given an infeasible cell in U^I, either all the cells to the right (in the same row) or all the cells below (in the same column) are infeasible.*

Proof. Consider an infeasible cell $(i, i+r)$ in U^I. For a cell to be infeasible, at least one of the three inequalities in (19) needs to be violated.

(a) First, consider the case $c_i\phi_{s-1} \geq k_a - r \Rightarrow c_i\phi_{s-1} \geq k_a - r', \quad \forall r' \geq r$. In other words, if $c_i\phi_{s-1} \geq k_a - r$, there is no feasible solution in $(i, i+r')^{\text{th}}$ entry of U^I for all $r' \geq r$.
(b) Next, consider the case, $k_a - r > c_i\phi_s$. Since $c_{i+1}\phi_{s-1} = c_i\phi_{s-1} + 1$, $k_a - r + 1 > c_{i+1}\phi_{s-1} \Rightarrow (i+1, i+r)^{\text{th}}$ entry of U^I cannot be feasible. Since i is arbitrary, we can conclude that $(i+j, i+r)^{\text{th}}$ entry of U^I cannot be feasible for all $j \geq 1$.
(c) Finally, consider the case in which the inequality $c_i\phi_{s-r} > (i-k-k_d+m)$ is the only one that is violated at $(i, i+r)^{\text{th}}$ entry of U^I. Therefore, $c_i\phi_s \geq k_a - r > c_i\phi_{s-1} \Rightarrow k_a - r + 1 > c_{i+1}\phi_{s-1}$, and consequently, there is no feasible solution in $(i+j, i+r)^{\text{th}}$ entry of U^I for all $j \geq 1$. Therefore, any column of U^I contains at most one feasible (non-zero) entry.

Corollary 3. *At most one cell in a column of U^I is feasible.*

Proof. The proof follows directly from the arguments for Lemma 3 (c).

Theorem 2. *v^*, α^* can be computed in $\mathcal{O}(k)$ time.*

Proof. From Lemma 3 and Corollary 3, we can conclude that from a current cell (i, j) in U^I, one needs to search either in cell $(i+1, j)$ or cell $(i, j+1)$ to find the next feasible element. Therefore, a linear search ($\mathcal{O}(k)$) that alternates between rows and columns leads to the cell containing the maximum element.

Next, we show that all feasible entries in U^{II} can be computed in $\mathcal{O}(k)$ time. For each row i, there is at most one r which satisfies $c_i\phi_s \geq k_a - r > c_i\phi_s - 1$ in (20). Therefore, for each row in U^{II}, we can find the feasible cell in constant time. This implies that all feasible entries in U^{II} can be computed in $\mathcal{O}(k)$ time, and a linear or a logarithmic search among the feasible entries provides the maximum element. □

Algorithm 1 gives v^*, α^* and active targets for the attacker and the defender in linear time.

Algorithm 1 Computation of the value, and active targets

Input: $\phi_1, \ldots, \phi_m$ and k_a, k_d
Output: $v^*, \alpha^*, \mathcal{U}_a, \mathcal{U}_d$
Construct U based on Theorem 1 and Theorem 2.
$i_1 \leftarrow 1$
for $j = 1 : m - k_d$ **do**
  for $i = i_1 : j$ **do**
    if $c_i\phi_s \geq k_a - r > c_i\phi_{s-1}$ **then**
      if $c_i\phi - s - r > i - k - k_d + m$ **then**
        $U_{i,i+r} = \sum_{l=s-r}^{s-1} \phi_l + \frac{(k_a - r)i - k - k_d + m}{c_i}$,
      end if
      $i_1 \leftarrow i$
      return i
    else if $k_a - r > c_i\phi_s$ **then**
      $i_1 \leftarrow i$
      return i
    else
      $U_{i,i+r} = 0$
      $i_1 \leftarrow i$
    end if
  end for
end for
for $i = 1 : k$ **do**
  find r such that $c_i\phi_s \geq k_a - r > c_i\phi_s - 1$
  if $c_i\phi_{s-r} \leq i - k - k_d + m$, and $c_i\phi_s \geq k_a - r > c_i\phi_s - 1$ **then**
    $U_{i,i+r} = (k_a - r - c_{i-1}\phi_s)\phi_{s-r} + \sum_{l=s-r+1}^{s-1} \phi_l + (i - k - k_d + m)\phi_s$
  else
    $U_{i,i+r} = 0$
  end if
end for
$v^* \leftarrow \max U_{i,j}$
$(i^*, j^*) \leftarrow \arg\max U_{i,j}$
$\mathcal{U}_a \leftarrow \{k - j^* + 1, \ldots, m\}$
$\mathcal{U}_d \leftarrow \{k - i^* + 1, \ldots, m\}$

