Randomized Functions with High Round Complexity

Abstract. Consider two-party secure function evaluation against an honest-but-curious adversary in the information-theoretic plain model. We study the round complexity to realize a given secure function evaluation functionality securely.

For any securely realizable deterministic function evaluation, Kushilevitz-Beaver (1989) proved an upper bound on its round complexity – solely determined by the cardinality of its domain and range. This phenomenon also extends to functions with randomized output over small output sets, It is folklore that this property extends to arbitrary randomized functions.

Recently, Basu-Khorasgani-Maji-Nguyen (FOCS–2022) introduced a geometric approach to investigate the round complexity of randomized functions. They translate the round complexity question into a geometric question about an object embedded in a space whose dimension depends only on the cardinality of the input and output sets – adding further support to this folklore.

This paper refutes this folklore. For every r, we construct a function f_r, with binary inputs and five output alphabets, that has round complexity r. Previously, Basu et al. constructed such a function with $(r+1)$ output alphabets.

Our counter-examples are optimal – any function with binary inputs and four output alphabets has constant round complexity.

1 Introduction

Secure multi-party computation [8, 10] (MPC) allows mutually distrusting parties to compute over their private data. In general, MPC requires an honest majority or oblivious transfer to compute tasks securely. Even if honest parties are not in the majority, several tasks are securely computable in the information-theoretic plain model, i.e., without oblivious transfer or other hardness of computation assumptions. For example, the Dutch auction mechanism [4] securely performs auctions. These information-theoretic protocols, if they exist, are highly desirable – they are perfectly secure, fast, and require no setup or preprocessing. With rapid increases in the computational power of parties, the round complexity of these protocols becomes the primary bottleneck, significantly impacting their adoption.

This work studies the round complexity of MPC in the two-party information-theoretic plain model against honest-but-curious adversaries. Alice and Bob have private inputs $x \in X$ and $y \in Y$, respectively, and their objective is to securely sample an output z from the distribution $f(x, y)$ (over the sample space Z). The distribution $f(x, y)$ is publicly known, and both parties must receive the same output z. Parties have unbounded computation power and honestly follow the protocol; however, they are curious to obtain additional information about the other party's private input. An ideal communication channel connects the parties, and they send messages in alternating rounds.[1] The round complexity of securely computing f is the (worst-case) minimum number of rounds required to perform this sampling task securely.

A particular class of functions widely studied in communication complexity and cryptography is the class of deterministic functions. The function f is deterministic if the support of the distribution $f(x, y)$ is a singleton set for every $(x, y) \in X \times Y$. That is, the output z is determined entirely by the parties' private inputs (x, y). For example, in an auction, the price is determined by the bids.

Round complexity of deterministic functions. Chor-Kushilevitz-Beaver [3, 6, 9] characterized all deterministic functions that are securely computable in the two-party information-theoretic plain model against honest-but-curious adversaries. The secure protocols for such functions follow a general template – parties rule out specific outputs in each round. Excluding outputs, in turn, rules out private input pairs (because each input pair produces one output). For example, in the Dutch auction mechanism, the price that receives no bids is ruled out. Such functions are called *decomposable functions* because these secure protocols incrementally decompose the feasible input-output space during their evolution. Decomposable functions are securely computable with perfect security.

Now, let us reason about the round complexity of a deterministic function $f\colon X \times Y \to Z$, represented by round (f). One has to exclude card $(Z) - 1$ outputs so that only the output $z = f(x, y)$ remains feasible, where card (Z) represents

[1] Both parties know which party speaks in which round.

the cardinality of the set Z. So, if f has a secure protocol in this model, then

$$\operatorname{round}(f) \leqslant \operatorname{card}(Z) - 1.$$

Furthermore, the Markov property for interactive protocols holds in the information-theoretic plain. The joint distribution of inputs conditioned on the protocol's evolution always is a product distribution. Excluding outputs also excludes private inputs of the parties. For example, if Alice sends a message in a round, she rules out some of her private inputs. This observation leads to the bound

$$\operatorname{round}(f) \leqslant 2 \cdot \operatorname{card}(X) - 1.$$

Likewise, we also have

$$\operatorname{round}(f) \leqslant 2 \cdot \operatorname{card}(Y) - 1.$$

Combining these observations, Chor-Kushilevitz-Beaver [3,6,9] concluded

$$\operatorname{round}(f) \leqslant \min\{2 \cdot \operatorname{card}(X), 2 \cdot \operatorname{card}(Y), \operatorname{card}(Z)\} - 1. \tag{1}$$

The cardinalities of the private input and output sets determine the upper bound on the round complexity of f if it has a secure protocol. This phenomenon led to a general folklore/conjecture.

Folklore. There is a global function $R\colon \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that

$$\operatorname{round}(f) \leqslant R(\operatorname{card}(X), \operatorname{card}(Y), \operatorname{card}(Z))$$

for all functions f (even randomized).

Round complexity of randomized functions with small output domains. For functions with randomized output, this phenomenon already holds for small values of $\operatorname{card}(Z)$. For example, $\operatorname{card}(Z) \leqslant 3$ implies that $\operatorname{round}(f) \leqslant 2$ [7]. In fact, this paper will also show that $\operatorname{card}(Z) \leqslant 4$ implies $\operatorname{round}(f) \leqslant 4$. It is fascinating that these bounds are independent of the number of random bits required to sample the output.

For an analogy, consider the *communication complexity* objective of correctly (possibly insecurely) evaluating a randomized output function with minimum communication. Alice sends her input x to Bob. Bob samples $s \sim f(x, y)$ and sends the output z to Alice. The communication complexity of this (insecure) interactive protocol is $\log \operatorname{card}(X) + \log \operatorname{card}(Z)$. This upper bound on the communication complexity holds irrespective of the complexity of representing the individual probabilities $f(x, y)_z$. Intuitively, the sampling complexity of the output did not reflect in the round complexity because its impact was contained within the complexity of the respective parties' private computation. For small output sets, this is precisely that phenomenon that is witnessed for the secure evaluation case [7]. The possibility of this phenomenon extending to securely evaluating arbitrary randomized output functions, in general, remains open.

Round complexity of arbitrary randomized functions. For three decades, there was essentially no progress in determining the round complexity of securely computing general randomized functions – barring a few highly specialized cases [7]. Last year, Basu, Khorasgani, Maji, and Nguyen (FOCS 2022) showed that determining "whether a randomized f has an r-round protocol or not" is decidable. They reduce this question to a geometric one: "does a query point Q belong to a recursively-generated set $\mathcal{S}^{(r)}$." They start with an initial set of points $\mathcal{S}^{(0)}$, and recursively build $\mathcal{S}^{(i+1)}$ from the set $\mathcal{S}^{(i)}$ using a geometric action, for $i \in \{0, 1, \dots\}$. The function f has an r round protocol if (and only if) a specific query point Q belongs to the set $\mathcal{S}^{(r)}$; otherwise not.

These set of points $\left\{\mathcal{S}^{(i)}\right\}_{i \geqslant 0}$ lie in the ambient space

$$\mathbb{R}^{\mathrm{card}(X)-1} \times \mathbb{R}^{\mathrm{card}(Y)-1} \times \mathbb{R}^{\mathrm{card}(Z)}.$$

Again, the dimension of the ambient space (of their embedding) is determined entirely by the cardinalities of the inputs and output sets. This feature of their embedding added additional support to the folklore.

Consider an analogy. Suppose there are n initial points in $\mathbb{R}^d$, where $n \gg d$. At the outset, any point inside the convex hull can be expressed as a convex linear combination of the initial points that lie on the convex hull; their number can be $\gg d$. However, Carathéodory's theorem [5] states that every point in its interior is expressible as a convex linear combination of (at most) $(d+1)$ initial points on the convex hull. At an abstract level: canonical representations may have significantly lower complexity. It is similar to the Pumping lemma for regular languages and (more generally) the Ogden lemma for context-free languages.

Likewise, in the context of Basu et al.'s geometric problem, a fascinating possibility opens up. The canonical protocol for f could have round complexity determined solely by the dimension of their ambient space, which (in turn) is determined by the cardinality of the input and output sets. In fact, they optimistically conjecture an $\mathcal{O}\Big(\mathrm{card}\,(Z)^2\Big)$ upper bound on the round complexity in the full version of their paper [2, Section 7, Conjecture 1]. So,

Is the folklore true?

We refute this folklore. The analogies break exactly at $|Z| = 5$. Represent a randomized function with input set $X \times Y$ and output set Z as $f\colon X \times Y \to \mathbb{R}^Z$. For every $r \in \{1, 2, \dots\}$, we construct a function $f_r\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4,5\}}$ with round complexity r. Previously, Basu et al. constructed functions $g_r\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,\dots,r+1\}}$ with round complexity r, i.e., their example had $\mathrm{card}\,(Z) = r + 1$. In our example, $\mathrm{card}\,(Z) = 5$, a constant. Moreover, our counterexamples are minimal: Any $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4\}}$ has round complexity $\leqslant 4$.

Looking ahead. Our results indicate that any upper bound on the round complexity of f must involve the complexity of representing (the probabilities appearing in) the function f. For example, consider a randomized function whose probabilities are integral multiples of $1/B$. Then, the round complexity of f should be upper bounded by some function of $\mathrm{card}\,(X)$, $\mathrm{card}\,(Y)$, $\mathrm{card}\,(Z)$, and B. The B-term represents (intuitively) "the condition number of the function f." One can only wonder whether this dependence on B can, in fact, be a $\mathsf{poly}(\log(B))$ dependence, which leads to efficient secure algorithms.

Our work considers the round complexity of perfectly secure protocols. The case of statistically secure protocols remains an interesting open problem. In fact, the decidability of "is there an r-round ε-secure protocol for f" remains unknown, which is a more fundamental problem. Basu et al. [1] only considered the perfect security case. The technical machinery to handle statistical security for general randomized output functions does not exist.

