A Candidate Access Structure for Super-polynomial Lower Bound on Information Ratio

Shahram Khazaei

Sharif University of Technology
Department of Mathematical Sciences
shahram.khazaei@sharif.ir

May 30, 2019

Abstract. The contribution vector (convec) of a secret sharing scheme is the vector of all share sizes divided by the secret size. A measure on the convec (e.g., its maximum or average) is considered as a criterion of efficiency of secret sharing schemes, which is referred to as the *information ratio*.
It is generally believed that there exists a family of access structures such that the information ratio of any secret sharing scheme realizing it is $2^{\Omega(n)}$, where the parameter n stands for the number of participants. The best known lower bound, due to Csirmaz (1994), is $\Omega(n/\log n)$. Closing this gap is a long-standing open problem in cryptology.
Using a technique called *substitution*, we recursively construct a family of access structures by starting from that of Csirmaz, which might be a candidate for super-polynomial information ratio. We provide support for this possibility by showing that our family has information ratio $n^{\Omega(\frac{\log n}{\log\log n})}$, assuming the truth of a well-stated information-theoretic conjecture, called the *substitution conjecture*. The substitution method is a technique for composition of access structures, similar to the so called block composition of Boolean functions, and the substitution conjecture is reminiscent of the Karchmer-Raz-Wigderson conjecture on depth complexity of Boolean functions. It emerges after introducing the notion of *convec set* for an access structure, a subset of n-dimensional real space, which includes all achievable convecs. We prove some topological properties about convec sets and raise several open problems.
Key words: secret sharing, general access structures, information ratio, communication complexity

1 Introduction

In a *secret sharing scheme* [52,10,30], a secret is shared among some fixed set of participants by giving each one a string, called the *share* of that participant. It is required that only certain pre-specified subsets of participants, called *qualified* subsets, be able to recover the secret. The collection of all qualified subsets is called an *access structure*, which is supposed to be monotone; because, if a subset is qualified, so is any superset of it. The *unqualified (forbidden)* subsets, on the other hand, must not gain any information on the secret.

The *information ratio* [14,11,44] of a participant in a secret sharing scheme is defined as the ratio between the size of his share and the size of the secret. The maximum/average information ratio of a secret sharing scheme is the maximum/average of all participants information ratios. The maximum/average information ratio of an access structure is defined as the infimum of the maximum/average information ratios of all secret sharing schemes that realize it.

Surprisingly, very basic questions about the information ratio of access structures have remained open. For example, despite several important results (e.g., [13,51,54,45,46]), the class of access structures with information ratio one, called *ideal* and known to contain the threshold

access structures, is far from being fully characterized yet. Also, determining the exact value of information ratio of several simple access structures on a small number of participants (for example, see [57,31] and [24,26] for their latest status) is still open while very few cases have been resolved (see [21,20] for two notable examples).

One can construct a secret sharing scheme realizing any access structure on n participants with information ratio 2^n [30], which can further be improved to $2^{n-o(n)}$ [9]. This upper-bound has been recently reduced in [41] to $2^{(1-\epsilon)n}$ for some small constant $\epsilon > 0$. It is generally believed that this upper bound is tight for most access structures. Particularly, it is conjectured (e.g., see [4]) that there exists a family of access structures with information ratio $2^{\Omega(n)}$. Csirmaz has explicitly constructed a family of access structures with maximum [19] (earlier presented in [17]) and average [18] information ratio $\Omega(n/\log n)$ and no better lower bound is known. In particular, Csirmaz has also shown that his approach, a standard information-theoretic method [36,15] based on *Shannon type information inequalities*, cannot be used to show a superlinear lower bound. This negative result was further strengthened in [8,47] by showing that certain additional *non-Shannon type* information inequalities [62] also fail to bypass the linear barrier.

Bridging the exponential gap between the two above-mentioned bounds is an important open problems in cryptology. For the restricted class of *multi-linear* secret-sharing schemes (which we simply refer to as *linear* in this paper), however, a supper-polynomial lower-bound $n^{\Omega(\log n)}$ is known [5]. For a more restricted class of linear schemes in which the secret is allowed to contain only one field element, an exponential lower-bound $2^{\Omega(n^{1/14}\log n)}$ has been recently found [49], closing the gap with former super-polynomial lower bounds [1,6].

1.1 Our main results and ideas

Beating Csirmaz celebrated lower bound has turned out to be a very difficult problem. We recursively construct a family of access structures by building on Csirmaz access structure that might have supper-linear (or even super-polynomial up to the limit $n^{\Omega(\frac{\log n}{\log\log n})}$) information ratio. We provide some evidence, by introducing a conjecture, called the *substitution conjecture*. Our conjecture emerges after introducing the notion of convec set and notions of composition (substitution) for real vectors and access structures. Our conjecture can be compared with a well-known conjecture by Karchmer-Raz-Wigderson [35] on depth complexity of Boolean functions. A *lifting theorem*, useful for possibly boosting the information ratio of a carefully-chosen family of access structures, lies at the heart of our construction.

The main ideas of the paper are discussed below.

1. **Introducing the notion of convec set**. We attribute a subset of $\mathbb{R}^n$, the n-dimensional real space, to an access structure on n participants, referred to as the *convec set*, where convec is short for contribution vector [31]. The convec of a secret sharing scheme is defined as the vector of all participants information ratios. We define the convec set of an access structure as the set of all convecs of all secret sharing schemes realizing it. Our geometrical treatment of access structures may seem reminiscent of Yeung's [61] framework for studying the so called *entropy region*. The notion of convec set provides an interesting ground for studying the information ratio of access structures. In particular, viewing the problem of finding *extreme convecs* of an access structure as a *multi-objective optimization problem* brings new insight in the study of the information ratio of access structures. This line of research has been explored in [2] which has lead to determining the linear convec set of all well-known access structures on a small number of participants. In this paper, we follow another line by introducing the notion of *substitution factor* for access structures based on their convec sets.

2. **Using Martin's notion of access structure substitution**. Given minimal representations of two access structures (in the Sperner system), with disjoint participant sets of size n and m, we substitute one for some participant of the other one. The resulting access structure will have $n + m - 1$ participants. For example, by substituting the access structure $\Gamma_2 = a' + b'c'$ for participant b in the access structure $\Gamma_1 = ab + bcd$, we get $\Gamma_1 \Diamond_b \Gamma_2 = a(a' + b'c') + (a' + b'c')cd = aa' + ab'c' + a'cd + b'c'cd$. This concept has already been introduced by Martin in [44] and some basic properties of the operation has also been studied. More generally, for a subset I of participants of Γ_1, we let $\Gamma_1 \Diamond_I \Gamma_2$ denote the access access derived by substituting every participants of Γ_1 in the set I with a copy of Γ_2. We are interested in studying how the convec set of the resulting access structure is related to those of the original ones.
3. **Composition of vectors and sets.** For real vectors $\boldsymbol{x}_1 \in \mathbb{R}^n$ and $\boldsymbol{x}_2 \in \mathbb{R}^m$ and a given index $i \in [n]$, we define the composition $\boldsymbol{x}_1 \Diamond_i \boldsymbol{x}_2 \in \mathbb{R}^{n+m-1}$ as the vector achieved by substituting the i'th element of $\boldsymbol{x}_1$, say a_i, with the vector $a_i \boldsymbol{x}_2$. Given two subsets $\mathcal{X}_1 \subset \mathbb{R}^n$ and $\mathcal{X}_2 \subset \mathbb{R}^m$ and an index $i \in [n]$, the subset $\mathcal{X}_1 \Diamond_i \mathcal{X}_2 \subset \mathbb{R}^{n+m-1}$ is defined to contain all vectors $\boldsymbol{x}_1 \Diamond_i \boldsymbol{x}_2$ with $\boldsymbol{x}_1 \in \mathcal{X}_1$ and $\boldsymbol{x}_2 \in \mathcal{X}_2$. For a subset $I \subset [n]$ of indices, $\mathcal{X}_1 \Diamond_I \mathcal{X}_2$ is defined by recursively composing $\mathcal{X}_2$ at each index in I where the starting set is $\mathcal{X}_1$.
4. **Substitution factor and substitution conjecture.** Let $\Gamma_3 = \Gamma_1 \Diamond_{p_i} \Gamma_2$ and denote the closure of the convec set of Γ_j by $\mathcal{X}_j$. We will prove that $\mathcal{X}_1 \Diamond_i \mathcal{X}_2 \subseteq \mathcal{X}_3$ where i corresponds to the index of participant p_i; however, we need a mild conjecture, that we call the "Uniform Share Distribution" (USD) conjecture[1] in order for the proof to go through. The intuition behind the proof is as follows. A simple scheme for Γ_3 can be constructed by first sharing the secret using a scheme for Γ_1 and then sharing the share of p_i in this scheme using a scheme for Γ_2. The substitution conjecture is that, basically, such schemes are "almost" the most efficient schemes realizing Γ_3 and "very small" saving in the share size is possible by other methods. The situation can be compared with other complexity models such as the depth complexity of Boolean circuits [35], however, we need a somewhat more involved statement to formalize a reasonable conjecture. To this end we define the notion of *substitution factor* for an access structure Γ_1, with convec set $\mathcal{X}_1$, as the largest value of s that satisfies

$$\mathcal{X}_3 \subseteq s \cdot \mathcal{X}_1 \Diamond_I \mathcal{X}_2 \ ,$$

over all access access structures Γ_2 with convec set $\mathcal{X}_2$, where $\mathcal{X}_3$ is the convec set of $\Gamma_3 = \Gamma_1 \Diamond_I \Gamma_2$, and I is an arbitrary subset of participants of Γ_1. We conjecture that the substitution factor is not "large"; i.e., $\mathcal{X}_3 \approx \mathcal{X}_1 \Diamond_I \mathcal{X}_2$. More precisely, we provide the following conjecture.

Conjecture (Substitution conjecture) *The substitution factor of every family of access structures is*

$$s(n) = \frac{(\log n)^{g(n)}}{n} \ , \tag{1.1}$$

for some function $2 < g(n) \leqslant \frac{\log n}{\log \log n}$ *where* n *stands for the number of participants.*

Notice that the upper-bound $g(n) \leqslant \frac{\log n}{\log \log n}$ comes from the limit $s(n) \leqslant 1$ on the substitution factor. To justify the plausibility of the lower-bound $2 < g(n)$, we study the substitution

[1] Informally, the USD conjecture states that in the optimal schemes, all share distributions (and also the secret) are uniform. It remains open, if the USD holds true for total security or even the weaker notion of statistical security. However, it can be shown to hold for another relaxation called quasi-total security [33], due to a well-known result by Chan and Yeung [16] on the equality of the entropy region and the cone of group-characterizable polymatroids.

factor with respect to the *polymatroidal set* of an access structure (defined as the lower bound obtained by considering all Shannon inequities) instead of the convec set measure. We will show that the corresponding substitution factor is at most $\frac{(\log n)^2}{n}$ for Csirmaz family, which we conjecture to be tight.

5. **A lifting theorem.** Raz and McKenzie [50] have shown how to "lift" lower bounds for query complexity of Boolean functions to their communication complexity [50]. Similar techniques have been applied in other complexity areas, e.g., see [53,39,28,29,38]. We present a lifting theorem, useful for boosting the information ratio of a family of access structures. The idea is to define a recursive procedure for constructing a family of access structures by starting from a given one. Below, we present a simplified and informal statement of the theorem.

   Theorem (Lifting theorem—informal and simplified) *Let $b, t, s : \mathbb{R}^+ \to \mathbb{R}^+$ be three functions and $\{\Gamma_k\}_{k\in\mathbb{N}}$ be a family of access structures. Suppose that for every k, it holds that Γ_k, with n_k participants and substitution factor $s(n_k)$, has a subset of participants of size $b(n_k)$ with minimum total share size $t(n_k)$. Assuming that the function $f(x) = \frac{\log(s(x)t(x))}{\log b(x)}$ satisfies some "mild" conditions, then there exists a family of access structures with average (and consequently maximum) information ratio $n^{f(n)-1}$.*

   Our family is constructed as follows. We start from the given family and "replace" the $b(n)$ specific parties with a copy of the original access structure and apply the procedure $\frac{\log n}{\log b(n)}$ times.

