

# Randomized Sampling for Large Zero-Sum Games<sup>☆,☆☆</sup>

Shaunak D. Bopardikar<sup>a,\*</sup>, Alessandro Borri<sup>b</sup>, João P. Hespanha<sup>c</sup>, Maria Prandini<sup>d</sup>, Maria D. Di Benedetto<sup>b</sup>

<sup>a</sup>United Technologies Research Center Inc., Berkeley, CA, USA

<sup>b</sup>Department of Electrical and Information Engineering, University of L'Aquila, Italy

<sup>c</sup>Center for Control, Dynamical Systems and Computation, University of California at Santa Barbara, CA 93106, USA

<sup>d</sup>Dipartimento di Eletttronica e Informazione of the Politecnico di Milano, Italy

---

## Abstract

This paper addresses the solution of large zero-sum matrix games using randomized methods. We formalize a procedure, termed as *sampled saddle point (SSP)*, by which a player can compute mixed policies that, with a high confidence, are security policies against an adversary playing the same game and who is also using the SSP procedure. The computational savings result from solving stochastically sampled subgames that are much smaller than the original game. We provide two methodologies and determine how large the subgames should be to guarantee the desired level of confidence. The first methodology provides a game-independent bound on the size of the subgames that can be computed a-priori. The second methodology is useful when computation limitations prevent a player from satisfying the first game-independent bound and provides a high-probability bound on how much the outcome of the game can violate the precomputed security level. We also derive bounds on the sizes of subgames in the case of mismatch between the distributions used by the two players to obtain their respective subgames using the SSP procedure. We demonstrate the usefulness of these results in solving a hide-and-seek game that is known to exhibit exponential complexity.

*Keywords:* Game theory, Randomized algorithms, Zero-Sum Games, Optimization

---

## 1. Introduction

A zero-sum matrix game is played between a minimizer who selects a row, and a maximizer who selects a column from a matrix, with the pay-off given by the corresponding entry of the matrix. While a large number of robust design problems can be formulated as zero-sum matrix games, in practice, such games lead to extremely large — often infinite — matrices. This is the case in combinatorial problems, where the decision makers are faced with a number of possible options that increases exponentially with the size of the problem; for example, in path planning problems where the number of paths increases combinatorially with the number of points to visit [cf. Bellman (1962)]. Large zero-sum matrix games also arise in partial information feedback games [cf. Hespanha and Prandini (2001)] wherein optimal strategies are functions of the players' past actions and observations and thus, the number of strategies grows exponentially with the size of the players' action spaces.

Inspired by the use of randomized approaches to solve optimization problems, we consider an approach to solve very large zero-sum matrix games by using randomized sampling. Each player reduces her search space by taking a random sample of the available actions to construct a much smaller version of the original game. Players then solve these smaller games and utilize the saddle-point policies so obtained against each other. We call this procedure the *sampled saddle-point (SSP)* algorithm. Since each player only considers a small submatrix of the original game, the two players typically consider very different submatrices. Therefore, the saddle-point policies obtained by this process will generally not be security policies for the whole game. This means that each player may obtain an outcome that is strictly worse than the value computed based on her submatrix. However, we show that this happens with low probability as long as the size of the submatrix is sufficiently large.

In this framework, a reasonable notion of security policy for a player is that the outcome of the game should not be much larger than what the minimizer expects or much smaller than what the maximizer expects, based on the computation of the value of her submatrix. In this paper, we analyze the SSP algorithm for zero-sum games

---

<sup>☆</sup>This material is based upon work supported in part by ARO MURI Grant number W911NF0910553, in part by the Center of Excellence for Research DEWS, University of L'Aquila, Italy, and in part by the European Commission under the MoVeS project, FP7-ICT-2009-257005.

<sup>☆☆</sup>A preliminary version of this work entitled "Randomized Sampling for Large Zero-Sum Games" was presented at the 2010 IEEE Conference on Decision and Control, Atlanta, GA, USA.

\*Corresponding author. This work was performed while this author was at the University of California Santa Barbara, CA, USA.

*Email addresses:* bshaunak@gmail.com (Shaunak D. Bopardikar), alessandro.borri@univaq.it (Alessandro Borri), hespanha@ece.ucsb.edu (João P. Hespanha), prandini@elet.polimi.it (Maria Prandini), mariadomenica.dibenedetto@univaq.it (Maria D. Di Benedetto)

and provide conditions under which it leads to a security policy with high probability.

### Related Work

Two-player zero-sum matrix games have been studied extensively over the past decades [cf. the textbook by Basar and Olsder (1999)]. The classical Mini-Max theorem [cf. Von Neumann (1928)] guarantees the existence of an optimal pair of strategies for the two players, each of which is a security policy for the corresponding player. However, when the matrix is of large size, the computation of the optimal strategies involves solving optimization problems with a large number of variables and constraints.

A probabilistic approach has proven to be computationally efficient in evaluating games with large sizes. Using probabilistic analysis, the existence of simple, near-optimal strategies over a subset with logarithmically smaller size of the original matrix game was established in Lipton and Young (1994). A popular method to solve win-lose type of multi-stage or dynamic games is to evaluate the root of a game tree, in which every node is alternately an *AND* and an *OR* operation, while the leaves have a value of either 0 or 1. Motwani and Raghavan (1995) present randomized algorithms to evaluate such game trees more efficiently than using deterministic algorithms.

Randomized methods have been successful in providing efficient solutions to complex control design problems with probabilistic guarantees. Khargonekar and Tikku (1996) adopt a probabilistic approach to show the existence of randomized algorithms with polynomial complexity to solve complex robust stability analysis problems. Tempo et al. (1997) propose a randomized method for a probabilistic analysis of the worst-case controller performance, and determine sample size bounds. A randomized approach is used in the linear programming reformulation of approximate dynamic programming in de Farias and Roy (2004). Vidyasagar (1998); Vidyasagar and Blondel (2001) demonstrate the use of randomized algorithms to solve control design problems and a number of well known complex problems in matrix theory through a statistical learning approach. Statistical learning theory [cf. Vapnik (1998)] provides a framework for probabilistic robust control synthesis. Using these tools, Alamo et al. (2009) consider semi-infinite optimization problems under uncertainty with a possibly non-convex objective function.

In Calafiore and Campi (2006); Campi and Garatti (2008); Campi and Calafiore (2009), the authors introduce the so-called *scenario approach* to solve convex optimization problems with an infinite number of constraints. Possible applications of this approach to systems and control are discussed in Campi et al. (2009). In Alamo et al. (2010), the authors study the sample complexity of randomized approaches to system analysis and design, and provide, in particular, an explicit expression of the sample-size for the scenario approach to convex optimization based on an approximation of the implicit expression given in Campi and Garatti (2008). The results in these papers

are instrumental to establish several of the results in the present paper.

### Contributions

The contributions of this paper are four-fold. First, based on results from the scenario approach, we show that when the sizes of the subgames solved by each player are sufficiently large, the SSP algorithm provides security policies for both players with some pre-specified high probability  $1 - \delta$ . The bounds on the sizes of the subgames are *game independent* and are computable a-priori. Not surprisingly, they grow with the desired confidence level  $1 - \delta$ . However, they are *independent of the size of the original matrix game*, which could, in fact, be even infinite and not even have a value.

Second, we propose a methodology that provides an a-posteriori, high-probability bound on the deviation of the game outcome from the pre-computed security level. In particular, regardless of the size of the subgames solved by each player, we provide a high-probability bound on how much a player can expect the outcome of the game to violate the security value computed based on the submatrix used to determine her saddle-point equilibrium. This bound is computed after a player selects and solves her subgame.

The above two contributions refer to the case when the players use identical distributions to select their subgames. We then analyze the effect of a mismatch between the sampling distributions used by the players via two approaches. The first approach adopts sample complexity bounds obtained in Erdoğan and Iyengar (2006), which deals with the so-called *ambiguous chance constrained problems*. More precisely, we determine bounds on the sizes of the submatrices in the SSP algorithm for players using different distributions that are within a specified distance  $\rho < 1$ , measured in the Prohorov metric. This approach requires no knowledge of the original matrix, but the bounds hold only when the confidence parameter satisfies the condition  $\delta > \rho$ . We then provide a second approach based on a different characterization of the mismatch between the sampling distributions, and determine bounds on the sizes of the submatrices for which the SSP algorithm provides security policies with high probability. In comparison to the first approach, the bounds in the second approach hold for any  $\delta$ , but require the knowledge of the entries of the original matrix of the game. Further, we show that when the mismatch is associated with policy domination in the matrix game, then the bounds in the latter approach reduce to the sample complexity bounds of the case of no mismatch. This means that, if the minimizer figures out that a set of actions for the other player would always lead to a larger outcome than another set of actions, then the minimizer can secure herself by sampling actions out of the former set instead of the latter set, without any change in the probabilistic bounds.

Fourth and finally, we apply the methodologies to solve a hide-and-seek game, in which one player hides a treasure

in one of  $N$  points and the other player searches for the treasure by visiting each of the points. This is formalized as a zero-sum game in which the player that hides the treasure wants to maximize the distance that the other player needs to travel until the treasure is found. To determine the optimal strategy for this game, one needs to solve a matrix game whose size is  $N \times N!$ . Thus, exact solutions to this problem require computation that scales exponentially with the number of points  $N$ . Our approach is *independent of the size of the game* and therefore the size of the matrix plays no role in the amount of computation required.

As compared to the preliminary conference version [cf. Bopardikar et al. (2010)], this paper presents new results on mismatch in the distributions used by the players to construct the subgames, and improves upon the *explicit* sample size bounds based on results from Alamo et al. (2010).

### Organization

This paper is organized as follows. The problem formulation and the SSP algorithm are presented in Section 2. Bounds on probabilistic guarantees when the two players use identical distributions to sample the matrix are established in Section 3. These bounds are extended in Section 4 to allow mismatch between the distributions. Finally, we demonstrate the procedure applied to the hide-and-seek problem in Section 5.

## 2. Sampled Saddle-Point Algorithm

Consider a zero-sum matrix game defined by an  $M \times N$  matrix  $A$ , in which player  $P_1$  is the minimizer and selects rows and player  $P_2$  is the maximizer and selects columns. We are interested in problems for which the matrix  $A$  is too large to permit the computation of mixed saddle-points and therefore the players are forced to consider only submatrices of  $A$  to select their policies. This scenario motivates the introduction of the *sampled saddle-point (SSP) Algorithm 1*.

We call the outcomes  $\bar{V}(A_1)$  and  $\underline{V}(A_2)$  of Algorithm 1 the *sampled security values of the game* for  $P_1$  and  $P_2$ , respectively. Similarly, we call  $y^*$  and  $z^*$  the *sampled security policies* for players  $P_1$  and  $P_2$ , respectively.