1.1 Our Contributions

Suppose $r = 4k + 1$, where $k \in \{0, 1, 2, \dots\}$. Define the sequence $\{\sigma_k\}_{k \geqslant 0}$ as follows.

$$\sigma_k \;:=\; \sum_{j=0}^{k-1} \frac{1}{16^j} = \frac{1 - (1/16)^k}{1 - 1/16}, \qquad (\text{for } k \geqslant 0)$$

Consider a randomized function $f_r\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4,5\}}$,where $r = 4k + 1$, defined below.

$$f_{4k+1}(0,0) = \left(\frac{3}{16} \cdot \sigma_k, \frac{1}{4} \cdot \sigma_{k+1}, \frac{1}{8} \cdot \sigma_k, \frac{3}{8} \cdot \sigma_k, \frac{3}{2^{4k+2}}\right), \tag{2}$$

$$f_{4k+1}(0,1) = \left(\frac{9}{16} \cdot \sigma_k, \frac{1}{4} \cdot \sigma_{k+1}, 0 \cdot \sigma_k, \frac{1}{8} \cdot \sigma_k, \frac{3}{2^{4k+2}}\right), \tag{3}$$

$$f_{4k+1}(1,0) = \left(\frac{1}{16} \cdot \sigma_k, \frac{3}{4} \cdot \sigma_{k+1}, \frac{1}{8} \cdot \sigma_k, 0 \cdot \sigma_k, \frac{1}{2^{4k+2}}\right), \tag{4}$$

$$f_{4k+1}(1,1) = \left(\frac{3}{16} \cdot \sigma_k, \frac{3}{4} \cdot \sigma_{k+1}, 0 \cdot \sigma_k, 0 \cdot \sigma_k, \frac{1}{2^{4k+2}}\right). \tag{5}$$

Here, $f_r(x,y)_z$ represents the probability of output being $z \in Z$ conditioned on the input pair being $(x,y) \in X \times Y$. We prove the following result.

Corollary 1 (Arbitrarily High Round Complexity for $\operatorname{card}(Z) = 5$). *We claim this construction for $r \in \{1, 5, 9, \dots\}$ only for simplicity of presentation. We can construct such functions for any $r \in \{1, 2, \dots\}$. For every $r \in \{1, 5, 9, \dots\}$ ($r = 4k + 1$ for some k), the randomized function $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4,5\}}$ define by Equation 2 to Equation 5 has an r-round secure protocol but no $(r-1)$-round secure protocol.*

Theorem 1 and Theorem 2 yields this corollary. Section 3 presents these theorems and their proofs. Corollary 3 presents another interpretation: there are functions with constant-size input and output sets such that perfectly secure protocols need $\log \lambda$ rounds, where λ is the security parameter.

Our constructions are optimal in the following sense.

Corollary 2 (Bounded Round Complexity for $\operatorname{card}(Z) \leqslant 4$). *For $\operatorname{card}(Z) \leqslant 4$, the $\operatorname{round}(f) \leqslant 4$ for any randomized function $f : \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$,*

Theorem 3 implies this corollary. Section 4 presents this theorem and its proof. We proceed by an exhaustive enumeration of all possible cases.

1.2 Technical Overview

The presentation in this work is entirely geometric. No background in security is necessary. We use the geometric embedding of BKMN [1] to translate round complexity problems into geometric problems. Security is already folded inside their geometric embedding.

BMKN Geometric Sets. Fix the dimension of our ambient space $d \in \{1, 2, \dots\}$. In the context of demonstrating arbitrarily high round complexity, we shall use $d = 7$. To show the round complexity bound for $\operatorname{card}(Z) \leqslant 4$, we shall use $d = 6$. All our sets of points will lie in $\mathbb{R}^d$. We shall have an initial set of points $\mathcal{S}^{(0)} \subseteq \mathbb{R}^d$ (of a specific form).

Next, we consider the BKMN geometric action to recursively generate $\mathcal{S}^{(i+1)}$ from $\mathcal{S}^{(i)}$. For simplicity, we restrict to the case that $X = Y = \{0,1\}$. For this case, their geometric action is the following.

Geometric Action: Constructing $\mathcal{S}^{(i+1)}$ from $\mathcal{S}^{(i)}$ when $X = Y = \{0,1\}$

For any $t \in \{1, 2, \dots\}$ and points $P^{(1)}, P^{(2)}, \dots, P^{(t)} \in \mathcal{S}^{(i)}$, add all convex linear combinations of the points $\{P^{(1)}, P^{(2)}, \dots, P^{(t)}\}$ to the set $\mathcal{S}^{(i+1)}$ if (and only if)

1. $P_1^{(1)} = P_1^{(2)} = \cdots = P_1^{(t)}$, or
2. $P_2^{(1)} = P_2^{(2)} = \cdots = P_2^{(t)}$.

Some clarifications.

1. For a point $P \in \mathbb{R}^d$, P_1 represents the first coordinate of P and P_2 represents the second coordinate of P.

2. A convex linear combination of the points $P^{(1)}, \ldots, P^{(t)}$, is a point of the form $\lambda^{(1)} \cdot P^{(1)} + \cdots + \lambda^{(t)} \cdot P^{(t)}$, where $\lambda^{(1)}, \ldots, \lambda^{(t)} \geqslant 0$ and $\sum_{i=1}^{t} \lambda^{(i)} = 1$. All possible convex linear combinations consider all possible such $\lambda^{(1)}, \ldots \lambda^{(t)}$ values.
3. The points $P^{(1)}, \ldots, P^{(t)}$ in the definition need not be distinct
4. Considering $t = 1$ in the definition above ensures that $\mathcal{S}^{(i)} \subseteq \mathcal{S}^{(i+1)}$.
5. Since efficiency is not a consideration in the current context, we consider $t \in \{1, 2, \ldots\}$. Otherwise, by Carathéodory's theorem [5], it suffices to consider only $t = (d + 1)$.

If there is a point $P \in \mathcal{S}^{(r)}$ such that $P_1 = 1/2$ and $P_2 = 1/2$ then there is a function $f_P \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^{\{1,2,3,4,d-2\}}$ that has an r-round protocol. The mapping $P \mapsto f_P$ is injective. If $P \notin \mathcal{S}^{(r-1)}$, then the function f_P has no $(r-1)$-round protocol.

Geometric proxies for our MPC objectives. Now, our geometric problems of interest are as follows.

1. We want to construct functions with arbitrarily large round complexity. To this end, we will start with an appropriate $\mathcal{S}^{(0)} \subseteq \mathbb{R}^7$. Next, we will consider the evolution
$$\mathcal{S}^{(0)} \subseteq \mathcal{S}^{(1)} \subseteq \mathcal{S}^{(2)} \subseteq \cdots.$$
For any $r \in \{1, 2, \ldots\}$, we will show $P \in \mathcal{S}^{(r)} \setminus \mathcal{S}^{(r-1)}$ such that $P_1 = 1/2$ and $P_2 = 1/2$. Now, the function f_P has round complexity r, and no $(r-1)$ round protocol can securely compute it.
2. To show that our examples are minimal, we consider any $\mathcal{S}^{(0)} \subseteq \mathbb{R}^6$ (of a certain form). We show that $\mathcal{S}^{(i+1)} = \mathcal{S}^{(i)}$, for some $i \leqslant 4$.

High round complexity. Let us start with $\mathcal{S}^{(0)}$ containing the following five initial points (one point representing one output).

$$P^{(1)} = \left(\frac{3}{4}, \frac{1}{4}, 1, 0, 0, 0, 0\right)$$
$$P^{(2)} = \left(\frac{1}{4}, \frac{1}{2}, 0, 1, 0, 0, 0\right)$$
$$P^{(3)} = \left(\frac{1}{2}, 1, 0, 0, 1, 0, 0\right)$$
$$P^{(4)} = \left(1, \frac{3}{4}, 0, 0, 0, 1, 0\right)$$
$$P^{(5)} = \left(\frac{3}{4}, \frac{1}{2}, 0, 0, 0, 0, 1\right)$$

Define $Q^{(1)} = \left(\frac{1}{2}, \frac{1}{2}, 0, \frac{1}{2}, 0, 0, \frac{1}{2}\right)$ as the midpoint of $P^{(5)}$ and $P^{(2)}$. Note that $Q^{(1)} \in \mathcal{S}^{(1)} \setminus \mathcal{S}^{(0)}$ and $Q_1^{(1)} = Q_2^{(1)} = 1/2$. So, the function $f_{Q^{(1)}}$ has a one-round protocol but no zero-round protocol.

Define $Q^{(2)} = \left(\frac{1}{2}, \frac{3}{4}, 0, \frac{1}{4}, \frac{1}{2}, 0, \frac{1}{4}\right)$ as the midpoint of $Q^{(1)}$ and $P^{(3)}$. We shall prove that $Q^{(2)} \in \mathcal{S}^{(2)} \setminus \mathcal{S}^{(1)}$. Note that it is evident that $Q^{(2)} \in \mathcal{S}^{(2)}$ (because $Q^{(1)} \in \mathcal{S}^{(1)}$). The non-triviality is in proving that $Q^{(2)} \notin \mathcal{S}^{(1)}$. We will prove these types of results using a carefully crafted inductive hypothesis.

Define $Q^{(3)} = \left(\frac{3}{4}, \frac{3}{4}, 0, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, \frac{1}{8}\right)$ as the midpoint of $Q^{(2)}$ and $P^{(4)}$. We shall prove that $Q^{(3)} \in \mathcal{S}^{(3)} \setminus \mathcal{S}^{(2)}$.

Define $Q^{(4)} = \left(\frac{3}{4}, \frac{1}{2}, \frac{1}{2}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{16}\right)$ as the midpoint of $Q^{(3)}$ and $P^{(1)}$. We shall prove that $Q^{(4)} \in \mathcal{S}^{(4)} \setminus \mathcal{S}^{(3)}$.

Now, define $Q^{(5)} = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{4}, \frac{1}{2} + \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{32}\right)$ as the midpoint of $Q^{(4)}$ and $P^{(2)}$. Now, exciting things have started to happen. We shall prove that $Q^{(5)} \in \mathcal{S}^{(5)} \setminus \mathcal{S}^{(4)}$. So, the function $F_{Q^{(5)}}$ has a five-round protocol but no four-round protocol.

And we continue to construct these points inductively. For $i \in \{1, 2, 3, \dots\}$, define $Q^{(i+1)}$ as the midpoint of $Q^{(i)}$ and $P^{(1+(i+1 \mod 4))}$. We shall inductively show that $Q^{(i+1)} \in \mathcal{S}^{(i+1)} \setminus \mathcal{S}^{(i)}$.

The sequence $\{Q^{(1)}, Q^{(5)}, Q^{(9)}, \dots\}$ of distinct points will be of interest. for any k, the point $Q^{(4k+1)}$ will satisfy $Q_1^{(4k+1)} = Q_2^{(4k+1)} = 1/2$ and the function $f_{Q^{(4k+1)}}$ will have a $(4k+1)$ round secure protocol, but no $4k$ round protocol. Intuitively, as k increases, the contribution of $P^{(5)}$ to the point $Q^{(4k+1)}$ reduces – tending to 0; but never becoming 0.

Minimality of our example. We shall start with $\mathcal{S}^{(0)} \subseteq \mathbb{R}^6$ containing the following four points.

$$
\begin{aligned}
P^{(1)} &= (x_1, y_1, 1, 0, 0, 0) \\
P^{(2)} &= (x_2, y_2, 0, 1, 0, 0) \\
P^{(3)} &= (x_3, y_3, 0, 0, 1, 0) \\
P^{(4)} &= (x_4, y_4, 0, 0, 0, 1)
\end{aligned}
$$

We know that functions with three outputs have (at most) 2-round protocols [7]. If the points above have some form of degeneracy, then the upper bound for three outputs will be applicable. First, all (x_i, y_i) has to be distinct. If $(x_i, y_i) = (x_j, y_j)$, for $i \neq j$, then those two outputs are "essentially identical" (as noted in [7]). And the total number of outputs reduce to three, for which an upper bound of 2 on the round complexity is known.

