

# Quasi-regular sequences and optimal schedules for security games

David Kempe\*

Leonard J. Schulman†

Omer Tamuz‡

November 3, 2016

In security games, a defender commits to a mixed strategy for protecting a set of  $n$  targets of values  $\alpha_i$ ; an attacker, knowing the defender's strategy, chooses which target to attack and for how long. We study a natural version in which the attacker's utility grows linearly with the time he spends at the target, but drops to 0 if he is caught. The defender's goal is to minimize the attacker's utility. The defender's strategy consists of a schedule for visiting the targets; switching between targets takes unit time. Such games naturally model a number of real-world scenarios, including protecting computer networks from intruders, animals from poachers, etc.

We show that such security games, although played in continuous time, give rise to a combinatorial question regarding the existence of infinite sequences over a finite alphabet, with the following properties for each symbol  $i$ : (1)  $i$  constitutes a prescribed fraction  $p_i$  of the sequence, and (2) the occurrences of  $i$  are spread apart close to evenly, in that the ratio of the longest to shortest interval between consecutive occurrences is bounded by some small constant  $K$ . We call such sequences  $K$ -quasi-regular; 1-quasi-regular sequences are regular, in the sense that each symbol appears evenly spaced. We show that regular sequences over the set of targets correspond to optimal strategies for the defender, but that, in fact, 2-quasi-regular sequences already generate optimal strategies.

It is easy to see that  $K$ -quasi-regular sequences do not always exist when  $K < 2$ . We show that 2-quasi-regular random sequences always exist, and can be calculated efficiently. Using an ergodic theoretical approach, we show that deterministic 3-quasi-regular sequences always exist, and can likewise be calculated efficiently. We do not know if  $K < 3$  is possible deterministically, but give a sufficient condition on the  $p_i$  for the existence of a deterministic 2-quasi-regular sequence. We prove that our deterministic 3-regular sequences give rise to a  $\approx 1.006$ -approximation algorithm for defender's optimal strategy.

---

\*Department of Computer Science, University of Southern California

†Engineering and Applied Science, California Institute of Technology. Supported in part by NSF grants 1319745 and 1618795.

‡Departments of Economics and Mathematics, California Institute of Technology

# 1 Introduction

Game Theory, by its nature, analyzes situations with conflicting objectives between parties [15]. Among the most pronounced such conflicts is that of a defender trying to use limited resources to deter or intercept an attacker. This is the high-level topic of *inspection games* [2] and of *security games* [20]. Inspection games model interactions as varied as arms control, accounting and auditing, environmental controls, or data verification, while security games have recently become a popular model for the protection of infrastructure (airports, ports, flights), deterrence of fare evasion and smuggling, as well as protection of wildlife and plants.

Because the defender operates on a long time scale, while the attacker carries out one or a few attacks only, in security games it is typically assumed that the attacker knows the defender’s strategy; thus, the defender’s goal is to design optimal first-mover strategies, a scenario referred to as a *Stackelberg Game* [4, 23]. Hence, the defender needs to randomize her<sup>1</sup> strategy.

In the general model of security games, there are  $n$  targets of different values that the defender is trying to protect with her limited resources. An attacker, perhaps constrained in his abilities, chooses which target(s) to attack. Different assumptions and scenarios can lead to different interesting combinatorial scenarios; see, e.g., [20] for an overview of much recent work on the topic.

In the present work, we are concerned with the fact that it is not instantaneous for the defender to switch between the protection of different targets, leading to a timing component and a scheduling problem. At a high level, this models many natural security settings, including:

1. Protection of computer networks (with multiple databases or account holders) from infiltrators.
2. The protection of wildlife from poachers (e.g., [7, 6]), crops or other plants from thieves, or homes in a neighborhood from burglars.

Stripping away details, we model these settings as follows: If the attacker has access to an unprotected target, he gains utility in proportion to the value of the target and to the time he spends at the target.<sup>2</sup> The game is zero-sum in that the attacker’s gain is the defender’s loss. If the attack is interrupted by the defender at any time, both players receive utility 0. Due to physical distances between targets or switching costs between databases, the defender requires one unit of time to switch between any two targets. The problem of interest is to determine a schedule for the defender that will minimize the expected time which the attacker gets to spend at his chosen target before the defender visits that same target and halts the attack (or deters the attacker from long attacks).

More formally, the problem parameters are the number of targets,  $n$ , and the values of the targets,  $\alpha_i, 1 \leq i \leq n$ . We assume w.l.o.g. that  $\sum_i \alpha_i = 1$ . We also assume that that no target is strictly more valuable than all other targets combined,<sup>3</sup> so that  $\alpha_i \leq 1/2$ . If the attacker spends the interval  $[t, t')$  at target  $i$  without the defender being at target  $i$  during this interval, he obtains

---

<sup>1</sup>For consistency, we always refer to the attacker with male and the defender with female pronouns.

<sup>2</sup>In the case of access to computer systems, this models a scenario observed in recent attacks where the attacker lurks—whether in order to monitor legitimate users, create ongoing damage, or because file sizes or bandwidth concerns make it impossible to download the entire database in a short amount of time, or in order to cause ongoing damage.

<sup>3</sup>See Section 7 for a discussion of this choice; outside of this assumption is a different régime that requires different analysis.

a utility of  $U = (t' - t) \cdot \alpha_i$ , the defender receiving utility  $-U$ . If the defender visits the target at any point during the interval, both players' utilities are 0.

We assume that the attacker knows the defender's distribution over patrol schedules. A patrol schedule is a partial mapping from  $\mathbb{R}^{\geq 0}$  to the set of targets, where undefined values (denoted by  $\perp$ ) capture times when the defender is in transit. The switching time constraint is modeled by the constraint that visits to distinct targets are separated by at least one unit of time in transit.

Several generalizations are naturally of interest and are discussed briefly in Section 7. These include non-uniform switching times between targets, non-zero sum games, non-linear attacker rewards, and multiple defenders as in [13].

## 1.1 From Strategies to Distributions over Sequences

We first show (in Section 2) that w.l.o.g., the defender's strategy (or schedule) is *shift-invariant*, in the sense that regardless of his chosen start time  $t$  for his attack, the attacker will face the exact same distribution over subsequent schedules. Furthermore, we prove that it suffices to consider only defender strategies satisfying the following two properties: (1) The defender never waits at any target, (2) The defender travels between targets within one time unit.

Properties (1) and (2) reduce the problem of constructing optimal defender strategies to one of constructing sequences  $s : \mathbb{N} \rightarrow \{1, \dots, n\}$ ; random sequences correspond to mixed strategies, and shift-invariant random sequences correspond to shift-invariant mixed strategies.

We show that a random, shift-invariant sequence corresponds to an optimal schedule for the defender if it is *regular* — i.e., each target appears in it evenly spaced, and  $\mathbb{P}[s_k = i] = \alpha_i$  for all targets  $i$ .<sup>4</sup> Our first result (Theorem 3.1) is that — perhaps surprisingly — it in fact suffices for optimality that the sequence is *2-quasi-regular*; a shift-invariant random sequence  $s$  is  $K$ -quasi-regular if, as before,  $\mathbb{P}[s_k = i] = \alpha_i$ , and if the ratio of the longest to shortest interval between consecutive occurrences of  $i$  in  $s$  is bounded by  $K$ . Some intuition is derived from the famous “Inspection Paradox” or “Waiting Time Problem”: passengers of a bus service which departs a station with perfect regularity (e.g., 15 minutes apart) wait on average half as long as passengers of a service with the same frequency of operation but Poisson departure times. In our case, higher variance in the defender's interarrival times make longer attacks more attractive.

We say that a deterministic sequence  $s : \mathbb{N} \rightarrow \{1, \dots, n\}$  is  $K$ -quasi-regular if the *density*<sup>5</sup> of  $i$  in  $s$  is equal to  $\alpha_i$ , and if  $s$  satisfies the same constraint on the intervals between consecutive occurrences. Shift-invariant quasi-regular random sequences can be constructed from deterministic quasi-regular ones, and therefore it is natural to ask when the latter exist. Similar questions have a significant history of study, see, e.g., [1, 10, 21, 22]. The goal in previous work has been low *discrepancy*: that up to any time  $t$ , the number of visits to target  $i$  approximates  $t\alpha_i$  as closely as possible. For our application, the rate of convergence of the frequencies to  $\alpha_i$  is not essential; but it is on the other hand crucial that the defender's interarrival times at each target be as regular as possible.

## 1.2 Our Main Result

It is fairly straightforward to show that there is some vector  $(\alpha_i)_i$  such that there are no  $(2 - \epsilon)$ -quasi-regular sequences for any  $\epsilon > 0$ ; we do this in Section 3. It is then a natural question how

<sup>4</sup>By shift invariance, this probability is independent of  $k$ .

<sup>5</sup>The density of  $i$  in  $s$  is  $\lim_{t \rightarrow \infty} \frac{1}{t} |s^{-1}(i) \cap [t]|$ .

small  $K$  can be such that we can still obtain  $K$ -quasi-regular sequences.

Our main result (Theorem 4.1 in Section 4) is that for any values  $\alpha_i$ , there exists a 2-quasi-regular random sequence, which can furthermore be efficiently computed from the  $\alpha_i$ . By the aforementioned Theorem 3.1, the corresponding defender mixed strategy is optimal.

### 1.3 Ergodic Schedules

The existence of quasi-regular sequences may be of interest in its own right, as fundamental combinatorial objects. One limitation of our main result (although it may not affect the application) is that the resulting schedules are not ergodic: they randomize between different schedules in which the items have frequencies differing from the desired  $\alpha_i$ . It is then a natural question whether 2-quasi-regular ergodic sequences can be obtained as well. This is equivalent to the following combinatorial question: given densities  $\alpha_i$ , does there always exist a 2-quasi regular deterministic sequence?

We provide two partial answers to this question. In Section 5, we analyze a very simple schedule called the *Golden Ratio Schedule* (studied in the context of hashing [12, pp. 510,511,543], bandwidth sharing [11, 16] and elsewhere). This schedule is generated by the following random sequence: label the unit circle with intervals of size  $\alpha_i$  corresponding to the targets  $i$ . Choose a uniformly random starting point in the unit interval. In each step, add  $1/\varphi$  to the current point, wrapping around from 1 to 0; here,  $\varphi = \frac{1}{2}(1 + \sqrt{5})$  is the golden ratio. In each time step, the defender visits the target  $i$  into whose interval the current point falls.

This random sequence is shift-invariant and ergodic, and at worst 3-quasi-regular.<sup>6</sup> Moreover, for any choice of the random starting point, the deterministic sequence is 3-quasi-regular. Thus we show that there always exist deterministic 3-quasi-regular sequences. We do not know if this is true for any  $K < 3$ .

It is interesting that such a simple schedule achieves constant quasi-regularity, but the bound is not strong enough to guarantee optimality of the schedule for the defender. However, we show that the schedule is nearly optimal for the defender: the attacker’s utility is within a factor of at most 1.006 of the minimum attacker utility. The proof of this approximation guarantee relies on a theorem of Slater about simple dynamical systems like the Golden Ratio shift, and a somewhat intricate analysis of the attacker’s response. We find it remarkable that such a simple policy comes provably within 0.6% of the optimum, in particular compared to another very simple policy: as we show in Appendix A, the simple *i.i.d. schedule*, which always chooses the next target  $i$  to visit with probability  $\alpha_i$ , independent of the history, is only a 4/e-approximation.

As a second partial result towards obtaining an optimal ergodic schedule, in Section 6, we give a sufficient condition for its existence. Let  $M$  be the smallest common denominator of all  $\alpha_i$ . Whenever  $M < e^{(1/9-\epsilon)n}$  for any  $\epsilon > 0$ , a defender-optimal ergodic schedule exists and can be found efficiently using a randomized algorithm that succeeds with high probability.

The algorithm is based on placing points for target  $i$  at uniform distance proportional to  $1/\alpha_i$  on the unit circle, with independent uniformly random offsets. Points can only be matched to sufficiently close multiples of  $1/M$ . An application of Hall’s Theorem, similar to [10], shows that under the conditions of the theorem, this algorithm succeeds with high probability in producing a 2-quasi-regular sequence.

---

<sup>6</sup>When all  $\alpha_i \leq 1 - 1/\varphi$ , the bound improves to 8/3, and as  $\alpha_i \rightarrow 0$ , it converges to  $\varphi^2$ .

## 2 Preliminaries

The  $n$  targets have values  $\alpha_i > 0$  for all  $i$ . Because the units in which target values are measured are irrelevant, we assume that  $\sum_i \alpha_i = 1$ . We assume that no target has value exceeding the sum of all other targets' values, meaning (after normalization) that  $\alpha_i \leq \frac{1}{2}$  for all  $i$ .

A *pure strategy* (or *schedule*) for the defender is a measurable mapping  $\ell : \mathbb{R}^{\geq 0} \rightarrow \{1, 2, \dots, n, \perp\}$ , where  $\perp$  denotes that the defender is in transit. A schedule  $\ell$  is *valid* if  $\ell(t) = i$  and  $\ell(t') = j \neq i$  implies that  $|t' - t| \geq 1$ . In other words, there is enough time for the defender to move from  $i$  to  $j$  (or from  $j$  to  $i$ ). We use  $\mathcal{S}$  to denote the set of all valid pure defender strategies.

The defender moves first and commits to a mixed strategy, i.e., a distribution  $\Lambda$  over  $\mathcal{S}$ , or a random  $\ell$ . Then, the attacker chooses a target  $i$  and interval  $[t, t']$ . Subsequently, a mapping  $\ell$  is drawn from the defender's distribution  $\Lambda$ . The attacker's utility is

$$U(\ell, (i, t, t')) = \begin{cases} 0 & \text{if } \ell(\tau) = i \text{ for some } t \leq \tau \leq t' \\ \alpha_i \cdot (t' - t) & \text{otherwise.} \end{cases} \quad (1)$$

Since we are considering a zero-sum game (see Section 7 for a discussion), the defender's utility is  $-U(\ell, (i, t, t'))$ .

Since a rational attacker will choose  $i, t, t'$  so as to maximize  $\mathbb{E}_{\ell \sim \Lambda} [U(\ell, (i, x, t))]$ , the defender's goal is to choose  $\Lambda$  to minimize

$$U(\Lambda) = \sup_{i, t, t'} \mathbb{E}_{\ell \sim \Lambda} [U(\ell, (i, t, t'))].$$

### 2.1 Canonical, Shift-Invariant, and Ergodic Schedules

The general definition of defender schedules allows for strange schedules that are clearly suboptimal. We would like to restrict our attention to “reasonable” schedules. In particular, we will assume the two following conditions, which we later show is without loss of generality. (Here, we will be slightly informal in our definitions. Precise definitions and constructions ensuring these properties are given in Appendix B.)

- The defender does not spend time in transit unnecessarily. Specifically, the defender (1) never visits the same target  $i$  both immediately before and after time in transit, (2) is never in transit at time 0, and (3) never spends more than one unit consecutively in transit. We call schedules satisfying (1)–(3) *canonical*.
- To the attacker, any two times  $t$  and  $t'$  “look the same”, in that for any  $t, t', \tau \in \mathbb{R}^+$ , the distributions of the defender's schedule restricted to the time intervals  $[t, t + \tau]$  and  $[t', t' + \tau]$  are the same. We call such schedules *shift-invariant*.