5 Dual Analysis: Structural Properties of the Defender's Strategy and Algorithms

In this section, we present structural results for the optimal strategy of the defender, and present an $\mathcal{O}(m)$ algorithm to compute v^* and its corresponding optimal strategy. From the definition of v^*, we obtain the following:

$$v^* = \min_{q} \max_{1 \le j \le n_a} (Aq)_j.$$

where $(Aq)_j$ denote the j^{th} element of Aq. From (1), $(Aq)_j$ can be written in the following form,

$$(Aq)_j = \sum_{i=1}^{n_d} q_i a_{ji} = \sum_{i=1}^{n_d} q_i \sum_{l \in x_j \cap {y_i}^c} \phi_l = \sum_{l \in x_j} \beta_l \phi_l,$$

where,

$$\beta_j = \sum_{\{i | j \in {y_i}^c\}} q_i \implies \beta = M_{[m,m-k_d]} q, \tag{21}$$

where $\beta = [\beta_1, \ldots, \beta_m]^T$, and $M_{[m,(m-k_d)]} \in \mathbb{R}^{m \times n_d}$ is a *combinatorial matrix*. Since $M_{[m,m-k_d]}$ is a combinatorial matrix, $\sum_{i=1}^{n_d} \beta_i = m - k_d$. Moreover, from lemma 1, for any feasible β there exists a feasible q.

The following lemma provides the structure of β^*.

Lemma 4. *β^* satisfies one of the following conditions:*

(a) $\phi_{s-r} \ge \beta_s^* \phi_s = \cdots = \beta_m^* \phi_m \ge \phi_{s-r-1}$, *and* $\beta_1^* = \cdots = \beta_{s-1}^* = 1$,
(b) $\phi_{s-r} \ge \beta_s^* \phi_s = \cdots = \beta_m^* \phi_m = \phi_{s-r-1}$, *and* $\beta_{s-1}^* \phi_{s-1} \ge \beta_s^* \phi_s$,
and $\beta_1^* = \cdots = \beta_{s-2}^* = 1$,
where $1 \le s \le m$, $0 \le r \le s-1$, $r+1 \le k_a \le r+m-s$.

Proof. Let the sequence $\{i_1, \ldots, i_m\}$ of indices satisfy the following condition:

$$\beta_{i_1}^* \phi_{i_1} \ge \cdots \ge \beta_{i_m}^* \phi_{i_m} \tag{22}$$

Note that $v^* = \sum_{l=i_1}^{i_{k_a}} \beta_l^* \phi_l$.

First, we show that $\beta_{i_{k_a}}^* \phi_{i_{k_a}} = \beta_{i_{k_a+1}}^* \phi_{i_{k_a+1}}$. Assume 1) $\beta_{i_{k_a}}^* \phi_{i_{k_a}} > \beta_{i_{k_a+1}}^* \phi_{i_{k_a+1}}$ 2) there exists an $i \in \{i_{k_a}, \ldots, i_m\}$ such that $\beta_i^* < 1$. Since $(e_i - e_{i_{k_a}})^T \nabla_\beta v|_{v^*} < 0$ at v^*, we arrive at a contradiction. Now, assume $\beta_{i_{k_a+1}}^* = \cdots = \beta_{i_m}^* = 1$. Since $\sum_{l=1}^{m} \beta_l = m - k_d$ and $k_d \ge 1$, there exist $i, j \in \{i_1, \ldots, i_{k_a}\}, i > j$ such that $\beta_i^*, \beta_j^* < 1$. Therefore, $(e_j - e_i)^T \nabla_\beta v|_{v^*} < 0$, and we arrive at a contradiction. Therefore, $\beta_{i_{k_a}}^* \phi_{i_{k_a}} = \beta_{i_{k_a+1}}^* \phi_{i_{k_a+1}}$. In a similar manner, we can show that $\beta_m^* \phi_m = \beta_{i_{k_a}}^* \phi_{i_{k_a}}$.