The set $\mathcal{S}^{(i)}$, as i increases, must eventually become connected. It is instructive to know some cases when the $\mathcal{S}^{(i)}$ will never become connected. For example, suppose x_is are all distinct, and y_js are all distinct. In this case, $\mathcal{S}^{(2)} = \mathcal{S}^{(1)}$ because no two points are axis aligned The cases where $\mathcal{S}^{(i)}$ always remain disconnected (with growing i) lead to functions where at least one output is absent. This case again leads to (at most) three different outputs, for which an upper bound of 2 on the round complexity is known.

Next, we finally exhaustively enumerate all such cases (modulo their relative positioning) and prove that, in every case, $\mathcal{S}^{(4)} = \mathcal{S}^{(5)}$. That is, no function

requires 5 rounds of communication. The upper bound of 4 is tight (BKMN presents a four-output function requiring 4 rounds of communication).

1.3 Overview of the paper

Section 2 introduces notations and preliminaries. Section 3 contains all results pertaining to constructing high-round complexity randomized functions. Section 4 shows that our counterexamples are optimal.

2 Preliminaries

This section introduces some notations and definitions to facilitate our presentation.

2.1 Notations

We will use the following notations for a point $p \in \mathbb{R}^d$, a scalar $c \in \mathbb{R}$, and a set $\mathcal{S} \subseteq \mathbb{R}^d$.

$$p + \mathcal{S} \;:=\; \{p + q \colon q \in \mathcal{S}\}, \quad c \cdot \mathcal{S} \;:=\; \{c \cdot q \colon q \in \mathcal{S}\}.$$

We use the standard notations $\setminus, \cup, \cap$ to denote the minus, union, and intersection operators on sets, respectively.

2.2 Convex Geometry

For any two points $x, y \in \mathbb{R}^d$, the *line segment* between x and y, denoted as $\overline{xy}$, is the set of all points $t \cdot x + (1-t) \cdot y$ for $t \in [0, 1]$. A subset of $\mathbb{R}^d$ is a *convex set* if, given any two points in the subset, the subset contains the whole line segment joining them. A *convex combination* is a linear combination of points in which all coefficients are non-negative and sum up to 1. An *extreme point* of a convex set $S \subseteq \mathbb{R}^d$ is a point that does not lie on any open line segment joining two distinct points of S.

Definition 1 (Convex Hull). *For any set $S \subseteq \mathbb{R}^d$, the convex hull of S, denoted as $\mathsf{conv}(S)$, is the set of all convex combinations of points in S.*

For example, every line segment is the convex hull of the two endpoints. The following facts follow directly from the definition of the convex hull.

Fact 1 *For any subset $\mathcal{S} \subseteq \mathbb{R}^d$, it holds that $\mathsf{conv}(\mathsf{conv}(\mathcal{S})) = \mathsf{conv}(\mathcal{S})$.*

Fact 2 *For any $\mathcal{S} \subseteq \mathcal{T} \subseteq \mathbb{R}^d$, it holds that $\mathsf{conv}(\mathcal{S}) \subseteq \mathsf{conv}(\mathcal{T})$.*

3 Functions with High Round Complexity

Let $P = (P_1, P_2, P_3, P_4, P_5, P_6, P_7)$ denote a point in $\mathbb{R}^2 \times \mathbb{R}^5$. We define the following projections

$$\begin{aligned} &\pi\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}^2, && \pi(P) \;:=\; (P_1, P_2) \\ &\pi_1\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}, && \pi_1(P) \;:=\; P_1 \\ &\pi_2\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}, && \pi_2(P) \;:=\; P_2 \\ &\rho\colon \mathbb{R}^2 \times \mathbb{R}^5 \to \mathbb{R}^5, && \rho(P) \;:=\; (P_3, P_4, P_5, P_6, P_7) \end{aligned}$$

We use $e_i \in \mathbb{R}^5$, where $i \in \{1, \ldots, 5\}$, to represent the i^{th} vector of the standard basis for $\mathbb{R}^5$. All coordinates of e_i are 0 except the i^{th} coordinate equal to 1. For example, if $P = (1/4, 1/2, 0, 1, 0, 0, 0)$, then

$$\pi(P) = (1/4, 1/2), \quad \pi_1(P) = 1/4,\ \pi_2(P) = 1/2, \quad \rho(P) = (0, 1, 0, 0, 0) = e_2.$$

For $t \in \{1, 2, \ldots\}$ and any points $Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)} \in \mathcal{S}^{(i-1)}$ satisfying

$$\pi_1(Q^{(1)}) = \pi_1(Q^{(2)}) = \cdots = \pi_1(Q^{(t)}), \text{ or}$$
$$\pi_2(Q^{(1)}) = \pi_2(Q^{(2)}) = \cdots = \pi_2(Q^{(t)})$$

add all possible convex linear combinations of $Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)}$ to the set $\mathcal{S}^{(i)}$.

Fig. 1: Recursive procedure to construct $\mathcal{S}^{(i)}$ from $\mathcal{S}^{(i-1)}$ for $i \in \{1, 2, \ldots\}$.

Theorem 1. *Define the following points in* $\mathbb{R}^2$

$$a_1 = (3/4, 1/4),\ a_2 = (1/4, 1/2),\ a_3 = (1/2, 1),\ a_4 = (1, 3/4),\ a_5 = (3/4, 1/2).$$

We define the initial set $\mathcal{S}^{(0)}$ *as follows.*

$$\mathcal{S}^{(0)} \;:=\; \{P \in \mathbb{R}^2 \times \mathbb{R}^5 \colon \exists\ i \in \{1, 2, 3, 4, 5\},\ \pi(P) = a_i \text{ and } \rho(P) = e_i\}.$$

For $i \in \{1, 2, \ldots\}$, *let* $\mathcal{S}^{(i)} \subseteq \mathbb{R}^2 \times \mathbb{R}^5$ *be the set defined recursively from* $\mathcal{S}^{(i-1)}$ *according to Figure 1. Then, for all* $i \in \{1, 2, \ldots\}$,

$$\mathcal{S}^{(i-1)} \subsetneq \mathcal{S}^{(i)}.$$

We begin the proof of Theorem 1 by introducing some notations (refer to Figure 2). We define the following additional points for our analysis.

$$a_6 = (1/2, 1/2),\ a_7 = (1/2, 3/4),\ a_8 = (3/4, 3/4)$$

Let $\overline{a_1 a_8}$ denote the set of points on the line segment that connects the point

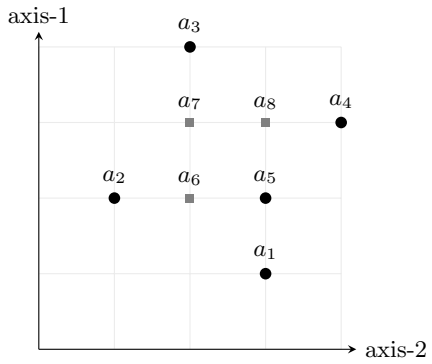


Fig. 2: An example showing that the sequence $\{\mathcal{S}^{(i)}\}_{i=0}^{\infty}$ does not stabilize.

a_1 to the point a_5. The segments $\overline{a_2a_5}, \overline{a_3a_6}, \overline{a_4a_7}$ are defined similarly. For any set $\Omega \subseteq \mathbb{R}^2$, we define the set $\mathcal{S}_{\Omega}^{(i)}$ as follows.

$$\mathcal{S}_{\Omega}^{(i)} \ := \ \{Q \in \mathcal{S}^{(i)} : \pi(Q) \in \Omega\}$$

Whenever Ω is a singleton set, we omit the brackets. For example,

$$\begin{aligned}
&\mathcal{S}_{a_1}^{(0)} = \{(3/4, 1/4, 1, 0, 0, 0, 0)\}, \quad \mathcal{S}_{a_2}^{(0)} = \{(1/4, 1/2, 0, 1, 0, 0, 0)\},\\
&\mathcal{S}_{a_3}^{(0)} = \{(1/2, \quad 1, 0, 0, 1, 0, 0)\}, \quad \mathcal{S}_{a_4}^{(0)} = \{(1, 3/4, 0, 0, 0, 1, 0)\},\\
&\mathcal{S}_{a_5}^{(0)} = \{(3/4, 1/2, 0, 0, 0, 0, 1)\}, \quad \mathcal{S}_{a_6}^{(0)} = \mathcal{S}_{a_7}^{(0)} = \mathcal{S}_{a_8}^{(0)} = \emptyset.
\end{aligned}$$

Moreover, for any set $\Omega \subseteq \mathbb{R}^2 \times \mathbb{R}^5$, we define

$$\rho\,(\Omega) \ := \ \{\rho(P) : P \in \Omega\}.$$

For example, $\rho(\mathcal{S}_{a_4}^{(0)}) = \{(0, 0, 0, 1, 0)\} = \{e_4\}$. The lemma below follows directly from the definition of the sequence $\{\mathcal{S}_i\}_{i=0}^{\infty}$.

Proposition 1. *For any set Ω and any $i \in \{0, 1, \dots\}$, the following property holds.*

$$\mathcal{S}_{\Omega}^{(i)} \subseteq \mathcal{S}_{\Omega}^{(i+1)}.$$

The following result says that for any $i \in \{0, 1, \dots\}$, all the points in the line segment $\overline{a_1a_8}$ at round $(i+1)$ except the new ones at the point a_8 are constructed solely from the points at a_1, a_8, a_5 at round i.