In Appendix B, we show that an optimal mixed defender strategy exists (which is not a priori obvious), and is w.l.o.g. canonical and shift-invariant. Therefore, for the remainder of this paper, we will focus only on shift-invariant canonical schedules. Shift-invariance allows us to implicitly assume that the attacker always attacks at time 0. We then simply write  $U(\Lambda, (i, t))$  for the attacker's utility from attacking target  $i$  for  $t$  units of time.

An additional desirable property of shift-invariant mixed schedules  $\Lambda$  is *ergodicity*:  $\Lambda$  is ergodic if  $\Lambda$  cannot be written as the convex combination  $\Lambda = \lambda\Lambda_1 + (1 - \lambda)\Lambda_2$  of two different shift-invariant

mixed schedules. By the Ergodic Theorem, this is equivalent to  $\Lambda$  being the limit of a uniformly random shift (over a larger and larger range of shifts) of a single pure schedule  $\ell_0$ . (A formal discussion is again given in Appendix B.)

## 2.2 Schedules from Sequences

All the constructions of mixed defender schedules in this paper will have  $F_i(0) = 0$ , i.e., the defender never waits at any target. Canonical schedules without waiting are readily identified with schedules defined only on integers, since the defender must only choose, after visiting a target, which target she will visit next.

We call such schedules *sequences*, defined as  $s: \mathbb{N} \rightarrow \{1, \dots, n\}$ . A sequence, together with a start time  $t_0$ , naturally defines a canonical schedule, by setting  $\ell(t) = s_{t-t_0}$  if  $t-t_0 \in \mathbb{N}$ , and  $\ell(t) = \perp$  otherwise.  $S$  denotes a distribution over sequences, or the distribution of a random sequence  $s$ .

Shift-invariance can be defined for random sequences as for (continuous) mixed schedules. When  $s$  is a periodic sequence, i.e., there is a  $k$  such that  $s_{t+k} = s_t$  for all  $t$ , a shift-invariant random sequence can be obtained particularly easily, by choosing a uniformly random  $\kappa \in \{0, \dots, k-1\}$ , and defining  $s'$  via  $s'_t = s_{t+\kappa}$ . From a shift-invariant random sequence, we can obtain a shift-invariant mixed schedule straightforwardly, by choosing the start time  $t_0 \in [0, 1]$  uniformly.

## 2.3 Return Times and Target Visit Frequencies

Since the attacker chooses only the target  $i$  and the duration  $t$  of the attack, from his perspective, the property of the defender's strategy that matters is the distribution of her next *return time* to target  $i$ , defined as  $R_i = \min\{t \geq 0 \mid \ell(t) = i\}$ . Given a target  $i$ , let  $F_i(t) = \mathbb{P}[R_i \leq t]$  denote the CDF of  $R_i$ . In particular, notice that  $F_i(0)$  is the fraction of time the defender spends waiting at target  $i$ . In terms of the distribution of return times  $F_i$ , the attacker's utility can be expressed as follows:

$$U(F_i, (i, t)) = \alpha_i \cdot t \cdot (1 - F_i(t)). \quad (2)$$

Several quantities are useful for reasoning about the  $F_i$ . First, for a random shift-invariant sequence  $s$ , we let  $y_i = \mathbb{P}[s_1 = i]$  denote the fraction of target visits devoted to target  $i$ . (The choice of time  $t = 1$  here is immaterial by shift-invariance.) We also define  $z_i = 1/y_i$ . If  $s$  is periodic, then  $z_i$  is the expected number of steps between consecutive occurrences of  $i$ . Generalizations of these definitions to arbitrary mixed schedules are given in Appendix B; one can take  $y_i = F_i(1)$  and  $z_i = \frac{1-F_i(0)}{y_i-F_i(0)}$ .

The number of steps between consecutive occurrences of  $i$  is very useful for our analysis. Intuitively, we would like  $B_i$  to be the random variable capturing the time between consecutive visits to target  $i$ . Defining the distribution precisely requires some care, and is done formally in Appendix B. The construction formalizes the following intuition: we can consider the limit as we shift the random sequence  $s$  left by  $t \rightarrow \infty$ . This extends a shift-invariant random sequence from the natural numbers to all integers, and allows us to consider the random variable

$$B_i = (\min\{t > 0 \mid s_t = i\}) - (\max\{t \leq 0 \mid s_t = i\}).$$

The random variable  $B_i$  captures the time between consecutive visits before and after time 0 — by shift-invariance, the time 0 is again arbitrary. Notice that the distribution of  $B_i$  “assigns higher

probability to higher values”; as in the inspection paradox, larger gaps are more likely to appear at a fixed time than on average over a long time stretch. Our constructions will always ensure that  $B_i$  is finite. We can relate  $F_i$ ,  $z_i$ ,  $y_i$ , and  $B_i$  as follows.

$$\begin{aligned}
 F_i(t) &= \frac{1}{\mathbb{E}[B_i]} \cdot \sum_{\tau=0}^{t-1} \mathbb{P}[B_i > \tau], \\
 y_i &= F_i(1) = \frac{1}{\mathbb{E}[B_i]} \cdot \mathbb{P}[B_i > 0] = \frac{1}{\mathbb{E}[B_i]}, \\
 z_i &= \frac{1}{y_i} = \mathbb{E}[B_i].
 \end{aligned} \tag{3}$$

Equation (3), as well as the assertion that  $\mathbb{E}[B_i] < \infty$ , follow from standard facts in the theory of stationary renewal processes [5, Thm. 4]; the other equalities are derived directly from it. The most useful facts about  $F_i$  are summarized by the following proposition:

**Proposition 2.1**    1.  $F_i(t) \leq y_i \cdot t$ , with equality iff  $\mathbb{P}[B_i > t - 1] = 1$ .  
 2.  $F_i$  is concave.

**Proof.** For the first part, we use Equation (3) to get

$$F_i(t) = \frac{1}{\mathbb{E}[B_i]} \cdot \sum_{\tau=0}^{t-1} \mathbb{P}[B_i > \tau] \leq \frac{1}{\mathbb{E}[B_i]} \cdot t = y_i \cdot t,$$

with equality iff  $\mathbb{P}[B_i > t] = 1$ .

For the second part, simply notice that  $\mathbb{P}[B_i > \tau]$  is monotone non-increasing in  $\tau$ . ■

## 2.4 Regular and Quasi-Regular Sequences

We say that a random sequence  $s$  is  $K$ -quasi-regular if the following two hold for each target  $i$ :

1.  $\mathbb{P}[s_1 = i] = \alpha_i$ .
2. There is some  $b_i$  such that  $\mathbb{P}[b_i \leq B_i \leq K \cdot b_i] = 1$ .

In other words, each target is visited with frequency  $\alpha_i$ , and the maximum gap for consecutive visits to target  $i$  is within a factor  $K$  of the minimum gap with probability 1. A random sequence is *regular* if it is 1-quasi-regular, meaning that all visits to target  $i$  are spaced exactly  $z_i$  apart. (All definitions extend directly to canonical, mixed, shift-invariant schedules.)

A particularly straightforward way to obtain a  $K$ -quasi-regular random sequence  $S$  is to consider the limit of uniformly random shifts of a sequence  $s$  in which the gaps between consecutive visits to  $i$  are bounded between  $b_i$  and  $Kb_i$ , and the density of entries which are  $i$  is  $\alpha_i$ .

Combinatorial objects similar to quasi-regular sequences have been studied in the past (e.g., [21, 10]).

### 3 The Attacker's Response, and Optimal Schedules

In this section, we show the following main theorem, a sufficient condition for a random sequence to be optimal for the defender.

**Theorem 3.1** *Consider a random shift-invariant sequence such that the following two hold for each target  $i$ :*

- $z_i = 1/\alpha_i$ .
- For each  $i$ , there exists an  $\eta_i$  such that  $\mathbb{P}[\frac{\eta_i}{\eta_i+1}z_i \leq B_i \leq \eta_i z_i] = 1$ .

*Then, the associated mixed strategy is optimal for the defender.*

*In particular, the second condition holds for 2-quasi-regular random sequences.*

In Section 4, we show that there always exists a 2-quasi-regular sequence with  $z_i = 1/\alpha_i$  for all  $i$ .

With the eventual goal of proving Theorem 3.1, we fix a target  $i$ , and for now drop the subscript  $i$ , so that

$$y = y_i \qquad F(t) = F_i(t) \qquad z = z_i.$$

We fix  $y$  and  $z$  and study which sequences — among all those with these  $y$  and  $z$  — are optimal.

**Proposition 3.2** *Consider any canonical shift-invariant mixed defender schedule (over the non-negative real numbers). By choosing  $t = z/2$ , the attacker guarantees himself a utility of at least  $\frac{1}{4} \cdot \alpha \cdot z$ .*

**Proof.** By Equation (2), the attacker's utility at time  $t = z/2$  is  $\alpha \cdot (z/2) \cdot (1 - F(z/2))$ . Using Proposition B.4 (the straightforward generalization of Proposition 2.1 to mixed schedules), we can bound

$$1 - F(z/2) \geq 1 - F(0) - (y - F(0)) \cdot (z/2) = (1 - F(0)) \cdot \left(1 - \frac{y - F(0)}{1 - F(0)} \cdot (z/2)\right) = \frac{1 - F(0)}{2}.$$

Hence, the attacker's utility is at least  $\alpha \cdot \frac{1 - F(0)}{4} \cdot z$ . ■

**Proof.** By Equation (2), the attacker's utility at time  $t = z/2$  is  $\alpha \cdot z/2 \cdot (1 - F(z/2))$ . Using Proposition 2.1, we can bound

$$1 - F(z/2) \geq 1 - y \cdot \frac{z}{2} = \frac{1}{2}.$$

Hence, the attacker's utility is at least  $\frac{1}{4} \cdot \alpha \cdot z$ . ■

We obtain the following simple corollary about random sequences that are worst for the attacker:

**Corollary 3.3** *Among random sequences with fixed  $z$  and  $y$ , any random sequence is optimal for the defender if the attacker's optimal attack duration guarantees him a payoff of  $\frac{1}{4} \cdot \alpha \cdot z$ .*



The following corollary is particularly useful:

**Corollary 3.4** *Fix  $z$  and  $y$ , and choose a random sequence such that  $\mathbb{P}[B_i > t] = 1$ , where  $t$  is the attacker's optimal attack duration. Then, this random sequence is optimal for the defender. Furthermore, in this case, w.l.o.g.,  $t = z/2$ .*

**Proof.** By the assumption that  $\mathbb{P}[B_i > t] = 1$  and Proposition 2.1, we have that

$$F_i(t) = y_i \cdot t.$$

Hence, the attacker's utility is

$$\alpha \cdot (1 - y \cdot t) \cdot t = \alpha \cdot \frac{t \cdot (z - t)}{z} \leq \alpha \cdot \frac{z}{4}.$$

Now, the claim follows directly from Corollary 3.3. That  $t = z/2$  is a best response follows from Proposition 3.2.  $\blacksquare$

We can now apply these corollaries to show optimality for a single target for which the “quasi-regularity” of return times holds.

**Proposition 3.5** *Fix  $z$  and  $y$ , and consider a random sequence such that for some  $\eta$ ,*

$$\mathbb{P}\left[\frac{\eta_i}{\eta_i + 1} z_i \leq B_i \leq \eta_i z_i\right] = 1.$$

*Then, this schedule is optimal for the defender among schedules with the these  $z$  and  $y$ .*

**Proof.** We write  $\xi = \frac{\eta}{\eta+1}$ . By Proposition 3.2, choosing  $t = z/2$ , the attacker can guarantee himself at least a utility of  $\frac{1}{4} \cdot \alpha \cdot z$ . We will show below that the attacker's utility for any attack duration  $t \in [\xi z, \infty)$  is at most  $\frac{1}{4} \cdot \alpha \cdot z$ .

Hence, the attacker has an optimal attack duration  $t \leq \xi z$  (either  $t = z/2$  or a different  $t$ ). By the assumption and Proposition 2.1,  $F(\xi z) = y \cdot \xi z$ . Using the concavity of  $F$ , this implies that  $F(t) = y \cdot t$  for all  $t \leq \xi z$ . Thus, whichever such  $t$  is optimal for the attacker, Corollary 3.4 implies that  $F$  is worst for the attacker, and furthermore, that  $t = z/2$  is optimal for the attacker after all.

It remains to prove the upper bound for  $t \geq \xi z$ . For any  $t \geq \eta z$ , the assumption that  $F(\eta z) = 1$  implies a utility of 0 for the attacker. So we focus on  $t \in [\xi z, \eta z]$ , and show that in this range, the maximum utility of the attacker is  $z/4$ .

By assumption and Proposition 2.1,  $F(\xi z) = \xi$  and  $F(\eta z) = 1$ . Since  $F$  is concave by Proposition 2.1, for  $t \in [\xi z, \eta z]$ ,  $F$  is bounded below by the line connecting  $(\xi z, \xi)$  and  $(\eta z, 1)$ , so

$$\begin{aligned} F(t) &\geq \xi + \frac{t - \xi z}{(\eta - \xi)z} \cdot (1 - \xi) = \left( \xi + \frac{t - \xi z}{(\eta - \xi)z} \cdot (1 - \xi) \right) \\ &= \left( \xi \cdot \frac{\eta - 1}{\eta - \xi} + \frac{1 - \xi}{(\eta - \xi)z} \cdot t \right) = \left( \frac{\eta - 1}{\eta} + \frac{1}{\eta^2} \cdot \frac{t}{z} \right). \end{aligned}$$

Hence, the attacker's utility is upper-bounded by

$$\alpha \cdot t \cdot (1 - F(t)) \leq \alpha \cdot t \cdot \left( \frac{1}{\eta} - \frac{1}{\eta^2} \cdot \frac{t}{z} \right).$$

This is maximized at  $t^* = \frac{\eta z}{2}$ , so we obtain that

$$\alpha \cdot t \cdot (1 - F(t)) \leq \alpha \cdot t^* \cdot \left( \frac{1}{\eta} - \frac{1}{\eta^2} \cdot \frac{t^*}{z} \right) = \alpha \cdot \frac{z}{4}.$$

This completes the proof. ■

**Proof of Theorem 3.1.** To complete the proof of Theorem 3.1, we now consider multiple targets  $i$ . By the assumptions of the theorem and Proposition 3.5, against the proposed class of random sequences, the attacker can obtain utility of at most  $\frac{1}{4}$ , regardless of which target  $i$  he attacks and for how long, by choosing  $z_i = 1/y_i = 1/\alpha_i$ .

We will show that no shift-invariant mixed defender schedule (now considered over the non-negative real numbers) can achieve an expected attacker payoff strictly smaller than  $\frac{1}{4}$ . Focus on a shift-invariant mixed defender schedule  $\Lambda$ . By Lemma B.2, we may assume that  $\Lambda$  is canonical.