We say that *the SSP algorithm is  $\epsilon$ -secure for player  $P_1$  with confidence  $1 - \delta$*  if

$$P_{\Gamma_1, \Pi_1, \Gamma_2, \Pi_2} (y^{*'} A z^* \leq \bar{V}(A_1) + \epsilon) \geq 1 - \delta. \quad (1)$$

Here and in the sequel, we use a subscript in the probability measure  $P$  to emphasize which random variables define the event that is being measured. In essence, condition (1) states that the probability that the outcome of the game will violate  $P_1$ 's sampled security value by more than  $\epsilon$  is smaller than  $\delta$ . Similarly, we say that *the SSP algorithm is  $\epsilon$ -secure for player  $P_2$  with confidence  $1 - \delta$*  if

$$P_{\Gamma_1, \Pi_1, \Gamma_2, \Pi_2} (y^{*'} A z^* \geq \underline{V}(A_2) - \epsilon) \geq 1 - \delta. \quad (2)$$

---

### Algorithm 1 [SSP algorithm]

---

- 1: Each player  $P_k$ ,  $k \in \{1, 2\}$  randomly selects  $m_k$  rows and  $n_k$  columns of  $A$ , which she uses to construct an  $m_k \times n_k$  submatrix  $A_k$  of  $A$ . Denoting by  $\mathcal{B}^{k \times \ell}$  the set of  $k \times \ell$  left-stochastic  $(0, 1)$ -matrices (i.e., matrices whose entries belong to the set  $\{0, 1\}$  and whose columns add up to one), we can express the process of constructing each submatrix  $A_k$  by randomly selecting two random matrices  $\Gamma_k \in \mathcal{B}^{M \times m_k}$  and  $\Pi_k \in \mathcal{B}^{N \times n_k}$  and then computing the product:

$$A_k = \Gamma_k' A \Pi_k.$$

- 2: Each player  $P_k$ ,  $k \in \{1, 2\}$  computes the mixed security value and the corresponding security policy for her submatrix  $A_k$ :

$$\bar{V}(A_1) = \max_{z \in \mathcal{S}_{n_1}} y_1^{*'} A_1 z = \min_{y \in \mathcal{S}_{m_1}} \max_{z \in \mathcal{S}_{n_1}} y' A_1 z$$

$$\underline{V}(A_2) = \min_{y \in \mathcal{S}_{m_2}} y' A_2 z_2^* = \max_{z \in \mathcal{S}_{n_2}} \min_{y \in \mathcal{S}_{m_2}} y' A_2 z$$

where  $y_1^*$  (resp.  $z_2^*$ ) is a mixed security policy for  $P_1$  (resp.  $P_2$ ) in the submatrix game  $A_1$  (resp.  $A_2$ ).  $\mathcal{S}_{m_k}$  and  $\mathcal{S}_{n_k}$  denote the probability simplexes of appropriate dimensions.

- 3: Player  $P_1$  selects a row according to the distribution  $y_1^*$ , whereas  $P_2$  selects a column according to the distribution  $z_2^*$ , which correspond to the following policies for the original game:  $y^* := \Gamma_1 y_1^*$ ,  $z^* := \Pi_2 z_2^*$  and the following game outcome:

$$y^{*'} A z^* = y_1^{*'} \Gamma_1' A \Pi_2 z_2^*.$$


---

The previous definitions guarantee that the two players will be surprised with (low) probability  $\delta$  when playing with policies obtained from a one-shot solution to the SSP algorithm. However, no specific guarantee is given regarding the inherent safety of the policies/values obtained using this algorithm. So, e.g., suppose that player  $P_1$  computes  $y^*$  once using the SSP algorithm and then plays this policy multiple times against a sequence of policies  $z^*$  that  $P_2$  obtained by running the SSP algorithm multiple times,  $P_1$  could conceivably be surprised many more times that one would expect for a low value of  $\delta$ . This would happen if she was “unlucky” and got a particular (low probability)  $y^*$  that is particularly bad or a value  $\bar{V}(A_1)$  that is particularly optimistic. To avoid this scenario, we introduce additional notions of security that refer to specific policies/values: we say that *a policy  $y^*$  with value  $\bar{V}(A_1)$  is  $\epsilon$ -secure for player  $P_1$  with confidence  $1 - \delta$*  if

$$P_{\Gamma_2, \Pi_2} (y^{*'} A z^* \leq \bar{V}(A_1) + \epsilon \mid y^*, \bar{V}(A_1)) \geq 1 - \delta \quad (3)$$

and that *a policy  $z^*$  with value  $\underline{V}(A_2)$  is  $\epsilon$ -secure for player  $P_2$  with confidence  $1 - \delta$*  if

$$P_{\Gamma_1, \Pi_1} (y^{*'} A z^* \geq \underline{V}(A_2) - \epsilon \mid z^*, \underline{V}(A_1)) \geq 1 - \delta.$$

Note that the subscripts in the probability measure now only include the matrices corresponding to random extractions by the other player, since the probability guarantees are given for specific policies and values of one player.

So far, we have not specified the joint distribution of the row/column extraction matrices  $\Gamma_1, \Gamma_2, \Pi_1, \Pi_2$ , but this distribution will clearly affect the outcomes of the algorithm. In the context of noncooperative games, one should presume the extractions of the two players to be independent of each other. For simplicity, we will further assume that players extract rows and columns independently, as stated in the following assumption:

**Assumption 2.1 (Independence)** *The random matrices  $\Gamma_1, \Pi_1, \Gamma_2, \Pi_2$  are statistically independent and each of them has independent and identically distributed columns.*

**Remark 2.1 (Non-matrix games)** The results in this paper do not depend on the fact that the original game is a matrix game. They extend trivially to any cost-function  $J(u, d)$ ,  $u \in \mathcal{U}$ ,  $d \in \mathcal{D}$  where  $\mathcal{U}$  and  $\mathcal{D}$  denote the sets of policies for the minimizer and maximizer, respectively. In fact, it is not even necessary that the original game has saddle-point policies since all that the SSP algorithm uses is the fact that when we take finite samples of the sets of policies, we obtain finite matrix games. ■

**Remark 2.2 (Non-unique security policies)** When the matrices  $A_1$  and  $A_2$  have multiple security policies, the SSP algorithm does not specify *which* of these should be used to define the sampled security policies. However, the choice of security policy may have a significant effect on the value of the probabilities in (1) and (2). The results in the scenario approach, which we will subsequently use, hold under the assumption that the solution to the sampled convex program exists and is unique. If this is not the case, then, in Campi and Garatti (2008), it is suggested to break the tie by selecting the solution with the minimum Euclidean norm for the results of the scenario approach to still hold. This rule can be applied to choose from the non-unique security policies. ■

### 3. Bounds for Probabilistic Guarantees

In this section, we present theoretical bounds on the size of the submatrices that guarantee that the SSP algorithm and the resulting policies are probabilistically secure. The results of this section focus on the case when the players sample their submatrices from identical distributions. This assumption will be relaxed in Section 4.

#### 3.1. A-priori Bounds

The main result of this section provides an a-priori bound on the size of the submatrices for the players that guarantees  $\epsilon$ -security with  $\epsilon = 0$ . We state the result for player  $P_1$ . The result for  $P_2$  is analogous.

**Theorem 3.1 (A-priori bounds)** *Suppose that Assumption 2.1 holds and that  $\Pi_1$  and  $\Pi_2$  have identically distributed columns. Let  $\delta \in (0, 1)$ . If  $n_1$  satisfies*

$$n_1 = \left\lceil \frac{m_1 + 1}{\delta} - 1 \right\rceil \bar{n}_2 \quad (4)$$

for some  $\bar{n}_2 \geq n_2$ , then the SSP algorithm is  $\epsilon = 0$ -secure for  $P_1$  with confidence  $1 - \delta$ .

If  $n_1$  is further increased so as to satisfy

$$n_1 = \left\lceil \frac{1}{\delta} \left( \ln \frac{1}{\beta} + m_1 + \sqrt{2m_1 \ln \frac{1}{\beta}} \right) \right\rceil \bar{n}_2 \quad (5)$$

for some  $\beta \in (0, 1)$ , then, with probability<sup>1</sup> higher than  $1 - \beta$ , the policy  $y^*$  with value  $\bar{V}(A_1)$  is  $\epsilon = 0$ -secure for  $P_1$  with confidence  $1 - \delta$ .

In words, this results states that it is always possible to guarantee  $\epsilon = 0$ -security for  $P_1$ , if she constructs her submatrix  $A_1$  utilizing a sufficiently large number of columns. In particular, she always needs to choose a number of columns  $n_1$  larger than the number of columns  $n_2$  that  $P_2$  is considering for her mixed policies [cf. (4) and (5)]. The additional number of columns that  $P_1$  needs to consider is a function of the number  $m_1$  of rows that  $P_1$  wants to consider for her mixed policy and the desired confidence levels.

The confidence level  $1 - \beta$  that appears in the bound (5) for  $P_1$ 's policy-specific probabilistic guarantees refers to the probability that the bound fails altogether due to an "unfortunate" sample used by  $P_1$  to compute the policy  $y^*$ . However, note that only the logarithm of the confidence level  $\beta$  appears in bounds regarding the security of  $y^*$ . One can therefore make  $\beta$  extremely small with a relatively small additional computational cost.

In the probabilistic guarantees provided by Theorem 3.1 with (4), the confidence  $1 - \delta$  refers to the extraction of all the row/column matrices  $\Gamma_1, \Gamma_2, \Pi_1, \Pi_2$  as in (1). However, for the probabilistic guaranteed with (5), the confidence  $1 - \delta$  refers to the extraction of  $\Gamma_2, \Pi_2$  as in (3), whereas the confidence  $1 - \beta$  refers solely to the extraction of the matrix  $\Pi_1$  and holds for any given matrix  $\Gamma_1$  (as shown in the proof).

**Remark 3.2 ( $P_1$ 's knowledge of  $n_2$ )** According to Theorem 3.1, for player  $P_1$  to enjoy guaranteed  $\epsilon = 0$ -security with confidence  $1 - \delta$ , she must know an upper bound  $\bar{n}_2$  on the number of columns that  $P_2$  is using to construct her submatrix  $A_2$ . Even if  $P_1$  does not know  $\bar{n}_2$  precisely and, e.g., underestimates  $\bar{n}_2$  by a certain percentage, then (4) and (5) are still useful in that they predict that the performance degradation in the confidence level  $\delta$  should grow proportionately with  $\bar{n}_2$ . This is because the bounds in (4) and (5) essentially scale with  $\bar{n}_2/\delta$ . ■

<sup>1</sup>The confidence level  $\beta$  for  $P_1$  refers solely to the extraction of the matrix  $\Pi_1$  and holds for any given matrix  $\Gamma_1$ .

Suppose that one of the player, say  $P_1$ , restricts herself to pure policies instead of mixed policies. Then, she will apply the following procedure.

---

**Algorithm 2 [SSP algorithm with pure policies]**

---

- 1:  $P_1$  randomly selects two matrices  $\Gamma_1 \in \mathcal{B}^{M \times m_1}$  and  $\Pi_1 \in \mathcal{B}^{N \times n_1}$  and then computes the product:

$$A_1 = \Gamma_1' A \Pi_1.$$

- 2:  $P_1$  computes the pure security value and the corresponding pure security policy for her submatrix  $A_1$ :

$$\begin{aligned} \bar{V}_p(A_1) &= \max_{z \in \mathcal{S}_{n_1}} e_{i^*}(m_1)' A_1 z \\ &= \min_{i \in \{1, \dots, m_1\}} \max_{z \in \mathcal{S}_{n_1}} e_i(m_1)' A_1 z, \\ y_1^* &= e_{i^*}(m_1), \end{aligned}$$

where  $e_i(m_1)$  denotes the  $i$ th element of the canonical basis of  $\mathbb{R}^{m_1}$ .

- 3:  $P_1$  selects row  $i^*$  of  $A_1$ , which corresponds to the following sampled pure policy for the original game:  $y_p^* := \Gamma_1 y_1^*$ .
- 

A bound similar to (5) can be established for a sampled pure security policy  $y_p^*$  with pure security level  $\bar{V}_p(A_1)$ . This bound holds irrespectively of the fact that player  $P_2$  adopts a pure rather than a mixed policy.

**Theorem 3.3 (Bound with pure policies)** *Suppose that Assumption 2.1 holds and that  $\Pi_1$  and  $\Pi_2$  have identically distributed columns. Let  $\text{dis}(\Gamma_1 A)$  denote the number of distinct entries in the submatrix  $\Gamma_1 A$ , and  $\delta \in (0, 1)$ . If  $n_1$  satisfies*

$$n_1 = \left\lceil \frac{1}{\delta} \ln \frac{m_1 \cdot \text{dis}(\Gamma_1 A)}{\beta} \right\rceil \bar{n}_2,$$

for some  $\beta \in (0, 1)$  and  $\bar{n}_2 \geq n_2$ , then with probability higher than  $1 - \beta$ , the sampled pure policy  $y_p^*$  with the pure security value  $\bar{V}_p(A_1)$  obtained through Algorithm 2 is  $\epsilon = 0$ -secure for  $P_1$  with confidence  $1 - \delta$ .