6. **Our candidate family.** Csirmaz [19] proves his $\Omega(n/\log n)$ lower bound on information ratio, by constructing a family of access structures and exhibiting a subset of participants of size $b(n) = \Theta(\log n)$ with minimum total share size $t(n) = \Omega(n)$. By lifting theorem, the information ratio of our constructed family is then $n^{g(n)-1}$ (see (1.1)), where $g(n)$ remains unknown. By the substitution conjecture, the expected lower bound could range from super-linear up to super-polynomial, depending on the assumption made on $g(n)$.

1.2 Related work

We would like to bring the following pieces of work to the reader's attention for comparison and completes.

Composition versus decomposition. The way that we use the substitution method provides a simple means of *composition* of access structures which (might) lead to proving lower-bounds on the information ratio of access structures. We are not aware of any similar method in the secret sharing context. On the other hand, several *decomposition* methods have been introduced for achieving upper-bounds on information ratio of secret sharing schemes. These techniques have mainly been used to find upper-bounds on the information ratio of several concrete access structures on a small number of participants [11,55,57,31,59,43,40,26,27]. These methods build on Stinson's λ-decomposition [55] method (see [58,56,26] for extensions) in which an access structure is decomposed into several (usually simpler) sub-access structures.

Given a sub-scheme for each sub-access structure, the sub-schemes are then combined to construct a scheme for the original access structure, providing an upper-bound on its information ratio. Therefore, these methods essentially concern decomposition of access structures and composition of secret sharing schemes while ours is a method of composition of access structures.

The Karchmer-Raz-Wigderson conjecture on depths of circuits. The substitution method is similar to the so called block composition of Boolean functions. The composition of two

Boolean functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^m \to \{0,1\}$ is the function $f\Diamond g$ that takes as inputs m strings $x_1, \cdots, x_m \in \{0,1\}^n$ and computes $(f\Diamond g)(x_1, \ldots, x_m) = f(g(x_1), \cdots, g(x_m))$.

The depth complexity of a Boolean function f, denoted by $\mathrm{d}(f)$, is the depth of the shallowest fan-in-2 circuit that computes it. Karchmer, Raz, and Wigderson [35] has conjectured that $\mathrm{d}(f\Diamond g) \approx \mathrm{d}(f) + \mathrm{d}(g)$. They then showed that the truth of their conjecture implies super-logarithmic lower bounds on the depth complexity of an explicit function, resolving an outstanding open problem of complexity theory. Their explicit function is constructed by a repeated application of the composition operation.

Lifting theorems. Raz and McKenzie [50] have used the composition operation to lift lower bounds from query complexity to communication complexity of Boolean functions. In particular, they used their lifting theorem to prove that the monotone NC-hierarchy does not collapse. Similar lifting theorems were later proved for deriving several important complexity separations. We refer the reader to [53,39,28,29,38] for some examples.

1.3 Paper organization

In Section 2, we provide the required background and notations. The notion of convec set and its topological properties, along with a list of open problems, are studied in Section 3. The substitution method and our lifting theorem are presented in Sections 4 and 5. Our candidate construction is presented in Section 6 and the limit of our method is discussed in Section 7. Section 8 studies the behavior of the substitution factor with respect to the polymatroidal set. The USD conjecture and its consequences are discussed in Section 9. Finally, we conclude the paper in Section 11.

2 Preliminaries and notation

In this section, we provide the basic background along with some notations and conventions. The information-theoretic and topological notions can be found in any standard textbook. We refer the reader to [4,48] for surveys on secret sharing. Readers familiar with the subjects can safely skip this section, but we encourage the reader to take a look at Remark 2.1 and Lemma 2.2.

2.1 Basic topology

Let $\boldsymbol{a} = (a_1, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, \ldots, b_n)$ be two vectors in $\mathbb{R}^n$, the n-dimensional real space. We write $\boldsymbol{a} \preceq \boldsymbol{b}$ (resp. $\boldsymbol{a} \prec \boldsymbol{b}$) if and only if $a_i \leqslant b_i$ (resp. $a_i < b_i$) for every $i \in [n]$, where $[n]$ stands for the set $\{1, \ldots, n\}$. We use $[\boldsymbol{a}, \infty)$ to denote the set of all points $\boldsymbol{b}$ such that $\boldsymbol{a} \preceq \boldsymbol{b}$. For a vector $\boldsymbol{a} = (a_1, \ldots, a_n)$, we let $\max(\boldsymbol{a}) = \max\{a_1, \ldots, a_n\}$ and $\|\boldsymbol{a}\| = \sum_{i=1}^{n} |a_i|$. The all-one vector is denoted by $\mathbf{1}$, whose dimension is understood from the context.

A subset of $\mathbb{R}^n$ is said to be *convex* if for every pair of points $\boldsymbol{a}, \boldsymbol{b}$ in the set and for every real $\lambda \in [0,1]$, the point $\lambda\boldsymbol{a} + (1-\lambda)\boldsymbol{b}$, called a convex combination of $\boldsymbol{a}$ and $\boldsymbol{b}$, is also in the set. In this paper, the intersection of finitely many half-spaces is called a *convex polytope*, or simply a *polytope*. Let $\mathcal{X}$ be a convex subset of $\mathbb{R}^n$. A point of $\mathcal{X}$ is said to be an *extreme point* if it does not lie in any line segment with endpoints in $\mathcal{X}$.

A point $\boldsymbol{a} \in \mathbb{R}^n$ is called a *limit point* for a set $\mathcal{X} \subseteq \mathbb{R}^n$ if every open ball containing $\boldsymbol{a}$ includes at least one point of $\mathcal{X}$, different from $\boldsymbol{a}$ itself. A set is called *closed* if it contains all of its limit-points and it is called *open* if its complement is closed. The *closure* of a set $\mathcal{X} \subseteq \mathbb{R}^n$, denoted by $\overline{\mathcal{X}}$, is the union of $\mathcal{X}$ with all its limit points. When $\overline{\mathcal{X}}$ is convex, we refer to $\mathcal{X}$ as a set with a *convex closure*. A point $\boldsymbol{a}$ is called an *interior* point of $\mathcal{X}$ if there exists an open ball

containing $\boldsymbol{a}$ which is completely contained in $\mathcal{X}$. The set of all interior points of $\mathcal{X}$ is denoted by $\mathrm{int}(\mathcal{X})$. The *boundary* of a set $\mathcal{X}$ is defined as the set of all points in its closure which does not belong to its interior, i.e., $\overline{\mathcal{X}}\backslash\mathrm{int}(\mathcal{X})$. In this paper, we define the *frontier* of $\mathcal{X}$ as the set $\overline{\mathcal{X}}\backslash\mathcal{X}$.

Remark 2.1 (Frontier vs. boundary) *In the literature the boundary is also referred to as the frontier and some authors (for example [60]) even use the term frontier instead of boundary. However, similar to [3], our definition of frontier is different from boundary.*

2.2 Basic information theory

Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be discrete random variables. The support of $\boldsymbol{X}$ (i.e., the set of all values that it accepts with positive probability) is denoted by $\mathrm{supp}(\boldsymbol{X})$. The Shannon entropy of $\boldsymbol{X}$ is defined as $\mathrm{H}(\boldsymbol{X}) = -\sum_{x\in\mathrm{supp}(\boldsymbol{X})} \Pr[\boldsymbol{X}=x]\log_2\Pr[\boldsymbol{X}=x]$. The entropy of $\boldsymbol{X}$ conditioned on $\boldsymbol{Y}$ is defined as $\mathrm{H}(\boldsymbol{X}|\boldsymbol{Y}) = \sum_{y\in\mathrm{supp}(\boldsymbol{Y})}\Pr[\boldsymbol{Y}=y]\mathrm{H}(\boldsymbol{X}|\boldsymbol{Y}=y)$, where $\mathrm{H}(\boldsymbol{X}|\boldsymbol{Y}=y) = -\sum_{x\in\mathrm{supp}(\boldsymbol{X}):\Pr[\boldsymbol{X}=x\wedge\boldsymbol{Y}=y]>0}\Pr[\boldsymbol{X}=x|\boldsymbol{Y}=y]\log_2\Pr[\boldsymbol{X}=x|\boldsymbol{Y}=y]$. Finally, the mutual information of $\boldsymbol{X}$ and $\boldsymbol{Y}$ is defined as $\mathrm{I}(\boldsymbol{X},\boldsymbol{Y}) = \mathrm{H}(\boldsymbol{X}) - \mathrm{H}(\boldsymbol{X}|\boldsymbol{Y})$.

2.3 Secret sharing schemes

Access structure. Let $P = \{p_1,\ldots,p_n\}$ be a finite set of *participants*. A subset $\Gamma\subseteq 2^P$ is called an *access structure* on P if it is *monotone*; that is, for every $A\in\Gamma$ and every set B, where $A\subseteq B\subseteq P$, it holds that $B\in\Gamma$. A subset $A\subseteq P$ is called *qualified* if $A\in\Gamma$; otherwise, it is called *unqualified* or *forbidden*. A qualified subset is called *minimal* if none of its proper subsets is qualified. A forbidden subset is called *maximal* if none of its proper supersets is forbidden. The set of all minimal qualified subsets and that of maximal forbidden sets are, respectively, denoted by Γ^- and Γ^+. A participant $p\in P$ is called *important* for Γ, if it appears in at least one minimal qualified subset. A distinguished participant $p_0\notin P$ is referred to as the *dealer*. In the Sperner system, an access structure can be symbolically represented as $\Gamma = \sum_{A\in\Gamma^-}\prod_{p\in A} p$. When the participant set of an access structure Γ is not given a priori, we use the notation $P(\Gamma)$ to denote its participant set.

Secret sharing scheme. A tuple $\Pi = \left(\boldsymbol{S}_p\right)_{p\in P\cup\{p_0\}}$ of jointly distributed random variables, with finite supports, is called a *secret sharing scheme* on participant set P when $\mathrm{H}(\boldsymbol{S}_{p_0}) > 0$. The random variable $\boldsymbol{S}_{p_0}$ is called the *secret* random variable and its support is called the *secret space*. The random variable $\boldsymbol{S}_p$, for any participant $p\in P$, is called the *share* random variable of the participant p and its support is called his *share space*.

A secret sharing scheme Π is said to be *linear* if there exists a finite field $\mathbb{F}$ such the support of every marginal random variable is an $\mathbb{F}$-vector space of finite dimension with uniform distribution.

When we say that a secret $s\in\mathrm{supp}(\boldsymbol{S}_{p_0})$ *is shared using* Π, we mean that a tuple $\left(s_p\right)_{p\in P\cup\{p_0\}}$ is sampled according to the distribution Π conditioned on the event $\boldsymbol{S}_{p_0}=s$.

Realization. We say that Π is a secret sharing scheme for Γ, or Π *realizes* Γ, when: 1) $\mathrm{H}(\boldsymbol{S}_{p_0}\mid\boldsymbol{S}_A)=0$, for every qualified set $A\in\Gamma$ and 2) $\mathrm{H}(\boldsymbol{S}_{p_0}\mid\boldsymbol{S}_B)=\mathrm{H}(\boldsymbol{S}_{p_0})$, for every forbidden set $B\in\Gamma^c$, where $\boldsymbol{S}_A=(\boldsymbol{S}_p)_{p\in A}$, for a subset $A\subseteq P$. These requirements are referred to as the *correctness* and *privacy* conditions, respectively.

Information ratio. The *information ratio* of participant $p \in P$ is defined as $\sigma_p = \mathrm{H}(\boldsymbol{S}_p)/\mathrm{H}(\boldsymbol{S}_{p_0})$. The *convec* of Π (where convec is abbreviation for *contribution vector* [31]) is defined and denoted by $\mathrm{cv}(\Pi) = (\sigma_p)_{p\in P}$. A secret sharing scheme Π is called ideal if $\mathrm{cv}(\Pi) = \mathbf{1}$.

The maximum (resp. average) *information ratio* of an access structure Γ is denoted by $\sigma(\Gamma)$ (resp. $\tilde{\sigma}(\Gamma)$) and is defined as the infimum of $\max\big(\mathrm{cv}(\Pi)\big)$ (resp. $\frac{1}{|P|}\|\mathrm{cv}(\Pi)\|$) over all secret sharing schemes Π realizing Γ. Lower bounds on the maximum and average information ratio of Γ, derived by taking into account the so-called *Shannon inequalities*, are denoted by $\kappa(\Gamma)$ and $\tilde{\kappa}(\Gamma)$, respectively [42].