Lemma 1. *For every $i \in \{0, 1, \dots\}$,*

$$\mathcal{S}_{\overline{a_1a_8}}^{(i+1)} \setminus \left(\mathcal{S}_{a_8}^{(i+1)} \setminus \mathcal{S}_{a_8}^{(i)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_1}^{(i)} \cup \mathcal{S}_{a_8}^{(i)} \cup \mathcal{S}_{a_5}^{(i)}\right),$$

$$\mathcal{S}_{\overline{a_2a_5}}^{(i+1)} \setminus \left(\mathcal{S}_{a_5}^{(i+1)} \setminus \mathcal{S}_{a_5}^{(i)}\right) = \mathsf{conv}\left(\mathcal{S}_{a_2}^{(i)} \cup \mathcal{S}_{a_5}^{(i)} \cup \mathcal{S}_{a_6}^{(i)}\right),$$

$$\mathcal{S}^{(i+1)}_{\overline{a_3a_6}} \setminus \left(\mathcal{S}^{(i+1)}_{a_6} \setminus \mathcal{S}^{(i)}_{a_6}\right) = \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_3} \cup \mathcal{S}^{(i)}_{a_6} \cup \mathcal{S}^{(i)}_{a_7}\right),$$
$$\mathcal{S}^{(i+1)}_{\overline{a_4a_7}} \setminus \left(\mathcal{S}^{(i+1)}_{a_7} \setminus \mathcal{S}^{(i)}_{a_7}\right) = \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_4} \cup \mathcal{S}^{(i)}_{a_7} \cup \mathcal{S}^{(i)}_{a_8}\right).$$

Proof. We prove by induction on i.
Base case. For $i = 0$, we have

$$\mathcal{S}^{(0)}_{a_1} = \{(3/4, 1/4, 1, 0, 0, 0, 0, 0)\},\ \mathcal{S}^{(0)}_{a_5} = \{(3/4, 1/2, 0, 0, 0, 0, 1)\},\ \mathcal{S}^{(0)}_{a_8} = \emptyset.$$

It implies that

$$\mathsf{conv}\left(\mathcal{S}^{(0)}_{a_1} \cup \mathcal{S}^{(0)}_{a_8} \cup \mathcal{S}^{(0)}_{a_5}\right) = \mathsf{conv}\left(\mathcal{S}^{(0)}_{a_1} \cup \mathcal{S}^{(0)}_{a_5}\right).$$

Observe that $\pi_1(P) = 3/4$, for any point $P \in \mathcal{S}^{(0)}_{a_1} \cup \mathcal{S}^{(0)}_{a_5}$. Therefore, any convex combination of a point in $\mathcal{S}^{(0)}_{a_1}$ and a point in $\mathcal{S}^{(0)}_{a_5}$ is in the set $\mathcal{S}^{(1)}_{\overline{a_1a_8}}$. Notice that $\mathcal{S}^{(0)}_{a_8} = \mathcal{S}^{(1)}_{a_8} = \emptyset$. This shows that

$$\mathsf{conv}\left(\mathcal{S}^{(0)}_{a_1} \cup \mathcal{S}^{(0)}_{a_8} \cup \mathcal{S}^{(0)}_{a_5}\right) \subseteq \mathcal{S}^{(1)}_{\overline{a_1a_8}} = \mathcal{S}^{(1)}_{\overline{a_1a_8}} \setminus \left(\mathcal{S}^{(1)}_{a_8} \setminus \mathcal{S}^{(0)}_{a_8}\right).$$

To prove the other direction, observe that any point in $\mathcal{S}^{(1)}_{\overline{a_1a_8}}$ except for the points in $\mathcal{S}^{(1)}_{a_8} \setminus \mathcal{S}^{(0)}_{a_8}$ is a convex combination of a set of points in $\mathcal{S}^{(0)}_{\overline{a_1a_8}} = \mathcal{S}^{(0)}_{a_1} \cup \mathcal{S}^{(0)}_{a_5}$ by definition. Thus, it follows that

$$\mathcal{S}^{(1)}_{\overline{a_1a_8}} \setminus \left(\mathcal{S}^{(1)}_{a_8} \setminus \mathcal{S}^{(0)}_{a_8}\right) = \mathcal{S}^{(1)}_{\overline{a_1a_8}} \subseteq \mathsf{conv}\left(\mathcal{S}^{(0)}_{a_1} \cup \mathcal{S}^{(0)}_{a_5}\right) = \mathsf{conv}\left(\mathcal{S}^{(0)}_{a_1} \cup \mathcal{S}^{(0)}_{a_8} \cup \mathcal{S}^{(0)}_{a_5}\right).$$

Induction Hypothesis. We assume that

$$\mathcal{S}^{(i)}_{\overline{a_1a_8}} \setminus \left(\mathcal{S}^{(i)}_{a_8} \setminus \mathcal{S}^{(i-1)}_{a_8}\right) = \mathsf{conv}\left(\mathcal{S}^{(i-1)}_{a_1} \cup \mathcal{S}^{(i-1)}_{a_8} \cup \mathcal{S}^{(i-1)}_{a_5}\right),$$

and similarly for other equations.
Induction Step. Note that for any point P in the set $\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}$, we have $\pi_1(P) = 3/4$. Therefore,

$$\mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right) \subseteq \mathcal{S}^{(i+1)}_{\overline{a_1a_8}}$$

Since $\overline{a_4a_7}$ is the only line segment that contains a_8 such that a_8 is not an end point of it, we have:

$$\left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) \cap \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right) = \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) \cap \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_8}\right) = \emptyset.$$

Therefore, we conclude that

$$\mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right) \subseteq \mathcal{S}^{(i+1)}_{\overline{a_1a_8}} \setminus \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right).$$

To prove the other direction, note that any point in $\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i+1)}_{a_8}$ is constructed from a convex combination of the points in $\mathcal{S}^{(i)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i)}_{a_8}$. Thus, we have

$$\begin{aligned}
\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i+1)}_{a_8} &\subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i)}_{a_8}\right) \\
&\subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i)}_{a_8} \setminus \mathcal{S}^{(i-1)}_{a_8}\right)\right) && (\textit{Fact 2}) \\
&= \mathsf{conv}\left(\mathsf{conv}\left(\mathcal{S}^{(i-1)}_{a_1} \cup \mathcal{S}^{(i-1)}_{a_8} \cup \mathcal{S}^{(i-1)}_{a_5}\right)\right) && (\text{Induction hypothesis}) \\
&= \mathsf{conv}\left(\mathcal{S}^{(i-1)}_{a_1} \cup \mathcal{S}^{(i-1)}_{a_8} \cup \mathcal{S}^{(i-1)}_{a_5}\right) && (\textit{Fact 1}) \\
&\subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right), && (\textit{Prop. 1} \text{ and } \textit{Fact 2})
\end{aligned}$$

Since $\mathcal{S}^{(i)}_{a_8} \subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right)$, it follows that

$$\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) = \left(\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \mathcal{S}^{(i+1)}_{a_8}\right) \cup \mathcal{S}^{(i)}_{a_8} \subseteq \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right).$$

We have shown that

$$\mathcal{S}^{(i+1)}_{\overline{a_1 a_8}} \setminus \left(\mathcal{S}^{(i+1)}_{a_8} \setminus \mathcal{S}^{(i)}_{a_8}\right) = \mathsf{conv}\left(\mathcal{S}^{(i)}_{a_1} \cup \mathcal{S}^{(i)}_{a_8} \cup \mathcal{S}^{(i)}_{a_5}\right).$$

We prove other equations in a similar manner, which completes the proof.

Next, using Lemma 1, we prove a recursive construction of the projection ρ at the points a_i for $1 \leqslant i \leqslant 8$.

Lemma 2. *For all $i \in \{0, 1, \dots\}$,*

$$\rho(\mathcal{S}^{(i)}_{a_1}) = \{e_1\},\ \rho(\mathcal{S}^{(i)}_{a_2}) = \{e_2\},\ \rho(\mathcal{S}^{(i)}_{a_3}) = \{e_3\},\ \rho(\mathcal{S}^{(i)}_{a_4}) = \{e_4\}.$$

Furthermore, for all $i \in \{1, 2, \dots, \}$,

$$\begin{aligned}
\rho(\mathcal{S}^{(0)}_{a_5}) = \{e_5\},\ \rho(\mathcal{S}^{(i+1)}_{a_5}) &= \mathsf{conv}\left(\rho(\mathcal{S}^{(i)}_{a_5}) \cup \frac{1}{2} \cdot \left(e_1 + \rho(\mathcal{S}^{(i)}_{a_8})\right)\right), \\
\rho(\mathcal{S}^{(0)}_{a_6}) = \emptyset,\ \rho(\mathcal{S}^{(i+1)}_{a_6}) &= \mathsf{conv}\left(\rho(\mathcal{S}^{(i)}_{a_6}) \cup \frac{1}{2} \cdot \left(e_2 + \rho(\mathcal{S}^{(i)}_{a_5})\right)\right), \\
\rho(\mathcal{S}^{(0)}_{a_7}) = \emptyset,\ \rho(\mathcal{S}^{(i+1)}_{a_7}) &= \mathsf{conv}\left(\rho(\mathcal{S}^{(i)}_{a_7}) \cup \frac{1}{2} \cdot \left(e_3 + \rho(\mathcal{S}^{(i)}_{a_6})\right)\right), \\
\rho(\mathcal{S}^{(0)}_{a_8}) = \emptyset,\ \rho(\mathcal{S}^{(i+1)}_{a_8}) &= \mathsf{conv}\left(\rho(\mathcal{S}^{(i)}_{a_8}) \cup \frac{1}{2} \cdot \left(e_4 + \rho(\mathcal{S}^{(i)}_{a_7})\right)\right).
\end{aligned}$$

Proof. Initially, $\rho(\mathcal{S}^{(0)}_{a_1}) = \{e_1\}$. At any round $i \in \{1, 2 \dots\}$, there is no new point constructed at a_1, since a_1 is an extreme point of $\mathsf{conv}(a_1, a_2, a_3, a_4, a_5)$. Therefore, $\rho(\mathcal{S}^{(i)}_{a_1}) = \{e_1\}$. Similarly, we have

$$\rho(\mathcal{S}^{(i)}_{a_2}) = \{e_2\},\ \rho(\mathcal{S}^{(i)}_{a_3}) = \{e_3\},\ \rho(\mathcal{S}^{(i)}_{a_4}) = \{e_4\},\ \text{for every } i \in \{0, 1, \dots\}.$$

Let $P \in \mathcal{S}_{a_5}^{(i+1)}$. It follows from Lemma 1 that there are points $P_{a_1} \in \mathcal{S}_{a_1}^{(i)}$, $P_{a_8} \in \mathcal{S}_{a_8}^{(i)}$, $P_{a_5} \in \mathcal{S}_{a_5}^{(i)}$, and $\lambda_1, \lambda_8, \lambda_5 \geqslant 0$ such that

$$P = \lambda_1 \cdot P_{a_1} + \lambda_8 \cdot P_{a_8} + \lambda_5 \cdot P_{a_5}, \text{ and } \lambda_1 + \lambda_8 + \lambda_5 = 1.$$

Projecting these points into the second coordinate, we have

$$\pi_2(P) = \lambda_1 \cdot \pi_2(P_{a_1}) + \lambda_8 \cdot \pi_2(P_{a_8}) + \lambda_5 \cdot \pi_2(P_{a_5}).$$