In several matrix games, e.g., situations of win-lose-tie, the number of distinct entries in the matrix  $A$ , and therefore  $\text{dis}(\Gamma_1 A)$ , is small. Even if this is not the case, computational savings occur even for a large size  $N$  of matrix  $A$  since  $\text{dis}(\Gamma_1 A) \leq m_1 N$  and, hence,  $n_1$  depends logarithmically on  $N$ . Note that Theorem 3.3 provides a significant improvement with respect to Theorem 3.1 in terms of computational complexity, since  $n_1$  only grows with the logarithm of  $m_1$  instead of linearly as in (5). However, the corresponding pure security level  $\bar{V}_p(A_1)$  could be much higher than the one obtained with mixed policies  $\bar{V}(A_1)$ . Thus, pure policies are useful to consider only if faced with computational difficulties.

We now present the proof of Theorem 3.1.

*Proof of Theorem 3.1:* By definition of the security value  $\bar{V}(A_1)$ , we have that

$$\begin{aligned} \bar{V}(A_1) &= \min_{y \in \mathcal{S}_{m_1}} \max_{z \in \mathcal{S}_{n_1}} y' \Gamma_1' A \Pi_1 z \\ &= \min_{y \in \mathcal{S}_{m_1}} \max_{j \in \{1, \dots, n_1\}} y' \Gamma_1' A \Pi_1 e_j(n_1) \\ &= \min_{\theta \in \Theta} \left\{ v : y' \Gamma_1' A \Pi_1 e_j(n_1) \leq v, \forall j \in \{1, \dots, n_1\} \right\}, \end{aligned} \quad (6)$$

where the notation  $e_j(n)$  denotes the  $j$ th element of the canonical basis of  $\mathbb{R}^n$ ,  $\theta := (y_1, v)$ , and  $\Theta := \mathcal{S}_{m_1} \times \mathbb{R}$ .

Since  $n_1$  is an integer multiple of  $\bar{n}_2$ , i.e.,  $n_1 = K \bar{n}_2$  with  $K = \left\lceil \frac{m_1 + 1}{\delta} - 1 \right\rceil$ , we can take the  $K \bar{n}_2$  columns of  $\Pi_1 \in \mathcal{B}^{N \times K \bar{n}_2}$  to construct  $K$  independent and identically distributed (i.i.d.) matrices  $\Delta_1, \Delta_2, \dots, \Delta_K$ , each in the set  $\mathcal{B}^{N \times \bar{n}_2}$ . If we then define the function  $f_\Gamma : \Theta \times \mathcal{B}^{N \times \bar{n}_2}$ , parameterized by  $\Gamma \in \mathcal{B}^{M \times m_1}$

$$f_\Gamma(\theta, \Delta) = \max_{j \in \{1, \dots, \bar{n}_2\}} y_1' \Gamma' A \Delta e_j(\bar{n}_2) - v, \quad (7)$$

we can rewrite (6) as

$$\bar{V}(A_1) = \min_{\theta \in \Theta} \left\{ v : f_{\Gamma_1}(\theta, \Delta_i) \leq 0, \forall i \in \{1, \dots, K\} \right\},$$

Let the minimum above be achieved for some  $\theta^* = (y_1^*, \bar{V}(A_1))$ . For any given realization of the matrix  $\Gamma_1$  (which is independent of the  $\Delta_i$  by Assumption 2.1) we conclude from (Campi and Calafiore, 2009, Proposition 3) that the (conditional) probability that another matrix  $\Delta$  sampled independently from the same distribution as the  $\Delta_i$  satisfies the constraint  $f_{\Gamma_1}(\theta^*, \Delta) \leq 0$  can be lower-bounded as follows:

$$P_{\Pi_1, \Delta} (f_{\Gamma_1}(\theta^*, \Delta) \leq 0 \mid \Gamma_1) \geq \frac{K - m_1}{K + 1} \geq 1 - \delta, \quad (8)$$

where the second inequality is a consequence of (4). Using the definition of  $f_\Gamma$  and  $\theta^*$ , we can re-write (8) as

$$\begin{aligned} P_{\Pi_1, \Delta} (y_1^{*'} \Gamma_1' A \Delta e_j(\bar{n}_2) \leq \bar{V}(A_1), \\ \forall j \in \{1, \dots, \bar{n}_2\} \mid \Gamma_1) \geq 1 - \delta. \end{aligned}$$

Since  $n_2 \leq \bar{n}_2$ , we further conclude that

$$\begin{aligned} P_{\Pi_1, \Delta} (y_1^{*'} \Gamma_1' A \Delta e_j(n_2) \leq \bar{V}(A_1), \\ \forall j \in \{1, \dots, n_2\} \mid \Gamma_1) \geq 1 - \delta. \end{aligned}$$

Under Assumption 2.1, when the columns of  $\Pi_1$  and  $\Pi_2$  are identically distributed, the matrix consisting of the first  $n_2$  columns of  $\Delta$  can be viewed as the matrix  $\Pi_2$  and we conclude from the inequality above that

$$\begin{aligned} P_{\Pi_1, \Pi_2} (y_1^{*'} \Gamma_1' A \Pi_2 e_j(n_2) \leq \bar{V}(A_1), \\ \forall j \in \{1, \dots, n_2\} \mid \Gamma_1) \geq 1 - \delta. \end{aligned}$$

Since

$$\begin{aligned} y_1^* \Gamma_1' A \Pi_2 e_j(n_2) &\leq \bar{V}(A_1), \forall j \in \{1, \dots, n_2\} \Rightarrow \\ y_1^* \Gamma_1' A \Pi_2 z &\leq \bar{V}(A_1), \forall z \in \mathcal{S}^{n_2}, \end{aligned}$$

we conclude that

$$\mathbb{P}_{\Pi_1, \Gamma_2, \Pi_2} (y_1^* \Gamma_1' A \Pi_2 z_2^* \leq \bar{V}(A_1) \mid \Gamma_1) \geq 1 - \delta.$$

We have shown that this bound holds for an arbitrary realization of  $\Gamma_1$ , therefore it also holds for the unconditional probability, which shows that the SSP algorithm is  $\epsilon = 0$ -secure for  $\mathbb{P}_1$  with confidence  $1 - \delta$ .

If instead of applying (Campi and Calafiore, 2009, Proposition 3) we apply (Alamo et al., 2010, Theorem 4), then using (5), we conclude that

$$\mathbb{P}_\Delta (f_{\Gamma_1}(\theta^*, \Delta) \leq 0 \mid \Gamma_1, \theta^*) \geq 1 - \delta \quad (9)$$

with probability higher than  $1 - \beta$ , where the confidence level  $1 - \beta$  refers to the extraction of  $\Pi_1 = [\Delta_1, \dots, \Delta_K]$  that defines  $\theta^*$  (given  $\Gamma_1$ ). The proof can now proceed exactly as before, but with (8) replaced by inequality (9), which now involves a probability conditioned to  $y^*$  and  $\bar{V}(A_1)$ . This shows that if  $n_1$  satisfies (5), then with probability higher than  $1 - \beta$ , the policy  $y^*$  with value  $\bar{V}(A_1)$  is  $\epsilon = 0$ -secure for  $\mathbb{P}_1$  with confidence  $1 - \delta$ . ■

The proof of Theorem 3.3 is similar to the second part of the proof of Theorem 3.1, with the main difference being that the policy selection involves optimizing over a finite set of cardinality  $\text{dis}(\Gamma_1 A)$ , and, hence, one can use the bounds in (Alamo et al., 2010, Theorem 3) instead of those in (Alamo et al., 2010, Theorem 4).

*Proof of Theorem 3.3:* By the definition of the pure security value, we have that

$$\begin{aligned} \bar{V}_p(A_1) &= \min_{i \in \{1, \dots, m_1\}} \max_{z \in \mathcal{S}_{n_1}} e_i(m_1) \Gamma_1' A \Pi_1 z \\ &= \min_{i \in \{1, \dots, m_1\}} \max_{j \in \{1, \dots, n_1\}} e_i(m_1) \Gamma_1' A \Pi_1 e_j(n_1) \\ &= \min_{\theta \in \Theta} \{v : e_i(m_1) \Gamma_1' A \Pi_1 e_j(n_1) \leq v, \forall j \in \{1, \dots, n_1\}\}, \end{aligned} \quad (10)$$

where  $\theta := (e_i(m_1), v)$ , and  $\Theta := \text{Basis}(\mathbb{R}^{m_1}) \times D(\Gamma_1 A)$ , where  $\text{Basis}(\mathbb{R}^{m_1})$  denotes the canonical basis on  $\mathbb{R}^{m_1}$  and  $D(\Gamma_1 A)$  denotes the set of distinct entries in the matrix  $\Gamma_1 A$ . In other words, the cardinality of  $\Theta$  is  $m_1 \cdot \text{dis}(\Gamma_1 A)$ .

Since  $n_1$  is an integer multiple of  $\bar{n}_2$ , i.e.,  $n_1 = K \bar{n}_2$  with  $K = \left\lceil \frac{1}{\delta} \ln \frac{m_1 \cdot \text{dis}(\Gamma_1 A)}{\beta} \right\rceil$ , we can take the  $K \bar{n}_2$  columns of  $\Pi_1 \in \mathcal{B}^{N \times K \bar{n}_2}$  to construct  $K$  i.i.d. matrices  $\Delta_1, \Delta_2, \dots, \Delta_K$ , each in the set  $\mathcal{B}^{N \times \bar{n}_2}$ . If we define the function  $g_\Gamma : \Theta \times \mathcal{B}^{N \times \bar{n}_2}$  parameterized by  $\Gamma \in \mathcal{B}^{M \times m_1}$

$$g_\Gamma(\theta, \Delta) = \begin{cases} 0, & \max_{j \in \{1, \dots, \bar{n}_2\}} e_i(m_1) \Gamma' A \Delta e_j(\bar{n}_2) - v \leq 0, \\ 1, & \text{otherwise,} \end{cases}$$

then we can rewrite (10) as

$$\bar{V}_p(A_1) = \min_{\theta \in \Theta} \left\{ v : \sum_{k=1}^K g_{\Gamma_1}(\theta, \Delta_k) \leq 0 \right\},$$

Let the minimum above be achieved for some  $\theta^* = (e_{i^*}(m_1), \bar{V}_p(A_1))$ . For any given realization of the matrix  $\Gamma_1$ , we conclude from (Alamo et al., 2010, Theorem 3) that the (conditional) probability that another matrix  $\Delta$  sampled independently from the same distribution as the  $\Delta_i$  satisfies the constraint  $g_{\Gamma_1}(\theta^*, \Delta) = 0$  can be lower-bounded as follows:

$$\mathbb{P}_\Delta (g_{\Gamma_1}(\theta^*, \Delta) = 0 \mid \Gamma_1, \theta^*) \geq 1 - \delta,$$

with probability higher than  $1 - \beta$ , where the confidence level  $1 - \beta$  refers to the extraction of  $\Pi_1 = [\Delta_1, \dots, \Delta_K]$  that defines  $\theta^*$  (given  $\Gamma_1$ ). Based on the definition of  $\theta$  and  $g_{\Gamma_1}(\theta, \Delta)$ , this is equivalent to

$$\begin{aligned} \mathbb{P}_\Delta (e_{i^*}(m_1) \Gamma_1' A \Delta e_j(\bar{n}_2) \leq \bar{V}_p(A_1), \forall j \in \{1, \dots, \bar{n}_2\} \\ \mid \Gamma_1, e_{i^*}(m_1), \bar{V}_p(A_1)) \geq 1 - \delta. \end{aligned}$$

Since  $n_2 \leq \bar{n}_2$ , we further conclude that

$$\begin{aligned} \mathbb{P}_\Delta (e_{i^*}(m_1) \Gamma_1' A \Delta e_j(n_2) \leq \bar{V}_p(A_1), \forall j \in \{1, \dots, n_2\} \\ \mid \Gamma_1, e_{i^*}(m_1), \bar{V}_p(A_1)) \geq 1 - \delta. \end{aligned}$$

Due to Assumption 2.1, when the columns of  $\Pi_1$  and  $\Pi_2$  are identically distributed, the matrix consisting of the first  $n_2$  columns of  $\Delta$  can be viewed as the matrix  $\Pi_2$  and we conclude from the inequality above that

$$\begin{aligned} \mathbb{P}_{\Pi_2} (e_{i^*}(m_1) \Gamma_1' A \Pi_2 e_j(n_2) \leq \bar{V}_p(A_1), \forall j \in \{1, \dots, n_2\} \\ \mid \Gamma_1, e_{i^*}(m_1), \bar{V}_p(A_1)) \geq 1 - \delta. \end{aligned}$$