We close this section by introducing a lemma by Blundo *et. al.* [12].

Lemma 2.2 ([12]) *Let $\Pi = (\boldsymbol{S}_p)_{p\in P\cup\{p_0\}}$ be a secret sharing scheme for Γ. Let $\Pi' = (\boldsymbol{S}'_p)_{p\in P\cup\{p_0\}}$ be a secret sharing scheme obtained from Π by changing the secret distribution to a (non-certain) distribution $\boldsymbol{S}'_{p_0}$ over $\mathrm{supp}(\boldsymbol{S}_{p_0})$ (more precisely, to generate a sample according to Π', a secret is sampled from $\boldsymbol{S}'_{p_0}$ and then shared using Π). Then, Π' also realizes Γ. Moreover, the random variables $\boldsymbol{S}_A$ and $\boldsymbol{S}'_A$ are identically distributed, for any unqualified subset $A \in \Gamma^c$.*

3 Convec set

In this section, we introduce the notion of *convec set* for access structures and study its topological properties. Two illustrative examples are provided and some open problems are suggested.

Definition 3.1 (Convec set) *Let Γ be an access structure. The convec set of Γ, denoted by $\Sigma(\Gamma)$ and also called the Σ-set of Γ, is defined as the set of all convecs of all secret sharing schemes that realize Γ.*

Definition 3.2 (Polymatroidal set—informal) *We introduce the K-set as a generalization of the κ-parameter introduced in [42]. More precisely, the polymatroidal set of an access structure Γ, denoted by $K(\Gamma)$, is defined as the polytope derived by taking into account all the Shannon inequalities as well as the correctness and privacy conditions. A more formal definition is given in Appendix A.*

The relation between polymatroids and random variables was first realized by Fujishige in [25]. The left inclusion in the following proposition is an extension of the inequality $\kappa(\Gamma) \leqslant \sigma(\Gamma)$ [42]. The right one follows by a well-known result of [36,15], stating that each important participant's share size is not smaller than the secret itself.

Proposition 3.3 (Trivial inclusions) *For any access structure Γ, it holds that:*

$$\Sigma(\Gamma) \subseteq K(\Gamma) \subseteq [\mathbf{1}, \infty) \ ,$$

where for the rightmost inclusion we need to additionally assume that all participants of Γ are important.

3.1 Basic properties of convec sets

In this section we provide two lemmas about the properties of convec sets, which will be used in this section. For our convenience, we provide the following definition.

Definition 3.4 (Shifted orthant inclusion property) *We say that a set $\mathcal{X} \subseteq \mathbb{R}^n$ has the shifted orthant inclusion property if $\boldsymbol{a} \in \mathcal{X}$ implies $[\boldsymbol{a}, \infty) \subseteq \mathcal{X}$.*

The following lemmas shows that the convec set of access structures have the shifted orthant inclusion property.

Lemma 3.5 (Shifted orthant inclusion property) *The convec set of any access structure has the shifted orthant inclusion property.*

Proof. Let Γ be an access structure and $\boldsymbol{a} \in \Sigma(\Gamma)$. For any point $\boldsymbol{a}' \in [\boldsymbol{a}, \infty)$ we show that $\boldsymbol{a}' \in \Sigma(\Gamma)$. The reason is that given a secret sharing scheme $\Pi = (\boldsymbol{S}_p)_{p \in P \cup \{p_0\}}$ for Γ with $\mathrm{cv}(\Pi) = \boldsymbol{a}$, it is easy to construct a secret sharing scheme Π' for Γ with $\mathrm{cv}(\Pi') = \boldsymbol{a}'$; simply give dummy shares to the participant to increase their share size. More precisely, let $\Pi' = \big(\boldsymbol{S}_{p_0}, (\boldsymbol{S}_p, \boldsymbol{S}'_p)_{p \in P}\big)$ where $(\boldsymbol{S}'_p)_{p \in P}$ is independent form Π and it is chosen such that $\big(\mathrm{H}(\boldsymbol{S}'_p)\big)_{p \in P} = \mathrm{H}(\boldsymbol{S}_{p_0})(\boldsymbol{a}' - \boldsymbol{a}) \succeq \boldsymbol{0}$. Clearly, Π' realizes Γ and $\mathrm{cv}(\Pi') = \boldsymbol{a}'$; hence, $\boldsymbol{a}' \in \Sigma(\Gamma)$. □

Lemma 3.6 (Uniform secret invariance property) *Let Γ be an access structure. The convec set of Γ is the set of all convecs of all secret sharing schemes having uniform secret distribution and realizing Γ.*

Proof. Let $\boldsymbol{a} \in \Sigma(\Gamma)$ and suppose that $\Pi = (\boldsymbol{S}_p)_{p \in P \cup \{p_0\}}$ is a secret sharing scheme for Γ with convec $\boldsymbol{a}$. We show that there exists a secret sharing scheme Π', with uniform secret distribution, for Γ with the same convec.

We prove the claim under the assumption that Γ does not contain singleton sets; that is, no participant is qualified on its own. It is easy to remove this assumption and we leave it to the reader. By Lemma 2.2, there exists a secret sharing scheme $\Pi'' = (\boldsymbol{S}''_p)_{p \in P \cup \{p_0\}}$ for Γ such that $\boldsymbol{S}''_{p_0}$ is uniform over $\mathrm{supp}(\boldsymbol{S}_{p_0})$, and $\boldsymbol{S}''_p$ is distributed identically as $\boldsymbol{S}_p$ for every $p \in P$, since $\{p\}$ is unqualified.

Consequently, $\boldsymbol{a}'' = \mathrm{cv}(\Pi'') = \frac{\mathrm{H}(\boldsymbol{S}_{p_0})}{\mathrm{H}(\boldsymbol{S}''_{p_0})}\boldsymbol{a} \preceq \boldsymbol{a}$; that is, $\boldsymbol{a} \in [\boldsymbol{a}'', \infty)$. We can then construct Π', realizing Γ with $\mathrm{cv}(\Pi') = \boldsymbol{a}$, from Π'' similar to the proof of the shifted orthant inclusion property (Lemma 3.5), by increasing each participant's share size, without changing the secret distribution. □

3.2 On closure convexity of convec sets

It is easy to show that the closure of a convec set is convex. Indeed, for an access structure Γ on n participants, the closure convexity of its Σ-set is induced by convexity of the cone of the entropy region on $n+1$ random variables. The convec set of Γ can be equivalently computed by the following steps. The intersection of the entropy region on $n+1$ random variables and the planes that describe the correctness and privacy conditions is computed. Each point of the resulting area is then scaled by dividing all coordinates to the entry that corresponds to the secret entropy. The convec set is essentially the projection on the n-entries that correspond to the participants share entropies. The claim then follows since the properties are kept intact at each step.

Proposition 3.7 (Closure convexity) *The convec set of every access structure is a set with convex closure.*

The following proposition follows by the shifted orthant inclusion property (Lemma 3.5) of convec sets.

Proposition 3.8 (Interior closure) *The interior of the Σ-set of every access structure is closed.*

3.3 On frontiers of convec sets

In this section, we prove that there is no access structure with an open convec set; that is, the frontier of a convec set is a proper subset of its boundary. We conclude that the convec set of an access structure is either closed or neither-open-nor-closed (NONC). Subsequently, we define the notion of *closed/NONC access structures*. The frontier of a closed access structure is empty whereas that of a NONC access structure is non-empty and a proper subset of its boundary. First, we provide a lemma, then a proposition and finally the definition.

Lemma 3.9 (Participant-specific rate-one scheme) *Let Γ be an access structure, $m \geqslant 2$ be an integer and $p \in P(\Gamma)$. Then, there exist a secret sharing scheme, with secret space size m, realizing Γ, such that the information ratio of participant p is one.*

Proof. In the Sperner system, let $\Gamma^- = \Gamma_0^- + p\Gamma_1^-$, where Γ_0, Γ_1 are access structures both on the participant set $P' = P \backslash \{p\}$. More precisely, $\Gamma_0 = \{A \subseteq P' \mid A \in \Gamma\}$ and $\Gamma_1 = \{A \subseteq P' \mid A \notin \Gamma, A \cup \{p\} \in \Gamma\}$. It is well-known that every access structure admits a secret sharing scheme with secret space $\mathbb{Z}_m$ [30]. Let Π_0, Π_1 be, respectively, such secret sharing schemes for Γ_0, Γ_1. We construct a secret sharing scheme for Γ such that the secret is uniform over $\mathbb{Z}_m$ and the information ratio of participant p is one. To share a secret $s \in \mathbb{Z}_m$, we choose a uniformly random $r \in \mathbb{Z}_m$ and give the share r to p. Then, we share $s + r$ as a secret using the scheme Π_1 and share the secret s using the scheme Π_0. Consequently, every participant in P' receives a share from each of the schemes. But p receives a random element of $\mathbb{Z}_m$ as his share. Clearly, the resulting scheme realizes Γ and the information ratio of participant p is one. □

Proposition 3.10 (Convec sets are not open) *There does not exist an access structure with an open convec set.*

Proof. Let Γ be an access structure on n participants. By Proposition 3.3, we have $\Sigma(\Gamma) \subseteq [\mathbf{1}, \infty)$. Also, by Lemma 3.9, for every $i \in [n]$, there exists a convec $(\sigma_1, \ldots, \sigma_n) \in \Sigma(\Gamma)$, such that $\sigma_i = 1$. Clearly, all these convecs lie on the boundary of $\Sigma(\Gamma)$. Therefore, $\Sigma(\Gamma)$ is not open. □

Definition 3.11 (Closed and NONC access structures) *An access structure is called closed (resp. NONC) if its convec set is closed (resp. neither-open-nor-closed).*

Corollary 3.12 (Frontiers of closed and NONC access structures) *The frontier of the convec set of a closed access structure is empty and that of a NONC access structure is a non-empty proper subset of its boundary.*

3.4 Pareto-optimality

In this section, we first define two notions of optimality for convecs and a notion of optimality for secret sharing schemes. Then, we provide an equivalent definition of maximum and average information ratio of an access structure, already given in Section 2.3.

First, we recall the definition of Pareto-optimality for a subset of multi-dimensional real space, as a partially ordered set.

Pareto-optimal points. Let $\mathcal{X} \subseteq \mathbb{R}^n$. A point $\boldsymbol{a} \in \mathcal{X}$ is said to be *Pareto-minimal* for $\mathcal{X}$ if for any vector $\boldsymbol{b} \in \mathcal{X}$, which is comparable with $\boldsymbol{a}$, it holds that $\boldsymbol{a} \preceq \boldsymbol{b}$. A point $\boldsymbol{a} \in \overline{\mathcal{X}}$ is said to be *Pareto-infimal* for $\mathcal{X}$ if it is Pareto-minimal for $\overline{\mathcal{X}}$. The set of all Pareto-infimal and Pareto-minimal points of $\mathcal{X}$ are, respectively, denoted by $\inf_{\mathrm{P}}(\mathcal{X})$ and $\min_{\mathrm{P}}(\mathcal{X})$. Notice that $\inf_{\mathrm{P}}(\mathcal{X}) = \min_{\mathrm{P}}(\overline{\mathcal{X}})$.

Definition 3.13 (Pareto-minimal/infimal convecs) *Let Γ be an access structure. Any vector in the set of Pareto-minimal points of $\Sigma(\Gamma)$, i.e., $\min_{\mathrm{P}}\big(\Sigma(\Gamma)\big)$, is called a Pareto-minimal vector (convec). Any vector in the set of Pareto-infimal points of $\Sigma(\Gamma)$, i.e., $\inf_{\mathrm{P}}\big(\Sigma(\Gamma)\big)$, is called a Pareto-infimal vector.*

According to the shifted orthant inclusion property (Lemma 3.5) of convec sets, the closure of a convec set is uniquely determined by its Pareto-infimal convecs. More precisely, we have the following corollary.