Fix some index  $i$  such that  $\alpha_i/y_i \geq 1$ . Such an index must exist because  $\sum_i \alpha_i = 1$  and  $\sum_i y_i \leq 1$ . Because we assumed that  $\alpha_i \leq \frac{1}{2}$  for all  $i$ , this also implies that  $y_i \leq \frac{1}{2}$ .

By Proposition 3.2, attacking target  $i$  for  $t = z_i/2$  units of time, the attacker can guarantee himself a utility of at least

$$\alpha_i \cdot \frac{1 - F_i(0)}{4} \cdot z_i = \alpha_i \cdot \frac{(1 - F_i(0))^2}{4(y_i - F_i(0))} \stackrel{y_i \leq \frac{1}{2}}{\geq} \alpha_i \cdot \frac{1}{4y_i} \geq \frac{1}{4},$$

where the final inequality followed because the chosen index  $i$  satisfied  $\alpha_i/y_i \geq 1$ . Hence, the attacker can guarantee himself a payoff of at least  $\frac{1}{4}$  against any mixed defender schedule, proving optimality of the proposed class of random sequences.

Finally, we show that this applies to 2-quasi-regular random sequences. Assume that there exists a  $b$  such that  $\mathbb{P}[b \leq B_i \leq 2b] = 1$ , and define  $\eta_i = 2b/z_i$ . Then,  $\xi_i z_i = \frac{\eta_i}{\eta_i + 1} z_i = \frac{2b}{2b/z_i + 1}$ . This implies that  $b \leq z_i \leq 2b$ , and thus  $\frac{\eta_i}{\eta_i + 1} z_i \geq b$ . Therefore, we obtain that  $\mathbb{P}[\frac{\eta_i}{\eta_i + 1} z_i \leq B_i \leq \eta_i z_i] = 1$ , completing the proof. ■

We end this section with a result that shows that the optimality result for 2-quasi-regular random sequences cannot be improved.

**Proposition 3.6** *Let  $n = 3$  and  $\alpha = (1/2, 1/3, 1/6)$ . Then, for every  $\epsilon > 0$ , there are no  $(2 - \epsilon)$ -quasi-regular random sequences.*

We prove this result in Appendix C. An immediate corollary is the following.

**Corollary 3.7** *Let  $n = 3$  and  $\alpha = (1/2, 1/3, 1/6)$ . Then for every  $\epsilon > 0$ , there exists no  $(2 - \epsilon)$ -quasi-regular deterministic sequence.*

## 4 An Optimal Defender Strategy

In this section, we present Algorithm 1, constructing a 2-quasi-regular random sequence. Such a random sequence is optimal for the defender by Theorem 3.1.

Notice that the sequence produced by Algorithm 1 is shift-invariant by construction, but not ergodic, since it randomizes over different shift-invariant distributions.

---

**Algorithm 1** An optimal schedule for the defender

---

- 1: Let  $p_i = \alpha_i$  for all  $i$ .
  - 2: For each  $i$ , let  $m_i$  be such that  $2^{-m_i} \leq p_i < 2^{1-m_i}$ . Let  $I_i = [2^{-m_i}, 2^{1-m_i}]$ .
  - 3: Use the algorithm from the proof of Lemma 4.3 for  $\mathbf{p}$  and the  $I_i$  to randomly round  $\mathbf{p}$  to a probability vector  $\mathbf{q}$ , such that all but at most one index  $i$  have  $q_i = 2^{-m_i}$  or  $q_i = 2^{1-m_i}$ .
  - 4: Use the algorithm from the proof of Lemma 4.5 to produce a periodic sequence  $s$ .
  - 5: Return the random sequence obtained by choosing a uniform random shift of  $s$ .
- 

**Theorem 4.1** *The random sequence generated by Algorithm 1 is 2-quasi-regular, and hence optimal for the defender.*

We begin with a simple technical lemma.

**Lemma 4.2** *Let  $S$  be a multiset of powers of 2, such that  $\max_{p \in S} p \leq 2^{-k} \leq \sum_{p \in S} p$ . Then, there exists a subset  $T \subseteq S$  with  $\sum_{p \in T} p = 2^{-k}$ .*

**Proof.** We prove this claim by induction on  $|S|$ . The claim is trivial for  $|S| = 1$ . Consider  $|S| \geq 2$ , and distinguish two cases.

1. If  $S$  contains two copies of some number  $p < 2^{-k}$ , then construct  $S'$  by replacing these two copies with  $p' = 2p$ . By induction hypothesis,  $S'$  contains a subset  $T'$  adding up to  $2^{-k}$ . If  $T'$  contained the newly constructed element  $p'$ , then replace it with the two copies of  $p$ . In either case, we have the desired set  $T \subseteq S$ .
2. Otherwise,  $S$  contains at most one copy of each number  $p \leq 2^{-k}$ . If  $S$  did not contain  $2^{-k}$ , then  $\sum_{p \in S} p < \sum_{i=1}^{\infty} 2^{-(k+i)} = 2^{-k}$ , contradicting the assumptions of the lemma. Hence,  $S$  contains  $2^{-k}$ , and the singleton set of that number is the desired subset. ■

Next, we show that distributions can be rounded “almost to powers of two.”

**Lemma 4.3** *Let  $\mathbf{p} = (p_1, p_2, \dots, p_n)$  be a probability distribution. For each  $i$ , let  $I_i = [\ell_i, r_i] \ni p_i$  be an interval. Then, there exists a distribution  $\mathcal{D}$  over probability distributions  $\mathbf{q} = (q_1, q_2, \dots, q_n)$  such that:*

1.  $\mathbb{E}[q_i] = p_i$  for all  $i$ ,
2.  $q_i \in I_i$  for all  $\mathbf{q}$  in the support of  $\mathcal{D}$ , and
3. For each  $\mathbf{q}$  in the support of  $\mathcal{D}$ , all but at most one of the  $q_i$  are equal to  $\ell_i$  or  $r_i$ .

**Proof.** We will give a randomized “rounding” procedure that starts with  $\mathbf{p}$  and produces a  $\mathbf{q}$ , satisfying all of the claimed properties, by making the  $p_i$  equal to  $\ell_i$  or  $r_i$  one at a time. The randomized rounding bears similarity to dependent randomized rounding algorithms in the approximation algorithms literature (e.g., [3, 8, 19]), though we do not require concentration bounds, and allow one of the  $q_i$  to be an interior point of its interval. In the rounding, we always consider two indices  $i, j$  with  $p_i = \ell_i + \epsilon_i, p_j = \ell_j + \epsilon_j$ , such that  $0 < \epsilon_i < r_i - \ell_i, 0 < \epsilon_j < r_j - \ell_j$ . (That is, neither  $p_i$  nor  $p_j$  is on the boundary of its interval.) We probabilistically replace them with  $p'_i, p'_j$ , such that all of the following hold:

- At least one of  $p'_i, p'_j$  is at the boundary of its interval.
- $\ell_i \leq p'_i \leq r_i$  and  $\ell_j \leq p'_j \leq r_j$ .
- $p'_i + p'_j = p_i + p_j$ .
- $\mathbb{E}[p'_i] = p_i$  and  $\mathbb{E}[p'_j] = p_j$ .

The rounding terminates when there is at most one  $p_i$  that is not at the boundary of its interval; let  $\mathbf{q}$  be the vector of probabilities at that point. By iterating expectations, we obtain that  $\mathbb{E}[q_i] = p_i$  for all  $i$ . The upper and lower bounds on  $q_i$  are maintained inductively, and the termination condition ensures the third claimed property of  $\mathbf{q}$ .

So consider arbitrary  $p_i, p_j$  as above. Let  $\delta_i = \min(\epsilon_i, r_j - \ell_j - \epsilon_j)$  and  $\delta_j = \min(\epsilon_j, r_i - \ell_i - \epsilon_i)$ . With probability  $\frac{\delta_j}{\delta_i + \delta_j}$ , round  $p_i$  to  $p'_i = p_i - \delta_i$  and  $p_j$  to  $p'_j = p_j + \delta_i$ . With probability  $1 - \frac{\delta_j}{\delta_i + \delta_j} = \frac{\delta_i}{\delta_i + \delta_j}$ , round  $p_i$  to  $p'_i = p_i + \delta_j$  and  $p_j$  to  $p'_j = p_j - \delta_j$ .

First, it is clear that  $p'_i + p'_j = p_i + p_j$ . Also, by definition of  $\delta_i, \delta_j$ , we get that  $\ell_i \leq p'_i \leq r_i$  and  $\ell_j \leq p'_j \leq r_j$ . If we round according to the first case, then  $p'_i = p_i - \delta_i$  and  $p'_j = p_j + \delta_i$ . If  $\delta_i = \epsilon_i$ , then we get that  $p'_i = \ell_i$ , while if  $\delta_i = r_j - \epsilon_j$ , then  $p'_j = \ell_j + \epsilon_j + (r_j - \ell_j - \epsilon_j) = r_j$ . Calculations are similar in the other case. Finally,

$$\mathbb{E}[p'_i] = \frac{\delta_j}{\delta_i + \delta_j} \cdot (p_i - \delta_i) + \frac{\delta_i}{\delta_i + \delta_j} \cdot (p_i + \delta_j) = p_i.$$

Hence, all the claimed properties hold in each step. ■

As a first step towards a 2-quasi-regular random sequence, we consider the case of probability vectors in which all probabilities are powers of 2.<sup>7</sup>

**Lemma 4.4** *Assume that the probability vector  $\mathbf{p}$  is such that each  $p_i = 2^{-m_i}$  is a power of 2. Then, there exists a regular sequence for  $\mathbf{p}$ .*

**Proof.** We will prove this claim by induction on the number of targets. If we have a single target, then its probability must be 1, so it is visited at intervals of 1 and we set  $s$  to be the constant sequence. Otherwise, the maximum probability of any target is  $\frac{1}{2}$ , and the sum of all probabilities is 1. Lemma 4.2 therefore guarantees the existence of a subset  $S$  whose probabilities add up to  $\frac{1}{2}$ .

Consider instances obtained from  $S$  and  $\bar{S}$  by scaling up all probabilities by a factor of 2, resulting in  $p'_i = 2p_i$ . By induction hypothesis, each of those instances can be scheduled such that each target  $i$  is visited every  $1/p'_i = 1/(2p_i)$  time steps. Now alternate between the two sequences. In this new sequence, each target  $i$  is visited every  $2/p'_i = 1/p_i$  steps, as desired. ■

Next, we show that sufficiently good sequences can also be achieved when at most one of the probabilities is not a power of 2.

**Lemma 4.5** *Assume that the probability vector  $\mathbf{p}$  is such that each  $p_i = 2^{-m_i}$  is a power of 2, except for (possibly)  $p_1 = 2^{-m_1} - \epsilon$ , with  $0 \leq \epsilon < 2^{-(m_1+1)}$ . Then, there exists a (non-random) sequence  $s$  with the following properties:*

<sup>7</sup>Lemma 4.4 generalizes to powers of any integer, and in fact to any probabilities  $p_i$  such that there are integers  $a_1, a_2, \dots$  and indices  $k_i$  such that  $p_i = (\prod_{j=1}^{k_i} a_j)^{-1}$  for all  $i$ .

1. The time between consecutive visits to target  $i > 1$  is always exactly  $1/p_i$ .
2. The time between consecutive visits to target 1 is always either  $2^{m_1}$  or  $2^{m_1+1}$ .
3. The frequency of target  $i$  is  $p_i$  for all  $i$ .

**Proof.** Without loss of generality, assume that  $p_2 \geq p_3 \geq \dots \geq p_n$ . Write  $\epsilon = \sum_j 2^{-k_j}$ , where  $m_1 + 1 < k_1 < k_2 < \dots$ , and the sum could be empty. First, we will show that for each  $j$ , there is a subset  $S_j \subseteq \{2, \dots, n\}$  of targets such that  $\sum_{i \in S_j} p_i = 2^{-k_j}$ , and the  $S_j$  are pairwise disjoint. We inductively construct these sets  $S_j$ .

First, notice that  $k_j \leq m_n$  for all  $j$ ; in particular, the sum representation of  $\epsilon$  must be finite. This is because  $\sum_i p_i = 1 \equiv 0 \pmod{p_n}$ . Now consider the largest  $j$  in the sum, and let  $T := \{i \geq 2 \mid m_i \geq k_j\}$ . Because

$$2^{-k_j} + \sum_{i \in T} p_i = 1 - ((p_1 - 2^{-k_j}) + \sum_{i \geq 2, i \notin T} p_i) \equiv 0 \pmod{2^{1-k_j}},$$

we get that  $\sum_{i \in T} p_i \geq 2^{-k_j}$ . Thus, by Lemma 4.2, there is a subset  $S_j \subseteq T$  summing up to exactly  $2^{-k_j}$ . Consider an instance in which the targets in  $S_j$  have been removed, and  $\epsilon$  has been replaced with  $\epsilon' = \epsilon - 2^{-k_j}$ . Since this instance has fewer targets, we can apply induction to construct the remaining  $S_{j'}$ . Eventually, we will have constructed the disjoint sets  $S_j$ , as claimed.

Now consider a revised instance, in which the targets 1 and all  $i \in S_j$  (for all  $j$ ) have been combined into a new target of probability  $p'_1 = 2^{-m_1}$ . This is now an instance in which the probabilities still add up to 1, and each probability is a power of 2. By Lemma 4.4, this instance admits a regular sequence. For all  $i \neq 1, i \notin S_j$  (for all  $j$ ), keep this sequence fixed.

Finally, we have to deal with the targets in the sets  $S_j$ . Notice that  $\sum_{i \in S_j} p_i = 2^{-k_j}$  for all  $j$ . Consider the set  $\hat{T}$  of all the slots assigned to the “target” of probability  $p'_1$ ; without loss of generality,  $\hat{T} = \{k \mid k \equiv 0 \pmod{2^{m_1}}\}$ . Define  $\hat{T}_j = \{k \mid k \equiv 2^{k_j-1} \pmod{2^{k_j}}\}$ . Notice that the  $\hat{T}_j$  are pairwise disjoint, and because  $k_j > m_1 + 1$ , we have that  $\hat{T}_j \subseteq \hat{T}$  for all  $j$ . We will give all slots in  $\hat{T}_j$  to targets in  $S_j$ , and all other slots in  $\hat{T}$  to target 1. By definition, the frequency of slots in  $\hat{T}_j$  is  $2^{-k_j}$ , and by Lemma 4.4, using the slots in  $T_j$ , the targets  $i \in S_j$  can be scheduled regularly.

Because  $k_j \geq k_1 > m_1 + 1$ , at least all slots in  $\hat{T}_{m_1+1}$  are assigned to target 1, and possibly some of the other slots as well. Thus, the distance between consecutive visits to target 1 are either  $2^{m_1}$  or  $2^{1+m_1}$ .