Since

$$\begin{aligned} e_{i^*}(m_1) \Gamma_1' A \Pi_2 e_j(n_2) \leq \bar{V}_p(A_1), \forall j \in \{1, \dots, n_2\} \\ \Rightarrow e_{i^*}(m_1) \Gamma_1' A \Pi_2 z_2^* \leq \bar{V}_p(A_1), \end{aligned}$$

where  $z^*$  is the sampled security policy for player  $\mathbb{P}_2$ , we conclude that

$$\mathbb{P}_{\Gamma_2, \Pi_2} (y_p^* A z_2^* \leq \bar{V}_p(A_1) \mid y_p^*, \bar{V}_p(A_1)) \geq 1 - \delta.$$

This shows that, with probability higher than  $1 - \beta$ , the sampled pure policy  $y_p^*$  with pure security level  $\bar{V}_p(A_1)$  is  $\epsilon = 0$ -secure for  $\mathbb{P}_1$  with confidence  $1 - \delta$ . ■

### 3.2. A-posteriori Probabilistic Guarantees

Suppose that, due to computational limitations, player  $\mathbb{P}_1$  cannot satisfy the bounds in Theorem 3.1 to obtain  $\epsilon = 0$ -security for a given level of confidence  $1 - \delta$ . One option to overcome this difficulty would be to settle for a lower level of confidence until the bounds in Theorem 3.1 hold for a value of  $n_1$  that is computationally acceptable

---

**Algorithm 3 [SSP algorithm with a-posteriori guarantees]**


---

- 1:  $P_1$  picks values for  $m_1, n_1$  and executes the SSP Algorithm 1 to compute a sampled security policy  $y^* = \Gamma_1 y_1^*$ , and the corresponding sampled security value  $\bar{V}(A_1)$ .
- 2: Using the column distribution of  $\Pi_1$ ,  $P_1$  randomly select a matrix  $\bar{\Pi}_1 \in \mathcal{B}^{N \times k_1}$  and computes

$$\bar{v} = \max_{j \in \{1, \dots, k_1\}} y^{*'} A \bar{\Pi}_1 e_j(k_1), \quad (11)$$

where  $e_j(k_1)$  denotes the  $j$ th element of the canonical basis of  $\mathbb{R}^{k_1}$ .

---

for  $P_1$ . However, one may desire to maintain the same high level of confidence, and instead accept a *violation*  $\epsilon$  of the sampled security value. In this section, we explore this option, which is not covered by Theorem 3.1.

The following result provides an a-posteriori guarantee on the quality of the so-obtained solution.

**Theorem 3.4 (A-posteriori bounds)** *Suppose that Assumption 2.1 holds and  $\Pi_1$  and  $\Pi_2$  have identically distributed columns. Let  $\delta \in (0, 1)$ . If  $k_1$  satisfies*

$$k_1 = \left\lceil \frac{1}{\delta} - 1 \right\rceil \bar{n}_2, \quad (12)$$

for some  $\bar{n}_2 \geq n_2$ , then the SSP Algorithm 3 is  $\epsilon$ -secure for  $P_1$  with confidence  $1 - \delta$  for any

$$\epsilon \geq \bar{v} - \bar{V}(A_1). \quad (13)$$

If  $k_1$  is further increased so as to satisfy

$$k_1 = \left\lceil \frac{1}{\delta} \ln \frac{1}{\beta} \right\rceil \bar{n}_2, \quad (14)$$

for some  $\beta \in (0, 1)$ , then, with probability higher than  $1 - \beta$ , the policy  $y^*$  with value  $\bar{V}(A_1)$  is  $\epsilon$ -secure for  $P_1$  with confidence  $1 - \delta$ . ■

In the probabilistic guarantee provided by Theorem 3.4 with (12), the confidence  $1 - \delta$  refers not only to the extraction of the row/column matrices  $\Gamma_1, \Gamma_2, \Pi_1, \Pi_2$ , but also to the test matrix  $\bar{\Pi}_1$  since  $\epsilon$  depends on it, i.e., (1) should be understood as

$$P_{\Gamma_1, \Pi_1, \Gamma_2, \Pi_2, \bar{\Pi}_1} (y^{*'} A z^* \leq \bar{V}(A_1) + \epsilon) \geq 1 - \delta. \quad (15)$$

For the probabilistic guarantee with (14), the confidence  $1 - \delta$  refers to the extraction of  $\Gamma_2, \Pi_2$ , i.e., (3) should be understood as

$$P_{\Gamma_2, \Pi_2} (y^{*'} A z^* \leq \bar{V}(A_1) + \epsilon \mid y^*, \bar{V}(A_1), \epsilon) \geq 1 - \delta$$

whereas the confidence  $1 - \beta$  refers solely to the extraction of the matrix  $\bar{\Pi}_1$ .

*Proof of Theorem 3.4:* From the definition of  $\bar{v}$  and (13), we conclude that

$$\bar{V}(A_1) + \epsilon \geq \bar{v} = \max_{j \in \{1, \dots, K \bar{n}_2\}} y^{*'} A \bar{\Pi}_1 e_j(K \bar{n}_2), \quad (16)$$

where  $K := \left\lceil \frac{1}{\delta} - 1 \right\rceil$ .

Define the function  $\bar{f} : \mathcal{S}_M \times \mathcal{B}^{N \times \bar{n}_2}$

$$\bar{f}(y, \Delta) = \max_{j \in \{1, \dots, \bar{n}_2\}} y' A \Delta e_j(\bar{n}_2), \quad (17)$$

Partitioning the columns of  $\bar{\Pi}_1 \in \mathcal{B}^{N \times K \bar{n}_2}$  to construct  $K$  i.i.d. matrices  $\Delta_1, \Delta_2, \dots, \Delta_K$ , each in the set  $\mathcal{B}^{N \times \bar{n}_2}$ , we can rewrite (16) as

$$\bar{V}(A_1) + \epsilon \geq \max_{i \in \{1, \dots, K\}} \bar{f}(y^*, \Delta_i). \quad (18)$$

For any given realizations of  $y^*$  and  $\bar{V}(A_1)$  (which are independent of the  $\Delta_i$ ), we conclude from (Campi and Calafiore, 2009, Proposition 4) that the (conditional) probability that another matrix  $\Delta$ , sampled independently from the same distribution as the  $\Delta_i$ , satisfies the constraint  $\bar{f}(y^*, \Delta) \leq \max_{i \in \{1, \dots, K\}} \bar{f}(y^*, \Delta_i)$  can be lower-bounded as follows:

$$\begin{aligned} P_{\bar{\Pi}_1, \Delta} \left( \bar{f}(y^*, \Delta) \leq \max_{i \in \{1, \dots, K\}} \bar{f}(y^*, \Delta_i) \mid y^*, \bar{V}(A_1) \right) \\ \geq \frac{K}{K+1} \geq 1 - \delta, \end{aligned} \quad (19)$$

where the second inequality is a consequence of (12). From the definition of  $\bar{f}$  and (18), we conclude from (19) that

$$\begin{aligned} P_{\bar{\Pi}_1, \Delta} \left( \max_{j \in \{1, \dots, \bar{n}_2\}} y^{*'} A \Delta e_j(\bar{n}_2) \leq \bar{V}(A_1) + \epsilon \mid y^*, \bar{V}(A_1) \right) \\ \geq 1 - \delta, \end{aligned}$$

and therefore

$$\begin{aligned} P_{\bar{\Pi}_1, \Delta} \left( y^{*'} A \Delta e_j(\bar{n}_2) \leq \bar{V}(A_1) + \epsilon, \forall j \in \{1, \dots, \bar{n}_2\} \right. \\ \left. \mid y^*, \bar{V}(A_1) \right) \geq 1 - \delta. \end{aligned}$$

Since  $n_2 \leq \bar{n}_2$ , we further conclude that

$$\begin{aligned} P_{\bar{\Pi}_1, \Delta} \left( y^{*'} A \Delta e_j(n_2) \leq \bar{V}(A_1) + \epsilon, \forall j \in \{1, \dots, n_2\} \right. \\ \left. \mid y^*, \bar{V}(A_1) \right) \geq 1 - \delta. \end{aligned}$$

Under Assumption 2.1, when the columns of  $\Pi_1$  and  $\Pi_2$  are identically distributed, the matrix consisting of the first  $n_2$  columns of  $\Delta$  can be viewed as the matrix  $\Pi_2$  and we conclude from the inequality above that

$$\begin{aligned} P_{\bar{\Pi}_1, \Pi_2} \left( y^{*'} A \Pi_2 e_j(n_2) \leq \bar{V}(A_1) + \epsilon, \forall j \in \{1, \dots, n_2\} \right. \\ \left. \mid y^*, \bar{V}(A_1) \right) \geq 1 - \delta. \end{aligned}$$

Given that

$$\begin{aligned} y^{*'} A \Pi_2 e_j(n_2) &\leq \bar{V}(A_1) + \epsilon, \quad \forall j \in \{1, \dots, n_2\} \\ \Rightarrow y^{*'} A \Pi_2 z &\leq \bar{V}(A_1) + \epsilon, \quad \forall z \in \mathcal{S}_{n_2}, \end{aligned}$$

we get that

$$\mathbb{P}_{\Gamma_2, \Pi_2, \bar{\Pi}_1} \left( y^{*'} A \Pi_2 z_2^* \leq \bar{V}(A_1) + \epsilon \mid y^*, \bar{V}(A_1) \right) \geq 1 - \delta.$$

Since we have shown that this bound holds for arbitrary realizations of  $y^*$  and  $\bar{V}(A_1)$ , it also holds for the unconditional probability, from which (15) follows.

If instead of applying (Campi and Calafiore, 2009, Proposition 4) we use (14) and apply (Campi and Garatti, 2008, Theorem 1), we conclude that

$$\mathbb{P}_\Delta \left( \bar{f}(y^*, \Delta) \leq \max_{i \in \{1, \dots, K\}} \bar{f}(y^*, \Delta_i) \mid y^*, \bar{V}(A_1), \epsilon \right) \geq 1 - \delta,$$

with probability higher than  $1 - \beta$ , where the confidence level  $1 - \beta$  refers to the extraction of  $\bar{\Pi}_1 = [\Delta_1, \dots, \Delta_K]$  that defines  $\epsilon$ . The proof can now proceed exactly as before, but with (19) replaced by the inequality above that now involves a probability conditioned to  $y^*$ ,  $\bar{V}(A_1)$ , and  $\epsilon$ . This shows that, with probability higher than  $1 - \beta$ , the policy  $y^*$  with value  $\bar{V}(A_1)$  is  $\epsilon$ -secure for  $\mathbb{P}_1$  with confidence  $1 - \delta$ . ■

#### 4. Mismatch in the Sampling Distributions

In this section, we analyze the effect of a mismatch between the sampling distributions used by the players through two different approaches. The first approach is independent of the game matrix  $A$  and relies on the characterization of the mismatch in Erdoğın and Iyengar (2006). The second approach provides a novel characterization of the mismatch, which depends on matrix  $A$ , and, as a side result, extends the scenario bounds to mismatched distributions.

In both cases, statements will be given from the perspective of player  $\mathbb{P}_1$ , by considering a possible mismatch in the column distributions of  $\Pi_1$  and  $\Pi_2$ . Similar results hold for player  $\mathbb{P}_2$  when there is a mismatch in the column distributions of  $\Gamma_1$  and  $\Gamma_2$ . All proofs are provided in the Appendix.