Corollary 3.14 *We have $\overline{\Sigma(\Gamma)} = \bigcup_{\boldsymbol{x}\in\inf_{\mathrm{P}}\left(\Sigma(\Gamma)\right)}[\boldsymbol{x},\infty)$, for every access structure Γ.*

Note that for a given access structure, there does not necessarily exist a secret sharing scheme for a given Pareto-infimal vector; see Example 3.18. However, by definition, a Pareto-minimal vector corresponds to some secret sharing scheme realizing the access structure. Thus, we provide the following notion of optimality for secret sharing schemes.

Definition 3.15 (Pareto-minimal secret sharing scheme) *Let Π be a secret sharing scheme realizing an access structure Γ. We call Π a Pareto-minimal scheme for Γ if its convec is Pareto-minimal, i.e., $\mathrm{cv}(\Pi) \in \min_{\mathrm{P}}\big(\Sigma(\Gamma)\big)$.*

Corollary 3.16 (Equivalent definition of information ratio) *Let Γ be an access structure on n participants. Then,*

$$\sigma(\Gamma) = \min\{\max(\boldsymbol{x}) : \boldsymbol{x} \in \inf_{\mathrm{P}}\big(\Sigma(\Gamma)\big)\} \ ,$$

and

$$\tilde{\sigma}(\Gamma) = \frac{1}{n}\min\{\|\boldsymbol{x}\| : \boldsymbol{x} \in \inf_{\mathrm{P}}\big(\Sigma(\Gamma)\big)\} \ .$$

3.5 Two examples

In this section, we introduce two examples that will be referred to in later sections. Two related open problems are mentioned in Section 3.6.

Example 3.17 ($\mathcal{P}_3$ access structure) *Consider the graph access structure $\mathcal{P}_3 = ab+bc+cd$, i.e., a path of length 3. It can be shown [15] that $\overline{\Sigma(\mathcal{P}_3)}$ has two extreme points, $(1,1,2,1)$ and $(1,2,1,1)$, which we call* extreme convecs. *Therefore, any Pareto-infimal convec $\boldsymbol{x} \in \inf_{\mathrm{P}}\big(\Sigma(\mathcal{P}_3)\big)$ is a convex combination of the two extreme convecs, that is, of the form $\boldsymbol{x} = (1, 1+x, 2-x, 1)$ for some real number $x \in [0,1]$. It can be shown (e.g., using Stinson's λ-decomposition method [55]) that when x is rational, these convecs are Pareto-minimal as well. Thus, $\tilde{\sigma}(\mathcal{P}_3) = \frac{5}{4}$, which is achieved by any Pareto-infimal convec, and $\sigma(\mathcal{P}_3) = \frac{3}{2}$, which is achieved only by the Pareto-minimal convec $(1, \frac{3}{2}, \frac{3}{2}, 1)$. We do not know if this access structure is closed (see Question 3.24).*

Example 3.18 ($\mathcal{F}\cdot\mathcal{N}$ access structure) *Beimel-Livne [7] and Matús [46] have independently introduced an access structure on 12 participants, which we denote by $\mathcal{F}\cdot\mathcal{N}$ (see also Example 4.2 and Figure 1). In the Sperner system, the minimal representation of $\mathcal{F}\cdot\mathcal{N}$ is the product of the Sperner representations of the following two ideal access structures*

$$\mathcal{F} = p_1p_4 + p_2p_5 + p_3p_6 + p_1p_2p_6 + p_1p_3p_5 + p_2p_3p_4 + p_4p_5p_6$$

and

$$\mathcal{N} = q_1q_4 + q_2q_5 + q_3q_6 + q_1q_2q_6 + q_1q_3q_5 + q_2q_3q_4 + q_4q_5q_6 + q_3q_4q_5 \ ,$$

derived form Fano and non-Fano matroids, respectively.

Matús [46] has proved that $\mathcal{F}$ (resp. $\mathcal{N}$) does not have an ideal scheme when the secret space size is odd (resp. even). The access structure $\mathcal{F} \cdot \mathcal{N}$ is called nearly ideal *since while it is not ideal [46], its information ratio is one [7]; that is, the all-one vector is Pareto-infimal but not Pareto-minimal. Therefore, $\mathcal{F} \cdot \mathcal{N}$ is a NONC access structure and $\overline{\Sigma(\mathcal{F} \cdot \mathcal{N})} = [\mathbf{1}, \infty)$. The results of [7] can be used to show that $\Sigma(\mathcal{F} \cdot \mathcal{N})$ includes the points of the set $\{(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^6, (\mathbf{1} \preceq \boldsymbol{x} \wedge \mathbf{1} \prec \boldsymbol{y}) \vee (\mathbf{1} \prec \boldsymbol{x} \wedge \mathbf{1} \preceq \boldsymbol{y})\}$. Lemma 3.9 can be used to show that $\Sigma(\mathcal{F} \cdot \mathcal{N})$ includes additional points as well; for example, for any $i \in \{1, \ldots, 6\}$, some vector of the form $(x_1, \ldots, x_6, \mathbf{1})$ (resp. $(\mathbf{1}, y_1, \ldots, y_6)$), in $\mathbb{R}^{12}$, is in the set where $x_i = 1$ (resp. $y_i = 1$). The exact form of $\Sigma(\mathcal{F} \cdot \mathcal{N})$ is unknown to us, and in particular, we do not know if $\mathcal{F} \cdot \mathcal{N}$ has any Pareto-minimal convec (see Question 3.25). In a follow-up work [32], we have almost determined the convec set closure of $\mathcal{F} \cdot \mathcal{N}$, when restricted to the linear schemes, and have shown that it is non-convex (the exact value of its linear information ratios has been determined, however).*

3.6 Some open problems

Several problems regarding convec sets remain open, which may be interesting in an information-theoretic point of view. The ideal access structures are closed since their convec set is $[\mathbf{1}, \infty)$. We are not aware of any other closed access structure.

Question 3.19 (Non-ideal closed access structure) *Is there a non-ideal closed access structure?*

More generally, characterizing access structures with respect to Definition 3.11 seems an interesting question.

Question 3.20 (Characterizing closed access structures) *Determine which access structures are closed and which ones are NONC (i.e., characterizing them in terms of emptiness of the frontiers of their convec sets; see Corollary 3.12).*

Also, note that the convec set of closed access structures are convex by themselves (i.e., without taking closure). We do not know if there exists any NONC access structures with a convex convec set.

Question 3.21 (Characterizing NONC access structures w.r.t. convexity) *Determine which NONC access structures are convex and which ones are non-convex. In particular, is there a NONC access structure whose convec set is convex (resp. non-convex)?*

Trivially, every access structure has at least one Pareto-infimal convec. However, it is unclear if this is also the case for some Pareto-minimal convec.

Question 3.22 (Existence of a Pareto-minimal scheme) *Does every access structure admit at least one Pareto-minimal secret sharing scheme?*

The (closure of) convec set of some access structures (e.g., Examples 3.17 and 3.18) can be proved to be polytopes. It is intriguing to think that this is the case for every access structure.

Question 3.23 (Non-polytope convec sets) *Is there an access structure such that its convec set is not a polytope?*

Finally, concerning Examples 3.17 and 3.18, we present two more specific questions in the following.

Question 3.24 (Convec set of $\mathcal{P}_3$) *Following Example 3.17, is the set $\Sigma(\mathcal{P}_3)$ convex (equivalently, is $(1, 1+x, 2-x, 1)$ a Pareto-minimal convec for $\mathcal{P}_3$ for every irrational $x \in (0,1)$)?*

Question 3.25 (Convec set of $\mathcal{F} \cdot \mathcal{N}$) *Following Example 3.18, determine the set $\Sigma(\mathcal{F} \cdot \mathcal{N})$. Is it a convex set? Does it have any Pareto-minimal convec?*

Note that a positive answer to Question 3.24 leads to a positive answer to Question 3.19, while a negative answer partially answers Question 3.21 (i.e., there exists non-convex NONC access structures).

4 The substitution technique

In this section, we describe different notions of *compositions* for real vectors, subsets of the real space and access structures. We then propose a conjecture, referred to as the *substitution conjecture*, that approximates the convec set of composition of two access structures with the composition of the original convec sets.

Our composition method resembles the "block" composition of Boolean functions and our substitution conjecture is reminiscent of the Karchmer-Raz-Wigderson [35] conjecture on depth complexity of Boolean functions.

4.1 Vector/Subset composition

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_m)$ be two real vectors. The vector $\boldsymbol{x}$, in which the p'th element has been substituted with $x_p \boldsymbol{y}$, is denoted by $\boldsymbol{x} \diamondsuit_p \boldsymbol{y}$; that is,

$$\boldsymbol{x} \diamondsuit_p \boldsymbol{y} = (x_1, \ldots, x_{p-1}, x_p y_1, \ldots, x_p y_m, x_{p+1}, \ldots, x_n) \ .$$

More generally, let P, Q be two finite sets and $\boldsymbol{x} = (x_p)_{p \in P} \in \mathbb{R}^P$ and $\boldsymbol{y} = (y_q)_{q \in Q} \in \mathbb{R}^Q$ be two vectors; i.e., their indices are indexed by P and Q respectively. Assume that $P \times Q$ and P are disjoint. The reason for this will be clear in the sequel. For an element $p \in P$, the composition $\boldsymbol{x} \diamondsuit_p \boldsymbol{y} = (z_i)_{i \in P_p}$ is a vector in $\mathbb{R}^{P_p}$, where

$$P_p = \big(P \backslash \{p\}\big) \cup \big(\{p\} \times Q\big)$$

and

$$z_i = \begin{cases} x_i & \text{if } i \in P \backslash \{p\} \\ x_p y_q & \text{if } i = (p,q) \in \{p\} \times Q \end{cases} \ .$$

Let $\mathcal{X} \subseteq \mathbb{R}^P$ and $\mathcal{Y} \subseteq \mathbb{R}^Q$ be two arbitrary sets. For every $p \in P$, we define the composition $\mathcal{X} \diamondsuit_p \mathcal{Y}$ as follows:

$$\mathcal{X} \diamondsuit_p \mathcal{Y} = \{\boldsymbol{x} \diamondsuit_p \boldsymbol{y} \mid (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{X} \times \mathcal{Y}\} \ .$$

For a subset $I = \{p_1, \ldots, p_b\} \subseteq P$, the composition operation $\mathcal{X} \diamondsuit_I \mathcal{Y}$ is recursively defined as follows:

$$\mathcal{X} \diamondsuit_I \mathcal{Y} = (\ldots((\mathcal{X} \diamondsuit_{p_1} \mathcal{Y}) \diamondsuit_{p_2} \mathcal{Y}) \ldots) \diamondsuit_{p_b} \mathcal{Y} \ . \tag{4.1}$$

4.2 Access structure composition (substitution)

Let Γ_1 and Γ_2 be two access structures, respectively on (not necessarily disjoint) participant sets P and Q, and let $p \in P$. We refer to $\Gamma_3 = \Gamma_1 \Diamond_p \Gamma_2$ as the access structure in which the participant p has been substituted with Γ_2, in the following sense. In the Sperner representation of Γ_1, we replace p with Γ_2 and then expand and simplify the expression naturally. This concept has already been introduced by Martin in [44] and some basic properties of the composed access structure has been also studied. More precisely, the participant set of Γ_3 is $P(\Gamma_3) = P_{-p} \cup Q$, where $P_{-p} = P \backslash \{p\}$, and for every $A \subseteq P(\Gamma_3)$ we have:

$$A \in \Gamma_3 \Leftrightarrow (A \cap P \in \Gamma_1) \vee \Big(\big((A \cap P) \cup \{p\} \in \Gamma_1\big) \wedge \big(A \cap Q \in \Gamma_2\big) \Big) \ .$$

Our particular case of interest is when P and Q are disjoint. For subsets A, B, let AB and Ap be respectively short notations for $A \cup B$ and $A \cup \{p\}$. In this case, in order to characterize the qualified sets and forbidden sets of $\Gamma_3 = \Gamma_1 \Diamond_p \Gamma_2$, we define:

$$\begin{array}{l} \mathcal{B} = \{B \mid B \subseteq P_{-p} \wedge B \in \Gamma_1\} \ , \\ \mathcal{C} = \{C \mid C \subseteq P_{-p} \wedge C \in \Gamma_1^c \wedge Cp \in \Gamma_1\} \ , \\ \mathcal{D} = \{D \mid D \subseteq P_{-p} \wedge Dp \in \Gamma_1^c\} \ . \end{array} \tag{4.2}$$

It is then easy to verify that:

$$\Gamma_3 = \{BA \mid B \in \mathcal{B} \wedge A \subseteq Q\} \ \cup \{CK \mid C \in \mathcal{C} \wedge K \in \Gamma_2\} \ , \tag{4.3}$$

and

$$\Gamma_3^c = \{CJ \mid C \in \mathcal{C} \wedge J \in \Gamma_2^c\} \cup \{DA \mid D \in \mathcal{D} \wedge A \subseteq Q\} \ . \tag{4.4}$$

Multi-substitution. We would like to define the composition $\Gamma_1 \Diamond_I \Gamma_2$ for a set $I = \{p_1, \ldots, p_b\} \subset P$ of distinct parties. Informally, $\Gamma_1 \Diamond_I \Gamma_2$ is an access structure obtained by substituting an instance of Γ_2 for every participant of I in Γ_1, where the participant sets of all involved $|I| + 1$ access structures are assumed to be disjoint. We will not bother to give a formal definition.