This together with $\pi_2(P) = \pi_2(P_{a_5}) = \frac{1}{2}(\pi_2(P_{a_1}) + \pi_2(P_{a_8}))$ implies that $\lambda_1 = \lambda_8$. Thus, the point P is in the set $\mathsf{conv}\left(\mathcal{S}_{a_5}^{(i)} \cup \frac{1}{2} \cdot \left(\mathcal{S}_{a_1}^{(i)} + \mathcal{S}_{a_8}^{(i)}\right)\right)$. This implies that

$$\mathcal{S}_{a_5}^{(i+1)} \subseteq \mathsf{conv}\left(\mathcal{S}_{a_5}^{(i)} \cup \frac{1}{2} \cdot \left(\mathcal{S}_{a_1}^{(i)} + \mathcal{S}_{a_8}^{(i)}\right)\right).$$

Projecting this fact into coordinates $\{3, 4, 5, 6, 7\}$ yields

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(i+1)}) &\subseteq \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(i)}) \cup \frac{1}{2} \cdot \left(\rho(\mathcal{S}_{a_1}^{(i)}) \cup \rho(\mathcal{S}_{a_8}^{(i)})\right)\right) \\
&= \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(i)}) \cup \frac{1}{2} \cdot \left(e_1 + \rho(\mathcal{S}_{a_8}^{(i)})\right)\right) \qquad (\text{since } \rho(\mathcal{S}_{a_1}^{(i)}) = \{e_1\}).
\end{aligned}$$

Conversely, it suffices to show that

$$\mathsf{conv}\left(\mathcal{S}_{a_5}^{(i)} \cup \frac{1}{2} \cdot \left(\mathcal{S}_{a_1}^{(i)} + \mathcal{S}_{a_8}^{(i)}\right)\right) \subseteq \mathcal{S}_{a_5}^{(i+1)}.$$

This follows directly from the fact that a_5 is the midpoint of the segment $\overline{a_1 a_8}$. We have proved that

$$\rho(\mathcal{S}_{a_5}^{(i+1)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(i)}) \cup \frac{1}{2} \cdot \left(e_1 + \rho(\mathcal{S}_{a_8}^{(i)})\right)\right).$$

Similarly, the other three equations for a_6, a_7, a_8 also hold.

Lemma 3. *For every $i \in \{0, 1, 2, \dots\}$, the following identities hold.*

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(4i)}) = \rho(\mathcal{S}_{a_5}^{(4i+1)}) = \rho(\mathcal{S}_{a_5}^{(4i+2)}) = \rho(\mathcal{S}_{a_5}^{(4i+3)}), \\
\rho(\mathcal{S}_{a_6}^{(4i+1)}) = \rho(\mathcal{S}_{a_6}^{(4i+2)}) = \rho(\mathcal{S}_{a_6}^{(4i+3)}) = \rho(\mathcal{S}_{a_6}^{(4i+4)}), \\
\rho(\mathcal{S}_{a_7}^{(4i+2)}) = \rho(\mathcal{S}_{a_7}^{(4i+3)}) = \rho(\mathcal{S}_{a_7}^{(4i+4)}) = \rho(\mathcal{S}_{a_5}^{(4i+5)}), \\
\rho(\mathcal{S}_{a_8}^{(4i+3)}) = \rho(\mathcal{S}_{a_8}^{(4i+4)}) = \rho(\mathcal{S}_{a_8}^{(4i+5)}) = \rho(\mathcal{S}_{a_8}^{(4i+6)}).
\end{aligned}$$

Proof. We prove by induction on i.

Base case. From the recursion in Lemma 2, one can verify that

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(0)}) = \rho(\mathcal{S}_{a_5}^{(1)}) = \rho(\mathcal{S}_{a_5}^{(2)}) = \rho(\mathcal{S}_{a_5}^{(3)}) &= \{e_5\}, \\
\rho(\mathcal{S}_{a_6}^{(1)}) = \rho(\mathcal{S}_{a_6}^{(2)}) = \rho(\mathcal{S}_{a_6}^{(3)}) = \rho(\mathcal{S}_{a_6}^{(4)}) &= \frac{e_2 + e_5}{2}, \\
\rho(\mathcal{S}_{a_7}^{(2)}) = \rho(\mathcal{S}_{a_7}^{(3)}) = \rho(\mathcal{S}_{a_7}^{(4)}) = \rho(\mathcal{S}_{a_7}^{(5)}) &= \frac{e_3}{2} + \frac{e_2 + e_5}{4}, \\
\rho(\mathcal{S}_{a_8}^{(3)}) = \rho(\mathcal{S}_{a_8}^{(4)}) = \rho(\mathcal{S}_{a_8}^{(5)}) = \rho(\mathcal{S}_{a_8}^{(6)}) &= \frac{e_4}{2} + \frac{e_3}{4} + \frac{e_2 + e_5}{8}.
\end{aligned}$$

Induction Step. Suppose the induction hypothesis holds for $(i-1)$. It follows from Lemma 2 that

$$\begin{aligned}\rho(\mathcal{S}_{a_5}^{(4i+3)}) &= \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+2)}) \cup \frac{1}{2}\cdot\left(e_1+\rho(\mathcal{S}_{a_8}^{(4i+2)})\right)\right)\\ &= \mathsf{conv}\left(\mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+1)}) \cup \frac{1}{2}\cdot\left(e_1+\rho(\mathcal{S}_{a_8}^{(4i+1)})\right)\right) \cup \frac{1}{2}\cdot\left(e_1+\rho(\mathcal{S}_{a_8}^{(4i+2)})\right)\right)\end{aligned}$$

By the induction hypothesis, $\rho(\mathcal{S}_{a_8}^{(4i+2)}) = \rho(\mathcal{S}_{a_8}^{(4i+1)})$. Therefore, we have

$$\frac{1}{2}\cdot\left(e_1+\rho(\mathcal{S}_{a_8}^{(4i+1)})\right) = \frac{1}{2}\cdot\left(e_1+\rho(\mathcal{S}_{a_8}^{(4i+2)})\right)$$

This, together with Fact 1 and Lemma 2, implies that

$$\rho(\mathcal{S}_{a_5}^{(4i+3)}) = \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+1)}) \cup \frac{1}{2}\cdot\left(e_1+\rho(\mathcal{S}_{a_8}^{(4i+1)})\right)\right) = \rho(\mathcal{S}_{a_5}^{(4i+2)}).$$

Likewise, one can show that $\rho(\mathcal{S}_{a_5}^{(4i+2)}) = \rho(\mathcal{S}_{a_5}^{(4i+1)})$ and $\rho(\mathcal{S}_{a_5}^{(4i+1)}) = \rho(\mathcal{S}_{a_5}^{(4i)})$. These imply that

$$\rho(\mathcal{S}_{a_5}^{(4i)}) = \rho(\mathcal{S}_{a_5}^{(4i+1)}) = \rho(\mathcal{S}_{a_5}^{(4i+2)}) = \rho(\mathcal{S}_{a_5}^{(4i+3)}).$$

The proof of other equalities is similar.

For $i \in \{0,1,2,\dots\}$, define

$$\begin{aligned}\sigma_i &:= \sum_{k=0}^{i-1}\frac{1}{16^k} = \frac{1-(1/16)^i}{1-1/16},\\ \alpha_i &:= \sigma_i\cdot\frac{e_1}{2} + \sigma_i\cdot\frac{e_4}{4} + \sigma_i\cdot\frac{e_3}{8} + \sigma_i\cdot\frac{e_2}{16} + \frac{e_5}{16^i},\\ \beta_i &:= \sigma_{i+1}\cdot\frac{e_2}{2} + \sigma_i\cdot\frac{e_1}{4} + \sigma_i\cdot\frac{e_4}{8} + \sigma_i\cdot\frac{e_3}{16} + \frac{e_5}{2^{4i+1}},\\ \gamma_i &:= \sigma_{i+1}\cdot\frac{e_3}{2} + \sigma_{i+1}\cdot\frac{e_2}{4} + \sigma_i\cdot\frac{e_1}{8} + \sigma_i\cdot\frac{e_4}{16} + \frac{e_5}{2^{4i+2}},\\ \delta_i &:= \sigma_{i+1}\cdot\frac{e_4}{2} + \sigma_{i+1}\cdot\frac{e_3}{4} + \sigma_{i+1}\cdot\frac{e_2}{8} + \sigma_i\cdot\frac{e_1}{16} + \frac{e_5}{2^{4i+3}}.\end{aligned}$$

The following proposition follows from the definition of σ_i.

Proposition 2. *For all $i \in \{1,2,\dots\}$,*

$$\sigma_i = 1 + \frac{1}{16}\sigma_{i-1}.$$

Proposition 3. *The following statements hold.*

$$\begin{aligned}\lim_{i\to\infty}\alpha_i &= \frac{8}{15}e_1+\frac{4}{15}e_4+\frac{2}{15}e_3+\frac{1}{15}e_2 := \alpha^*,\\ \lim_{i\to\infty}\beta_i &= \frac{8}{15}e_2+\frac{4}{15}e_1+\frac{2}{15}e_4+\frac{1}{15}e_3 := \beta^*,\\ \lim_{i\to\infty}\gamma_i &= \frac{8}{15}e_3+\frac{4}{15}e_2+\frac{2}{15}e_1+\frac{1}{15}e_4 := \gamma^*,\\ \lim_{i\to\infty}\delta_i &= \frac{8}{15}e_4+\frac{4}{15}e_3+\frac{2}{15}e_2+\frac{1}{15}e_1 := \delta^*.\end{aligned}$$

Proof. First, note that

$$\lim_{i\to\infty} \sigma_{i-1} = \lim_{i\to\infty} \sigma_i = \lim_{i\to\infty} \frac{1-(1/16)^i}{1-1/16} = 16/15.$$

Now, we have

$$\begin{aligned}\lim_{i\to\infty} \alpha_i &= \lim_{i\to\infty} \sigma_i \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^i} \\ &= \frac{16}{15} \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) \\ &= \frac{8}{15}e_1 + \frac{4}{15}e_4 + \frac{2}{15}e_3 + \frac{1}{15}e_2 = \alpha^*.\end{aligned}$$

Similarly, we can find the $\lim_{i\to\infty} \beta_i = \beta^*, \lim_{i\to\infty} \gamma_i = \gamma^*$, and $\lim_{i\to\infty} \delta_i = \delta^*$.