##### 4.1. A Matrix-independent Approach

We first recall the definition of Prohorov metric to evaluate the distance between probability measures. Let  $\mathbb{P}$  and  $\tilde{\mathbb{P}}$  denote two probability measures defined on some metric space  $(\mathcal{H}, d)$ . Then, the distance between  $\mathbb{P}$  and  $\tilde{\mathbb{P}}$  according to the Prohorov metric is given by

$$\pi(\mathbb{P}, \tilde{\mathbb{P}}) = \inf \{ r \mid \mathbb{P}(B) \leq \tilde{\mathbb{P}}(B^r) + r, \forall B \in \mathcal{F}(\mathcal{H}) \},$$

where  $\mathcal{F}(\mathcal{H})$  denotes the Borel sigma algebra on  $\mathcal{H}$  and

$$B^r := \{ x \in \mathcal{H} \mid \inf_{z \in B} d(x, z) \leq r \}. \quad (20)$$

In particular, if  $\mathcal{H}$  is a discrete set, then one can take  $d$  to be the discrete metric

$$d(x_1, x_2) = \begin{cases} 1, & x_1 \neq x_2, \\ 0, & x_1 = x_2. \end{cases}$$

Based on the results on ambiguous chance constrained problems in Erdoğın and Iyengar (2006), the following theorem can be proven. This result should be viewed as a generalization of Theorem 3.1 (for policy security) for the case of mismatched distributions.

**Theorem 4.1 (Matrix-independent mismatch)** *Suppose that Assumption 2.1 holds and that the columns of  $\Pi_1$  and  $\Pi_2$  are sampled according to distributions  $\mathbb{P}$  and  $\tilde{\mathbb{P}}$ , respectively, with  $\pi(\mathbb{P}^{\bar{n}_2}, \tilde{\mathbb{P}}^{\bar{n}_2}) \leq \rho < 1$  for some  $\bar{n}_2 \geq n_2$ .*

*Given  $\delta \in (\rho, 1)$  and  $\beta \in (0, 1)$ , let  $n_1 = K\bar{n}_2$ , where*

$$K \geq \left\lceil \frac{2}{\delta - \rho} \ln \frac{1}{\beta} + 2(m_1 + 1) + \frac{2(m_1 + 1)}{\delta - \rho} \ln \frac{2}{\delta - \rho} \right\rceil. \quad (21)$$

*Then, with probability<sup>2</sup> higher than  $1 - \beta$ , the policy  $y^*$  with security value  $\bar{V}(A_1)$  obtained through the SSP Algorithm 1 is  $\epsilon = 0$ -secure for  $\mathbb{P}_1$  with confidence  $1 - \delta$ .*

Note that a limitation of this approach is that it is applicable only for  $\delta > \rho$ . In the next sub-section, we will provide an alternative approach to characterizing the mismatch that leads to sample complexity bounds without this restriction on the confidence parameter  $\delta$ . This is achieved by exploiting the information on the entries of matrix  $A$ .

##### 4.2. A Matrix-dependent Mismatch Characterization

In this sub-section, we present an alternative characterization of mismatch between the sampling distributions and provide sample complexity bounds on the sizes of the submatrices to be sampled. In particular, we show that, in the case of mismatched distributions, Theorem 3.1 still holds but with the parameter  $\delta$  increased by a certain factor quantifying the mismatch between the two distributions.

We begin with two intermediate results. The first result extends (Campi and Calafiore, 2009, Proposition 3) to mismatched distributions. Consider a sequence of  $K$  random variables  $\Delta_1, \Delta_2, \dots, \Delta_K$ , which are independent and identically distributed over some set  $D$  according to the probability measure  $\mathbb{P}_\Delta$ <sup>3</sup>. Further consider a function  $f : \Theta \times D \rightarrow \mathbb{R}$  that is convex in its first argument, which takes values in some convex set  $\Theta \subseteq \mathbb{R}^{n_\theta}$ . Define the random variable<sup>4</sup>

$$\theta^* = \operatorname{argmin}_{\theta \in \Theta} \{ c'\theta : f(\theta, \Delta_i) \leq 0, \forall i = 1, \dots, K \}, \quad (22)$$

<sup>2</sup>This probability refers to the extraction of the matrix  $\Pi_1$  which defines the policy  $y^*$  and  $\bar{V}(A_1)$ .

<sup>3</sup>In what follows, we implicitly assume that all sets that appear as arguments of probability measures are measurable.

<sup>4</sup>In case of several possible multiple minima, the tie breaking rule in Remark 2.2 should be applied.

where  $c \in \mathbb{R}^{n_\theta}$ .

Let  $\bar{\Delta}$  be a random variable that is independent of  $\Delta_1, \dots, \Delta_K$  and distributed according to a distinct probability measure  $P_{\bar{\Delta}}$  on  $D$ . Then, the following result holds.

**Lemma 4.2** *Suppose that there exist non-negative numbers  $\epsilon, \mu$  such that*

$$P_{\bar{\Delta}}(f(\theta, \bar{\Delta}) > \epsilon) \leq \mu P_{\Delta}(f(\theta, \Delta) > 0), \forall \theta \in \Theta. \quad (23)$$

Then,

$$P_{\bar{\Delta}, \Delta_1, \dots, \Delta_K}(f(\theta^*, \bar{\Delta}) \leq \epsilon) \geq 1 - \frac{\mu n_\theta}{K+1}. \quad (24)$$

Note that (23) always holds for the following choice of  $\mu$ :

$$\mu = \mu(\epsilon) := \sup_{\theta \in \Theta} \frac{P_{\bar{\Delta}}(f(\theta, \bar{\Delta}) > \epsilon)}{P_{\Delta}(f(\theta, \Delta) > 0)}, \quad (25)$$

where  $\mu(\epsilon)$  can be viewed as a *mismatch parameter*. When the distribution of  $\Delta$  is identical to that of  $\bar{\Delta}$ , (23) holds for  $\epsilon = 0$ , and with  $\mu = \mu(0) = 1$ .

Next, we generalize (Alamo et al., 2010, Theorem 4), which involves two levels of probability, to the case of mismatched distributions.

**Lemma 4.3** *Given  $\delta \in (0, 1)$ ,  $\beta \in (0, 1)$  and  $\epsilon \geq 0$ , suppose that  $K$  satisfies*

$$K \geq \left\lceil \mu(\epsilon) \frac{1}{\delta} \left( \ln \frac{1}{\beta} + (n_\theta - 1) + \sqrt{2(n_\theta - 1) \ln \frac{1}{\beta}} \right) \right\rceil.$$

Then, with probability<sup>5</sup> higher than  $1 - \beta$ ,

$$P_{\bar{\Delta}}(f(\theta^*, \bar{\Delta}) \leq \epsilon | \theta^*) \geq 1 - \delta.$$

In the context of the SSP algorithm for player  $P_1$ ,  $\theta = (y_1, v) \in \Theta = (\mathcal{S}_{m_1}, \mathbb{R})$ ,  $\Delta \in D = \mathcal{B}^{N \times \bar{n}_2}$  for some  $\bar{n}_2 \geq n_2$ , and function  $f(\theta, \Delta)$  is parameterized by a matrix  $\Gamma \in \mathcal{B}^{M \times m_1}$  as follows

$$f_\Gamma(\theta, \Delta) = \max_{j \in \{1, \dots, \bar{n}_2\}} y_1' \Gamma' A \Delta e_j(\bar{n}_2) - v, \quad (26)$$

where  $\Gamma$  identifies the rows of  $A$  chosen by player  $P_1$  to construct her subgame matrix  $A_1$ . The above lemmas can be used to prove the following result, which should be viewed as an alternative generalization of Theorem 3.1 for the case of mismatched distributions.

**Theorem 4.4 (Matrix-dependent mismatch)** *Suppose that Assumption 2.1 holds and that the columns of the matrices  $\Pi_1$  and  $\Pi_2$  are sampled according to distributions  $P$  and  $\tilde{P}$ , respectively. Let  $\bar{n}_2 \geq n_2$  and*

$$\mu_{\text{mis}}(\epsilon) := \sup_{\theta \in \Theta, \Gamma \in \mathcal{B}^{M \times m_1}} \frac{P_{\bar{\Delta}}(f_\Gamma(\theta, \bar{\Delta}) > \epsilon)}{P_{\Delta}(f_\Gamma(\theta, \Delta) > 0)}, \quad (27)$$

<sup>5</sup>The confidence level  $1 - \beta$  refers to the extraction of  $\Delta_1, \dots, \Delta_K$  that defines  $\theta^*$ .

where  $f_\Gamma$  is defined in (26) and  $\Delta$  and  $\bar{\Delta}$  are random variables taking values on  $\mathcal{B}^{N \times \bar{n}_2}$  with distributions given by  $P_{\Delta} = P^{\bar{n}_2}$  and  $P_{\bar{\Delta}} = \tilde{P}^{\bar{n}_2}$ , respectively. If  $n_1$  satisfies

$$n_1 = \left\lceil \mu_{\text{mis}}(\epsilon) \frac{m_1 + 1}{\delta} - 1 \right\rceil \bar{n}_2, \quad (28)$$

for some  $\delta \in (0, 1)$  and  $\epsilon \geq 0$ , then the SSP Algorithm 1 is  $\epsilon$ -secure with confidence  $1 - \delta$  for player  $P_1$ . If  $n_1$  is further increased to satisfy

$$n_1 = \left\lceil \mu_{\text{mis}}(\epsilon) \frac{1}{\delta} \left( \ln \frac{1}{\beta} + m_1 + \sqrt{2m_1 \ln \frac{1}{\beta}} \right) \right\rceil \bar{n}_2 \quad (29)$$

for some  $\beta \in (0, 1)$ , then, with probability<sup>6</sup> higher than  $1 - \beta$ , the policy  $y^*$  with value  $\bar{V}(A_1)$  is  $\epsilon$ -secure for  $P_1$  with confidence  $1 - \delta$ .

Theorem 4.4 demonstrates that when there is a mismatch in the sampling distributions of the players, the sizes of the subgames should be selected taking into account the mismatch parameter  $\mu_{\text{mis}}(\epsilon)$  in (27). The larger the mismatch, the larger one should select the subgames for the same level of confidence. Alternatively, one can keep the subgames with the same size, but be prepared to accept for a lower confidence (larger  $\delta$ ).

The bounds in both the approaches described in Section 4.1 and in this subsection can be large. For the approach in Section 4.1, the bound is large if the probability of some columns being selected using the measure  $P$  is zero whereas using  $\tilde{P}$  is almost one, since in that case  $\pi(P^{\bar{n}_2}, \tilde{P}^{\bar{n}_2}) \simeq 1$ , irrespectively of  $A$ . For the approach in this section, the bounds are typically large when  $P_1$  (unlike  $P_2$ ) extracts with low probability those columns of  $\Gamma_1' A$  that are likely to result in *constraint violation*, e.g., if  $P_{\Delta}(f_{\Gamma_1}(\theta, \Delta) > 0) \simeq 0$  and  $P_{\bar{\Delta}}(f_{\Gamma_1}(\theta, \bar{\Delta}) > 0) \simeq 1$ , for some  $\theta \in \Theta$ .

The results in this section have the advantage over the ones in Section 4.1 that they exploit properties of the matrix  $A$ . This is important when the structure of the matrix  $A$  dictates that some mismatch should not lead to a degradation in the confidence levels. We shall see in the next section that this is the case when  $A$  exhibits some forms of policy domination. This is shown next with reference to player  $P_1$ . The result for  $P_2$  is symmetric.

#### 4.2.1. Matrix games with Dominated policies

Consider a situation when  $P_1$  knows of some particularly good policies that  $P_2$  may apply to play the game. For example, suppose that the entries in some column  $c_2$  of  $A$  are all element-wise larger than those in some other column  $c_1$ . In this case, it turns out that  $P_1$  can increase the probability of sampling the column  $c_2$  at the expense

<sup>6</sup>The confidence level  $1 - \beta$  refers to the extraction of  $[\Delta_1, \dots, \Delta_K] =: \Pi_1$  using the measure  $P_{\Delta}(\cdot)$  that defines  $y^*$  and  $\bar{V}(A_1)$ .

of decreasing the probability of selecting  $c_1$ . This mismatch should not require a larger bound on the number of columns to sample. This observation is formalized in the remaining of this section.

We begin with the following notion of dominance.