Finally, for all targets  $i \neq 1$ , exactly a  $p_i$  fraction of slots are used for target  $i$ , so  $z_1 = 1/y_1 = 1/p_1$ . ■

**Proof of Theorem 4.1.** Consider any target  $i$ . The rounding of Lemma 4.3 guarantees that  $2^{-m_i} \leq q_i \leq 2^{1-m_i}$ . Therefore, the algorithm of Lemma 4.5 produces a random sequence  $S_q$  in which the time intervals between consecutive occurrences of target  $i$  lie between  $2^{m_i-1}$  and  $2^{m_i}$ . Thus to verify that  $S_q$  is 2-quasi-regular it remains to show that the density of each target of the targets are equal to  $\alpha_i$ . But this is guaranteed by (1) in Lemma 4.3. The optimality of  $S_q$  now follows from Theorem 3.1. ■

## 5 Golden Ratio Scheduling

In this section, we present a very simple ergodic random sequence. The associated schedule may in general be suboptimal, but we prove that it is provably within less than 0.6% of optimal.

Let  $\varphi = \frac{1}{2}(1 + \sqrt{5})$  denote the golden ratio, solving  $\varphi^2 = \varphi + 1$ . Given a desired frequency vector  $\mathbf{p}$  (which will equal the targets' values,  $p_i = \alpha_i$ ), we identify the unit circle with  $[0, 1)$ , and equip it with addition modulo 1. We define the function  $h: [0, 1) \rightarrow \{1, \dots, n\}$  via  $h^{-1}(i) = [\sum_{i' < i} p_{i'}, p_i + \sum_{i' < i} p_{i'})$ ; that is, we assign consecutive intervals of length  $p_i$  for the targets  $i$ .

---

**Algorithm 2** The Golden Ratio Schedule

---

- 1: Let  $\lambda$  be uniformly random in  $[0, 1)$ .
  - 2: **for**  $t = 0, 1, 2, \dots$  **do**
  - 3:   In step  $t$ , set  $s_t = h((\lambda + t/\varphi) \bmod 1)$ .
- 

We can think of advancing a “dial” by  $1/\varphi$  at each step, and visiting the target whose interval the dial falls into. This algorithm is nearly identical to one previously proposed for hashing [12, pp. 510,511,543] and broadcast channel sharing [11, 16]. While the algorithm is simple, as stated, it seems to require precise arithmetic with real numbers. This issue is discussed in more detail in Appendix E.

That algorithm 2 returns an ergodic random sequence follows from the classical fact that the action on the interval by an irrational rotation is ergodic. Our main theorem in this section is the following:

**Theorem 5.1** *The Golden Ratio algorithm is a  $\frac{2966-1290\sqrt{5}}{81} \approx 1.00583$  approximation for the defender.*

The underlying reason that this schedule performs so well, and the reason for choosing this particular number, is related to the hardness of diophantine approximation of the golden ratio: it is an irrational number that is hardest to approximate by rational numbers (see, e.g., [9]).

Our analysis relies heavily on various properties of Fibonacci numbers. We denote the  $k^{\text{th}}$  Fibonacci number by  $f_k$ , indexed as  $f_0 = 0, f_1 = 1$  and  $f_{k+2} = f_k + f_{k+1}$ . The following basic facts about Fibonacci numbers are well-known, and easily proved directly or by induction.

**Lemma 5.2**   1. For any  $k$ , we have that  $f_{k+2}f_k - f_{k+1}^2 = (-1)^{k+1}$ .

2. For any  $k$ , we have that  $f_k = \frac{\varphi^k - (-1/\varphi)^k}{\sqrt{5}}$ .

3. For any odd  $k$ , we have that  $f_{k+1}/f_k < \varphi$ .

4. For any even  $k$ , we have that  $f_{k+1}/f_k > \varphi$ .

To prove Theorem 5.1, we analyze the distribution of  $B_i$  for any target  $i$ . The proof of Theorem 5.1 consists of two parts. First, Theorem 5.3 precisely characterizes the distribution of  $B_i$  for every target  $i$ , i.e., it characterizes exactly, for each target  $i$  and  $\tau$ , how frequently a visit to target  $i$  is followed by another visit  $\tau$  steps later. As a second part, we characterize the attacker’s best response against this distribution, and calculate its cost to the defender.

**Theorem 5.3 (Slater [17])** *Assume that  $\alpha \leq \frac{1}{2}$ . Let  $k$  be smallest such that*

$$|f_{k+1}/\varphi - f_k| \leq \alpha. \tag{4}$$

Then, the distribution of return times is

$$\begin{aligned}
\mathbb{P}[B_i = f_{k+1}] &= f_{k+1} \cdot (\alpha - (1/\varphi)^{k+2}) \cdot \frac{1 + \varphi^2}{\sqrt{5}}, \\
\mathbb{P}[B_i = f_{k+2}] &= f_{k+2} \cdot (\alpha - (1/\varphi)^{k+3}) \cdot \frac{1 + \varphi^2}{\sqrt{5}}, \\
\mathbb{P}[B_i = f_{k+3}] &= f_{k+3} \cdot (-\alpha + (1/\varphi)^{k+1}) \cdot \frac{1 + \varphi^2}{\sqrt{5}}, \\
\mathbb{P}[B_i = t] &= 0 \text{ for all other } t.
\end{aligned} \tag{5}$$

Theorem 5.3 shows, remarkably, that for each possible  $\alpha$ , there are at most three possible return times, and they are three consecutive Fibonacci numbers. Theorem 5.3 is a special case of a theorem of Slater [17, Theorem 4] (see also [18]), which characterizes the distribution when the Golden Ratio  $\varphi$  is replaced by an arbitrary real number. We give a self-contained proof for the simpler case of the Golden Ratio in Appendix D.

As a direct corollary of Theorem 5.3, we obtain an upper bound on the regularity of the Golden Ratio schedule.

**Corollary 5.4** *The Golden Ratio schedule is 3-quasi-regular. If  $\alpha_i \leq 1 - 1/\varphi$  for all  $i$ , then it is 8/3-quasi-regular. As the frequencies  $\alpha_i \rightarrow 0$ , the guarantee improves to  $\varphi^2$ -quasi-regular.*

**Proof.** Consider one target with desired frequency  $\alpha$ , and define  $k$  as in Theorem 5.3. The schedule is at worst  $(f_{k+3}/f_{k+1})$ -quasi-regular. For all  $k$ , we have the bound  $f_{k+3}/f_{k+1} \leq 3$ . If  $\alpha < 1 - 1/\varphi$ , then  $k \geq 2$ , and for  $k \geq 2$ , the ratio  $f_{k+3}/f_{k+1}$  is upper-bounded by 8/3, converging to  $\varphi^2$  as  $k \rightarrow \infty$ . ■

## 5.1 The Optimal Attacker Response to 3-Point Distributions

Next, we characterize the optimal attacker response to defender strategies in which the return time distribution to target  $i$  is supported on three points  $x_1 < x_2 < x_3$  only. Since we will apply this result to Fibonacci numbers, we assume that  $x_2 \leq 2x_1, x_3 \leq 2x_2$ . Let  $q_j = \mathbb{P}[B_i = x_j] \cdot \frac{\mathbb{E}[B_i]}{x_j}$ , and let  $X = \sum_j q_j x_j$ ; informally (but in a sense that can be formalized), the  $q_j$ 's are the return time probabilities from the point of view of the defender, rather than those of the attacker at a fixed time 0. (The attacker's distribution of  $B_i$  oversamples long return times, compared to the defender's distribution.) The attacker's response and utility are summarized by the following lemma.

**Lemma 5.5** *Let  $t_1^* = X/2$ , and  $t_2^* = \frac{X - q_1 x_1}{2(1 - q_1)}$ . Let  $u_1^* = \frac{1}{4} \cdot X$ , and  $u_2^* = \frac{1}{4} \cdot \frac{(X - q_1 x_1)^2}{X(1 - q_1)}$ . Whenever  $u_2^* > u_1^*$  and  $t_2^* > x_1^*$ , the attacker's best response is  $t_2^*$  and his utility  $u_2^*$ ; otherwise, his best response is  $t_1^*$  and his utility  $u_1^*$ .*

Notice that whenever the attacker responds  $t_1^*$ , this is optimal for the defender.

**Proof.** From the attacker's perspective, when arriving at a target, by Equations (5) and (3), the

CDF of the distribution of the defender's next return time is

$$F(t) = \begin{cases} \frac{1}{X} \cdot t & \text{for } t \leq x_1 \\ \frac{1}{X} \cdot (t(1 - q_1) + q_1 x_1) & \text{for } x_1 \leq t \leq x_2 \\ \frac{1}{X} \cdot (t(1 - q_1 - q_2) + q_1 x_1 + q_2 x_2) & \text{for } x_2 \leq t \leq x_3 \\ 1 & \text{for } t \geq x_3 \end{cases}$$

Since the attacker's utility for waiting for  $t$  steps is  $t(1 - F(t))$ ,  $t \geq x_3$  cannot be optimal for him. By taking derivatives with respect to  $t$ , we obtain the following local optima for the functions in the remaining three cases:

$$t_1^* = \frac{X}{2} \quad t_2^* = \frac{X - q_1 x_1}{2(1 - q_1)} \quad t_3^* = \frac{X - q_1 x_1 - q_2 x_2}{2(1 - q_1 - q_2)} = \frac{x_3}{2}.$$

These are all local maxima because the functions are concave. Whenever a  $t_i^*$  lies outside the interval for which it optimizes, the actual maximum is attained at an interval boundary, which means that it is also in the adjacent interval, and the interval can be ignored for the analysis. In particular, this applies for  $t_3^*$ , which is supposed to be in  $[x_2, x_3]$ . Under the assumption of the theorem, we get that  $t_3^* = x_3/2 \leq x_2$ .

For  $t_2^*$ , we obtain the constraints that  $x_1 \leq t_2^* \leq x_2$ . The second constraint is always satisfied under the assumptions of the theorem, because  $t_2^* \cdot \frac{q_2 x_2 + q_3 x_3}{2(q_2 + q_3)} \leq x_3/2 \leq x_2$ . The first constraint may or may not be satisfied. Next, we write the attacker's utility in the two remaining cases.

$$u_1^* = t_1^* \cdot (1 - F(t_1^*)) = \frac{X}{2} \cdot \frac{1}{2} = \frac{X}{4},$$

$$u_2^* = t_2^* \cdot (1 - F(t_2^*)) = \frac{X - q_1 x_1}{2(1 - q_1)} \cdot \left(1 - \frac{1}{X} \cdot \left(\frac{X - q_1 x_1}{2} + q_1 x_1\right)\right) = \frac{1}{4} \cdot \frac{(X - q_1 x_1)^2}{X(1 - q_1)} = \frac{1}{4} \cdot \frac{(q_2 x_2 + q_3 x_3)^2}{X(q_2 + q_3)}.$$

Whenever  $t_2^* > x_1$ , the attacker will thus choose the better utility of  $u_1^*, u_2^*$ , and otherwise will only get to choose utility  $u_1^*$ . ■

## 5.2 The Attacker's Response to the Golden Ratio Schedule

**Proof of Theorem 5.1.** According to Lemma 5.5, the attacker can obtain utility  $u_1^*$  (which is optimal for the defender), and sometimes a higher utility of  $u_2^*$ . To obtain the approximation guarantee, we will bound the worst-case ratio of  $u_2^*/u_1^*$  whenever the attacker responds with  $t_2^*$ .

In applying Lemma 5.5, we have  $X = 1/\alpha$ ,  $x_1 = f_{k+1}$ ,  $x_2 = f_{k+2}$ ,  $x_3 = f_{k+3}$ , and the  $q_j$  are given via Equation (5) and  $q_j = \mathbb{P}[B_i = x_j] \cdot \frac{\mathbb{E}[B_i]}{x_j}$ . Then, the attacker's utility from attacking for  $t_2^*$  units of time (assuming feasibility, and ignoring the factor  $\frac{1}{4}$  throughout) is



$$\begin{aligned}
\frac{(X - q_1 x_1)^2}{X(1 - q_1)} &= \frac{\alpha(q_2 f_{k+2} + q_3 f_{k+3})^2}{q_2 + q_3} \\
&= \frac{\left( \left( \alpha - (1/\varphi)^{k+3} \cdot \frac{1+\varphi^2}{\sqrt{5}} \right) \cdot f_{k+2} + \left( -\alpha + (1/\varphi)^{k+1} \cdot \frac{1+\varphi^2}{\sqrt{5}} \right) \cdot f_{k+3} \right)^2}{\left( \alpha - (1/\varphi)^{k+3} \cdot \frac{1+\varphi^2}{\sqrt{5}} \right) + \left( -\alpha + (1/\varphi)^{k+1} \cdot \frac{1+\varphi^2}{\sqrt{5}} \right)} \\
&= \frac{\left( (1/\varphi)^{k+3} \cdot (\varphi^2 - 1) \cdot \frac{1+\varphi^2}{\sqrt{5}} \cdot f_{k+2} + \left( -\alpha + (1/\varphi)^{k+1} \cdot \frac{1+\varphi^2}{\sqrt{5}} \right) \cdot f_{k+1} \right)^2}{(1/\varphi)^{k+3} \cdot (\varphi^2 - 1) \cdot \frac{1+\varphi^2}{\sqrt{5}}} \\
&= \frac{1 + \varphi^2}{\sqrt{5}} \cdot (1/\varphi)^{k+2} \cdot \left( f_{k+2} + \varphi f_{k+1} - \alpha \cdot \varphi^{k+2} \frac{\sqrt{5}}{1 + \varphi^2} \cdot f_{k+1} \right)^2. \tag{6}
\end{aligned}$$

Thus, the approximation ratio  $u_2^*/u_1^*$  is  $\alpha$  times the expression (6).

Treating everything except  $\alpha$  as a constant, the ratio is thus of the form  $g(\alpha) = a\alpha \cdot (c - b\alpha)^2$ .  $g$  has a local maximum of  $4ac^3/27b$  at  $\alpha = c/(3b)$ , a local minimum of 0 at  $\alpha = c/b$ , and goes to infinity as  $\alpha \rightarrow \infty$ . Thus, the two candidates for  $\alpha$  that we need to check are (1) the largest  $\alpha$  that is possible for a given  $k$ , and (2) the value  $c/(3b)$  if it is possible for given  $k$ . (If it is not, and  $c/(3b)$  lies to the left of the feasible region, then we also need to check the smallest possible  $\alpha$ .)