Proposition 4. *For all $i \in \{0, 1, \dots\}$,*

$$\begin{aligned}\alpha_{i+1} &= \frac{15}{16} \cdot \alpha^* + \frac{1}{16} \cdot \alpha_i, \quad & \beta_{i+1} &= \frac{15}{16} \cdot \beta^* + \frac{1}{16} \cdot \beta_i, \\ \gamma_{i+1} &= \frac{15}{16} \cdot \gamma^* + \frac{1}{16} \cdot \gamma_i, \quad & \delta_{i+1} &= \frac{15}{16} \cdot \delta^* + \frac{1}{16} \cdot \delta_i.\end{aligned}$$

Consequently, α_i is on the line segment between $\alpha_0 = e_5$ and α_{i+1}; and α_{i+1} is on the line segment between α_i and α^*. More formally,

$$\begin{aligned}&\alpha_i \in \mathsf{conv}(\alpha_0, \alpha_{i+1}),\ \alpha_{i+1} \in \mathsf{conv}(\alpha_i, \alpha^*), \\ &\beta_i \in \mathsf{conv}(\beta_0, \beta_{i+1}),\ \beta_{i+1} \in \mathsf{conv}(\beta_i, \beta^*), \\ &\gamma_i \in \mathsf{conv}(\gamma_0, \gamma_{i+1}),\ \gamma_{i+1} \in \mathsf{conv}(\gamma_i, \gamma^*), \\ &\delta_i \in \mathsf{conv}(\delta_0, \delta_{i+1}),\ \delta_{i+1} \in \mathsf{conv}(\delta_i, \delta^*).\end{aligned}$$

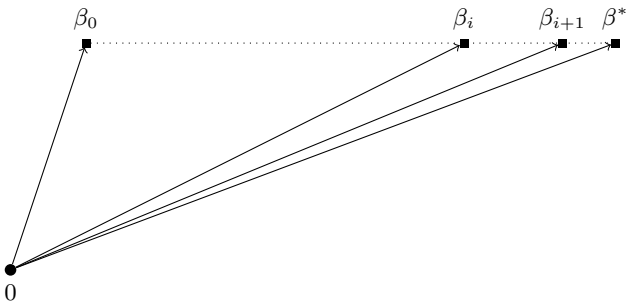


Fig. 3: Visualization of sequence $\{\beta_i\}_{i=1}^{\infty}$ (refer to Prop. 4)

Proof. By definition,

$$\alpha_i = \sigma_i \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^i}.$$

So, we have

$$\begin{aligned}
\alpha_{i+1} &= \sigma_{i+1} \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^{i+1}} \\
&= \left(1 + \frac{\sigma_i}{16}\right) \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^{i+1}} && (\textit{Prop. 2}) \\
&= \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{1}{16} \cdot \left(\sigma_i \cdot \left(\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}\right) + \frac{e_5}{16^i}\right) \\
&= \frac{15}{16} \cdot \alpha^* + \frac{1}{16} \cdot \alpha_i
\end{aligned}$$

The proofs of the three other equations are similar.

Proposition 5. *For all* $i \in \{0, 1, \dots\}$,

$$\alpha_{i+1} = \frac{e_1 + \delta_i}{2},\ \beta_i = \frac{e_2 + \alpha_i}{2},\ \gamma_i = \frac{e_3 + \beta_i}{2},\ \delta_i = \frac{e_4 + \gamma_i}{2}.$$

Proof. By definition,

$$\begin{aligned}
\frac{e_2 + \alpha_i}{2} &= \frac{e_2}{2} + \frac{\sigma_i}{2} \cdot (\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}) + \frac{e_5}{2 \cdot 16^i} \\
&= \frac{e_2}{2} + \frac{\sigma_i}{2} \cdot (\frac{e_1}{2} + \frac{e_4}{4} + \frac{e_3}{8} + \frac{e_2}{16}) + \frac{e_5}{2 \cdot 16^i} \\
&= \left(1 + \frac{\sigma_i}{16}\right) \cdot \frac{e_2}{2} + \sigma_i \cdot (\frac{e_1}{4} + \frac{e_4}{8} + \frac{e_3}{16}) + \frac{e_5}{2 \cdot 16^i} \\
&= \sigma_{i+1} \cdot \frac{e_2}{2} + \sigma_i \cdot (\frac{e_1}{4} + \frac{e_4}{8} + \frac{e_3}{16}) + \frac{e_5}{2 \cdot 16^i} && \textit{Prop. 2} \\
&= \beta_i
\end{aligned}$$

The proofs of the other equations are similar.

Lemma 4. *For all* $i \in \{0, 1. \dots\}$,

$$\rho(\mathcal{S}_{a_5}^{(4i)}) = \mathsf{conv}(\{\alpha_0, \alpha_i)\}),\ \rho(\mathcal{S}_{a_6}^{(4i+1)}) = \mathsf{conv}(\{\beta_0, \beta_i\}),$$
$$\rho(\mathcal{S}_{a_7}^{(4i+2))} = \mathsf{conv}(\{\gamma_0, \gamma_i\}),\ \rho(\mathcal{S}_{a_8}^{(4i+3)}) = \mathsf{conv}(\{\delta_0, \delta_i\}).$$

Proof. We prove by induction on i (refer to Figure 4).
Base case. For $i = 0$,

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(0)}) &= \{\alpha_0\} = \{e_5\}, \\
\rho(\mathcal{S}_{a_6}^{(1)}) &= \{\beta_0\} = \left\{\frac{e_2 + e_5}{2}\right\}, \\
\rho(\mathcal{S}_{a_7}^{(2)}) &= \{\gamma_0\} = \left\{\frac{e_3}{2} + \frac{e_2 + e_5}{4}\right\}, \\
\rho(\mathcal{S}_{a_8}^{(3)}) &= \{\delta_0\} = \left\{\frac{e_4}{2} + \frac{e_3}{4} + \frac{e_2 + e_5}{8}\right\}.
\end{aligned}$$

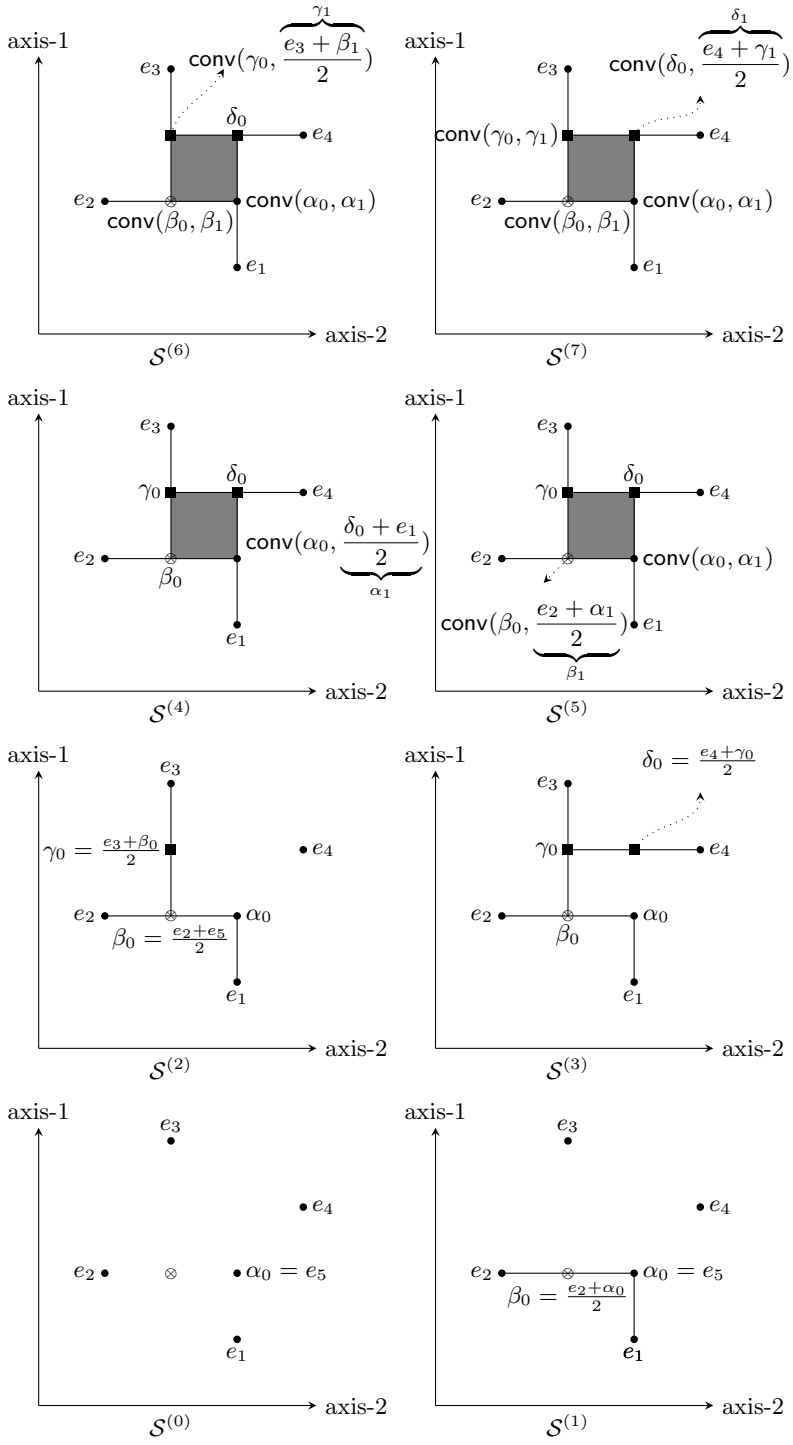


Fig. 4: The evolution of $\rho(\mathcal{S}^{(i)}_{a_5}), \rho(\mathcal{S}^{(i)}_{a_6}), \rho(\mathcal{S}^{(i)}_{a_7}), \rho(\mathcal{S}^{(i)}_{a_8})$

Induction Step. Suppose the lemma is true for i. We shall show that it is true for $i+1$.

$$\begin{aligned}
\rho(\mathcal{S}_{a_5}^{(4i+4))}) &= \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i+3)}) \cup \frac{1}{2}\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+3)})\right)\right) && (\textit{Lemma 2}) \\
&= \mathsf{conv}\left(\rho(\mathcal{S}_{a_5}^{(4i)}) \cup \frac{1}{2}\left(e_1 + \rho(\mathcal{S}_{a_8}^{(4i+3)})\right)\right) && (\textit{Lemma 3}) \\
&= \mathsf{conv}\left(\mathsf{conv}(\{\alpha_0, \alpha_i\}) \cup \frac{1}{2}\left(e_1 + \mathsf{conv}(\{\delta_0, \delta_i\})\right)\right) && \text{(Induction hypothesis)} \\
&= \mathsf{conv}\left(\{\alpha_0, \alpha_i\} \cup \left\{\frac{e_1+\delta_0}{2}, \frac{e_1+\delta_i}{2}\right\}\right) && (\textit{Fact 1}) \\
&= \mathsf{conv}\left(\{\alpha_0, \alpha_i\} \cup \{\alpha_1, \alpha_{i+1}\}\right) && \textit{Prop. 5} \\
&= \mathsf{conv}(\{\alpha_0, \alpha_{i+1}\}) && (\textit{Prop. 4} \text{ and } \textit{Fact 2})
\end{aligned}$$

Similarly, it holds that

$$\begin{aligned}
\rho(\mathcal{S}_{a_6}^{(4i+5)}) &= \mathsf{conv}(\{\beta_0, \beta_{i+1}\}), \\
\rho(\mathcal{S}_{a_7}^{(4i+6))}) &= \mathsf{conv}(\{\gamma_0, \gamma_{i+1}\}), \\
\rho(\mathcal{S}_{a_8}^{(4i+7)}) &= \mathsf{conv}(\{\delta_0, \delta_{i+1}\}),
\end{aligned}$$

which completes the proof.