**Definition 1 ( $\epsilon$ -Dominance)** *Given an  $M \times N$  matrix  $A$ , the vector  $d^* \in \mathcal{B}^{N \times 1}$  is said to be  $\epsilon$ -dominated by the vector  $d \in \mathcal{B}^{N \times 1}$  for some  $\epsilon \geq 0$  if*

$$e_i(M)'Ad^* \leq e_i(M)'Ad + \epsilon, \quad \forall i \in \{1, \dots, M\},$$

where  $e_i(M)$  denotes the  $i$ th element of the canonical basis of  $\mathbb{R}^M$ .

With  $\epsilon = 0$ , the above definition becomes identical to that of domination between pure policies in matrix games (cf. Basar and Olsder (1999)). Next, we introduce the notion of two sampling distributions being perturbed.

**Definition 2 (Perturbed sampling)** *Given two distinct elements  $d$  and  $d^*$  of  $\mathcal{B}^{N \times 1}$ , and two probability measures  $P$  and  $\tilde{P}$  on  $\mathcal{B}^{N \times 1}$ ,  $P$  is a perturbation of  $\tilde{P}$  with respect to the pair  $(d, d^*)$  if*

1.  $P$  differs from  $\tilde{P}$  only over  $\{d, d^*\} \subseteq \mathcal{B}^{N \times 1}$ , i.e.,

$$\tilde{P}(e_j(N)) = P(e_j(N)),$$

for all  $j$  such that  $e_j(N) \notin \{d^*, d\}$ , where  $e_j(N)$  denotes the  $j$ th element of the canonical basis of  $\mathbb{R}^N$ ;

2. the probability of extracting  $d^*$  according to  $P$  is smaller than according to  $\tilde{P}$ , i.e.,

$$P(d^*) \leq \tilde{P}(d^*).$$

We now present the main result of this sub-section.

**Theorem 4.5 (Domination)** *Given the game matrix  $A$ , suppose that for some  $\epsilon \geq 0$ , there exist distinct columns  $d^* \in \mathcal{B}^{N \times 1}$  and  $d \in \mathcal{B}^{N \times 1}$  such that  $d^*$  is  $\epsilon$ -dominated by  $d$ . Suppose that Assumption 2.1 holds and that the columns of matrices  $\Pi_1$  and  $\Pi_2$  are sampled according to distributions  $P$  and  $\tilde{P}$ , respectively. If  $P$  is a perturbation of  $\tilde{P}$  with respect to  $(d, d^*)$ , then Theorem 4.4 holds with  $\mu_{\text{mis}}(\epsilon) = 1$ .*

This result shows that even when  $P_1$  extracts with low probability (possibly equal to zero) the column  $d^*$ , the bounds of Section 3 hold.

## 5. Example: Hide-and-seek matrix game

In this section, we apply the procedures from Sections 3 to a classic search problem through many points in a plane.

Consider a zero-sum game where  $P_1$  hides a non-moving object (treasure) in one of  $N$  points  $\{p_1, \dots, p_N\} \subset \mathbb{R}^2$  on the plane and  $P_2$  has to find the treasure with minimum cost, by traveling from point to point until she finds it. The game is played over the set of mixed policies:

- $P_1$  chooses a probability distribution  $z \in \mathcal{S}_N$  for the treasure over the  $N$  points, and
- $P_2$  chooses a probability distribution  $y \in \mathcal{S}_M$  over the set  $\mathcal{R} := \{r_j : j = 1, \dots, M\}$  of  $M := N!$  routes that start at  $P_1$ 's initial position  $p_0 \in \mathbb{R}^2$  and go through all possible permutations of the points.

Each route is assigned a cost equal to its total Euclidean length:

$$c(r_j) = \sum_{k=1}^N \|r_j(k) - r_j(k-1)\|,$$

where  $r_j(0) := p_0$  and each subsequent  $r_j(k) \in \mathbb{R}^2$ ,  $k \in \{1, \dots, N\}$  denotes the  $k$ th point in the route  $r_j$ . When  $P_1$  chooses to hide the treasure at point  $i$  and  $P_2$  selects route  $r_j$ , the outcome of the game is equal to the cost of route  $r_j$  from its initial point until the point  $p_i$  where the treasure lies. Namely,

$$A_{ij} = - \sum_{k=1}^{k_{ij}^*} \|r_j(k) - r_j(k-1)\|, \quad (30)$$

where the summation ends at the index  $k_{ij}^*$  for which  $r_j(k_{ij}^*)$  corresponds to the point  $i$  where the treasure is hidden. The minus sign in (30) is needed to maintain consistency with the formulation in the first part of the paper, where  $P_1$  is the minimizer. Indeed,  $P_1$  hides the treasure to maximize the distance and therefore to minimize the entries of  $A$ .

For a large  $N$ , the exact computation of the optimal mixed strategies is intractable because the size of the matrix  $A$  is  $N \times N!$ . However, the results in this paper lead to a computational complexity that is *independent of the size of the game*, which means that we can provide probabilistic guarantees for games with an arbitrarily large number of points.

In this particular game, only the player  $P_2$  that chooses paths has a large number of options ( $M = N!$ ) so we can assume that both players consider all possible  $N$  locations where  $P_1$  can hide the treasure (all rows of  $A$ ), but randomly select only a small number of paths (columns of  $A$ ) to construct their submatrices. This means that the player  $P_2$  that selects the paths will never be surprised since she always considers all options for the actions of  $P_1$ . However, the player  $P_1$  that hides the treasure should respect the bounds provided by Theorems 3.1 and 3.4 to avoid unpleasant surprises.

In our numerical experiments, we considered  $N = 10$  points distributed uniformly randomly in a square region of side length equal to 50 units. For a fixed value of  $\bar{n}_2$ ,  $\beta$ , and  $\delta$ , we ran the a-posteriori procedure multiple times (described in Section 3.2) using the bound in (14), and studied the outcome  $\bar{v}$  in (11) for increasing values of  $n_1$  up to the corresponding a-priori bound (5), indicated by an

arrow in Figure 1. Since  $\bar{v}$  is obtained through a randomized procedure, it is a random variable and takes different values in the different Monte Carlo runs. Figure 1 shows the 90 percentile curve (dot-dashed) such that 90% of the realizations of  $\bar{v}$  fall below this curve. The 50 percentile curve is also shown (dashed). We then repeated the experiments using the a-posteriori bound in (12), and studied the outcome  $\bar{v}$  in (11) for increasing values of  $n_1$  up to the corresponding a-priori bound (4). The 90% (solid) and the 50% (thin dashed) percentile curves for the bound in (12) are also shown in Figure 1.

We observe that all of these curves are reasonably "flat", implying that with choices of  $n_1$  a few orders of magnitude lower than the a-priori bound, one can obtain a security strategy with a relatively small increase in the a-posteriori security level  $\bar{v}$ . For example, from Figure 1, we conclude that with a value of  $n_1$  up to 40 times lower than the a-priori bound (5) needed for  $\epsilon = 0$ -security of the policy  $y^*$ , in 90% (resp. 50%) of the simulations, the increase in the a-posteriori security level  $\bar{v}$  for the strategy  $y^*$  is at most 5 (resp. 3) units.

Figure 2 summarizes numerical results obtained with a higher value of the number  $\bar{n}_2$ . Akin to Figure 1, we observe that all of the curves are reasonably flat. Compared to Figure 1, the outcome  $\bar{v}$  increases on average, as is expected because player  $P_2$  is now allowed to search over a larger number of columns. E.g., for  $n_1 = 1000$ , the 90 percentile curve is higher than in Figure 1 by at most 5 units. Our numerical results indicate that allowing for a small increase in the a-posteriori security level, the minimizer needs to sample much fewer columns than the corresponding a-priori bound, thereby leading to significant computational savings.

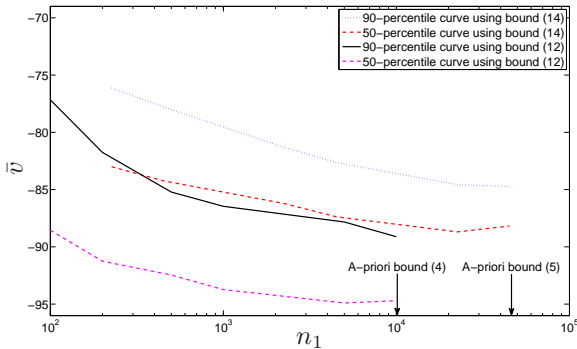


Figure 1: Numerically determined percentile values of the a-posteriori outcome  $\bar{v}$  (cf. Section 3.2) for different values of  $n_1$ . In these experiments, the number of points is  $N = 10$ , side length of the square region is 50 units,  $m_1 = \bar{n}_2 = 10$ ,  $\delta = 0.01$ ,  $\beta = 10^{-5}$ , and the rows and the columns were drawn uniformly randomly.

## 6. Conclusions and Future Directions

We addressed the solution of large zero-sum matrix games using randomized techniques. We provided a pro-

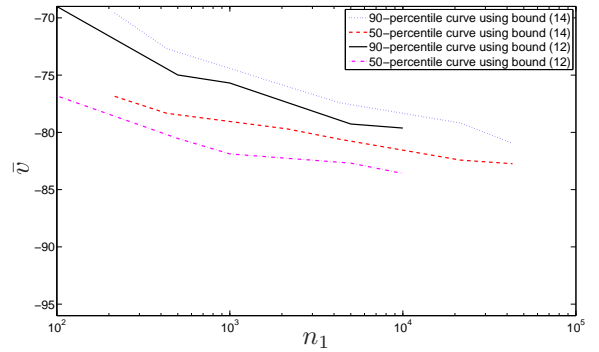


Figure 2: Numerically determined values of the a-posteriori outcome  $\bar{v}$  (cf. Section 3.2) for different values of  $n_1$ . In these experiments,  $N = 10$ ,  $m_1 = 10$ ,  $\bar{n}_2 = 1000$ ,  $\delta = 0.01$ ,  $\beta = 10^{-5}$ , and the rows and the columns were drawn uniformly randomly.

cedure by which each player samples a submatrix, computes mixed policies for the submatrix and uses the resulting optimal strategy to play against the other player. We proposed a new probabilistic notion of security policy and level for each player, and derived a-priori game-independent bounds on the size of the submatrices that guarantees a security policy with high probability. We also presented an a-posteriori bound on how much the outcome of the game can violate the precomputed security level if the size of the submatrices do not satisfy the a-priori bounds. We then analyzed the effect of sampling mismatch between the two players. We extended the theoretical bounds given the distributions used by the two players, and also analyzed the case of policy domination in matrix games. Finally, we applied the technique to solve a combinatorial hide-and-seek game.

This work suggests a number of exciting future directions of research. One promising direction is to explore incremental optimization techniques to reduce the bound on the size of the submatrices. Another direction being presently explored is to extend the sampling procedure to dynamic or multi-stage games. Additionally, it would also be interesting to analyze closed-loop versions of the hide-and-seek game that involve the searcher taking measurements of the location of the treasure as it moves from point to point (cf. Borri et al. (2011)).

## References

- Alamo, T., Tempo, R., Camacho, E. F., November 2009. Randomized strategies for probabilistic solutions of uncertain feasibility and optimization problems. *IEEE Transactions on Automatic Control* 54 (11), 2545–2559.
- Alamo, T., Tempo, R., Luque, A., June–July 2010. On the sample complexity of randomized approaches to the analysis and design under uncertainty. In: *American Control Conference*. Baltimore, MD, USA, pp. 4671–4676.
- Basar, T., Olsder, G. J., 1999. *Dynamic Non-Cooperative Game Theory*. SIAM, Philadelphia, PA, USA.
- Bellman, R., 1962. Dynamic programming treatment of the traveling salesman problem. *J. Assoc. Comput. Mach.* 9, 61–63.

Bopardikar, S. D., Borri, A., Hespanha, J. P., Prandini, M., Di Benedetto, M. D., Dec. 2010. Randomized sampling for large zero-sum games. In: IEEE Conference on Decision and Control. Atlanta, GA, USA.

Borri, A., Bopardikar, S. D., Hespanha, J. P., Di Benedetto, M. D., Aug. 2011. Hide-and-Seek with Directional Sensing. In: International Federation of Automatic Control World Congress, Milan, Italy. Note: To appear

Calafiore, G. C., Campi, M. C., May 2006. The scenario approach to robust control design. IEEE Transactions on Automatic Control 51 (5), 742–753.