Fact 4.1 $|P(\Gamma_1 \Diamond_I \Gamma_2)| = |P(\Gamma_1)| + |I|(|P(\Gamma_2)| - 1)$.

Example 4.2 (Access structure substitution) *Let $\Gamma_1 = ab+ac+bc$ and $\Gamma_2 = a+cd+ce+f$. We then have $\Gamma_1 \Diamond_c \Gamma_2 = ab+a(a+cd+ce+f)+b(a+cd+ce+f) = a+bcd+bce+bf$. As another example, let $\Gamma = ab$ and $\mathcal{F}, \mathcal{N}, \mathcal{F} \cdot \mathcal{N}$ be as in Example 3.18. Then, $(\Gamma \Diamond_a \mathcal{F}) \Diamond_b \mathcal{N} = \mathcal{F} \cdot \mathcal{N}$. See Figure 1. Also see Example 5.2 for a multi-substitution example.*

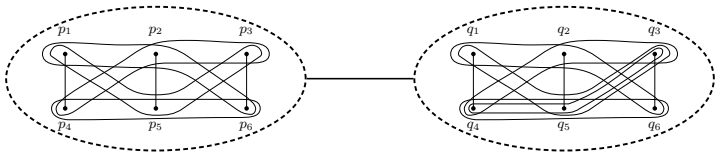


Fig. 1: The access structure $\mathcal{F} \cdot \mathcal{N} = (\Gamma \Diamond_a \mathcal{F}) \Diamond_b \mathcal{N}$ where $\Gamma = ab$ (see Example 4.2). Also, it can be viewed as $\mathcal{F} \cdot \mathcal{N} = \Gamma \Diamond_{p_7} \mathcal{F}$ where $\Gamma = \mathcal{F} \cdot p_7$. See Example 3.18 for descriptions of $\mathcal{F}, \mathcal{N}$ and $\mathcal{F} \cdot \mathcal{N}$.

4.3 The substitution conjecture

Let Γ_1 and Γ_2 be two access structures with disjoint participants sets and $p \in P(\Gamma_1)$. It is an interesting question to study how $\Sigma(\Gamma_1 \Diamond_p \Gamma_2)$ and $\Sigma(\Gamma_1) \Diamond_p \Sigma(\Gamma_2)$ are related. In Appendix 9, we prove the inclusion $\overline{\Sigma(\Gamma_1)} \Diamond_p \overline{\Sigma(\Gamma_2)} \subseteq \overline{\Sigma(\Gamma_1 \Diamond_p \Gamma_2)}$ under a mild conjecture called the Uniform Share Distribution conjecture.

The more interesting part is the reverse inclusion $\overline{\Sigma(\Gamma_1 \Diamond_p \Gamma_2)} \subseteq \overline{\Sigma(\Gamma_1)} \Diamond_p \overline{\Sigma(\Gamma_2)}$, which one may conjecture to hold true as well. Notice that this conjecture is equivalent to a multi-substitution variant in which it is conjectured that $\overline{\Sigma(\Gamma_1 \Diamond_I \Gamma_2)} \subseteq \overline{\Sigma(\Gamma_1)} \Diamond_I \overline{\Sigma(\Gamma_2)}$ for every $I \subset P(\Gamma_1)$. We are not aware of any counterexample and, in fact, the current techniques are not matured enough for proving or refuting the conjecture theoretically or experimentally (for example the information ratios of several access structures on five participants [31,24] are still unknown).

Remark 4.3 *We remark that a variant of the above conjecture in which the closures are ignored is not valid. Towards constructing a counterexample, let $\mathcal{F}, \mathcal{N}, \mathcal{F} \cdot \mathcal{N}$ be as in Example 3.18. Let $\Gamma_1 = \mathcal{F} \cdot p_7$ and $\Gamma_2 = \mathcal{N}$ and hence $\Gamma_3 = \Gamma_1 \Diamond_{p_7} \Gamma_2 = \mathcal{F} \cdot \mathcal{N}$. The access structures Γ_1 and Γ_2 are both ideal, respectively on 7 and 6 participants. Therefore, $\Sigma(\Gamma_1) \Diamond_{p_7} \Sigma(\Gamma_2) = [\mathbf{1}, \infty)$, but $\mathbf{1} \notin \Sigma(\Gamma_3)$ as we saw in Example 3.18.*

The above conjecture on the equality of the two sets sounds too strong. In other complexity models (such as the depth and query complexity of Boolean functions), some saving is possible when composing functions. Therefore, similar to Karchmer-Raz-Wigderson conjecture on depth complexity of Boolean functions [35], we conjecture that the two sets are "close" rather than being identical. In order to formalize this conjecture, we first present a definition.

Definition 4.4 (Substitution factor) *The substitution factor of an access structure Γ on participants set P is defined as*

$$s(\Gamma) = \inf_{I, \Gamma'} \left\{ \sup\{s \mid \overline{\Sigma(\Gamma \Diamond_I \Gamma')} \subseteq s \cdot \overline{\Sigma(\Gamma)} \Diamond_I \overline{\Sigma(\Gamma')} \} \right\} ,$$

where the infimum is taken over all subsets $I \subset P$ and access structures Γ'.

In the definition, $s\mathcal{X} = \{s\boldsymbol{x} \mid \boldsymbol{x} \in \mathcal{X}\}$ for a set $\mathcal{X} \subset \mathbb{R}^n$ and $s \in \mathbb{R}$. Notice that the closures can be ignored in the definition since the interior of convec sets are closed by Proposition 3.8. However, we keep them to be able to extend to the restricted convec sets which may not have this property.

Remark 4.5 *In definition of the substitution factor, we do not impose any constraint on the number of participants of Γ'. For achieving the main result of this paper, however, it is sufficient to restrict to access structures with $|P(\Gamma')| \leqslant n^{1/\epsilon}$ for any $0 < \epsilon < 1/2$, where $n = |P(\Gamma)|$. To keep our notation and discussion simple, we ignore this restriction.*

The substitution factor determines how well the substituted convec set fits the convec set of the substituted access structure. Notice that $S(\Gamma) \leqslant 1$. Determining the substitution factor remains a challenging problem as discussed above. In the following, we make some conjectures about the substitution factor of access structure, but first we need a definition.

Definition 4.6 (Substitution factor of a family of access structures) *Let $s : \mathbb{R} \to \mathbb{R}$ be some function and $\mathcal{F} = \{\Gamma_k\}_{k \in \mathbb{N}}$ be a family of access structures. We say that the substitution factor of $\mathcal{F}$ is $s(n)$, and write $s(\mathcal{F}) = s(n)$, if $s(\Gamma_k) = s(n_k)$, where $n_k = |P(\Gamma_k)|$.*

Similar to the Karchmer-Raz-Wigderson conjecture on depth complexity of Boolean functions, one may conjecture that for every family $\mathcal{F}$ of access structures, there exists some $0 < \delta \leqslant 1$ such that $s(\mathcal{F}) \geqslant \delta$. This conjecture may still be "too strong". For the purpose of this paper, the following weaker variants are sufficient.

Conjecture 4.7 (Substitution conjectures) *Let $\mathcal{F}$ be a family of access structures and denote its substitution factor by $s(n) = s(\mathcal{F})$. Then:*

*(***Strong***) there exists some $0 < \delta \leqslant 1$ such that $s(n) = \Omega\big(\frac{n^\delta}{n}\big)$.*
*(***Moderate***) $s(n) = \Omega\big(\frac{(\log n)^{\omega(1)}}{n}\big)$.*
*(***Weak***) there exists some $2 < \delta$ such that $s(n) = \Omega\big(\frac{(\log n)^\delta}{n}\big)$.*

In Section 6, we construct a candidate family based on Csirmaz access structure which has a conjectured super-polynomial lower bound on the information ratio $n^{\Omega(\frac{\log n}{\log\log n})}$ (resp. $n^{\omega(1)}$) assuming the truth of the "strong" (resp. "moderate") substitution conjecture. Additionally, assuming the truth of the "weak" conjecture, the (super-linear) polynomial lower bound $n^{(1-\epsilon)\delta-1}$ is expected for every $0 < \epsilon < 1$.

Our argument even holds under the looser assumption that the moderate/weak substitution conjecture holds for the Csirmaz family rather than "any" family. Therefore, we also present the following definition.

Definition 4.8 *We say that the "strong"/"moderate"/"weak" substitution conjecture holds for a family $\mathcal{F}$ of access structures if the corresponding condition in Conjecture 4.7 holds.*

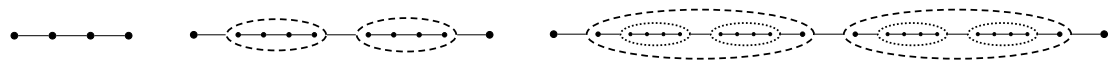
In Section 8, we study the substitution factor for the case where the Σ-set is replaced with the K-set and argue that $\frac{(\log n)^2}{n}$ "might" indeed be a tight upper-bound on the corresponding substitution factor for Csirmaz family.

5 A lifting theorem

In this section, we present a lifting theorem, useful for boosting the information ratio of a family of access structures. The idea is to define a recursive procedure for constructing a family of access structures by starting from a given family. We introduce some definitions and lemmas, before getting to the main theorem.

Definition 5.1 (The family $\mathcal{F}_{\Gamma,I}$ of access structures) *Let Γ be an access structure and $I \subseteq P(\Gamma)$. The family $\mathcal{F}_{\Gamma,I} = \{\Gamma_m\}_{m\in\mathbb{N}}$ of access structures is recursively defined as $\Gamma_m = \Gamma \Diamond_I \Gamma_{m-1}$, where $\Gamma_1 = \Gamma$.*

Example 5.2 *Figure 2 depicts the first three members of the family $\mathcal{F}_{\mathcal{P}_3,I}$ where $\mathcal{P}_3 = ab+bc+cd$ and $I = \{b, c\}$.*



(a) $\Gamma_1 = \mathcal{P}_3$ (b) $\Gamma_2 = \mathcal{P}_3 \Diamond_I \Gamma_1$ (c) $\Gamma_3 = \mathcal{P}_3 \Diamond_I \Gamma_2$

Fig. 2: The first three members of the family $\mathcal{F}_{\mathcal{P}_3,I}$ where $\mathcal{P}_3 = ab + bc + cd$ and $I = \{b, c\}$

Definition 5.3 ((b,t,s)-access structure) *Let $b \in \mathbb{N}$, $t \in \mathbb{R}^+$ and Γ be an access structure with substitution factor s. We call Γ a (b,t,s)-access structure if there exists a subset $I \subseteq P(\Gamma)$ of size $|I| = b$ with minimum total information ratio t. That is, for every $(\sigma_p)_{p\in P(\Gamma)} \in \Sigma(\Gamma)$ we have $\sum_{p\in I} \sigma_p \geqslant t$. When there is no emphasize on the substitution factor, we simply call it a (b,t)-access structure.*

Lemma 5.4 (Key lemma) *Let Γ be a (b,t,s)-access structure on participant set P and let $I \subseteq P$ be a subset of size b with minimum total information ratio t. Let $\mathcal{F}_{\Gamma,I} = \{\Gamma_m\}_{m\in\mathbb{N}}$. Then, for every $m \in \mathbb{N}$, we have*

I. $|P(\Gamma_m)| \leqslant |P|b^m$,
II. $\|\boldsymbol{x}\| \geqslant (st)^m$ *for every* $\boldsymbol{x} \in \overline{\Sigma(\Gamma_m)}$.