Next, we prove that $\forall i$ such that $\beta_i^* \phi_i \ne \beta_m^* \phi_m$, there is at most one $\beta_j^* < 1$ and $\beta_j^* \phi_j > \beta_m^* \phi_m$, and the rest of β_i^*'s are 1. Assume that there are $\beta_j^* <$

$1, \beta_k^* < 1$ such that $\beta_j^* \phi_j \neq \beta_m^* \phi_m$ and $\beta_k^* \phi_k \neq \beta_m^* \phi_m$. If $\beta_k^* \phi_k, \beta_j^* \phi_j > \beta_m^* \phi_m$, and $j > k$, then $(e_k - e_j)^T \nabla_\beta v|_{v^*} < 0$, and we arrive at a contradiction. Now, assume that $\beta_j^* \phi_j < \beta_m^* \phi_m$, and $\beta_j^* < 1$, therefore $(e_j - e_i)^T \nabla_\beta v|_{v^*} < 0$ for all i such that $\beta_i^* \phi_i > \beta_j^* \phi_j$, which leads to a contradiction.

Next, we prove that β^* always satisfies one of the conditions in the Lemma. Let $\Gamma = \{i | \beta_i^* \phi_i = \beta_m^* \phi_m\}$. First, we prove that $\forall j \in \Gamma$ if $\beta_j^* < 1$ then $j+1 \in \Gamma$. To begin with, we assume that $\beta_j^* < 1, \beta_j^* \phi_j = \beta_m^* \phi_m$ and $j+1 \notin \Gamma$. If $\beta_{j+1}^* \phi_{j+1} > \beta_j^* \phi_j$, $(e_j - e_{j+1})^T \nabla_\beta v|_{v^*} < 0$, which leads to a contradiction. Moreover, if $\beta_{j+1}^* \phi_{j+1} < \beta_j^* \phi_j$ then $\beta_{j+1}^* < 1$ and $(e_{j+1} - e_i)^T \nabla_\beta v|_{v^*} < 0$ for all i such that $\beta_{j+1}^* \phi_{j+1} < \beta_i^* \phi_i$. This completes the proof for the first structure in the Lemma. Let $j = \min(\Gamma)$ and $\beta_j * = 1$. Therefore, for any $i \in \Gamma$, either $\beta_i^* < 1 \Rightarrow i+1 \in \Gamma$ or $\beta_i^* = 1, \phi_j = \phi_i$. The last condition leads to the second structure in the Lemma. □

Similar to the analysis for the attacker, from the above Lemma, we can compute v^* and β^* by examining all possible solutions which satisfy conditions (a) or (b) in Lemma 4. Let W be a square matrix of dimension m.

Theorem 3. *$v^* = \min_{i,j}\{W_{i,j}\}$, where entries of W are defined as follows:*

$$\begin{cases} W_{i,i+r} = \frac{(k_a - r)(i - k_d)}{c_i} + \sum_{l=s-r}^{s-1} \phi_l, \\ \quad for \quad s-1 \geq r \geq 0, r+m-s \geq k_a \geq r+1, c_i\phi_{s-r} \geq i - k_d \geq c_i\phi_{s-r-1}, \\ W_{i,i+r} = (i - k_d + 1 - c_i\phi_{s-r-1})\phi_{s-1} + (k_a - r)\phi_{s-r-1} + \sum_{l=s-r}^{s-2} \phi_l, \\ \quad for \quad s-1 \geq r \geq 0, r+m-s \geq k_a \geq r+1, \\ \quad c_i\phi_{s-r-1} + 1 > i - k_d + 1 \geq c_{i+1}\phi_{s-r-1} \\ W_{i,i+r} = +\infty, \quad otherwise \end{cases}$$

where, $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$.

Proof. First case corresponds to the structure (a) in Lemma 4. In this case, $\beta_1 = \cdots = \beta_{s-1} = 1$. Since $\sum_{l=1}^{m} \beta_l = m - k_d$, and $\beta_s\phi_s = \cdots = \beta_m\phi_m$, we obtain the following expression for β_j

$$\beta_j = \frac{i - k_d}{c_i \phi_j}, \quad j = s, \ldots, m, \tag{23}$$

where $i = m - s + 1$ and $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$. Next, we provide the feasibility conditions for structure (a). Since $0 \leq \beta_j \leq 1$, $c_i\phi_s \geq i - k_d$. Moreover, $\phi_{s-r} \geq \beta_s\phi_s \Rightarrow c_i\phi_{s-r} \geq i - k_d$. Additionally, $\beta_s\phi_s \geq \phi_{s-r-1} \Rightarrow i - k_d \geq c_i\phi_{s-r-1}$. Note that k_a-largest terms of $\beta_l\phi_l$ contain at least one term in the set $\{\beta_s\phi_s, \ldots, \beta_m\phi_m\}$. Therefore, $r + m - s \geq k_a \geq r + 1$. By substituting (23) into $W_{i,i+r} = \sum_{l=i_1}^{i_{k_a}} \beta_l\phi_l$,

$$W_{i,i+r} = \frac{(k_a - r)(i - k_d)}{c_i} + \sum_{l=s-r}^{s-1} \phi_l. \tag{24}$$