The following result follows directly from Lemma 4 and Prop. 4.

Lemma 5. *For any $i \in \{0, 1, 2, \dots\}$, it holds that*

$$\alpha_{i+1} \notin \rho(\mathcal{S}_{a_5}^{(4i)}),\ \beta_{i+1} \notin \rho(\mathcal{S}_{a_6}^{(4i+1)}),\ \gamma_{i+1} \notin \rho(\mathcal{S}_{a_7}^{(4i+2)}),\ \delta_{i+1} \notin \rho(\mathcal{S}_{a_8}^{(4i+3)}).$$

Now, Theorem 1 follows directly from Lemma 5. As a other consequence, we have the following theorem.

Theorem 2. *For every $r \in \mathbb{N}$, there exists a function $f_r \colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ such that $|Z| = 5$ and f_r has r-round perfectly secure protocol but no $r-1$-round secure protocol.*

Proof. Suppose $r = 4k+1$, where $k \in \{0, 1, 2, \dots\}$. We want to find a function that has r round secure protocol but no $r-1$ round secure protocol. We define $Q^{(f_r)} := (1/2, 1/2, \beta_k)$. Then, we find the function corresponding to the following values:

$$\begin{aligned}
\mathcal{A} &= \begin{pmatrix} 3/4, & 1/4, & 1/2, & 1, & 3/4 \\ 1/4, & 3/4, & 1/2, & 0, & 1/4 \end{pmatrix}, \\
\mathcal{B} &= \begin{pmatrix} 1/4, & 1/2, & 1, & 3/4, & 1/2 \\ 3/4, & 1/2, & 0, & 1/4, & 1/2 \end{pmatrix}, \\
\mathcal{V} &= 4 \cdot \beta_k.
\end{aligned}$$

Note that $Q^{(f_r)} := (1/2, 1/2, \beta_k) \notin \mathcal{S}_{a_6}^{(r-1)}$. However, $Q^{(f_r)} := (1/2, 1/2, \beta_k) \in \mathcal{S}_{a_6}^{(r)}$. For example, when $r = 1$, then $k = 0$ and $Q^{(f_1)} := (1/2, 1/2, \beta_0) \notin \mathcal{S}_{a_6}^{(0)}$ but $Q^{(f_1)} \in \mathcal{S}_{a_6}^{(1)}$ or when $r = 5$, then $k = 1$ and $Q^{(f_5)} := (1/2, 1/2, \beta_1) \notin \mathcal{S}_{a_6}^{(4)}$ but $Q^{(f_5)} \in \mathcal{S}_{a_6}^{(5)}$. This implies that f_r has r round secure protocol but no $r-1$ secure protocol. Now, we have:

$$\mathcal{V} = 4 \cdot \beta_k = 4 \cdot \left(\sigma_k \cdot \frac{e_1}{4} + \sigma_{k+1} \cdot \frac{e_2}{2} + \sigma_k \cdot \frac{e_3}{16} + \sigma_k \cdot \frac{e_4}{8} + \frac{e_5}{2^{4k+1}} \right)$$

So, the vector representation of $\mathcal{V}$ is as follows:

$$\mathcal{V} = (\sigma_k, 2\sigma_{k+1}, \frac{\sigma_k}{4}, \frac{\sigma_k}{2}, \frac{1}{2^{4k-1}})$$

We provide the closed-form expression of f_r, when $r = 4k + 1$ for some $k \in \{0, 1, 2, \dots\}$, as follows:

$$f_{4k+1}(0,0) = \left(\frac{3}{16} \cdot \sigma_k, \frac{1}{4} \cdot \sigma_{k+1}, \frac{1}{8} \cdot \sigma_k, \frac{3}{8} \cdot \sigma_k, \frac{3}{2^{4k+2}} \right)$$
$$f_{4k+1}(0,1) = \left(\frac{9}{16} \cdot \sigma_k, \frac{1}{4} \cdot \sigma_{k+1}, 0 \cdot \sigma_k, \frac{1}{8} \cdot \sigma_k, \frac{3}{2^{4k+2}} \right)$$
$$f_{4k+1}(1,0) = \left(\frac{1}{16} \cdot \sigma_k, \frac{3}{4} \cdot \sigma_{k+1}, \frac{1}{8} \cdot \sigma_k, 0 \cdot \sigma_k, \frac{1}{2^{4k+2}} \right)$$
$$f_{4k+1}(1,1) = \left(\frac{3}{16} \cdot \sigma_k, \frac{3}{4} \cdot \sigma_{k+1}, 0 \cdot \sigma_k, 0 \cdot \sigma_k, \frac{1}{2^{4k+2}} \right)$$

We can extend the proof to the case that $r \neq 4k + 1$ for any k. The idea is similar. We can find 3 different family of functions corresponding to $r = 4k, r = 4k + 2, r = 4k + 3$. We only need to choose a different query point in Figure 2, a_5, a_7, or a_8 and scale that figure and transfer it appropriately such that query points $(1/2, 1/2)$ is on a_5, a_7, or a_8 depending on the remainder of division of r by 4.

Corollary 3. *Let λ be the security parameter. Then, there exists a randomized function $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^5$ such that the function f has description complexity $\mathcal{O}(\log \lambda)$, and any secure protocol for f has at least $\log \lambda$ rounds.*

4 On the Optimality of Our Constructions

This section proves that if the initial set $\mathcal{S}^{(0)}$ is a subset of $\mathbb{R}^6$ of size 4, the sequence $\{\mathcal{S}^{(i)}\}_{i=0}^{\infty}$ stabilizes after at most 4 steps.

Theorem 3. *Let $\mathcal{S}^{(0)}$ be a subset of $\mathbb{R}^6$ of size 4. Then, there exists an $i^* \in \{0, 1, 2, 3, 4\}$ such that $\mathcal{S}^{(i^*)} = \mathcal{S}^{(i^*+1)}$.*

The following result is a consequence of the above theorem and [1, 7].

Corollary 4. *Let $f\colon \{0,1\} \times \{0,1\} \to \mathbb{R}^Z$ such that $|Z| \leqslant 4$. If f has a perfectly secure protocol, then there is a perfectly secure protocol for f with at most 4 rounds.*

4.1 Proof of Theorem 3

We first give a proof by enumerating over all possible cases and showing that each case stabilizing using pictures. It was already shown in [7] that there is an at most two round secure protocol for a secure function with $|Z| \leqslant 3$. Therefore, without loss of generality, we only need to enumerate over the cases that the final result in $\mathcal{S}^{(\infty)}$ is connected. Moreover, we only need to consider one case among a set of cases that are similar. For example, in case 1, we consider 4 points that are aligned horizontally. The case that 4 points are aligned vertically is similar to case 1 and we do not need to consider it. We complete the proof by the following lemma (Lemma 6). Now, let us discuss case 6.

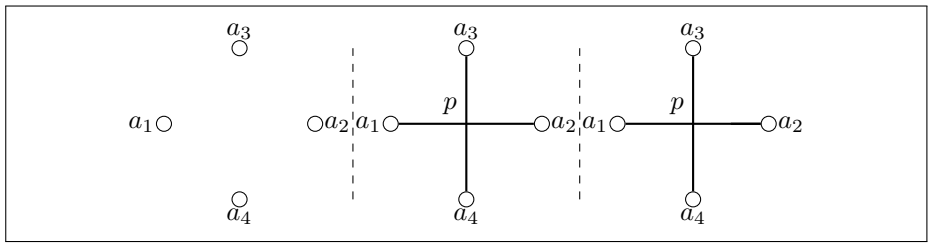
Lemma 6. *In the following table, we state i^* (defined in Theorem 3) for each of the following cases.*

Case Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
i^*	1	1	2	1	2	2	1	2	2	1	2	2	4	2	3	3	2

Table 1: The table of stabilization times for all distinct possible cases when $|Z| = 4$

Proof. In all cases except case 6, one can easily verify that $\mathcal{S}^{(i^*)} = \mathcal{S}^{(i^*+1)}$ for the i^* mentioned in the table. The reason is that in all those cases, when the final shape in the projected space (projection under π) stabilizes, then the whole shape stabilizes. More formally, in all cases except case 6, one can verify that $\pi(\mathcal{S}^{(i^*)}) = \pi(\mathcal{S}^{(i^*+1)})$ implies that $\mathcal{S}^{(i^*)} = \mathcal{S}^{(i^*+1)}$. For all cases except case 6, we show in the following that $\pi(\mathcal{S}^{(i^*)}) = \pi(\mathcal{S}^{(i^*+1)})$.

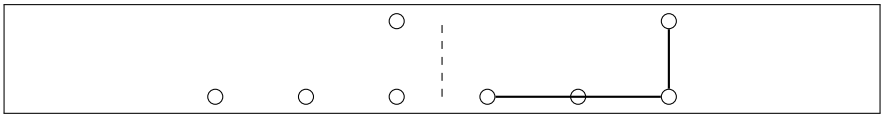
Now, we discuss case 6 in the following figure. At time 0, there are four points. Suppose $\rho(\mathcal{S}^{(0)}_{a_i}) = e_i$ where $e_i \in \mathbb{R}^4$ represents the i-th standard basis vector in $\mathbb{R}^4$. The points a_1 and a_2 are axis aligned, so $\rho(\mathcal{S}^{(1)}_{a_1a_2}) = \mathsf{conv}(e_1, e_2)$. Similarly, $\rho(\mathcal{S}^{(1)}_{a_3a_4}) = \mathsf{conv}(e_3, e_4)$. Now, notice that at the end of time 1, there are two objects at point p. One of them is $(p, \frac{e_1+e_2}{2})$ and the other one is $(p, \frac{e_3+e_4}{2})$. They are both axis aligned. So, we have $\rho(\mathcal{S}^{(2)}_p) = \mathsf{conv}(\frac{e_1+e_2}{2}, \frac{e_3+e_4}{2})$ and the shape stabilizes at time 2.

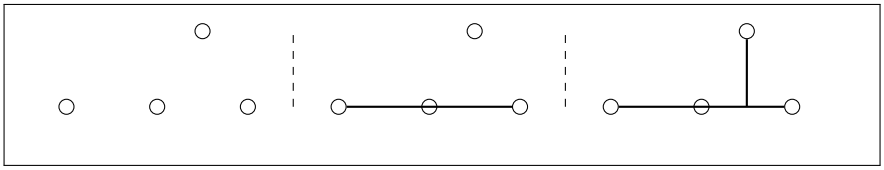


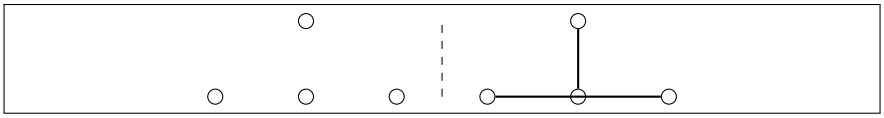
In the following, we enumerate over all possible cases and study the evolution of the sequence $\mathcal{S}^{(0)}, \mathcal{S}^{(1)}, \ldots$.