Proof. The equality $|P(\Gamma_m)| = (|P| - 1)(1 + b + \ldots + b^{m-1}) + 1$ can be proved by an easy induction on m and using Fact 4.1. This proves the first claim.

The second claim is also proved by induction on m. The base case, $m = 1$, trivially holds since $s \leqslant 1$. Assuming that the claim holds for $m \in \mathbb{N}$, we show that it holds as well for $m + 1$; that is, $\|\boldsymbol{x}'\| \geqslant (st)^{m+1}$ for every $\boldsymbol{x}' \in \overline{\Sigma(\Gamma_{m+1})}$. By definition of the substitution factor, there exists convecs $\boldsymbol{x} = (\sigma_p)_{p\in P} \in \overline{\Sigma(\Gamma)}$ and $\boldsymbol{x}_{p_{i_1}}, \ldots, \boldsymbol{x}_{p_{i_b}} \in \overline{\Sigma(\Gamma_m)}$ such that

$$\|\boldsymbol{x}'\| \geqslant s\Big(\sum_{p\in P\setminus I} \sigma_p + \sum_{p\in I} \big(\sigma_p \|\boldsymbol{x}_p\|\big)\Big) .$$

By the induction hypothesis, we have $\|\boldsymbol{x}_p\| \geqslant (st)^m$, for every $p \in I$. Also, by assumption, $\sum_{p\in I} \sigma_p \geqslant t$. Consequently,

$$\|\boldsymbol{x}'\| \geqslant s\Big(0 + \sum_{p\in I} \big(\sigma_p (st)^m\big)\Big) \geqslant (st)^{m+1} .$$

□

Definition 5.5 (Information ratio of a family of access structures) *Let $g : \mathbb{R} \to \mathbb{R}$ be some function and $\mathcal{F} = \{\Gamma_k\}_{k\in\mathbb{N}}$ be a family of access structures. We say that the average information ratio of $\mathcal{F}$ is $g(n)$, and write $\tilde{\sigma}(\mathcal{F}) = g(n)$, if $\tilde{\sigma}(\Gamma_k) = g(n_k)$, where $n_k = |P(\Gamma_k)|$. A similar definition is given for the maximum information ratio of the family $\mathcal{F}$, denoted by $\sigma(\mathcal{F})$.*

Proposition 5.6 (Simple lifting) *If there exist a (b,t,s)-access structure with $b \geqslant 2$, then there exists a family of access structures with average (and consequently maximum) information ratio $\Omega\big(n^{\log_b(st/b)}\big)$.*

Proof. Let Γ be a (b,t,s)-access structure on participant set P and let $I \subseteq P$ be a subset of size b with minimum total information ratio t. Define $\mathcal{F}_{\Gamma,I} = \{\Gamma_m\}_{m\in\mathbb{N}}$. The condition $b \geqslant 2$ implies $t \geqslant 2$. Consequently, by Lemma 5.4, it follows that $n = |P(\Gamma_m)| \leqslant |P|b^m$ and $\|\boldsymbol{x}\| \geqslant (st)^m \geqslant (st)^{\log_b(n/|P|)} = \Omega\big(n^{\log_b st}\big)$. Hence, $\tilde{\sigma}(\Gamma_m) = \Omega\big(n^{\log_b(st/b)}\big)$. □

Definition 5.7 ($\big(b(n),t(n),s(n)\big)$-family of access structures) *Let $b,t,s : \mathbb{R}^+ \to \mathbb{R}^+$ be three functions. Let $\mathcal{F} = \{\Gamma_k\}_{k\in\mathbb{N}}$ be a family of access structures and denote $n_k = |P(\Gamma_k)|$. We call $\mathcal{F}$ a $(b(n),t(n),s(n))$-family if, for every $k \in \mathbb{N}$, Γ_k is a $\big(b(n_k),t(n_k),s(n_k)\big)$-access structure. That is, the substitution factor of the access structure Γ_k is $s(n_k)$ and there exists a subset $I_k \subseteq P(\Gamma_k)$ of size $|I_k| = b(n_k)$ with minimum total information ratio $t(n_k)$. When there is no emphasize on the substitution factor, we simply call it a $(b(n),t(n))$-family.*

Theorem 5.8 (Lifting theorem) *Let $b, t, s : \mathbb{R}^+ \to \mathbb{R}^+$ be three functions such that $b(x) \geqslant 2$ and $f(x) = \frac{\log(s(x)t(x))}{\log b(x)}$ is increasing. If there exists a $\big(b(n), t(n), s(n)\big)$-family of access structures, then, for any $0 < \epsilon < \frac{1}{2}$, there exists a family of access structures with total information ratio at least $n^{(1-2\epsilon)f(n^\epsilon)}$.*

Additionally, if $f(x)$ is eventually everywhere differentiable, $\frac{f'(x)x\ln x}{f(x)} = \mathrm{O}(1)$, and $f(x) = \omega(1)$, then the average (and consequently maximum) information ratio of the family is $n^{\Omega(f(n))}$.

Proof. Let $\mathcal{F} = \{\Gamma_k\}_{k\in\mathbb{N}}$ be the $\big(b(n), t(n), s(n)\big)$-family. For every $k \in \mathbb{N}$, denote $n_k = |P(\Gamma_k)|$ and let $I_k \subseteq P(\Gamma_k)$ be a subset of size $|I_k| = b(n_k)$ with minimum total information ratio $t(n_k)$. That is, for every $(\sigma_p)_{p\in P(\Gamma_k)} \in \Sigma(\Gamma_k)$ it holds that $\sum_{p\in I_k} \sigma_p \geqslant t(n_k)$.

Consider the setting of Lemma 5.4 for the family $\mathcal{F}_{\Gamma_k, I_k} = \{\Gamma_{k,m}\}_{m\in\mathbb{N}}$. We have $|P(\Gamma_k)| = n_k$, $b = b(n_k)$, $t = t(n_k)$ and $s = s(n_k)$. Let $d = \frac{1}{\epsilon} > 2$ and denote

$$m_k = (d-2)\frac{\log n_k}{\log b(n_k)} \ .$$

Consider the family $\mathcal{F}' = \{\Gamma'_k\}_{k\in\mathbb{N}}$ of access structures where $\Gamma'_k = \Gamma_{k,\lceil m_k\rceil}$. By Lemma 5.4 (Part I), our choice for m_k and taking into account that $2 \leqslant b(n_k) \leqslant n_k$, we have:

$$|P(\Gamma'_k)| \leqslant |P| b^{\lceil m_k\rceil} \leqslant n_k b(n_k)^{m_k+1} = n_k n_k^{d-2} b(n_k) \leqslant n_k^d \ .$$

Also, by Part II of Lemma 5.4, for every $\boldsymbol{x} \in \overline{\Sigma(\Gamma'_k)}$, we have

$$\|\boldsymbol{x}\| \geqslant (st)^{\lceil m_k\rceil} \geqslant \big(s(n_k)t(n_k)\big)^{m_k} = n_k^{(d-2)\frac{\log(s(n_k)t(n_k))}{\log b(n_k)}} = n_k^{(d-2)f(n_k)} \ .$$

By letting $n = |P(\Gamma'_k)|$ and taking into account the increasing propery of $f(x) = \frac{\log(s(x)t(x))}{\log b(x)}$, we then get:

$$\|\boldsymbol{x}\| \geqslant n^{\frac{d-2}{d} f(\sqrt[d]{n})} = n^{(1-2\epsilon)f(n^\epsilon)} \ ,$$

proving the first part of the claim.

Consequently, $\tilde{\sigma}(\mathcal{F}') \geqslant n^{(1-2\epsilon)f(n^\epsilon)-1}$ and the additional condition $f(x) = \omega(1)$ implies that $\tilde{\sigma}(\mathcal{F}') = n^{\Omega\left((1-2\epsilon)f(n^\epsilon)\right)}$. The remaining part of the claim is a corollary of Lemma 5.9 (Part I), given below. □

For proving the final claim of Theorem 5.8, we only relied on the Part I of Lemma 5.9. Roughly speaking, Part II of the lemma shows that if, for some function $f(x)$, it is possible to ignore ϵ and simplify the lower bound, then f is polylogarithmic (that is, $f(x) = \mathrm{O}((\log x)^k)$ for some real number $k \geqslant 0$). Part III of the lemma indicates that, not for every polylogarithmic function, the simplification is allowed. In fact, due to Part I, $\frac{f'(x)x\ln x}{f(x)}$ is necessarily unbounded for such functions.

Lemma 5.9 *Let $f : \mathbb{R}^+ \to \mathbb{R}^+$ be some function.*

I. If f is eventually everywhere differentiable and $\frac{f'(x)x\ln x}{f(x)} = \mathrm{O}(1)$, then $f(x^\epsilon) = \Omega(f(x))$ for every $0 < \epsilon < 1$.

II. If f is bounded on any bounded interval and $f(x^\epsilon) = \Omega(f(x))$ for some $0 < \epsilon < 1$, then f is polylogarithmic.

III. There exist a continuous, differentiable and polylogarithmic f such that $f(x^\epsilon) \neq \Omega(f(x))$ for every $0 < \epsilon < 1$.

Proof. To prove I, assume that $\frac{f'(x)x\ln x}{f(x)} = \mathrm{O}(1)$. We show that, for any $0 < \epsilon < 1$, $\frac{f(x)}{f(x^\epsilon)} = \mathrm{O}(1)$; this is equivalent to $f(x^\epsilon) = \Omega(f(x))$.

Let $h(x) = \ln f(e^{e^x})$ and hence $f(x) = e^{h(\ln\ln x)}$. We have $\ln\frac{f(x)}{f(x^\epsilon)} = h(z) - h(z-\epsilon')$ where $\epsilon' = -\ln\epsilon > 0$ and $z = \ln\ln x$. Also, by the Mean Value Theorem, we have $h(z) - h(z-\epsilon') = h'(z_0)\epsilon'$ for some $z_0 \in (z-\epsilon', z)$. Since $h'(z) = \frac{f'(x)x\ln x}{f(x)} = \mathrm{O}(1)$, it then follows that $h(z) - h(z-\epsilon') = \mathrm{O}(1)$ for any $\epsilon' > 0$, indicating that $\frac{f(x)}{f(x^\epsilon)} = \mathrm{O}(1)$.

To prove II, let $f(x^\epsilon) = \Omega(f(x))$ for some $0 < \epsilon < 1$. That is, there exisit some $M > 1$ and $\alpha > 1$ such that $f(x) \leqslant \alpha f(x^\epsilon)$ for all $x \geqslant M$.

Let $x \geqslant M$ and choose an integer m such that

$$x^{\epsilon^m} < M \leqslant x^{\epsilon^{m-1}} ,$$

or equivalently, $m = \lceil \frac{\log\log M - \log\log x}{\log\epsilon} \rceil + 1$.

It is easy to prove by induction that $f(x) \leqslant \alpha^m f\big(x^{\epsilon^m}\big)$. Also, note that

$$\alpha^{m-1} \leqslant \alpha^{\frac{\log\log M - \log\log x}{\log\epsilon}} = \alpha^{\frac{\log\log M}{\log\epsilon}} \times (\log x)^{-\frac{\log\alpha}{\log\epsilon}} .$$

Since $1 \leqslant x^{\epsilon^m} < M$ and f is bounded on any bounded interval, it holds that $f\big(x^{\epsilon^m}\big) \leqslant T$, for some $T \in \mathbb{R}^+$. Consequently, we have

$$f(x) \leqslant \alpha\alpha^{m-1}T = \alpha^{\frac{\log\log M}{\log\epsilon}+1} \times T \times (\log x)^{-\frac{\log\alpha}{\log\epsilon}} .$$

That is, $f(x) = \mathrm{O}((\log x)^k)$ for $k = -\frac{\log\alpha}{\log\epsilon}$.

The function $f(x) = 2^{2^{\lceil \log\log\log x \rceil}}$ is an example for Part III, but it is not continuous. It is easy to construct continuous and differentiable approximations of this function, satisfying the required conditions.