The second case corresponds to the structure (b) in Lemma 4. In this case, $\beta_1 = \cdots = \beta_{s-2} = 1$. Since $\sum_{l=1}^{m} \beta_l = m - k_d$ and $\beta_s\phi_s = \cdots = \beta_m\phi_m = \phi_{s-r-1}$, we obtain the following:

$$\beta_j = \frac{\phi_{s-r-1}}{\phi_j}, \quad j = s, \ldots, m, \tag{25}$$

$$\beta_{s-1} = i - k_d + 1 - c_i\phi_{s-r-1}, \tag{26}$$

where $i = m-s+1$ and $c_i = \sum_{j=s}^{m} \frac{1}{\phi_j}$. Next, we provide the feasibility conditions for structure (b). Since $\beta_{s-1}\phi_{s-1} \geq \phi_{s-r-1}$, and $0 \leq \beta_{s-1} < 1$, $c_i\phi_{s-r-1} + 1 > i - k_d + 1 \geq c_{i+1}\phi_{s-r-1}$. Note that k_a-largest terms of $\beta_l\phi_l$ contain at least one term in the set $\{\beta_s\phi_s, \ldots, \beta_m\phi_m\}$. Therefore, $r + m - s \geq k_a \geq r + 1$. By substituting (25), (26) into $W_{i,i+r} = \sum_{l=i_1}^{i_{k_a}} \beta_l\phi_l$,

$$W_{i,i+r} = (i - k_d + 1 - c_i\phi_{s-r-1})\phi_{s-1} + (k_a - r)\phi_{s-r-1} + \sum_{l=s-r}^{s-2} \phi_l. \tag{27}$$

□

Since W is a square amtrix of dimension m, v^* can be computed in $\mathcal{O}(m^2)$. As in the case of the defender, we can show that W can be computed in $\mathcal{O}(m)$ due to sparsity of W (the feasiblity consitions).

Theorem 4. *v^* can be computed in $\mathcal{O}(m)$.*

Proof. Please refer to the Appendix for the proof.

6 Conclusion

In this work, we address a security game as a zero-sum game in which the utility function has additive property. We analyzed the problem from attacker and defender's perspective, and we provided necessary conditions for the optimal solutions. Consequently, the structural properties of the saddle-point strategy for both players are given. Using the structural properties, we reach to the linear time algorithm, and semi-closed form solutions for computing the saddle points and value of the game.

There are several directions of future research. One direction is to use the proposed structural properties to formulate a network design problem to minimize the impact of attacks, which leads to design resilient networks from security perspective. Another direction of future research is to generalize the results of this work to nonzero-sum games with different utility functions for attacker and defender. Finally, we plan to extend our analysis to security games with non-additive utility functions.