If there are 3 collinear points. There will be 4 cases as follows.

1. 

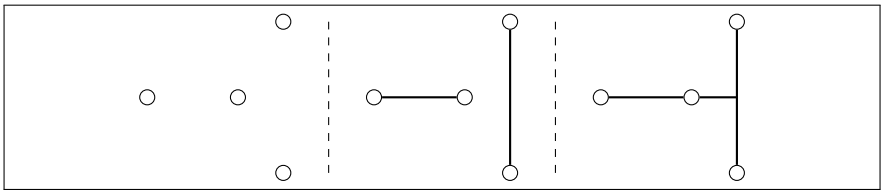
2. 

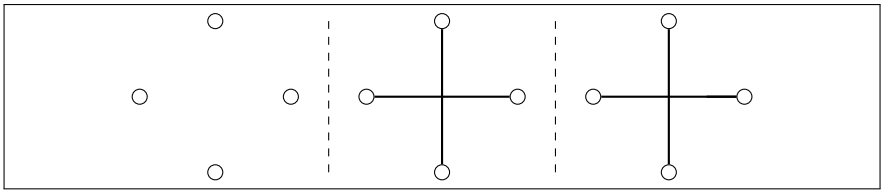
3. 

4. 

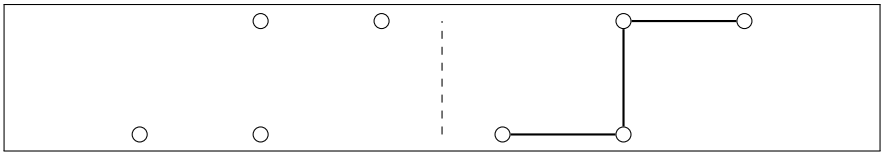
There are no 3 coolinear points.

Subcase 1: Two points are horizontally collinear and the other two points are vertically collinear. There are 2 cases as follows.

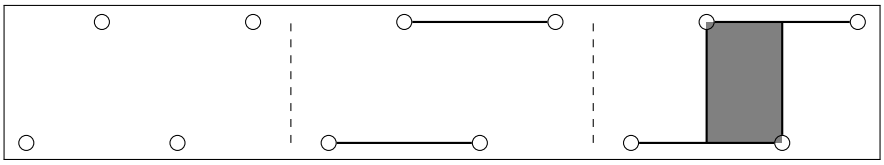
5. 

6. 

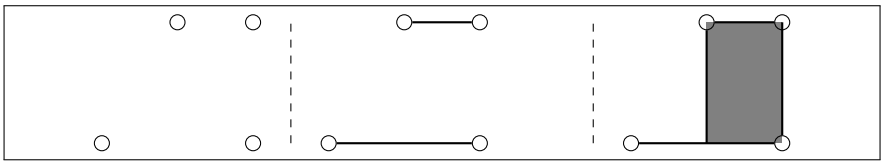
Subcase 2: Two points are horizontally collinear and the other two points are also horizontally collinear.

7. 

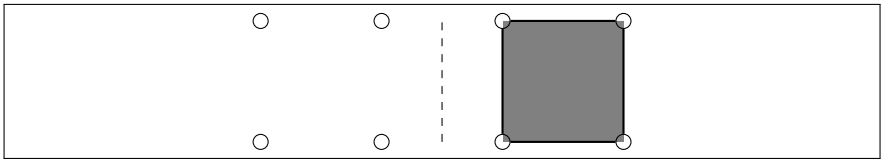
8.



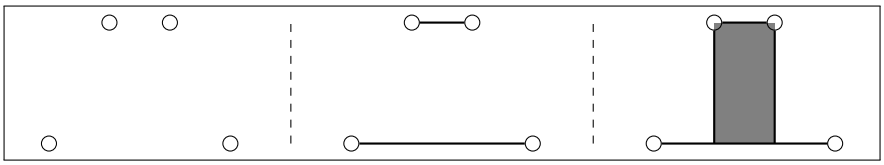
9.



10.

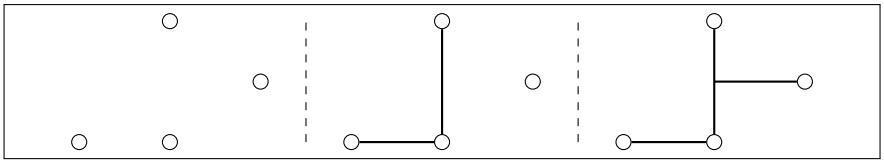


11.

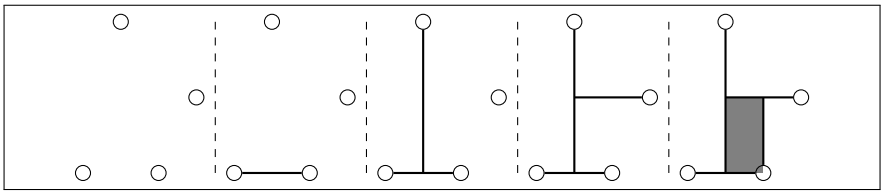


Subcase 3: Two points are horizontally collinear, the other two points are not collinear

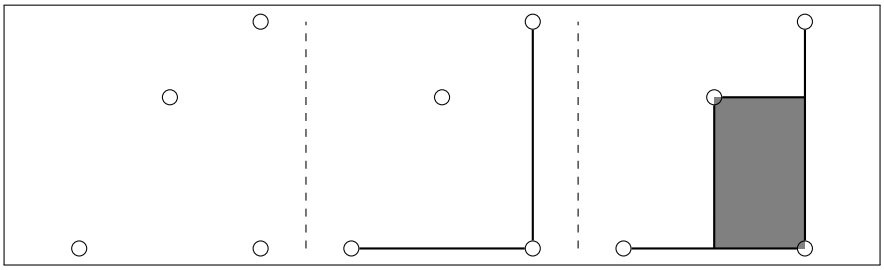
12.



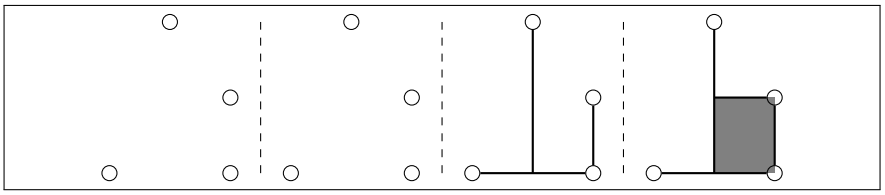
13.



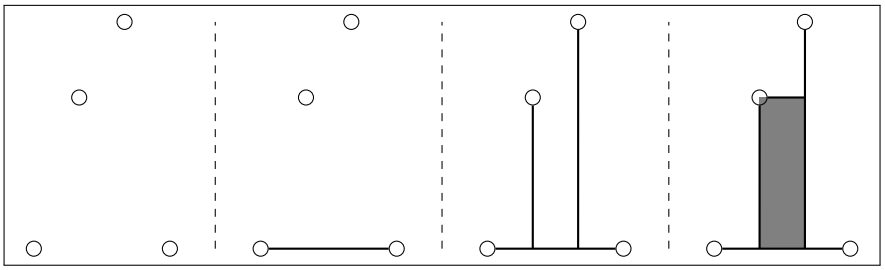
14.



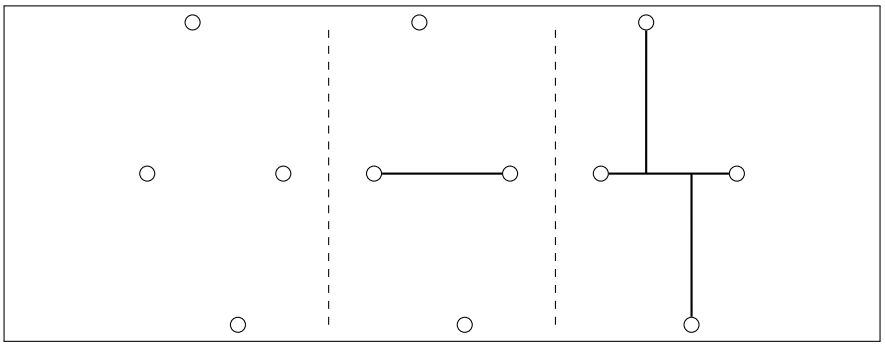
15.



16.



17.



References

1. Saugata Basu, Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Geometry of secure two-party computation. In *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*, pages 1035–1044. IEEE, 2022. doi:10.1109/FOCS54457.2022.00101. 5, 6, 20
2. Saugata Basu, Hamidreza Amini Khorashgani, Hemanta K. Maji, and Hai H. Nguyen. Geometry of secure two-party computation. https://www.cs.purdue.edu/homes/hmaji/papers/BKMN22.pdf (Fetched on 15 February, 2023), 2022. 4
3. Donald Beaver. Perfect privacy for two-party protocols. In *Proceedings of DIMACS Workshop on Distributed Computing and Cryptography*, volume 2, pages 65–77, 1991. 2, 3
4. Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, et al. Secure multiparty computation goes live. In *Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers 13*, pages 325–343. Springer, 2009. 2
5. Constantin Carathéodory. Über den variabilitätsbereich der fourier'schen konstanten von positiven harmonischen funktionen. *Rendiconti Del Circolo Matematico di Palermo (1884-1940)*, 32(1):193–217, 1911. 4, 7
6. Benny Chor and Eyal Kushilevitz. A zero-one law for Boolean privacy (extended abstract). In *21st ACM STOC*, pages 62–72. ACM Press, May 1989. doi:10.1145/73007.73013. 2, 3
7. Deepesh Data and Manoj Prabhakaran. Towards characterizing securely computable two-party randomized functions. In Michel Abdalla and Ricardo Dahab, editors, *PKC 2018, Part I*, volume 10769 of *LNCS*, pages 675–697. Springer, Heidelberg, March 2018. doi:10.1007/978-3-319-76578-5_23. 3, 4, 8, 20, 21
8. Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987. doi:10.1145/28395.28420. 2
9. Eyal Kushilevitz. Privacy and communication complexity. In *30th FOCS*, pages 416–421. IEEE Computer Society Press, October / November 1989. doi:10.1109/SFCS.1989.63512. 2, 3
10. Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In *27th FOCS*, pages 162–167. IEEE Computer Society Press, October 1986. doi:10.1109/SFCS.1986.25. 2