We therefore next work out what is the largest possible  $\alpha$  for a given  $k$ . By recalling the definition of  $k$  from Equation (4) (smallest such that  $|f_{k+1}/\varphi - f_k| \leq \alpha$ ), and using Lemma D.1, we can solve for  $\alpha$  to determine the range in which we obtain a particular  $k$ , giving us that

$$\alpha \in \left[ (1/\varphi)^{k+2} \frac{1 + \varphi^2}{\sqrt{5}}, (1/\varphi)^{k+1} \frac{1 + \varphi^2}{\sqrt{5}} \right].$$

1. If we substitute the upper bound  $\alpha = (1/\varphi)^{k+1} \frac{1+\varphi^2}{\sqrt{5}}$ , Equation (6) simplifies to

$$\begin{aligned}
&\frac{1 + \varphi^2}{\sqrt{5}} \cdot (1/\varphi)^{k+2} \cdot \left( f_{k+2} + \varphi f_{k+1} - (1/\varphi)^{k+1} \frac{1 + \varphi^2}{\sqrt{5}} \cdot \varphi^{k+2} \frac{\sqrt{5}}{1 + \varphi^2} \cdot f_{k+1} \right)^2 \\
&= \frac{1 + \varphi^2}{\sqrt{5}} \cdot (1/\varphi)^{k+2} \cdot (f_{k+2} + \varphi f_{k+1} - \varphi f_{k+1})^2 \\
&= \frac{1 + \varphi^2}{\sqrt{5}} \cdot (1/\varphi)^{k+2} \cdot f_{k+2}^2.
\end{aligned}$$

To obtain the approximation ratio, we multiply with  $\alpha$ , obtaining

$$\begin{aligned}
\frac{(1 + \varphi^2)^2}{5} \cdot (1/\varphi)^{2k+3} \cdot f_{k+2}^2 &= \frac{(1 + \varphi^2)^2}{25} \cdot (1/\varphi)^{2k+3} \cdot \left( \varphi^{2k+4} - 2\varphi^{k+2}(-1/\varphi)^{k+2} + (-1/\varphi)^{2k+4} \right) \\
&= \frac{(1 + \varphi^2)^2}{25} \cdot (1/\varphi)^{2k+3} \cdot \left( \varphi^{2k+4} - 2(-1)^k + (1/\varphi)^{2k+4} \right) \\
&\leq \frac{(1 + \varphi^2)^2}{25} \cdot (\varphi + 3/\varphi^{2k+3}) \\
&\leq \frac{(1 + \varphi^2)^2}{25} \cdot (\varphi + 3/\varphi^5) \\
&< 1.
\end{aligned}$$

This shows that the attacker's utility cannot be maximized by waiting for more than  $x_1$  steps when  $\alpha$  is as large as it can be for a given  $k$ .

2. Next, we investigate the local maximum of the cubic expression obtained from multiplying Equation (6) with  $\alpha$ . This local maximum is indeed always a feasible choice for  $\alpha$  for a given  $k$ , but since we are only interested in an upper bound, we omit the feasibility proof. (We can only overestimate the approximation ratio this way.)

Substituting  $a = \frac{1+\varphi^2}{\sqrt{5}} \cdot (1/\varphi)^{k+2}$ ,  $b = \varphi^{k+2} \frac{\sqrt{5}}{1+\varphi^2} \cdot f_{k+1}$ , and  $c = f_{k+2} + \varphi f_{k+1}$ , the attacker's utility is

$$\begin{aligned} & \frac{4}{27} \frac{(1+\varphi^2)^2}{5} \cdot (1/\varphi)^{2k+4} \cdot \frac{(f_{k+2} + \varphi f_{k+1})^3}{f_{k+1}} \\ &= \frac{4}{27} \cdot \frac{(1+\varphi^2)^2}{25} \cdot (1/\varphi)^{2k+4} \cdot \frac{(\varphi^{k+2} - (-1/\varphi)^{k+2} + \varphi \cdot \varphi^{k+1} - \varphi \cdot (-1/\varphi)^{k+1})^3}{\varphi^{k+1} - (-1/\varphi)^{k+1}} \\ &= \frac{4}{27} \cdot \frac{(1+\varphi^2)^2}{25} \cdot (1/\varphi)^{2k+4} \cdot \frac{(2\varphi^{k+2} - (-1/\varphi)^{k+1})^3}{\varphi^{k+1} - (-1/\varphi)^{k+1}}. \end{aligned}$$

We will approximate the function  $\frac{(2\varphi^{k+2} - (-1/\varphi)^{k+1})^3}{\varphi^{k+1} - (-1/\varphi)^{k+1}}$  by  $8\varphi^{2k+5}$ , its highest-order term. We therefore consider  $\frac{(2\varphi^{k+2} - (-1/\varphi)^{k+1})^3}{\varphi^{k+1} - (-1/\varphi)^{k+1}} / (8\varphi^{2k+5})$ . When  $k$  is even, this ratio is always upper-bounded by 1 (and increasing in  $k$ , converging to 1), so we can simply upper-bound it. When  $k$  is odd, this ratio is *lower-bounded by 1*, and decreasing in  $k$ , also converging to 1. Thus, it is maximized among feasible values of  $k$  for  $k = 3$ , where it equals  $\frac{8\varphi^{15} - 12\varphi^6 + 6\varphi^{-3} - \varphi^{-12}}{8\varphi^{15} - 8\varphi^7}$ . Overall, we get an upper bound on the attacker's utility of

$$\begin{aligned} & \frac{(1+\varphi^2)^2}{25} \cdot \frac{4}{27} \cdot \frac{8\varphi^{15} - 12\varphi^6 + 6\varphi^{-3} - \varphi^{-12}}{8\varphi^{15} - 8\varphi^7} \cdot (1/\varphi)^{2k+4} \cdot (8\varphi^{2k+5}) \\ &= \frac{\varphi(1+\varphi^2)^2}{25} \cdot \frac{4}{27} \cdot \frac{8\varphi^{15} - 12\varphi^6 + 6\varphi^{-3} - \varphi^{-12}}{\varphi^{15} - \varphi^7}. \end{aligned}$$

To evaluate this ratio, we can repeatedly apply the fact that  $\varphi^2 = 1 + \varphi$ , then substitute that  $\varphi = \frac{1+\sqrt{5}}{2}$ , make the denominator rational, and cancel out common factors. This shows that  $\frac{\varphi(1+\varphi^2)^2}{25} \cdot \frac{4}{27} \cdot \frac{8\varphi^{15} - 12\varphi^6 + 6\varphi^{-3} - \varphi^{-12}}{\varphi^{15} - \varphi^7} = \frac{2966 - 1290\sqrt{5}}{81} \approx 1.00583$ , completing the proof. ■

## 6 Scheduling via Matching

The strategies from Section 4 are optimal, but not ergodic. The strategies from Section 5 are ergodic, but not optimal or periodic. In this section, we give a sufficient condition for the existence of an optimal, ergodic, and periodic strategy for the defender.

In order to obtain a periodic strategy, it is clearly necessary for all target values  $\alpha_i$  (equaling the visit frequencies) to be rational. Write  $\alpha_i = a_i/b_i$ , and let  $M = scm(b_1, \dots, b_n)$ .

Our algorithm is based on embedding  $M$  slots for visits evenly on the unit circle, and matching them with targets to visit. We identify the circle with the interval  $[0, 1]$  and use the distance  $d(x, y) = \min(|x - y|, |1 - x - y|)$ .

---

**Algorithm 3** A matching-based algorithm for a periodic defender strategy

---

- 1: For each  $i$ , let  $\theta_i \in [0, 1]$  independently uniformly at random.
  - 2: For each  $i$ , let  $A_i = M \cdot a_i/b_i$ .
  - 3: For each  $i$  and  $j = 0, \dots, A_i - 1$ , let  $y_{i,j} = (\theta_i + j/A_i) \bmod 1$ .
  - 4: For each  $i$ , define  $\delta_i = \frac{1}{6A_i}$ .
  - 5: Let  $T = \{0, 1, \dots, M - 1\}$  and  $V = \{(i, j) \mid 0 \leq j < A_i\}$ . Define a bipartite graph  $G$  on  $T \cup V$  by including an edge between  $t \in T$  and  $(i, j) \in V$  iff  $d(y_{i,j}, t/M) \leq \delta_i$ .
  - 6: **if**  $G$  contains a perfect matching  $\mathcal{M}$  **then**
  - 7:   Define a sequence  $s$  with period  $M$  as follows: For each time  $t$ , set  $s_t$  to be the (unique) target  $i$  such that  $t$  is matched with  $(i, j)$  in  $\mathcal{M}$  for some  $j$ .
  - 8: **else**
  - 9:   Start from the beginning.
- 

**Theorem 6.1** *Whenever  $M < e^{(1/9-\epsilon)\cdot n}$ , Algorithm 3 succeeds with high probability. Whenever Algorithm 3 succeeds, it produces 2-quasi-regular (and hence defender-optimal) sequence.*

**Remark 6.2** By changing the constant 6 in the definition of  $\delta_i$  to a larger constant, and decreasing the 1/9 in the theorem statement accordingly, we can improve the quasi-regularity to any arbitrary constant  $c > 1$ , proving that when the common denominator of the target frequencies is small enough, sequences arbitrarily close to regular exist.

We begin by proving the second part of the theorem. If  $t$  is matched with  $(i, j)$ , by definition of the edges,  $d(y_{i,j}, t/M) \leq \delta_i = \frac{1}{6A_i}$ . Consider two occurrences  $j, j'$  of target  $i$ , and let  $t, t'$  be the slots they are matched to. Then, by triangle inequality,

$$d(t/M, t'/M) \geq d(y_{i,j}, y_{i,j'}) - \frac{2}{6A_i} \geq \frac{1}{A_i} - \frac{1}{3A_i} = \frac{2}{3A_i}.$$

Thus,  $|t - t'| \geq \frac{2}{3a_i}$ . On the other hand, specifically for consecutive occurrences of target  $i$ , i.e., the slots matched to  $y_{i,j}$  and  $y_{i,j+1}$ , we get

$$d(t/M, t'/M) \leq d(y_{i,j}, y_{i,j'}) + \frac{2}{6A_i} = \frac{1}{A_i} + \frac{1}{3A_i} = \frac{4}{3A_i},$$

and hence  $|t - t'| \leq \frac{4}{3a_i}$ .

In a perfect matching, exactly  $A_i$  of the  $M$  slots, i.e., an  $a_i/b_i$  fraction, are scheduled for target  $i$ , giving that  $y_i = a_i/b_i = \alpha_i$ . Thus,  $z_i = 1/\alpha_i$ . Thus, the proposed sequence is 2-quasi-regular, and the optimality of the schedule follows from Theorem 3.1.

To complete the proof, it remains to show that with high probability, the graph  $G$  contains a perfect matching. We will prove this using Hall's Theorem and a direct application of the Hoeffding Bound:

**Lemma 6.3 (Hoeffding Bound)** *Let  $X_i$  be independent random variables such that  $a_i \leq X_i \leq b_i$  with probability 1. Let  $X = \sum_i X_i$ . Then, for all  $t > 0$ ,*

$$\mathbb{P}[X < \mathbb{E}[X] - t], \mathbb{P}[X > \mathbb{E}[X] + t] < e^{-\frac{2t^2}{\sum_i (b_i - a_i)^2}}.$$

To establish the Hall condition of  $G$ , we begin with intervals  $T$  of slots, and then use the bounds for intervals to derive the condition for arbitrary sets of slots. A similar style of proof was used by Tijdeman [21] to construct a schedule with somewhat different specific combinatorial properties.

For any set  $T$  of slots, let  $\Gamma(T)$  denote the neighborhood of  $T$  in  $G$ . Fix an interval  $T = [\ell, r) \subseteq [0, M)$  with  $\ell, r$  integers. Let the random variable  $Y_T = |\Gamma(T)|$  denote the number of neighbors in  $G$  of slots in the interval  $T$ . For each target  $i$ , let  $X_{T,i}$  be the number of  $j$  such that  $(i, j) \in \Gamma(T)$ . Then,  $Y_T = \sum_i X_{T,i}$ , and the  $X_{T,i}$  are independent.

**Lemma 6.4** *Assume that  $|T| \leq (1 - 2\delta_i)M$ . Then,  $\mathbb{E}[X_{T,i}] = A_i \cdot (2\delta_i + (r - \ell)/M)$ , and  $X_{T,i} \in \{\lfloor A_i \cdot (2\delta_i + (r - \ell)/M) \rfloor, 1 + \lfloor A_i \cdot (2\delta_i + (r - \ell)/M) \rfloor\}$  always.*

**Proof.** For each slot  $t \in T$ , let  $J_t = [(t/M - \delta_i) \bmod 1, (t/M + \delta_i) \bmod 1]$ . Then, slot  $(i, j) \in \Gamma(\{t\})$  iff  $y_{i,j} \in J_t$ . Because  $\delta_i \geq 1/(2M)$ , we get that  $J_t \cap J_{t+1} \neq \emptyset$  for all  $t$ . Hence, defining  $J := \bigcup_{t \in T} J_t = [(\ell/M - \delta_i) \bmod 1, (r/M + \delta_i) \bmod 1]$ , we get that  $\Gamma(T) = \{(i, j) \mid y_{i,j} \in J\}$ ; the fact that  $J$  is an interval follows from the non-overlapping property.

The length of  $J$  is  $2\delta_i + (r - \ell)/M$ . Because each  $y_{i,j}$  is uniformly random in  $[0, 1]$ ,  $\mathbb{E}[X_{T,i}] = A_i \cdot (2\delta_i + (r - \ell)/M)$ . Furthermore, because  $d(y_{i,j}, y_{i,j+1}) = 1/A_i$ , there can be no more than  $1 + \lfloor \frac{2\delta_i + (r - \ell)/M}{1/A_i} \rfloor$  pairs  $(i, j)$  with  $y_{i,j} \in J$ , and no fewer than  $\lfloor \frac{2\delta_i + (r - \ell)/M}{1/A_i} \rfloor$ . Finally, note that  $\frac{2\delta_i + (r - \ell)/M}{A_i} = A_i(2\delta_i + (r - \ell)/M)$ .  $\blacksquare$

We use Lemma 6.4 to show that with high probability,  $G$  has a perfect matching.

**Lemma 6.5** *When  $M < e^{(1/9 - \epsilon)n}$ , with high probability,  $G$  contains a perfect matching.*

**Proof.** First, we show that when the Hall condition holds for all intervals  $T$  of slots, it holds for all sets  $T$ . We prove this by induction on the number of disjoint intervals that  $T$  comprises. The base case of  $T$  being an interval is true by definition. For the induction step, suppose that  $k \geq 2$  and  $T = \bigcup_{j=1}^k T_j$ , where the  $T_j$  are disjoint intervals.

If the neighborhoods of all the  $T_j$  are disjoint, then  $|\Gamma(T)| = \sum_j |\Gamma(T_j)| \geq \sum_j |T_j| = |T|$ , where the inequality was from the base case (intervals). Otherwise, w.l.o.g.,  $\Gamma(T_k) \cap \Gamma(T_{k-1}) \neq \emptyset$ . Then, there exists an interval  $I' \supset T_k \cup T_{k-1}$  with  $\Gamma(I') = \Gamma(T_k) \cup \Gamma(T_{k-1})$ . Let  $T' = T \cup I'$ . We get that  $|\Gamma(T)| = |\Gamma(T')| \geq |T'| \geq |T|$ , where the first inequality was by induction hypothesis (because  $T'$  has at least one fewer intervals).