References

1. Başar, T.: On the relative leadership property of stackelberg strategies. Journal of Optimization Theory and Applications **11**(6), 655–661 (1973)
2. Başar, T., Olsder, G.J.: Dynamic noncooperative game theory, vol. 23. Siam (1999)
3. Bhattacharya, S., Conitzer, V., Munagala, K.: Approximation algorithm for security games with costly resources. In: International Workshop on Internet and Network Economics. pp. 13–24. Springer (2011)
4. Boudko, S., Abie, H.: An evolutionary game for integrity attacks and defences for advanced metering infrastructure. In: Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings. pp. 1–7 (2018)
5. Boudko, S., Abie, H.: Adaptive cybersecurity framework for healthcare internet of things. In: 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT). pp. 1–6. IEEE (2019)
6. Emadi, H., Bhattacharya, S.: On security games with additive utility. IFAC-PapersOnLine **52**(20), 351–356 (2019)
7. Grossklags, J., Christin, N., Chuang, J.: Secure or insure? A game-theoretic analysis of information security games. In: Proceedings of the 17th international conference on World Wide Web. pp. 209–218 (2008)
8. Hamdi, M., Abie, H.: Game-based adaptive security in the internet of things for ehealth. In: 2014 IEEE International Conference on Communications (ICC). pp. 920–925. IEEE (2014)
9. Jiang, S., Song, Z., Weinstein, O., Zhang, H.: Faster dynamic matrix inverse for faster LPs. arXiv preprint arXiv:2004.07470 (2020)
10. Johnson, B., Grossklags, J., Christin, N., Chuang, J.: Uncertainty in interdependent security games. In: International Conference on Decision and Game Theory for Security. pp. 234–244. Springer (2010)
11. Khouzani, M., Mardziel, P., Cid, C., Srivatsa, M.: Picking vs. guessing secrets: A game-theoretic analysis. In: 2015 IEEE 28th Computer Security Foundations Symposium. pp. 243–257. IEEE (2015)
12. Kiekintveld, C., Jain, M., Tsai, J., Pita, J., Ordóñez, F., Tambe, M.: Computing optimal randomized resource allocations for massive security games. In: Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1. pp. 689–696. International Foundation for Autonomous Agents and Multiagent Systems (2009)
13. Korzhyk, D., Conitzer, V., Parr, R.: Complexity of computing optimal stackelberg strategies in security resource allocation games. In: Twenty-Fourth AAAI Conference on Artificial Intelligence (2010)
14. Korzhyk, D., Conitzer, V., Parr, R.: Security games with multiple attacker resources. In: Twenty-Second International Joint Conference on Artificial Intelligence (2011)
15. Korzhyk, D., Yin, Z., Kiekintveld, C., Conitzer, V., Tambe, M.: Stackelberg vs. nash in security games: An extended investigation of interchangeability, equivalence, and uniqueness. Journal of Artificial Intelligence Research **41**, 297–327 (2011)
16. Laszka, A., Vorobeychik, Y., Koutsoukos, X.: A game-theoretic approach for integrity assurance in resource-bounded systems. International Journal of Information Security **17**(2), 221–242 (2018)
17. Law, Y.W., Alpcan, T., Palaniswami, M.: Security games for risk minimization in automatic generation control. IEEE Transactions on Power Systems **30**(1), 223–232 (2014)

18. Lim, H.S., Ghinita, G., Bertino, E., Kantarcioglu, M.: A game-theoretic approach for high-assurance of data trustworthiness in sensor networks. In: 2012 IEEE 28th International Conference on Data Engineering. pp. 1192–1203. IEEE (2012)
19. Manshaei, M.H., Zhu, Q., Alpcan, T., Bacşar, T., Hubaux, J.P.: Game theory meets network security and privacy. ACM Computing Surveys (CSUR) **45**(3), 25 (2013)
20. Nugraha, Y., Hayakawa, T., Cetinkaya, A., Ishii, H., Zhu, Q.: Subgame perfect equilibrium analysis for jamming attacks on resilient graphs. In: 2019 American Control Conference (ACC). pp. 2060–2065. IEEE (2019)
21. Ogryczak, W., Tamir, A.: Minimizing the sum of the k largest functions in linear time. Information Processing Letters **85**(3), 117–122 (2003)
22. Pirani, M., Nekouei, E., Sandberg, H., Johansson, K.H.: A game-theoretic framework for security-aware sensor placement problem in networked control systems. In: 2019 American Control Conference (ACC). pp. 114–119. IEEE (2019)
23. Shan, X.G., Zhuang, J.: A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. Reliability Engineering & System Safety **195**, 106683 (2020)
24. Trajanovski, S., Kuipers, F.A., Hayel, Y., Altman, E., Van Mieghem, P.: Designing virus-resistant networks: a game-formation approach. In: 2015 54th IEEE Conference on Decision and Control (CDC). pp. 294–299. IEEE (2015)

A Proof of Lemma 1

Proof. The proof has already appeared in [6]. The proof is by induction. We assume that the lemma is true for $m' = m-1$ and $k'_a = 1, \ldots, m-1$. $M_{[m,k_a]}$ can be written as

$$M_{[m,k_a]} = \begin{bmatrix} \mathbf{1}^T & \mathbf{0}^T \\ M_{[m-1,k_a-1]} & M_{[m-1,k_a]} \end{bmatrix}. \tag{28}$$