□

6 Our candidate construction

In this section we study the different lower bounds that can be achieved by applying the lifting theorem to Csirmaz [19] family assuming the truth of the strong/moderate/weak substitution conjecture. The expected lower bound for our candidate may vary from super-linear to super-polynomial, depending on the kind of conjecture that is made on the substitution factor of Csirmaz family, which remains unknown.

For any integer $k \geqslant 2$, Csirmaz [19] has constructed an access structure Γ_k with $2^k + k - 2$ participants. Csirmaz has proved that the maximum information ratio of the family $\mathcal{C} = \{\Gamma_k\}$ is $\Omega(n/\log n)$. To show this, he has exhibited a subset $I \subseteq P(\Gamma_k)$ of size k such that for every $(\sigma_p)_{p\in P(\Gamma_k)} \in \Sigma(\Gamma_k)$ it holds that $\sum_{p\in I}\sigma_p \geqslant 2^k - 1$. That is, $\mathcal{C}$ is a $\big(\Theta(\log n), \Omega(n)\big)$-family.

Our candidate family. For every $0 < \epsilon < \frac{1}{2}$, we construct the family $\mathcal{F}_\epsilon$ of secret sharing schemes as in the proof of the lifting theorem by starting from that of Csirmaz and repeating the substitution procedure $(\frac{1}{\epsilon} - 2)\frac{\log n}{\log\log n}$ times.

The following corollary is a direct application of our lifting theorem.

Corollary 6.1 (Conjectured lower bound) *For every $0 < \epsilon < \frac{1}{2}$, let $\mathcal{F}_\epsilon$ be our candidate family. Then,*

- *If the "strong" substitution conjecture holds for the Csirmaz family, then $\tilde{\sigma}(\mathcal{F}_\epsilon) = n^{\Omega(\frac{\log n}{\log\log n})}$.*

– *If the "moderate" substitution conjecture holds for the Csirmaz family, then* $\tilde{\sigma}(\mathcal{F}_\epsilon) = n^{\omega(1)}$.
– *If the "weak" substitution conjecture holds for the Csirmaz family with* $\delta > 2$*, then* $\tilde{\sigma}(\mathcal{F}_\epsilon) = \Omega(n^{(1-2\epsilon)\delta-1})$.

We close this section by the following two problems.

Question 6.2 *Determine the substitution factor of Csirmaz family.*

Question 6.3 *For every* $0 < \epsilon < \frac{1}{2}$*, determine* $\kappa(\mathcal{F}_\epsilon)$.

Indeed, in Csirmaz paper it was left open if there exists a family of access structures whose κ-parameter is $\omega(n/\log n)$. We wonder if our family meets this bound.

7 Can we do better than $n^{\Omega(\frac{\log n}{\log\log n})}$?

In this section, we explore the possibility of improving the $n^{\Omega(\frac{\log n}{\log\log n})}$ lower bound by lifting any access structures for which a lower bound has been achieved via Shanon inequalities. As we will see the answer is negative even assuming the strongest assumption that $\overline{\Sigma(\Gamma_1 \Diamond_p \Gamma_2)} = \overline{\Sigma(\Gamma_1)} \Diamond_p \overline{\Sigma(\Gamma_2)}$ for every pair of access structures Γ_1, Γ_2 and $p \in P(\Gamma_1)$.

Let first introduce some definitions.

Definition 7.1 (Regular family of access structures) *Let* $b, t, f, g : \mathbb{R}^+ \to \mathbb{R}^+$ *be some functions. We say that* g *is* f*-regular if* $g = \mathrm{O}(f)$ *or* $g = \omega(f)$*. Let* $\mathcal{F}$ *be a* $\big(b(n), n^{t(n)}\big)$*-family of access structures. We call* $\mathcal{F}$ *an* $(f(n), n^{g(n)})$*-regular family if* b *is* f*-regular and* t *is* g*-regular.*

Definition 7.2 (Domain restriction) *The restriction of a function* f *with domain* D *on domain* $A \subseteq D$ *is denoted by* $f|_A$*. Let* $f, g : \mathbb{R}^+ \to \mathbb{R}^+$ *be two functions and* $A \subseteq \mathbb{R}^+$*. We say that* $f|_A(x) = O(g(x))$*, if there exists positive numbers* c, x_0 *such that for every* $x \in A \cap [x_0, \infty)$ *it holds that* $f(x) \leqslant cg(x)$.

Suppose that, assuming the truth of the very strong substitution, one wishes to improve the lower bound $n^{\Omega(\frac{\log n}{\log\log n})}$, by applying the lifting theorem to a $(\log n, n)$-regular family of access structures; i.e., one that falls into one of the following four categories:

– $\big(\mathrm{O}(\log n), n^{\mathrm{O}(1)}\big)$-family,
– $\big(\mathrm{O}(\log n), n^{\omega(1)}\big)$-family,
– $\big(\omega(\log n), n^{\mathrm{O}(1)}\big)$-family, or
– $\big(\omega(\log n), n^{\omega(1)}\big)$-family.

Lemma 7.4, stated and proved below, rules out the first three categories; that is, improvements may be possible only by lifting a $\big(\omega(\log n), n^{\omega(1)}\big)$-family when restricted to $(\log n, n)$-regular families. Unfortunately, Csirmaz negative result shows that the currently known techniques fail to find such a family. More precisely, he has shown that, by merely using the Shannon information inequalities [36,15], the best that one can achieve is to construct a $\big(b(n), t(n)\big)$-family of access structures with $t(n) \leqslant n^2$; see [19, Theorem 3.5]. Beimel and Orlov [8] have shown that even by incorporating the so-called non-Shannon information inequalities [62] with four or five variables, unknown at time of publication of [19], the Csirmaz barrier is still valid; see [47] for a follow-up. We conclude that the best lower bound that can be achieved by lifting a $(\log n, n)$-regular family of access structures, with proven lower bound using similar methods, is $n^{\Omega(\frac{\log n}{\log\log n})}$.

We need the following lemma, which is a generalization of Lemma 3.9, for proving Lemma 7.4.

Lemma 7.3 *Let Γ be a (b,t)-access structure. Then, $t \leqslant b2^{b-1}$.*

Proof. Let $I \subseteq P(\Gamma)$ be a subset of size b with total information ratio at least t. To prove the claim, we show that Γ admits a secret sharing scheme such that the information ratio of every participant $p \in I$ is exactly 2^{b-1}.

In the Sperner system, let $\Gamma = \sum_{J \subseteq I} \big(\Gamma_J \prod_{p \in J} p\big)$, where Γ_J is an access structure on participant set $P' = P \backslash I$. More precisely, $\Gamma^-_\varnothing = \{A \subseteq P' \mid A \in \Gamma^-\}$ and $\Gamma^-_J = \{A \subseteq P' \mid A \notin \Gamma^-, A \cup J \in \Gamma^-\}$, for every non-empty $J \subseteq I$.

Let $m \geqslant 2$ be an integer. It is well-known that every access structure admits a secret sharing scheme with secret space $\mathbb{Z}_m$ [30]. Let Π_J be such a secret sharing schemes for Γ_J. We construct a secret sharing scheme for Γ such that the secret is uniform over $\mathbb{Z}_m$ and every participant $p \in I$ receives a random vector of length 2^{b-1} over $\mathbb{Z}_m$. To share a secret $s \in \mathbb{Z}_m$, for each non-empty $J \subseteq I$, we choose a uniformly random $(r_{J,p})_{p \in J} \in \mathbb{Z}_m^{|J|}$ and give the share $r_{J,p}$ to $p \in J$. Then, we share $s + \sum_{p \in J} r_{J,p}$ as a secret using the scheme Π_J. The secret s is also shared using the scheme $\Pi_\varnothing$. Clearly, the resulting scheme realizes Γ. Every participant $p \in I$ receives an element of $\mathbb{Z}_m$ for each subset of I that includes p; there are exactly 2^{b-1} such subsets. Consequently, the information ratio of each participant $p \in I$ is 2^{b-1}. □

Lemma 7.4 (Lifting limit) *Let $b, t : \mathbb{R}^+ \to \mathbb{R}^+$ be two functions where $b(x) \geqslant 2$. Let $\mathcal{F} = \{\Gamma_k\}_{k \in \mathbb{N}}$ be a $\big(b(n), t(n)\big)$-family of access structures. Denote $A = \{|P(\Gamma_k)|\}_{k \in \mathbb{N}}$ and $f(x) = \frac{\log(s(x)t(x))}{\log b(x)}$, with $s(x) = 1$. Then:*

I. If $b(x) = \mathrm{O}(\log x)$, then $f|_A(x) = \mathrm{O}(\frac{\log x}{\log\log x})$.
II. If $b(x) = \omega(\log x)$ and $t(x) = x^{\mathrm{O}(1)}$, then $f|_A(x) = \mathrm{O}(\frac{\log x}{\log\log x})$.

Proof. By Lemma 7.3, we have $t(n) \leqslant b(n)2^{b(n)-1}$, for every $n \in A$. Consequently, $f(n) = \frac{\log(s(n)t(n))}{\log b(n)} \leqslant \frac{b(n)-1}{\log b(n)} + 1$, for every $n \in A$.

Note that the function $\frac{x-1}{\log x}$ is increasing for $x \geqslant 2$. Therefore, $b(x) = \mathrm{O}(\log x)$ implies that $f|_A(x) = \mathrm{O}(\frac{\log x}{\log\log x})$, proving Part I.

For proving Part II, first note that $t(x) = x^{\mathrm{O}(1)}$ implies $\log t(x) = \mathrm{O}(\log x)$ and $b(x) = \omega(\log x)$ implies $\log b(x) = \Omega(\log\log x)$. Consequently, $f|_A(x) = \mathrm{O}(\frac{\log x}{\log\log x})$. □

8 Substitution factor for other measures

Proving/disproving any of the substitution conjecture variants seems very challenging due to lack of techniques in determining the convec set of access structures. As mentioned earlier, even the information ratios of several access structures on five participants [31,24] are still unknown. Therefore, analysis of the substitution factor of access structures remains a challengingly difficult problem.

One can define the substitution factor of access structures with respect to some restricted class of secret sharing schemes. This approach is not also currently promising for the same reason, even for the class of linear schemes.

Another approach which might be more promising for understanding the behavior of the substitution factor is to work with a lower bound on the Σ-set such as the K-set (see Appendix A). Refer to the corresponding factor as the *polymatroidal substitution factor* and denote it by $k(\cdot)$ instead of $s(\cdot)$. More generally, for any set H which lies between the polymatorids region and the entropy region, one can define K^{H}-set as a lower bound measure on the Σ-set. Denote the corresponding substitution factor of a family $\mathcal{F}$ of access structures by $k^{\mathrm{H}}(\mathcal{F})$. We wonder if this parameter behaves well with respect to monotonicity.

Question 8.1 *Is it true that for every* $\mathrm{H}_1 \subseteq \mathrm{H}_2$ *and every family* $\mathcal{F}$*, it holds that* $k^{\mathrm{H}_1}(\mathcal{F}) = \mathrm{O}(k^{\mathrm{H}_2}(\mathcal{F}))$*?*

Let $\mathcal{F}$ be a $(b(n), t(n))$-family with polymatroidal substitution factor $k(n)$. As it was mentioned earlier, Csirmaz has proved that the total information ratio of any access structure on n participants is at most n^2 by considering only Shannon inequalities. By applying the lifting lemma to $\mathcal{F}$, we have

$$n^{(1-2\epsilon)\frac{\log\left(k(n^\epsilon)t(n^\epsilon)\right)}{\log b(n^\epsilon)}} \leqslant n^2 \ .$$

By letting

$$k(n) = \frac{(b(n))^{g(n)}}{t(n)} \ ,$$

we get $g(n) \leqslant \frac{2}{1-2\epsilon}$ for every $0 < \epsilon < 1/2$. Therefore,

$$k(n) \leqslant \max\left(1, \frac{(b(n))^2}{t(n)}\right) \ .$$

For Csirmaz family, we have

$$k(n) \leqslant \frac{(\log n)^2}{n} \ ,$$

and it remains open if this bound is tight.