Next, we establish that the Hall Condition holds with high probability for all  $M^2$  intervals. First, focus on one interval  $T = [\ell, r)$ , with  $\ell, r \in \mathbb{N}$ . If  $|T| > (1 - 2\delta_i)M$ , then  $\Gamma(T)$  contains all pairs  $(i, j)$ , so the Hall Condition is satisfied. So focus on  $|T| \leq (1 - 2\delta_i)M$ . From Lemma 6.4, we get that

$$\mathbb{E}[Y_T] = \sum_i A_i \cdot (2\delta_i + (r - \ell)/M) = 2 \sum_i A_i \delta_i + (r - \ell).$$

Furthermore,  $Y_T$  is the sum of independent random variables  $X_{T,i}$  which each takes on one of two adjacent values. From the Hoeffding Bound (Lemma 6.3), we get that

$$\mathbb{P}[Y_T < (r - \ell) + 2 \sum_i A_i \delta_i - \tau] < e^{-2\tau^2/n}.$$

Because  $|T| = r - \ell$ , choosing  $\tau = 2 \sum_i A_i \delta_i = n/3$ , we get that

$$|\Gamma(T)| = Y_T \geq (r - \ell) + 2 \sum_i A_i \delta_i - \tau = r - \ell.$$

Taking a union bound over all  $M^2$  candidate intervals  $T$ , we obtain that the probability of having a perfect matching is at least

$$1 - M^2 e^{-2n/9} > 1 - e^{2n(1/9 - \epsilon) - 2n/9} = 1 - e^{-2\epsilon n}.$$

Thus, with high probability,  $G$  contains a perfect matching. This completes the proof of Lemma 6.5 and thus also Theorem 6.1.  $\blacksquare$

## 7 Future Work

Our work suggests a number of directions for future work. Most immediately, it suggests trying to find optimal *ergodic* schedules for all value vectors (not only those covered by Theorem 6.1). A promising approach toward this goal is to use the randomized rounding of Section 4, but re-round the probabilities every  $T$  steps, for some sufficiently large “epoch size”  $T$ . The difficulty with this approach is “stitching together” the schedules for different rounded frequencies at the boundary of epochs, without violating the conditions of Theorem 3.1.

Throughout, we assumed that no target had value more than the sum of all other targets’ values, i.e.,  $\alpha_i \leq \frac{1}{2}$  for all  $i$ . When this assumption is violated, the optimal schedule will wait at the highest-value target. In the specific case of two targets of values  $\alpha_1 < \alpha_2$ , it is fairly straightforward to calculate that the wait time at target 2 is  $2(\sqrt{\frac{\alpha_2}{\alpha_1}} - 1)$ . We anticipate that this analysis will extend to more than two targets. The difficulty is that the waiting time at one target will result in qualitatively different schedules, likely to complicate the analysis.

We assumed here that the game is zero-sum. In general, the utilities of the attacker and defender may be different. A general treatment is likely quite difficult. One special case is motivated directly by the wildlife protection application, and appears quite amenable to analysis. Specifically, when a poacher kills animals (or chops down trees), even if the poacher is captured, the damage is not reversed. Thus, while the attacker’s utility is as before, the defender’s utility from visiting target  $i$  at time  $\tau$  when the attacker intends to stay for  $t$  units of time is  $-\alpha_i \cdot \min(\tau, t)$ . One can show that in this case, whenever the attacker attacks target  $i$  for  $t \leq z_i/2$  units of time, the defender’s utility is  $-\frac{3}{2}U(F_i, (i, t))$ . Since the optimal defender strategies of Section 4 and 6 ensure such a choice of  $t$  by the attacker, the algorithms in those sections are optimal in the non-zero sum model as well.

Among the other natural generalizations are the attacker’s (and defender’s) utility function and more complex constraints on the defender’s schedule. Throughout, we have assumed that the attacker’s utility grows linearly in the time spent at a target. The security game formulations studied in much of the prior work in the area [20] correspond to a step function at 0: when the attacker reaches an unprotected target, he immediately causes the maximum target-specific damage  $\alpha_i$  (e.g., by blowing up the target). Other natural utility functions suggest themselves: if the resources to collect at targets are limited, the utility function would be linear with a cap. If a destructive attack takes a non-zero amount of time to set up, one obtains a step function at a time other than 0. The latter leads to a scheduling problem with a harder constraint on the inter-visit

absence time from targets  $i$  — as in some of the prior security games literature, the defender may “sacrifice” some low-value targets to be able to fully protect the others.

The other natural generalization is to relax the assumption of uniform travel time between targets. If an arbitrary metric is defined between targets, the problem becomes significantly more complex: even if all targets have value 1, the attacker’s utility will be proportional to the cost of a minimum TSP tour, and thus the defender’s optimization problem is NP-hard. However, it is far from obvious how to adapt standard TSP approximation techniques to the general problem with non-uniform values: high-value targets should be visited more frequently, and TSP approximation algorithms are not suited to enforce constraints that these visits be spaced out over time.

As with TSP problems and past work on security games, a further natural generalization is to consider multiple defenders.

### **Acknowledgments**

We would like to thank Omer Angel, Sami Assaf, Bobby Kleinberg, Jim Propp, and Milind Tambe for useful discussions.

## A Utility of an i.i.d. Defender

One of the most natural random sequences to consider is the *i.i.d.* one, in which at each step  $t$ , the defender visits target  $i$  with probability  $p_i$ , independent of any past choices. Intuitively, this strategy is suboptimal because it may visit a target  $i$  several times in close succession, or go for a long time without visiting target  $i$ . Here, we calculate the approximation ratio of this strategy, showing:

**Proposition A.1** *The i.i.d. strategy is a  $4/e$ -approximation for the defender, and this is tight.*

**Proof.** From the attacker’s viewpoint, the defender’s next arrival time at target  $i$  is the sum of two independent random variables  $\text{geom}(p_i) + \text{unif}([0, 1])$ . Given a  $t$ , the defender will return within at most  $t$  steps if and only if  $\text{geom}(p_i) \leq \lfloor t \rfloor$  or  $\text{geom}(p_i) = 1 + \lfloor t \rfloor$  and  $\text{unif}([0, 1]) \leq (t \bmod 1)$ . The two events are disjoint, the first one having probability  $1 - (1 - p_i)^{\lfloor t \rfloor}$ , and the second having probability  $p_i \cdot (1 - p_i)^{\lfloor t \rfloor} \cdot (t \bmod 1)$ . Hence,  $F_i(t) = 1 - (1 - p_i \cdot (t \bmod 1)) \cdot (1 - p_i)^{\lfloor t \rfloor}$ , and the attacker’s utility from attacking target  $i$  for  $t$  time units is

$$\alpha_i \cdot t \cdot (1 - F_i(t)) = \alpha_i \cdot t \cdot (1 - p_i \cdot (t \bmod 1)) \cdot (1 - p_i)^{\lfloor t \rfloor}.$$

Writing  $t = x + k$  for an integer  $k = \lfloor t \rfloor$  and  $x = (t \bmod 1) \in [0, 1]$ , a derivative test shows that the expression is monotone decreasing in  $x$  for any  $k \geq 1$ , whereas for  $k = 0$ , it has a local maximum at  $x = \frac{1}{2p_i} \geq 1$ . Because the latter is not feasible, we only need to consider the case  $(t \bmod 1) = 0$  for the remainder, so the attacker’s utility simplifies to  $\alpha_i \cdot t \cdot (1 - p_i)^{\lfloor t \rfloor}$ .

Taking a derivative with respect to  $t$  and setting it to 0 gives us that the unique local extremum is at  $t = \frac{-1}{\ln(1-p_i)}$ , where the attacker’s utility is  $\frac{p_i}{e \cdot \ln(1/(1-p_i))}$ . This local extremum is a maximum because the attacker’s utility at  $t = 0$  and  $t = \infty$  is 0.

A derivative test and Taylor series bound shows that  $\frac{p_i}{e \cdot \ln(1/(1-p_i))}$  is monotone decreasing in  $p_i$ , so it is maximized as  $p_i \rightarrow 0$ , where it converges to  $1/e$ . Notice that as  $p_i \rightarrow 0$ , there are infinitely many values of  $p_i$  for which  $\frac{-1}{\ln(1-p_i)}$  is an integer, so the choice of  $t$  in our previous optimization is indeed valid.

Under an optimal schedule, the attacker’s expected utility is  $\frac{1}{4}$ , completing the proof of the approximation guarantee. ■

## B Formalization of Notions about Schedules

### B.1 Canonical Schedules

The general definition of defender schedules allows for strange schedules that are clearly suboptimal, such as the defender leaving a target  $i$  and returning to it shortly afterwards, or visiting a target infinitely often within a bounded time interval with shorter and shorter return times. For ease of notation and analysis, we would like to rule out such schedules. The following definition captures “reasonable” schedules.

**Definition B.1 (canonical schedules)** *We say that a valid schedule  $\ell$  is canonical if  $\mathbb{R}^+$  can be partitioned into countably many disjoint intervals  $I_1, I_2, I_3, \dots$  with the following properties:*

1. All odd intervals  $I_{2k-1}$  are open and of length exactly 1, and  $\ell(t) = \perp$  if and only if  $t \in \bigcup_k I_{2k-1}$ .

2. All even intervals  $I_{2k}$  are closed. (Even intervals could consist of a single point.) For all  $k$  and  $t \in I_{2k}, t' \in I_{2k+2}$ , we have that  $\ell(t) \neq \ell(t')$ .

A defender mixed schedule  $\Lambda$  is canonical if it is a distribution over canonical deterministic schedules.

Note that it follows from validity that any canonical  $\ell$  is constant on the even intervals.

Intuitively, a canonical schedule is one in which the defender travels as quickly as possible (in one unit of time) from one target to the next target, visits it for some (possibly zero) time, then travels to the next (necessarily different) target, etc. That we may focus on canonical schedules w.l.o.g. is captured by the following proposition:

**Proposition B.2** *For each schedule  $\ell$ , there exists a canonical schedule  $\ell'$  that is at least as good for the defender, in the sense for any choice  $i, t, t'$  of the attacker,*

$$U(\ell', (i, t, t')) \leq U(\ell, (i, t, t')).$$

**Proof.** Given  $\ell$ , define  $\ell'$  as follows.

1. For every  $t$  with  $\ell(t) \neq \perp$  let  $\ell'(t) = \ell(t)$ .
2. For every  $t$  with  $\ell(t) = \perp$ 
  - (a) If  $t$  is in the closure of  $\ell^{-1}(i)$ , set  $\ell'(t) = i$ .
  - (b) Denote by  $i(t)$  the last target visited before time  $t$  (setting  $i(t) = 1$  if none exists) and  $j(t)$  the first target visited after time  $t$  (again setting  $j(t) = 1$  if none exists). Note that  $i(t)$  and  $j(t)$  are well-defined because  $\ell$  is valid; this would not in general be true for an arbitrary  $\ell: \mathbb{R}^+ \rightarrow \{1, \dots, n, \perp\}$ .
  - (c) If  $i(t) = j(t)$  then set  $\ell'(t) = i(t)$ . That is, if in  $\ell$ , the defender leaves a target  $i$  and then comes back to it without visiting another, then in  $\ell'$ , the defender just stays at  $i$ .
  - (d) If  $i(t) \neq j(t)$  and the difference between  $t$  and  $\inf\{\tau > t \mid \ell(\tau) = j(t)\}$  is at least 1, then set  $\ell'(t) = i(t)$ . That is, if the defender took more than one unit of time to reach target  $j(t)$  from  $i(t)$ , then she might as well have stayed at  $i(t)$  until one time unit before getting to  $j(t)$ .
  - (e) Otherwise, set  $\ell'(t) = \perp$ .

It is easy to verify that  $\ell'$  is indeed canonical. Consider any choice of schedule by the attacker. Because the above transformations only replaced  $\perp$  (i.e., transit) times with times at targets, whenever the attacker is not caught in  $\ell'$ , he was not caught in  $\ell$ , so his utility can only decrease:

$$U(\ell', (i, t, t')) \leq U(\ell, (i, t, t')).$$

■



## B.2 Shift Invariance

To simplify the analysis, we would like to restrict our attention to *shift invariant* schedules for the defender: schedules such that the attacker's and defender's utility depends only on the duration  $t' - t$  of the attack, but not on the start time  $t$ . We formally define this notion as follows, and show that this restriction is without loss of generality, as there is always an optimal shift-invariant schedule. For each  $\tau \in \mathbb{R}^+$ , define the *shift operator*  $M_\tau : \mathcal{S} \rightarrow \mathcal{S}$  by

$$[M_\tau(\ell)](t) = \ell(t + \tau).$$

That is, the pure schedule  $M_\tau(\ell)$  is equal to  $\ell$ , but leaves out the first  $\tau$  time units of  $\ell$ , shifting the remainder of the schedule forward in time. Note that

$$U(M_\tau(\ell), (i, t, t')) = U(\ell, (i, t + \tau, t' + \tau)). \quad (7)$$

The operator  $M_\tau$  extends naturally to act on mixed schedules  $\Lambda$ .<sup>8</sup> We say that a mixed schedule  $\Lambda$  is *shift-invariant* if  $M_\tau(\Lambda) = \Lambda$  for all  $\tau \in \mathbb{R}^+$ . The following lemma shows that an optimal schedule exists, and that we may focus on shift-invariant schedules without loss of generality.

**Lemma B.3** *The defender has an optimal mixed schedule that is shift-invariant.*

**Proof.** To prove this lemma, we introduce a natural topology on  $\mathcal{S}$ , the space of valid canonical pure strategies. Given a  $\ell \in \mathcal{S}$ , define  $\bar{\ell} : \mathbb{R}^+ \rightarrow \{1, \dots, n, \perp\}$  by setting  $\bar{\ell}(t)$  to be either  $\ell(t)$ , if  $\ell(t) \neq \perp$ , or else setting it to be the first target visited after time  $t$ . Thus  $\bar{\ell}(t)$  is the target visited at time  $t$ , or the target that the defender is en route to visiting. Note that  $\bar{\ell}^{-1}(i)$  is the union of a countable set of intervals of length at least 1, each open on the left and closed on the right. Note also that the map  $\ell \mapsto \bar{\ell}$  is “almost” invertible; since travel times are always 1, we know when each visit to each target began. The exception is the first visit, and so  $\ell$  is determined by  $\bar{\ell}$ , together with the time of the beginning of the first target visit, which is always at most 1.

The topology on  $\mathcal{S}$  is the topology of convergence in  $\mathcal{L}^1$  on compact sets. Specifically, for any  $t_1, t_2 \in \mathbb{R}^+$ , define  $\Delta_{t_1, t_2}(\ell_n, \ell)$  to be the measure of the subset of  $[t_1, t_2]$  on which at least one of the following two holds: (1)  $\ell_n \neq \ell$ , or (2)  $\bar{\ell}_n \neq \bar{\ell}$ . Then, we say that the limit of  $\ell_n$  is equal to  $\ell$  iff  $\Delta_{t_1, t_2}(\ell_n, \ell) \rightarrow 0$  for all  $t_1, t_2 \in \mathbb{R}^+$ . It is straightforward to verify that this topology is compact and metrizable.<sup>9</sup> Hence the corresponding weak\* topology on mixed strategies is also compact. Note also that the shift operator  $M_\tau : \mathcal{S} \rightarrow \mathcal{S}$  is continuous in this topology.

Note that if  $\ell_n \rightarrow_n \ell$ , and if target  $i$  is visited in  $[t_1, t_2]$  in every  $\ell_n$ , then it is also visited in  $[t_1, t_2]$  in  $\ell$ . Hence,

$$\lim_{n \rightarrow \infty} U(\ell_n, (i, t, t')) \geq U(\ell, (i, t, t')),$$

and so  $U(\cdot, (i, t, t'))$  is a lower semi-continuous map from  $\mathcal{S}$  to  $\mathbb{R}^+$ . It follows that

$$\Lambda \mapsto \mathbb{E}_{\ell \sim \Lambda} [U(\ell, (i, t, t'))]$$

<sup>8</sup>A measurable map  $P : X \rightarrow X$  can be extended to a linear operator on probability measures on  $X$  as follows: For any measurable subset  $A \subseteq X$ , define  $[P(\mu)](A) = \mu(P^{-1}(A))$ . This defines a mapping  $\mu \mapsto P(\mu)$ .