By separating p into $\bar{p}_1$ and $\bar{p}_2$,

$$\begin{aligned} M_{[m,k_a]}p &= \begin{bmatrix} \mathbf{1}^T & \mathbf{0}^T \\ M_{[m-1,k_a-1]} & M_{[m-1,k_a]} \end{bmatrix} \begin{bmatrix} \bar{p}_1 \\ \bar{p}_2 \end{bmatrix} \\ &= \begin{bmatrix} \mathbf{1}^T\bar{p}_1 \\ M_{[m-1,k_a-1]}\bar{p}_1 + M_{[m-1,k_a]}\bar{p}_2 \end{bmatrix}. \end{aligned} \tag{29}$$

Second entry of the above matrix can be written in the following form:

$$\alpha_1 M_{[m-1,k_a-1]}{p'}_1 + (1-\alpha_1)M_{[m-1,k_a]}{p'}_2, \tag{30}$$

where, $\bar{p}_1 = \alpha_1 {p'}_1, \bar{p}_2 = (1-\alpha_1){p'}_2$. Since we assumed that the lemma is true for $m' = m-1$ and $k'_a = 1, \ldots, k_a - 1$, there exists ${p'}_1$ and ${p'}_2$ in a simplex such

that the following hold:

$$M_{[m-1,k_a-1]}{p'}_1 = \frac{k_a - 1}{k_a - \alpha_1} \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}, \tag{31}$$

$$M_{[m-1,k_a]}{p'}_2 = \frac{k_a}{k_a - \alpha_1} \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}. \tag{32}$$

By substituting the above expressions in (29), we conclude that $M_{[m,k_a]}p = \alpha$, where p lies on a simplex. In other words, α lies in a convex-hull of columns of M. In order to complete the proof, we need to show that the lemma holds for the base cases $M_{[m+1,m]}$ and $M_{[m,1]}$.

Note that $M_{[m,1]} = I_{m\times m}$. Therefore $p = \alpha$, and $\sum_{j=1}^{m} p_j = \sum_{j=1}^{m} \alpha_j = 1$. Next,

$$M_{[m+1,m]}p = (\mathbf{1}\mathbf{1}^T - I)p = \alpha \tag{33}$$

$$p = (\mathbf{1}\mathbf{1}^T - I)^{-1}\alpha = (\frac{\mathbf{1}\mathbf{1}^T}{m} - I)\alpha = \mathbf{1} - \alpha. \tag{34}$$

Consequently, lemma holds for base cases, which completes the proof. □

B Proof of Theorem 4

Proof. Let W^a and W^b denote matrices of the following form:

$$W^a_{i,i+r} = \begin{cases} W_{i,i+r} & \text{satisfying structure (a) in Lemma 4} \\ 0 & \text{otherwise} \end{cases}, \tag{35}$$

$$W^b_{i,i+r} = \begin{cases} W_{i,i+r} & \text{satisfying structure (b) in Lemma 4} \\ 0 & \text{otherwise} \end{cases}. \tag{36}$$

First, note that all feasible entries of W^a and feasible entries of W^b are disjoint due to complimentary feasibility conditions ($i - k_d \geq c_i\phi_{s-r-1}$ in W^a, and $i - k_d < c_i\phi_{s-r-1}$ in W^b). Moreover, since $c_i\phi_{s-r} \geq i - k_d \geq c_i\phi_{s-r-1}$, for any s there is at most one specific r which satisfies conditions of W^a. This implies that computation of all feasible entries of W^a is in $\mathcal{O}(m)$. Therefore, any row of W has at most one feasible entry of W^a.

Next, we show that computing all feasible entries of W^b is in $\mathcal{O}(m)$. From the second structure of Lemma 4, for any $\hat{s}, \hat{r}$ and $\hat{i} = m - \hat{s} + 1$, if $\beta_{\hat{s}-1} > 1$ ($\beta_{\hat{s}-1} < 0$), $(i, \hat{i} + r)^{\text{th}}$ entry of W is infeasible for all $i > \hat{i}, r > \hat{r}$ ($i < \hat{i}, r < \hat{r}$) since it implies $\beta_{s-1} > 1$ ($\beta_{s-1} < 0$). Therefore, at every entry of W, β_{s-1}

provides a criteria for which the rest of entries, in the same row and in the same column are entirely infeasible, and consequently it is not required to check the feasibility of those entries. In other words, value of β_{s-1} provides a criteria for direction of searching for feasible entries of W^b. Thus, computing feasible entries of W^b is in $\mathcal{O}(m)$. □