Campi, M. C., Calafiore, G. C., February 2009. Notes on the scenario design approach. IEEE Transactions on Automatic Control 54 (2), 382–385.

Campi, M. C., Garatti, S., 2008. The exact feasibility of randomized solutions of robust convex programs. SIAM Journal on Control and Optimization 19 (3), 1211–1230.

Campi, M. C., Garatti, S., Prandini, M., Dec. 2009. The scenario approach for systems and control design. Annual Reviews in Control 33 (2), 149–157.

de Fariasi, D. P., Roy, B. V., August 2004. On constraint sampling in the linear programming approach to approximate dynamic programming. Mathematics of Operations Research 29 (3), 462–478.

Erdogan, E., Iyengar, G., 2006. Ambiguous chance constrained problems and robust optimization. Mathematical Programming 107 (1–2), 37–61.

Hespanha, J. P., Prandini, M., December 2001. Nash equilibria in partial-information games on Markov chains. In: IEEE Conference on Decision and Control. Orlando, FL, USA, pp. 2102–2107.

Khargonekar, P., Tikku, A., Dec. 1996. Randomized algorithms for robust control analysis and synthesis have polynomial complexity. In: Proceedings of the 35th IEEE Conference on Decision and Control. Vol. 3. Kobe, Japan, pp. 3470–3475.

Lipton, R. J., Young, N. E., 1994. Simple strategies for large zero-sum games with applications to complexity theory. In: Twenty-sixth annual ACM Symposium on Theory of Computing. pp. 734–740.

Motwani, R., Raghavan, P., 1995. Randomized Algorithms. Cambridge University Press.

Tempo, R., Bai, E. W., Dabbene, F., 1997. Probabilistic robustness analysis: Explicit bounds for the minimum number of samples. Systems and Control Letters 30 (5), 237–242.

Vapnik, V., 1998. Statistical Learning Theory. John Wiley, New York.

Vidyasagar, M., Dec. 1998. Statistical learning theory and randomized algorithms for control. IEEE Control Systems Magazine 18 (6), 69–85.

Vidyasagar, M., Blondel, V. D., Sep. 2001. Probabilistic solutions to some NP-hard matrix problems. Automatica 37 (9), 1397–1405.

Von Neumann, J., 1928. Zur theorie der gesellschaftsspiele. Math. Annalen. 100, 295–320.

## Appendix

In this Appendix, we provide the proofs of the results in Section 4.

*Proof of Theorem 4.1:* Following the same steps as in the proof of Theorem 3.1, we obtain that the security value  $\bar{V}(A_1)$  can be expressed as:

$$\bar{V}(A_1) = \min_{\theta \in \Theta} \left\{ v : f_{\Gamma_1}(\theta, \Delta_i) \leq 0 \forall i \in \{1, \dots, K\} \right\}, \quad (31)$$

where  $\theta = (y, v) \in \mathcal{S}_{m_1} \times \mathbb{R}$  and  $f_{\Gamma}$  is defined in (7).

Given that for any  $\Delta_i \in \mathcal{B}^{N \times \bar{n}_2}$ ,

$$\Delta = \Delta_i \Leftrightarrow d(\Delta, \Delta_i) \leq \rho,$$

where  $0 \leq \rho < 1$  and  $d(\cdot, \cdot)$  is the discrete metric, (31) is equivalent to

$$\bar{V}(A_1) = \min_{\theta \in \Theta} \left\{ v : f_{\Gamma_1}(\theta, \Delta) \leq 0, \forall \Delta \text{ such that } d(\Delta, \Delta_i) \leq \rho \text{ for some } i \in \{1, \dots, K\} \right\}.$$

Suppose that the minimum above is achieved for some  $\theta^* = (y_1^*, \bar{V}(A_1))$ . Matrices  $\Delta_i$  are random variables with probability distribution  $\tilde{P}^{\bar{n}_2}$  over  $\mathcal{H} := \mathcal{B}^{N \times \bar{n}_2} \subset \mathbb{R}^{N \times \bar{n}_2}$ . Then, for any given realization of the matrix  $\Gamma_1$  (which is independent of the  $\Delta_i$ ), we can conclude from (Erdogan and Iyengar, 2006, Theorem 6) that for any random variable  $\Delta$  with probability distribution  $P_{\Delta} = \tilde{P}^{\bar{n}_2}$  over  $\mathcal{H}$

$$P_{\Delta} (f_{\Gamma_1}(\theta^*, \Delta) \leq 0 \mid \Gamma_1, \theta^*) \geq 1 - \delta, \quad (32)$$

with a confidence at least  $1 - \left(\frac{eK}{m_1+1}\right)^{m_1+1} e^{-(\delta-\rho)(K-(m_1+1))}$ .

Here, the confidence refers to the extraction of matrix  $\Pi_1 = [\Delta_1, \dots, \Delta_K]$  that defines  $\theta^*$  (given  $\Gamma_1$ ). Using the definition of  $f_{\Gamma}$  and  $\theta^*$ , we can re-write (32) as

$$P_{\Delta} (y_1^{*\prime} \Gamma_1' A \Delta e_j(\bar{n}_2) \leq \bar{V}(A_1), \forall j \in \{1, \dots, \bar{n}_2\} \mid \Gamma_1, y_1^*, \bar{V}(A_1)) \geq 1 - \delta.$$

Under Assumption 2.1, the matrix consisting of the first  $n_2$  columns of  $\Delta$  can be viewed as the matrix  $\Pi_2$  and we conclude from the inequality above that

$$P_{\Pi_2} (y_1^{*\prime} \Gamma_1' A \Pi_2 e_j(n_2) \leq \bar{V}(A_1), \forall j \in \{1, \dots, n_2\} \mid \Gamma_1, y_1^*, \bar{V}(A_1)) \geq 1 - \delta.$$

Since

$$y_1^{*\prime} \Gamma_1' A \Pi_2 e_j(n_2) \leq \bar{V}(A_1), \forall j \in \{1, \dots, n_2\} \Rightarrow y_1^{*\prime} \Gamma_1' A \Pi_2 z \leq \bar{V}(A_1), \forall z \in \mathcal{S}_{n_2},$$

we get that

$$P_{\Gamma_2, \Pi_2} (y_1^{*\prime} \Gamma_1' A \Pi_2 z^* \leq \bar{V}(A_1) \mid \Gamma_1, y_1^*, \bar{V}(A_1)) \geq 1 - \delta.$$

Since we have shown that this bound holds for an arbitrary realization of  $\Gamma_1$ , it also holds for the unconditional probability. This shows that, with probability higher than  $1 - \left(\frac{eK}{m_1+1}\right)^{m_1+1} e^{-(\delta-\rho)(K-(m_1+1))}$ , the policy  $y^*$  with value  $\bar{V}(A_1)$  obtained by the SSP algorithm 1 is  $\epsilon = 0$ -secure for  $P_1$  with confidence  $1 - \delta$ .

To conclude the proof, we only need to show that (21) implies that

$$\left(\frac{eK}{m_1+1}\right)^{m_1+1} e^{-(\delta-\rho)(K-(m_1+1))} \leq \beta. \quad (33)$$

For short, write  $m := m_1 + 1$ . Then,

$$\begin{aligned}
K &\geq \frac{2}{\delta - \rho} \ln \frac{1}{\beta} + 2m + \frac{2m}{\delta - \rho} \ln \frac{2}{\delta - \rho} \\
&\Rightarrow K \geq \frac{1}{\delta - \rho} \ln \frac{1}{\beta} + m + \frac{m}{\delta - \rho} \ln \frac{2}{\delta - \rho} + \frac{K}{2} \\
&\Rightarrow K \geq \frac{1}{\delta - \rho} \ln \frac{1}{\beta} + m + \frac{m}{\delta - \rho} \ln \frac{2}{\delta - \rho} + \frac{m}{\delta - \rho} \frac{K(\delta - \rho)}{2m} \\
&\Rightarrow K \geq \frac{1}{\delta - \rho} \ln \frac{1}{\beta} + m + \frac{m}{\delta - \rho} \ln \frac{2}{\delta - \rho} \\
&\quad + \frac{m}{\delta - \rho} \left(1 - \ln \frac{2m}{(\delta - \rho)K}\right), \quad \text{since } \frac{1}{x} \geq 1 - \ln x, \\
&\Rightarrow K \geq \frac{1}{\delta - \rho} \ln \frac{1}{\beta} + m + \frac{m}{\delta - \rho} \left(1 + \ln \frac{K}{m}\right) \\
&\Rightarrow \ln \frac{1}{\beta} \leq (\delta - \rho)(K - m) - m - m \ln \frac{K}{m} \\
&\Rightarrow \ln \beta \geq -(\delta - \rho)(K - m) + m \ln \frac{eK}{m} \\
&\Rightarrow \beta \geq \left(\frac{eK}{m}\right)^m e^{-(\delta - \rho)(K - m)},
\end{aligned}$$

and thus, (21) implies (33).  $\blacksquare$

*Proof of Lemma 4.2:* Given that

$$\begin{aligned}
&\mathbb{P}_{\bar{\Delta}, \Delta_1, \dots, \Delta_K} (f(\theta^*, \bar{\Delta}) > \epsilon) \\
&= \mathbb{E}_{\Delta_1, \dots, \Delta_K} \left[ \mathbb{P}_{\bar{\Delta}} (f(\theta^*, \bar{\Delta}) > \epsilon | \theta^*) \right],
\end{aligned}$$

we can use (23) to conclude that

$$\begin{aligned}
&\mathbb{P}_{\bar{\Delta}, \Delta_1, \dots, \Delta_K} (f(\theta^*, \bar{\Delta}) > \epsilon) \\
&\leq \mu \mathbb{E}_{\Delta_1, \dots, \Delta_K} \left[ \mathbb{P}_{\Delta} (f(\theta^*, \Delta) > 0 | \theta^*) \right] \\
&\leq \frac{\mu n_\theta}{K + 1},
\end{aligned}$$

where the second inequality follows from (Campi and Calafiore, 2009, Proposition 3).  $\blacksquare$

*Proof of Lemma 4.3:* By (Alamo et al., 2010, Theorem 4), if we fix an arbitrary  $\bar{\delta} \in (0, 1)$  and  $K$  satisfies

$$K \geq \left\lceil \frac{1}{\bar{\delta}} \left( \ln \frac{1}{\beta} + (n_\theta - 1) + \sqrt{2(n_\theta - 1) \ln \frac{1}{\beta}} \right) \right\rceil,$$

then, with probability <sup>7</sup> higher than  $1 - \beta$ ,

$$\mathbb{P}_{\Delta} (f(\theta^*, \Delta) > 0 | \theta^*) \leq \bar{\delta}.$$

From definition of  $\mu(\epsilon)$  in (25) it follows that

$$\mathbb{P}_{\bar{\Delta}} (f(\theta^*, \bar{\Delta}) > \epsilon | \theta^*) \leq \mu(\epsilon) \mathbb{P}_{\Delta} (f(\theta^*, \Delta) > 0 | \theta^*).$$

By combining the last two inequalities, we obtain

$$\begin{aligned}
\mathbb{P}_{\bar{\Delta}} (f(\theta^*, \bar{\Delta}) \leq \epsilon | \theta^*) &= 1 - \mathbb{P}_{\bar{\Delta}} (f(\theta^*, \bar{\Delta}) > \epsilon | \theta^*) \\
&\geq 1 - \mu(\epsilon) \bar{\delta},
\end{aligned}$$

so that setting  $\bar{\delta} := \delta / \mu(\epsilon)$ , the claim is proved.  $\blacksquare$

<sup>7</sup>The confidence level  $1 - \beta$  refers to the extraction of  $\Delta_1, \dots, \Delta_K$  that defines  $\theta^*$ .