<sup>9</sup>The metric is  $\sum_{n=1}^{\infty} 2^{-n} d_n(\ell_1, \ell_2)$ , where  $d_n(\ell_1, \ell_2)$  is the measure of the subset of  $[0, n]$  in which either  $\ell_1$  and  $\ell_2$  differ, or  $\bar{\ell}_1$  and  $\bar{\ell}_2$  differ.

is lower semi-continuous as well. Hence

$$U(\Lambda) = \sup_{i,t,t'} \mathbb{E}_{\ell \sim \Lambda} [U(\ell, (i, t, t'))]$$

is also lower-semicontinuous, and thus attains a minimum on the compact space of mixed strategies. Thus we have shown that an optimal schedule exists.

When the attacker can obtain expected utility  $u$  against  $M_\tau(\ell)$  by choosing  $i, t, t'$ , he can obtain the same utility  $u$  against  $\Lambda$  by choosing  $i, t + \tau, t' + \tau$ . Therefore, the defender's utility is (weakly) monotone in  $\tau$ , in the following sense:

$$U(M_\tau(\Lambda)) \leq U(\Lambda). \quad (8)$$

Let  $\Lambda_1$  and  $\Lambda_2$  be mixed strategies, and let  $\Lambda = \alpha\Lambda_1 + (1 - \alpha)\Lambda_2$  be the schedule in which  $\Lambda_1$  is carried out with probability  $\alpha$  and  $\Lambda_2$  with probability  $1 - \alpha$ . Since suprema are subadditive, the attacker's utility is convex:

$$U(\Lambda) \leq \alpha U(\Lambda_1) + (1 - \alpha)U(\Lambda_2). \quad (9)$$

Let  $\Lambda$  be an optimal mixed schedule. For  $n \in \mathbb{N}$  let

$$\Lambda_n = \frac{1}{n} \int_0^n M_\tau(\Lambda) d\tau.$$

By the monotonicity (Eq. (8)) and convexity (Eq. (9)) of  $U(\Lambda)$ , we have that  $U(\Lambda_n) \leq U(\Lambda)$ .

Since  $\mathcal{S}$  is compact, the sequence  $\{\Lambda_n\}$  has a converging subsequence that converges to some  $\Lambda_\infty$ . By the lower semi-continuity of  $U(\Lambda)$ ,

$$U(\Lambda_\infty) \leq \lim_{n \rightarrow \infty} U(\Lambda_n) \leq U(\Lambda);$$

therefore  $\Lambda_\infty$  is also optimal. Finally,  $\Lambda_\infty$  is by construction shift-invariant. ■

### B.3 Transitive and Ergodic Schedules

We say that a shift-invariant mixed schedule  $\Lambda$  is *transitive* if there is a single pure schedule  $\ell_0$  that is periodic with period  $\tau$  (i.e.,  $M_\tau(\ell_0) = \ell_0$ ) such that

$$\Lambda = \frac{1}{\tau} \int_0^\tau \delta_{M_t(\ell_0)} dt,$$

where  $\delta_\ell$  is the point mass on  $\ell$ . Intuitively,  $\Lambda$  simply repeats the same periodic schedule, with a phase chosen uniformly at random.

A weaker property of a shift-invariant mixed schedule  $\Lambda$  is *ergodicity*:  $\Lambda$  is ergodic if there is a single pure schedule  $\ell_0$  such that

$$\Lambda = \lim_{\tau \rightarrow \infty} \frac{1}{\tau} \int_0^\tau \delta_{M_t(\ell_0)} dt.$$

In fact, this is not the usual definition of an ergodic measure, but the conclusion of the Ergodic Theorem. An equivalent property is that  $\Lambda$  cannot be written as the convex combination  $\lambda\Lambda_1 + (1 - \lambda)\Lambda_2$  of two different shift-invariant measures. That is,  $\Lambda$  is an extremal point in the convex set (simplex, in fact) of shift-invariant measures.

## B.4 Time Spent on targets in general schedules

We generalize the definition of  $y_i$  from random sequences to mixed schedules. The right notion here is captured by considering the time that the defender spends *at target  $i$  or in transit to target  $i$* .

Formally, for a canonical pure schedule  $\ell$ , recall the definition  $\bar{\ell}$  from the proof of Lemma B.3:  $\bar{\ell}$  is obtained from  $\ell$  by replacing each transit interval with the next visited target. While  $\bar{\ell}$  is thus not a valid schedule, it naturally captures the amount of time spent on the targets.

In particular, we can define  $y_i = \mathbb{P}_{\ell \sim \Lambda}[\bar{\ell}(0) = i]$  to be the probability that at time 0, the defender is in transit to (or at) target  $i$ . Because of shift-invariance, the choice of time 0 was immaterial. Because  $\Lambda$  is canonical,  $\sum_i y_i = 1$ . Then, we can generalize the definition of  $z_i$  as well, to:

$$z_i = \frac{1 - F_i(0)}{y_i - F_i(0)}. \quad (10)$$

## B.5 Times Between Visits to Targets

We now more formally define the notion of the (random) time between visits to a target  $i$ . While the notion is intuitively clear, for arbitrary defender strategies  $\Lambda$ , a precise definition requires some subtlety. We give a general definition for arbitrary mixed schedules, not just random sequences.

Having defined schedules on  $\mathbb{R}^+$ , we now extend the definition to schedules on  $[-\tau, \infty)$  and eventually to  $\mathbb{R}$ . We define a modified shift operator  $\tilde{M}_\tau(\cdot)$ , mapping schedules ( $\ell: \mathbb{R}^+ \rightarrow \{1, \dots, n, \perp\}$ ) to  $\tau$ -schedules  $\ell': [-\tau, \infty) \rightarrow \{1, \dots, n, \perp\}$ , via  $[\tilde{M}_\tau(\ell)](t) = \ell(t+\tau)$ . Thus,  $\tilde{M}_\tau(\ell)$  is simply a version of  $\ell$  shifted  $\tau$  units to the left. The map  $\tilde{M}_\tau(\cdot)$  extends to a map on mixed schedules in the obvious way. For any shift-invariant mixed schedule  $\Lambda$ ,  $\tilde{M}_\tau(\Lambda)$  is also shift-invariant, and furthermore, for any  $\tau' < \tau$ , the distribution  $\tilde{M}_{\tau'}(\Lambda)$ , projected to  $[-\tau', \infty)$ , is the same distribution as  $\tilde{M}_\tau(\Lambda)$ . It follows that

$$\Lambda_\infty = \lim_{\tau \rightarrow \infty} \tilde{M}_\tau(\Lambda) \quad (11)$$

is a well defined measure on pure schedules that are functions  $\ell_\infty: \mathbb{R} \rightarrow \{1, \dots, n, \perp\}$ . We call  $\Lambda_\infty$  the *bi-infinite extension* of  $\Lambda$ . It is straightforward to verify that it, too, is shift-invariant. Note that the distribution of the first visit to  $i$  at non-negative times,  $R_i = \min\{t \geq 0 \mid \ell(t) = i\}$ , has the same distribution under  $\Lambda_\infty$  as under  $\Lambda$ , since the restriction of  $\Lambda_\infty$  to non-negative times is equal to  $\Lambda$ .

Given a target  $i$  and a shift-invariant mixed schedule  $\Lambda$ , let  $\tilde{\ell}: (-\infty, \infty) \rightarrow \{1, \dots, n, \perp\}$  be a random schedule with distribution  $\Lambda_\infty$ . Let  $B_i$  be the (random) time between the last visit to  $i$  before time zero, until the first visit to  $i$  after time zero:

$$B_i = (\inf\{t \geq 0 \mid \tilde{\ell}(t) = i\}) - (\sup\{t \leq 0 \mid \tilde{\ell}(t) = i\}).$$

The choice of time 0 here is immaterial because of shift invariance.  $B_i$  could be infinite, but this will never happen in an optimal  $\Lambda$ , because it would imply that the attacker's expected utility for choosing  $i$  is infinite; we hence assume henceforth  $\mathbb{P}[B_i = \infty] = 0$ . Finally, contrary to what one might intuitively guess, even for transitive  $\Lambda$ , the distribution of  $B_i$  is *not* the same as the long-run empirical distribution of times between visits, as gaps are chosen at time 0 with probability proportional to their length. The same holds for general  $\Lambda$ .

## B.6 Characterizing $F_i(t)$ in terms of $B_i$

Here, we generalize the characterization of  $F_i$  in terms of the distribution of  $B_i$  to arbitrary shift-invariant mixed schedules, in particular allowing  $F_i(t) \neq 0$ . First, we can generalize Equation 3 as follows:

$$F_i(t) = \mathbb{P}[B_i = 0] + \frac{1 - \mathbb{P}[B_i = 0]}{\mathbb{E}[B_i]} \int_0^t \mathbb{P}[B_i > \tau] d\tau. \quad (12)$$

Thus,  $F_i(0) = \mathbb{P}[B_i = 0]$ , and

$$y_i = F_i(1) = F_i(0) + \frac{1 - F_i(0)}{\mathbb{E}[B_i]} \int_0^1 \mathbb{P}[B_i > \tau] d\tau.$$

In canonical schedules, either  $B_i = 0$  or  $B_i \geq 2$ , so  $\mathbb{P}[B_i > \tau] = 1 - F_i(0)$  for all  $\tau \leq 1$ . Thus,

$$y_i = F_i(0) + \frac{(1 - F_i(0))^2}{\mathbb{E}[B_i]}.$$

Also,

$$z_i = \frac{1 - F_i(0)}{y_i - F_i(0)} = \frac{\mathbb{E}[B_i]}{1 - F_i(0)}.$$

Proposition 2.1 can be readily generalized as follows:

### Proposition B.4

$$F_i(t) \leq F_i(0) + (y_i - F_i(0)) \cdot t,$$

with equality iff

$$\mathbb{P}[B_i = 0 \text{ or } B_i > t] = 1. \quad (\star)$$

**Proof.** For all  $\tau \leq t$ , we have that

$$\mathbb{P}[B_i > \tau] \leq \mathbb{P}[B_i \neq 0] = 1 - F_i(0),$$

with equality when  $(\star)$  holds. Substituting this inequality into (3), we get

$$F_i(t) \leq F_i(0) + \frac{(1 - F_i(0))^2}{\mathbb{E}[B_i]} \cdot t = F_i(0) + (y_i - F_i(0)) \cdot t,$$

with equality iff  $(\star)$  holds. ■

## C Tightness of the 2-Quasi-Regularity Result

**Proof of Proposition 3.6.** Let  $s$  be a  $(2 - \epsilon)$ -quasi-regular random sequence. We claim that  $B_1 = 2$  with probability 1, and  $B_2 = 3$  with probability 1. For suppose that with positive probability  $B_1 \leq 1$ . Then, because  $z_1 = 2$ , we also would have to have  $B_1 \geq 3$  with positive probability, and vice versa. Similarly,  $B_2 \leq 2$  with positive probability iff  $B_2 \geq 4$  with positive probability. Either of those cases would lead to a ratio  $(3/1 \text{ or } 4/2)$  larger than  $2 - \epsilon$ , violating  $(2 - \epsilon)$ -quasi-regularity.

Hence, with probability one, target 1 appears in every other time period and target 2 appears in every third time period, which is impossible. ■

## D Proof of Theorem 5.3

We begin with a few simple, but useful, technical lemmas. First, we give a closed form for expressions of the form  $\frac{f_{k+1}}{\varphi} - f_k$ .

**Lemma D.1** *For any  $k$ , we have that*

$$\frac{f_{k+1}}{\varphi} - f_k = (-1/\varphi)^{k+2} \cdot \frac{1 + \varphi^2}{\sqrt{5}}.$$

**Proof.** Using the closed-form expression for Fibonacci Numbers (Part 2 of Lemma 5.2), we can write

$$\begin{aligned} \frac{f_{k+1}}{\varphi} - f_k &= \frac{(\varphi^{k+1}/\varphi - (-1/\varphi)^{k+1}/\varphi) - (\varphi^k - (-1/\varphi)^k)}{\sqrt{5}} \\ &= \frac{(-1/\varphi)^{k+2} + (-1/\varphi)^k}{\sqrt{5}} \\ &= (-1/\varphi)^{k+2} \frac{1 + \varphi^2}{\sqrt{5}}. \blacksquare \end{aligned}$$

**Lemma D.2** 1. *For all  $\delta \in (-\frac{1}{2}, \frac{1}{2}]$  and integers  $n > 1, m \geq 0$ , the following two are equivalent:*

- $\delta = ((n + m)/\varphi - m/\varphi) \pmod{1}$ .
- *There exists a positive integer  $D$  with  $n/D - \varphi = \delta\varphi/D$ .*

2. *Let  $\delta = (f_k/\varphi) \pmod{1}$  for  $k \geq 3$  (where we consider the range of the  $\pmod$  operation to be  $(-\frac{1}{2}, \frac{1}{2}]$ ). Then,  $\delta = f_k/\varphi - f_{k-1}$ .*

**Proof.** 1. The first condition can be rewritten as  $n/\varphi = \delta + D$  for some integer  $D \geq 0$ . Multiplying by  $\varphi/D$  now gives equivalence with the second condition.

2. In the first part of the lemma, set  $m = 0$  and  $n = f_k$ . Then, the condition is equivalent to the existence of a positive integer  $D$  with  $f_k/D - \varphi = \delta\varphi/D$ , implying that  $|f_k/\varphi - D| = |\delta|$ . By choosing  $D = f_{k-1}$ , according to Lemma D.1, we get that

$$|f_k/\varphi - f_{k-1}| = (1/\varphi)^{k+1} \cdot \frac{1 + \varphi^2}{\sqrt{5}} \leq \frac{1 + \varphi^2}{\sqrt{5}\varphi^4} < \frac{1}{2}.$$

Therefore, for any  $D \neq f_{k-1}$ , we get that  $|f_k/\varphi - D| > 1 - \frac{1}{2} = \frac{1}{2}$ , meaning that no  $D \neq f_{k-1}$  can satisfy  $f_k/D - \varphi = \delta\varphi/D$ . By substituting the unique choice  $D = f_{k-1}$ , we obtain the second part of the lemma.  $\blacksquare$

Because the Fibonacci numbers are the convergents of the Golden Ratio, they provide the best rational approximation, in the following sense.

**Theorem D.3** *Let  $M \geq 1$  be arbitrary. Let  $k$  be the largest even number with  $f_k \leq M$ , and  $k'$  the largest odd number with  $f_{k'} \leq M$ . Then, for all  $m \leq M$  and all  $n$ , we have the following:*

1.  $n/m > \varphi$  implies  $f_{k+1}/f_k \leq n/m$ .
2.  $n/m < \varphi$  implies  $f_{k'+1}/f_{k'} \geq n/m$ .