*Proof of Theorem 4.4:* Since matrix  $\Pi_1$  has  $n_1 = K\bar{n}_2$  columns with  $K = \left\lceil \mu_{\text{mis}}(\epsilon) \frac{m_1 + 1}{\delta} - 1 \right\rceil$ , following the same steps as in the proof of Theorem 3.1, we can partition  $\Pi_1$  into  $K$  i.i.d. matrices  $\Delta_1, \Delta_2, \dots, \Delta_K$ , each in the set  $\mathcal{B}^{N \times \bar{n}_2}$ , and express the security value  $\bar{V}(A_1)$  as:

$$\bar{V}(A_1) = \min_{\theta \in \Theta} \left\{ v : f_{\Gamma_1}(\theta, \Delta_i) \leq 0 \ \forall i \in \{1, \dots, K\} \right\}, \quad (34)$$

with  $\theta = (y, v) \in \Theta = \mathcal{S}_{m_1} \times \mathbb{R}$ , and  $f_{\Gamma}$  defined in (26).

Let the minimum in (34) be achieved for some  $\theta^* = (y_1^*, \bar{V}(A_1))$ . Matrices  $\Delta_i$  are random variables distributed according to  $\mathbb{P}_{\Delta} = \mathbb{P}^{\bar{n}_2}$  over  $\mathcal{B}^{N \times \bar{n}_2}$ . For any given realization of the matrix  $\Gamma_1$  (which is independent of the  $\Delta_i$  by Assumption 2.1) we conclude from Lemma 4.2 and the definition of  $\mu_{\text{mis}}(\epsilon)$  in (27), that the (conditional) probability that another matrix  $\bar{\Delta}$ , sampled independently of the  $\Delta_i$  according to probability  $\mathbb{P}_{\bar{\Delta}} = \tilde{\mathbb{P}}^{\bar{n}_2}$  over  $\mathcal{B}^{N \times \bar{n}_2}$ , satisfies

$$\mathbb{P}_{\Pi_1, \bar{\Delta}} (f_{\Gamma_1}(\theta^*, \bar{\Delta}) \leq \epsilon | \Gamma_1) \geq \frac{K - m_1}{K + 1} \geq 1 - \delta, \quad (35)$$

where the second inequality is a consequence of (28). Using the definition of  $f_{\Gamma}$  from (26) and  $\theta^*$ , we can re-write (35) as

$$\begin{aligned}
\mathbb{P}_{\Pi_1, \bar{\Delta}} (y_1^{*'} \Gamma_1' A \bar{\Delta} e_j(\bar{n}_2) \leq \bar{V}(A_1) + \epsilon, \\
\forall j \in \{1, \dots, \bar{n}_2\} | \Gamma_1) \geq 1 - \delta.
\end{aligned}$$

Since  $n_2 \leq \bar{n}_2$ , we further conclude that

$$\begin{aligned}
\mathbb{P}_{\Pi_1, \bar{\Delta}} (y_1^{*'} \Gamma_1' A \bar{\Delta} e_j(n_2) \leq \bar{V}(A_1) + \epsilon, \\
\forall j \in \{1, \dots, n_2\} | \Gamma_1) \geq 1 - \delta.
\end{aligned}$$

Under Assumption 2.1, the matrix consisting of the first  $n_2$  columns of  $\bar{\Delta}$  can be viewed as the matrix  $\Pi_2$  and we conclude from the inequality above that

$$\begin{aligned}
\mathbb{P}_{\Pi_1, \Pi_2} (y_1^{*'} \Gamma_1' A \Pi_2 e_j(n_2) \leq \bar{V}(A_1) + \epsilon, \\
\forall j \in \{1, \dots, n_2\} | \Gamma_1) \geq 1 - \delta.
\end{aligned}$$

Since

$$\begin{aligned}
y_1^{*'} \Gamma_1' A \Pi_2 e_j(n_2) \leq \bar{V}(A_1) + \epsilon, \ \forall j \in \{1, \dots, n_2\} \Rightarrow \\
y_1^{*'} \Gamma_1' A \Pi_2 z \leq \bar{V}(A_1) + \epsilon, \ \forall z \in \mathcal{S}_{n_2},
\end{aligned}$$

we conclude that

$$\mathbb{P}_{\Pi_1, \Gamma_2, \Pi_2} (y_1^{*'} \Gamma_1' A \Pi_2 z^* \leq \bar{V}(A_1) + \epsilon | \Gamma_1) \geq 1 - \delta.$$

Since we have shown that this bound holds for an arbitrary realization of  $\Gamma_1$ , it also holds for the unconditional probability, which shows that the SSP algorithm is  $\epsilon$ -secure for  $\mathbb{P}_1$  with confidence  $1 - \delta$ .

If instead of applying Lemma 4.2, we apply Lemma 4.3, then using (29), we conclude that

$$\mathbb{P}_{\bar{\Delta}} (f_{\Gamma_1}(\theta^*, \bar{\Delta}) \leq \epsilon | \Gamma_1, \theta^*) \geq 1 - \delta$$

with probability higher than  $1 - \beta$ , where the confidence level  $1 - \beta$  refers to the extraction of  $\Pi_1 = [\Delta_1, \dots, \Delta_K]$  that defines  $\theta^*$  (given  $\Gamma_1$ ). The proof can now proceed exactly as before, but with (35) replaced by the inequality above, which now involves a probability conditioned to  $y^*$  and  $\bar{V}(A_1)$ . This shows that, with probability higher than  $1 - \beta$ , the policy  $y^*$  with value  $\bar{V}(A_1)$  is  $\epsilon$ -secure for  $P_1$  with confidence  $1 - \delta$ . ■

*Proof of Theorem 4.5:*

To prove Theorem 4.5, we just need to show that

$$P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) > \epsilon) \leq P_{\Delta}(f_{\Gamma}(\theta, \Delta) > 0), \quad (36)$$

for any  $\theta \in \Theta$ ,  $\Gamma \in \mathcal{B}^{M \times m_1}$ , since from this condition we have that  $\mu_{\text{mis}}(\epsilon)$  defined in (27) is not larger than 1.

Fix  $\theta = (y_1, v) \in \Theta$  and  $\Gamma \in \mathcal{B}^{M \times m_1}$ . Let us distinguish between the following two cases:

Case 1)  $d^*$  satisfies

$$y_1' \Gamma' A d^* - v > \epsilon \quad (37)$$

Case 2)  $d^*$  satisfies

$$y_1' \Gamma' A d^* - v \leq \epsilon \quad (38)$$

As for case 1, observe that

$$P_{\Delta}(f_{\Gamma}(\theta, \Delta) > 0) = 1 - P_{\Delta}(f_{\Gamma}(\theta, \Delta) \leq 0). \quad (39)$$

Now, given that the columns of  $\Delta$  are extracted independently according to  $P$ , we have

$$P_{\Delta}(f_{\Gamma}(\theta, \Delta) \leq 0) = \sum_{\{\Delta=[c_1, \dots, c_{\bar{n}_2}]: f_{\Gamma}(\theta, \Delta) \leq 0\}} \prod_{j=1}^{\bar{n}_2} P(c_j),$$

where  $c_j \in \mathcal{B}^{N \times 1}$  denotes the  $j$ th column of  $\Delta$ . Since from Definition 1 of  $\epsilon$ -dominance and equation (37) we obtain

$$y_1' \Gamma' A d - v > y_1' \Gamma' A d^* - v - \epsilon > 0,$$

we can conclude that the columns  $c_j$ ,  $j = 1, \dots, \bar{n}_2$ , of  $\Delta$  such that  $f_{\Gamma}(\theta, \Delta) = \max_{j \in \{1, \dots, \bar{n}_2\}} y_1' \Gamma' A d e_j(\bar{n}_2) - v = \max_{j \in \{1, \dots, \bar{n}_2\}} y_1' \Gamma' A c_j - v \leq 0$  must be different from both  $d$  and  $d^*$ . By Definition 2, we then have that  $P(c_j) = \tilde{P}(c_j)$ ,  $j = 1, \dots, \bar{n}_2$ , and, hence,

$$\begin{aligned} P_{\Delta}(f_{\Gamma}(\theta, \Delta) \leq 0) &= \sum_{\{\Delta=[c_1, \dots, c_{\bar{n}_2}]: f_{\Gamma}(\theta, \Delta) \leq 0\}} \prod_{i=1}^{\bar{n}_2} \tilde{P}(c_i) \\ &= P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) \leq 0). \end{aligned}$$

Now, if we plug this in equation (39), we get that

$$\begin{aligned} P_{\Delta}(f_{\Gamma}(\theta, \Delta) > 0) &= P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) > 0) \\ &\geq P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) > \epsilon), \end{aligned}$$

i.e., equation (36) holds in case 1.

As for case 2, we start considering the case when  $d$  satisfies

$$y_1' \Gamma' A d - v > \epsilon.$$

Note that  $P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) \leq \epsilon)$  can be expressed as follows

$$P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) \leq \epsilon) = \sum_{\{\bar{\Delta}=[\bar{c}_1, \dots, \bar{c}_{\bar{n}_2}]: f_{\Gamma}(\theta, \bar{\Delta}) \leq \epsilon\}} \prod_{j=1}^{\bar{n}_2} \bar{P}(\bar{c}_j)$$

Since the columns  $\bar{c}_j$ ,  $j = 1, \dots, \bar{n}_2$ , of any  $\bar{\Delta} = [\bar{c}_1, \dots, \bar{c}_{\bar{n}_2}]$  such that  $f_{\Gamma}(\theta, \bar{\Delta}) = \max_{j \in \{1, \dots, \bar{n}_2\}} y_1' \Gamma' A \bar{c}_j - v \leq \epsilon$  must be different from  $d$  and the probability of extracting any such column according to  $\bar{P}$  is larger than according to  $P$  (see Definition 2), we get

$$\begin{aligned} P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) \leq \epsilon) &\geq \sum_{\{\bar{\Delta}=[\bar{c}_1, \dots, \bar{c}_{\bar{n}_2}]: f_{\Gamma}(\theta, \bar{\Delta}) \leq \epsilon\}} \prod_{j=1}^{\bar{n}_2} P(\bar{c}_j) \\ &= P_{\Delta}(f_{\Gamma}(\theta, \Delta) \leq \epsilon) \end{aligned}$$

From this it follows that

$$\begin{aligned} P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) > \epsilon) &= 1 - P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) \leq \epsilon) \\ &\leq 1 - P_{\Delta}(f_{\Gamma}(\theta, \Delta) \leq \epsilon) \\ &= P_{\Delta}(f_{\Gamma}(\theta, \Delta) > \epsilon) \\ &\leq P_{\Delta}(f_{\Gamma}(\theta, \Delta) > 0), \end{aligned}$$

i.e. equation (36) holds.

We shall consider now the last subcase when  $d$  satisfies

$$y_1' \Gamma' A d - v \leq \epsilon. \quad (40)$$

We start noting that  $P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) > \epsilon)$  is the probability that at least one of the columns, say  $\bar{c}$ , of  $\bar{\Delta}$  satisfies

$$y_1' \Gamma' A \bar{c} - v > \epsilon.$$

Let

$$C = \{c \in \mathcal{B}^{N \times 1} : y_1' \Gamma' A c - v > \epsilon\}.$$

Set  $p_C = \sum_{c \in C} P(c)$  and  $\tilde{p}_C = \sum_{c \in C} \tilde{P}(c)$ . Then,

$$P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) > \epsilon) = 1 - (1 - \tilde{p}_C)^{\bar{n}_2},$$

where  $(1 - \tilde{p}_C)^{\bar{n}_2}$  is the probability of all  $\bar{n}_2$  independently extracted columns of  $\bar{\Delta}$  not belonging to set  $C$ . Similarly,

$$P_{\Delta}(f_{\Gamma}(\theta, \Delta) > \epsilon) = 1 - (1 - p_C)^{\bar{n}_2}.$$

Now, since  $C \cap \{d, d^*\} = \emptyset$  (see equations (38) and (40) and the definition of set  $C$ ), from Definition 2 it follows that  $p_C = \tilde{p}_C$ , and therefore

$$\begin{aligned} P_{\bar{\Delta}}(f_{\Gamma}(\theta, \bar{\Delta}) > \epsilon) &= P_{\Delta}(f_{\Gamma}(\theta, \Delta) > \epsilon) \\ &\leq P_{\Delta}(f_{\Gamma}(\theta, \Delta) > 0). \end{aligned}$$

Given that we have shown that equation (36) holds for arbitrary values of  $\theta$  and  $\Gamma$ , the proof is completed. ■