Theorem D.3 follows directly from standard results stating that the convergents provide the best approximation to real numbers (e.g., [14, p.11]), noting that the second (intermediate) case cannot happen for the Golden Ratio.

We are now ready to prove the characterization of the distribution of  $B_i$  under the Golden Ratio schedule.

**Proof of Theorem 5.3.** We begin by showing that the support of return times consists only of Fibonacci Numbers. Consider the interval  $I = [0, \alpha)$ . Let  $m$  be a return time. Because  $\alpha \leq \frac{1}{2}$  by assumption, we get that  $m \geq 2$ . Let  $x \in I$  be arbitrary, and  $y = (x + m/\varphi) \bmod 1$ , which is in  $I$  by assumption. Define  $\delta = y - x$ . Because both  $x, y \in I$ , we have that  $\delta \in [-x, \alpha - x)$ . By Part 1 of Lemma D.2, there is a positive integer  $D$  such that

$$m/D - \varphi = \delta\varphi/D \in [-x\varphi/D, (\alpha - x)\varphi/D).$$

We now distinguish two cases:

- If  $m/D - \varphi > 0$ , then Case 1 of Theorem D.3 implies that the largest even  $j$  such that  $f_j \leq D$  satisfies  $f_{j+1}/f_j - \varphi > 0$  and  $f_{j+1}/f_j \leq m/D$ . Thus,  $(x + f_j/\varphi) \bmod 1 \in I$ , meaning that the defender returns to the target in  $f_j$  steps. Unless  $m = f_j$ , this contradicts the definition of  $m$  as a return time, so we have shown that  $m$  is a Fibonacci number.
- Similarly, if  $m/D - \varphi < 0$ , then Case 2 of Theorem D.3 implies that the largest odd  $j$  such that  $f_j \leq D$  satisfies  $f_{j+1}/f_j - \varphi < 0$  and  $f_{j+1}/f_j \geq m/D$ . By the same argument, we obtain now that  $m = f_j$ .

Next, we prove the second part of the theorem. First, notice that the  $k$  defined in the theorem actually exists. By Lemma D.1, we get that  $|\frac{f_{k+1}}{\varphi} - f_k| = (1/\varphi)^{k+2} \cdot \frac{1+\varphi^2}{\sqrt{5}} \rightarrow 0$  as  $k \rightarrow \infty$ , so there exists a  $k$  (and thus a smallest  $k$ ) with  $|f_{k+1}/\varphi - f_k| \leq \alpha$ .

We show that there cannot be a return time  $m < f_{k+1}$ . If there were, then by the previous part of the proof,  $m$  would be a Fibonacci number, say,  $m = f_\ell$ . And because  $m \geq 2$ , we get that  $\ell \geq 3$ . By Part 2 of Lemma D.2, that means that  $f_\ell/\varphi - f_{\ell-1} = y - x$ , and hence  $|f_\ell/\varphi - f_{\ell-1}| = |y - x| < \alpha$ , contradicting the definition of  $k$  as smallest with that property.

Consider a return to  $I$ , starting from  $x \in I$  and ending at  $y \in I$ , so that  $\delta_\ell := y - x$  satisfies  $|\delta_\ell| < \alpha$ , and within  $m$  steps, for  $m = f_\ell, \ell \geq k + 1$  by the previous analysis. Again, by Part 2 of Lemma D.2, we obtain that  $\delta_\ell = f_\ell/\varphi - f_{\ell-1}$ .

When  $\delta_\ell < 0$ , the  $x \in I$  with  $x + \delta_\ell \in I$  are exactly captured by the interval  $J_\ell := [|\delta_\ell|, \alpha]$ , while for  $\delta_\ell > 0$ , they are exactly the interval  $J_\ell := [0, \alpha - \delta_\ell)$ . In either case, the interval  $J_\ell$  has size exactly  $|J_\ell| = \alpha - |\delta_\ell|$ .

We will show that  $J_{k+2} \cup J_{k+3} = I$ . By Lemma 5.2, the signs of  $\delta_\ell$  are alternating, meaning that the intervals  $J_\ell$  alternate being of the form  $[0, x]$  and  $[y, \alpha)$ . In particular, to show that  $J_{k+2} \cup J_{k+3} = I$ , it suffices to show that  $|J_{k+2}| + |J_{k+3}| \geq \alpha$ . Because  $|J_{k+2}| + |J_{k+3}| = 2\alpha - |\delta_{k+2}| - |\delta_{k+3}|$ , this is equivalent to showing that  $|\delta_{k+2}| + |\delta_{k+3}| \leq \alpha$ . We distinguish two cases, based on whether  $k$  is even or odd.

- If  $k$  is even, then  $\delta_{k+2} = f_{k+2}/\varphi - f_{k+1} < 0$  and  $\delta_{k+3} = f_{k+3}/\varphi - f_{k+2} > 0$ , so we obtain that

$$|\delta_{k+3}| + |\delta_{k+2}| = f_{k+3}/\varphi - f_{k+2} - f_{k+2}/\varphi + f_{k+1} = f_{k+1}/\varphi - f_k = |f_{k+1}/\varphi - f_k| \leq \alpha,$$

by the definition of  $k$ .

- If  $k$  is odd, then  $\delta_{k+2} = f_{k+2}/\varphi - f_{k+1} > 0$  and  $\delta_{k+3} = f_{k+3}/\varphi - f_{k+2} < 0$ , so we obtain that

$$|\delta_{k+2}| + |\delta_{k+3}| = f_{k+2}/\varphi - f_{k+1} - f_{k+3}/\varphi + f_{k+2} = f_k - f_{k+1}/\varphi = |f_{k+1}/\varphi - f_k| \leq \alpha.$$

Thus, we have shown that the support of the distribution is indeed contained in  $\{f_{k+1}, f_{k+2}, f_{k+3}\}$ . Finally, we can work out the frequencies. Conditioned on being in the interval of size  $\alpha$ , the probability of being in  $J_\ell$  is  $q_\ell = |J_\ell|/\alpha$ . To arrive at the attacker's observed distribution of  $B_i$ , we notice that the probability of time 0 being in an interval of length  $f_\ell$  is

$$\frac{q_\ell f_\ell}{\sum_j q_j f_j} = \frac{q_\ell f_\ell}{1/\alpha} = f_\ell \cdot |J_\ell|.$$

Thus, we obtain that

$$\begin{aligned} \mathbb{P}[B_i = f_{k+1}] &= f_{k+1} \cdot |J_{k+1}| = f_{k+1} \cdot (\alpha - |f_{k+1}/\varphi - f_k|), \\ \mathbb{P}[B_i = f_{k+2}] &= f_{k+2} \cdot |J_{k+2}| = f_{k+2} \cdot (\alpha - |f_{k+1} - f_{k+2}/\varphi|), \\ \mathbb{P}[B_i = f_{k+3}] &= 1 - q_1 - q_2 \\ &= f_{k+3} \cdot (-\alpha + |f_{k+1}/\varphi - f_k + f_{k+1} - f_{k+2}/\varphi|) \\ &= f_{k+3} \cdot (-\alpha + |f_{k-1} - f_k/\varphi|). \end{aligned}$$

Notice that we arranged the terms inside absolute values such that for even  $k$ , they are all positive, while for odd  $k$ , they are all negative. This allowed us to simply add inside the absolute value. Applying Lemma D.1 to all three terms now completes the proof. ■

## E Computational Considerations for the Golden Ratio Schedule

As phrased, Algorithm 2 requires precise arithmetic on irrational numbers, and drawing a uniformly random number from  $[0, 1]$ . Here, we discuss how to implement the algorithm such that each target  $i$  visited in step  $t$  can be computed in time polynomial in the input size.

Let  $\alpha_i = a_i/b_i$  for each  $i$ , and write  $M = \text{scm}(b_1, \dots, b_m)$  for the common denominator. Notice that  $\log M \leq \sum_i \log b_i$  is polynomial in the input size.

For each  $i$ , the number  $P_i = \sum_{i' < i} p_{i'}$  is rational. To decide whether target  $i$  is visited in step  $t$ , the algorithm needs to decide if  $(\lambda + t/\varphi) \bmod 1 \in [P_i, P_{i+1}]$ , or — equivalently — if there is an integer  $D$  with  $\lambda + t/\varphi \in [D + P_i, D + P_{i+1}]$ . To decide whether  $\lambda + t/\varphi < D + P_j$  or  $\lambda + t/\varphi > D + P_j$  (for  $j \in \{i, i+1\}$ ), the algorithm needs to decide if  $\varphi < \frac{t}{D+P_j-\lambda}$  or  $\varphi > \frac{t}{D+P_j-\lambda}$ . The key question is how many digits of  $\varphi$  the algorithm needs to evaluate for this decision, and how many digits of the uniformly random offset  $\lambda$  it needs to decide on.

Suppose that the algorithm has generated the first  $k$  random digits of  $\lambda$ , having committed to  $\frac{\ell}{10^k} \leq \lambda < \frac{\ell+1}{10^k}$  for some  $\ell \in \{0, 1, \dots, 10^k - 1\}$ . Writing  $P_j = N_j/M$  (using the denominator

$M$  defined above), a decision about target  $P_j$  can be made whenever  $\varphi < \frac{tM10^k}{10^k \cdot MD + 10^k N_j - M \cdot \ell}$  or  $\varphi > \frac{tM10^k}{10^k \cdot MD + 10^k N_j - M \cdot (\ell + 1)}$ . In both cases, the right-hand side is a rational approximation to  $\varphi$  with denominator bounded by  $\hat{M} := 2 \cdot 10^k \cdot MD$ .

It is well known (see, e.g., [9, Theorems 193–194]) that  $|\varphi - \frac{\hat{N}}{M}| \geq \frac{1}{(\sqrt{5}-\epsilon)\hat{M}^2}$  for all  $\epsilon > 0$ . In particular, this implies that evaluating  $\varphi$  to within  $O(\log \hat{M}^2) = O(k + \log M + \log D)$  digits is sufficient to test whether  $\varphi < \frac{tM10^k}{10^k \cdot MD + 10^k N_j - M \cdot \ell}$ , and whether  $\varphi > \frac{tM10^k}{10^k \cdot MD + 10^k N_j - M \cdot (\ell + 1)}$ . In either of these cases, the algorithm has resolved whether  $\varphi < \frac{t}{D + P_j - \lambda}$ .

The only case where the algorithm cannot resolve whether  $\varphi < \frac{t}{D + P_j - \lambda}$  is when

$$\frac{tM10^k}{10^k \cdot MD + 10^k N_j - M \cdot (\ell + 1)} < \varphi < \frac{tM10^k}{10^k \cdot MD + 10^k N_j - M \cdot \ell}.$$

In this case, the number of digits for  $\lambda$  is insufficient. Notice that there is a unique value of  $\ell$  for which this happens, so the probability of failure is at most  $10^{-k}$ . Taking a union bound over all  $n$  interval boundaries and all  $t$  rounds, we see that in order to succeed with high probability, the number of digits of  $\lambda$  the algorithm needs to generate is  $O(\log n + \log t)$ .

In particular, the computation and required randomness are polynomial.

## References

- [1] Omer Angel, Alexander E. Holroyd, James B. Martin, and James Propp. Discrete low-discrepancy sequences. <https://arxiv.org/abs/0910.1077>, 2010.
- [2] Rudolf Avenhaus, Bernhard von Stengel, and Shmuel Zamir. Inspection games. In Robert J. Aumann and Sergiu Hart, editors, *Handbook of Game Theory, Vol. 3*, chapter 51, pages 1947–1987. North-Holland, Amsterdam, 2002.
- [3] Chandra Chekuri, Jan Vondák, and Rico Zenklusen. Dependent randomized rounding via exchange properties of combinatorial structures. In *Proc. 51st IEEE Symp. on Foundations of Computer Science*, pages 575–584, 2010.
- [4] Vincent Conitzer and Tuomas Sandholm. Computing the optimal strategy to commit to. In *Proc. 8th ACM Conf. on Electronic Commerce*, pages 82–90, 2006.
- [5] Joseph L. Doob. Renewal theory from the point of view of the theory of probability. *Transactions of the American Mathematical Society*, 63(3):422–438, 1948.
- [6] Fei Fang, Thanh H. Nguyen, Rob Pickles, Wai Y. Lam, Gopalasamy R. Clements, Bo An, Amandeep Singh, Brian C. Schwedock, Milind Tambe, and Andrew Lemieux. PAWS — a deployed game-theoretic application to combat poaching. *AI Magazine*, 2017. (to appear).
- [7] Fei Fang, Peter Stone, and Milind Tambe. When security games go green: Designing defender strategies to prevent poaching and illegal fishing. In *Proc. 30th Intl. Joint Conf. on Artificial Intelligence*, pages 2589–2595, 2015.



- [8] Rajiv Gandhi, Samir Khuller, Srinivasan Parthasarathy, and Aravind Srinivasan. Dependent rounding and its applications to approximation algorithms. *Journal of the ACM*, 53:324–360, 2006.
- [9] Godfrey H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, fourth edition, 1960.
- [10] Alexander E. Holroyd and James Propp. Rotor walks and markov chains. *Algorithmic probability and combinatorics*, 520:105–126, 2010.
- [11] Alon Itai and Zvi Rosberg. A golden ratio control policy for a multiple-access channel. *IEEE Transactions on Automatic Control*, 29(8):712–718, 1984.
- [12] Donald E. Knuth. *The Art of Computer Programming: Sorting and Searching*, volume 3. Pearson Education, 1998.
- [13] Dmytro Korzhyk, Vincent Conitzer, and Ronald Parr. Security games with multiple attacker resources. In *Proc. 26th Intl. Joint Conf. on Artificial Intelligence*, pages 273–279, 2011.
- [14] László Lovász. *An Algorithmic Theory of Numbers, Graphs and Convexity*, volume 50 of *CBMS-NSF Regional Conference Series in Applied Mathematics*. SIAM, 1986.
- [15] Roger B. Myerson. *Game Theory: Analysis of Conflict*. Harvard University Press, 1997.
- [16] Shivendra S. Panwar, Thomas K. Philips, and Mon Song Chen. Golden ratio scheduling for flow control with low buffer requirements. *IEEE Transactions on Communications*, 40(4):765–772, 1992.
- [17] Noel B. Slater. The distribution of the integers  $n$  for which  $\{\theta n\} < \varphi$ . *Proceedings of the Cambridge Philosophical Society*, 46(4):525–534, 1950.
- [18] Noel B. Slater. Gaps and steps for the sequence  $n\theta \pmod 1$ . *Mathematical Proceedings of the Cambridge Philosophical Society*, 63(04):1115–1123, 1967.
- [19] Aravind Srinivasan. Distributions on level-sets with applications to approximation algorithms. In *Proc. 42nd IEEE Symp. on Foundations of Computer Science*, pages 588–597, 2001.
- [20] Milind Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press, 2011.
- [21] Robert Tijdeman. On a distribution problem in finite and countable sets. *Journal of Combinatorial Theory, Series A*, 15(2):129–137, 1973.
- [22] Robert Tijdeman. The chairman assignment problem. *Discrete Mathematics*, 32:323–330, 1980.
- [23] Heinrich von Stackelberg. *Marktform und Gleichgewicht*. Springer, 1934.