Question 8.2 *Compute the k-factor for the Csirmaz family. Is it* $\Theta(\frac{(\log n)^2}{n})$*? Is there a family* $\mathcal{F}$ *of access structures with* $k(\mathcal{F}) = \omega(\frac{(\log n)^2}{n})$*?*

9 The uniform share distribution conjecture

In this section, we will prove that for every pair Γ_1, Γ_2 of access structures and every participant p_i of Γ_1 it holds that $\overline{\Sigma(\Gamma_1)}\Diamond_{p_i}\overline{\Sigma(\Gamma_2)} \subseteq \overline{\Sigma(\Gamma_1 \Diamond_{p_i} \Gamma_2)}$ assuming the *Uniform Share Distribution (USD) conjecture* holds true. Informally, the USD conjecture states that the share distributions (and also the secret) are uniform in optimal schemes.

Conjecture 9.1 (Uniform share distribution (USD) conjecture) *Let* Γ *be an access structure and let* $\boldsymbol{x} \in \inf_{\mathrm{P}}\big(\Sigma(\Gamma_1)\big)$*. Then, there exists a sequence* $\{\Pi_j\}_{j\in\mathbb{N}}$ *of secret sharing schemes such that: 1) each* Π_j *realizes* Γ*, 2) the sequence* $\{\mathrm{cv}(\Pi_j)\}_{j\in\mathbb{N}}$ *converges to* $\boldsymbol{x}$*, 3) every participant's share, in each* Π_j*, is uniform over its support, and 4) each secret random variable, in each* Π_j*, is uniform over its support.*

Remark 9.2 (USD conjecture and secret distribution) *By Lemma 2.2, the USD conjecture is equivalent to a seemingly weaker version that omits the fourth requirement. This fact justifies our selected running title for the conjecture.*

Let us see why we resort to the USD conjecture for proving the inclusion $\overline{\Sigma(\Gamma_1)}\Diamond_{p_i}\overline{\Sigma(\Gamma_2)} \subseteq \overline{\Sigma(\Gamma_1 \Diamond_{p_i} \Gamma_2)}$. Let $\Pi_1 = (\boldsymbol{S}_p)_{p\in P\cup\{p_0\}}$ and $\Pi_2 = (\boldsymbol{S}_q)_{q\in Q\cup\{q_0\}}$ be Pareto-optimal secret sharing schemes for Γ_1 and Γ_2, respectively. Roughly speaking, we need to argue that there exists a Pareto-optimal scheme Π for $\Gamma_1 \Diamond_{p_i} \Gamma_2$ such that the following holds:

$$\mathrm{cv}(\Pi) \preceq \mathrm{cv}(\Pi_1)\Diamond_{p_i}\mathrm{cv}(\Pi_2)\ .$$

A simple scheme Π for $\Gamma_1\Diamond_{p_i}\Gamma_2$ can be constructed by first sharing the secret using Π_1 and then sharing the share of p_i in Π using Π_2. This argument needs to additionally assume that $\mathrm{supp}(\boldsymbol{S}_{p_i}) = \mathrm{supp}(\boldsymbol{S}_{q_0})$. The convec of the constructed scheme, however, is

$$\mathrm{cv}(\Pi) = \mathrm{cv}(\Pi_1)\Diamond_{p_i}\Big(\frac{\mathrm{H}(\boldsymbol{S}_{q_0})}{\mathrm{H}(\boldsymbol{S}_{p_i})}\mathrm{cv}(\Pi_2)\Big)\ ,$$

further requiring to assume that $\mathrm{H}(\boldsymbol{S}_{q_0}) \leqslant \mathrm{H}(\boldsymbol{S}_{p_i})$. Since Π_2 is Pareto-optimal, $\boldsymbol{S}_{q_0}$ is uniform and so must be $\boldsymbol{S}_{p_i}$.

Therefore, we have the following proposition. The full proof is given in Appendix B.

Proposition 9.3 (USD conjecture ⇒ (9.1)) *The USD conjecture implies that for every access structures Γ_1, Γ_2 and every $p_i \in P(\Gamma_1)$, it holds that*

$$\overline{\Sigma(\Gamma_1)}\Diamond_{p_i}\overline{\Sigma(\Gamma_2)} \subseteq \overline{\Sigma(\Gamma_1\Diamond_{p_i}\Gamma_2)}\ . \tag{9.1}$$

We close this section by the following remarks, concerning the USD conjecture:

1. **USD and relaxed security notions.** It remains open, if the USD holds true for total security or even the weaker notion of statistical security. However, it can be shown to hold for another relaxation called quasi-total security [33], due to a well-known result by Chan and Yeung [16] on the equality of the entropy region and the cone of group-characterizable polymatroids. We refer the reader to Appendix C for details.
2. **USD for linear schemes.** The inclusion (9.1) does not hold when we restrict to the class of linear schemes even though the shares and secret are uniform in this case. Here is a counterexample. Let $\mathcal{F}, \mathcal{N}, \mathcal{F}\cdot\mathcal{N}$ be as in Example 3.18 and let $\Gamma_1 = \mathcal{F}\cdot p_7$ and $\Gamma_2 = \mathcal{N}$. The access structures Γ_1 and Γ_2 are both ideally realizable by linear schemes (but with different field characteristics), respectively on 7 and 6 participants. Nevertheless, $\Gamma_1\Diamond_{p_7}\Gamma_2 = \mathcal{F}\cdot\mathcal{N}$ is far from having nearly ideal linear schemes, even though it has nearly ideal nonlinear schemes. In a follow-up work [32] we have computed the linear convec set of $\mathcal{F}\cdot\mathcal{N}$ and shown that it is even non-convex. Nevertheless, the inclusion (9.1) holds when we restrict to the class of linear schemes on finite fields with a given characteristic.
3. **USD and information ratio variants.** Two different flavors of information ratio can be found in the literature [14,11,44]. One is defined based on the ratio between the share entropy and the secret entropy, also adopted by us in the course of this paper. The other one is defined as the ratio between the logarithm of the share space size and the logarithm of the secret space size. Consequently, the information ratio of an access structure Γ can be defined in two different ways. Denote the latter one by $\sigma_{\mathrm{s}}(\Gamma)$. It is known that $\sigma_{\mathrm{s}}(\Gamma) \geqslant \sigma(\Gamma)$; e.g., see [4, Section 5.2]. The USD conjecture implies these two notions are equivalent.

10 On plausibility of the substitution conjecture

One may be concerned about difficulty of proving/disproving the substitution conjecture. Here are a few remarks.

- Our conjecture has a novel information theoretic description and it is very different from reformulating the original problem (Beimel's conjecture).
- The notion of substitution factor gives the substitution conjecture a sort of *fuzzy* flavor. What we mean is that the smaller the substitution factor is assumed to be, the more plausible it is that the substitution conjecture holds true.

– We agree that there is no evidence for the validity of the substitution conjecture. On the other hand, there is also no strong argument that why the conjecture might not hold true.
– It is worth noting that we have a conjecture as well as a construction. This is very different from just having a conjecture that implies the open problem to be resolved. Therefore, it is a win-win progress as, either we have a construction with a super-linear lower bound, or we make progress towards understanding the barriers; this is not much different from the rest of crypto.

One could say that it is not promising to make progress on the substitution conjecture. Here are some arguments.

– The fact that it might be hopeless to advance towards resolving the substitution conjecture is not unique to the substitution conjecture. A similar situation holds for the well-known conjecture by Karchmer, Raz, and Wigderson on the depth complexity of Boolean functions, for which no substantial progress has been made. We emphasize that we do not claim that the substitution conjecture is *connected* to the KRW conjecture, but only on their *resemblance*.
– Even though proving/refuting the substitution conjecture seems difficult, it is plausible to advance in other directions. In particular, it is conceivable to be able to find loose lower bounds on our $\mathcal{F}_\epsilon$ family of access structures by considering only the Shannon type information inequalities, which is very well understood. But of course applying it on our family demands skills and innovation. This demands understanding the behavior of κ-parameter (K-set) with respect to substitution. Any progress in this plausible direction might lead to improve Csirmaz sub-linear lower bound into a linear one (see Question 8.2). To make it more clear, we feel that the Shannon lower bound for our $\mathcal{F}_\epsilon$ family is $n^{1-\epsilon}$, or something similar. Even though this is worse than that of Csirmaz, if true, it can be amplified to a linear lower bound in a straightforward way (recall Csirmaz impossibility result). We conclude that it is quite plausible that the research community progress in some directions such as above.

One may criticize the substitution conjecture for solely being supported by the limitations of the known methods to construct secret sharing schemes. Even though true, one can see it from the positive side. In order to refute the substitution conjecture one needs to develop new construction techniques tailored for the substituted access structures. If this ever happens, it will enhance our understating of algebraic behavior of access structures when viewed in the Sperner form.

11 Conclusion

The crypto community lacks suitable approaches for constructing complex, yet analyzable, access structures. The substitution technique, originally introduced by Martin in [44] and further developed in this paper, might be an initiation in this direction. The introduced notion of convec set leaves several problems (of information-theoretic nature) unanswered. However, the substitution conjecture (and substitution factor) might have implications in communication-complexity.

Acknowledgment. I am truly grateful to the anonymous reviewer for his/her valuable suggestions and, in particular, for bringing the Karchmer-Raz-Wigderson conjecture to my attention which led to relaxing the original substitution conjecture [37]. I also thank Morteza Fotouhi for the proof of Lemma 5.9 and Carles Padró for the useful discussions.

References

1. László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.
2. Sorush Bahariyan. A systematic approach for determining the linear convec set of small access structures (in persian). Master's thesis, Sharif University of Technology, 2019.
3. William F. Basener. *Topology and Its Applications (1. ed.)*. John Wiley & Sons, 2006.
4. Amos Beimel. Secret-sharing schemes: A survey. In *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, pages 11–46, 2011.
5. Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 394–418, 2014.
6. Amos Beimel, Anna Gál, and Mike Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997.
7. Amos Beimel and Noam Livne. On matroids and nonideal secret sharing. *IEEE Trans. Information Theory*, 54(6):2626–2643, 2008.
8. Amos Beimel and Ilan Orlov. Secret sharing and non-shannon information inequalities. *IEEE Trans. Information Theory*, 57(9):5634–5649, 2011.
9. Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, pages 27–35, 1988.
10. George Robert Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference1979*, 48:313–317, 1979.
11. Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, and Ugo Vaccaro. Graph decompositions and secret sharing schemes. In *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*, pages 1–24, 1992.
12. Carlo Blundo, Alfredo De Santis, and Ugo Vaccaro. On secret sharing schemes. *Inf. Process. Lett.*, 65(1):25–32, 1998.
13. Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4(2):123–134, 1991.
14. Ernest F. Brickell and Douglas R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology*, 5(3):153–166, 1992.
15. Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology*, 6(3):157–167, 1993.
16. Terence H. Chan and Raymond W. Yeung. On a relation between information inequalities and group theory. *IEEE Trans. Information Theory*, 48(7):1992–1995, 2002.
17. László Csirmaz. The size of a share must be large. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 13–22, 1994.
18. László Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar*, 32(4):429–437, 1996.
19. László Csirmaz. The size of a share must be large. *J. Cryptology*, 10(4):223–231, 1997.
20. László Csirmaz. Secret sharing on the d-dimensional cube. *Designs, Codes and Cryptography*, 74(3):719–729, 2015.
21. László Csirmaz and Gábor Tardos. Optimal information rate of secret sharing schemes on trees. *IEEE Trans. Information Theory*, 59(4):2527–2530, 2013.
22. Jack Edmonds. Submodular functions, matroids, and certain polyhedra. *Combinatorial structures and their applications*, pages 69–87, 1970.
23. Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. *Algorithmica*, 79(4):987–1013, 2017.
24. Oriol Farràs, Tarik Kaced, Sebastià Martín Molleví, and Carles Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 597–621, 2018.

25. Satoru Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39(1):55–72, 1978.
26. Motahhareh Gharahi and Shahram Khazaei. Optimal linear secret sharing schemes for graph access structures on six participants. *Theoretical Computer Science*, 2018.
27. Motahhareh Gharahi and Shahram Khazaei. Reduced access structures with four minimal qualified subsets on six participants. *Advances in Mathematics of Communications*, 12(1):199–214, 2018.
28. Mika Göös, Pritish Kamath, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for p^np. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, pages 12:1–12:16, 2017.
29. Mika Göös, Toniann Pitassi, and Thomas Watson. Query-to-communication lifting for BPP. In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 132–143, 2017.
30. Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.
31. Wen-Ai Jackson and Keith M Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9(3):267–286, 1996.
32. Amir Jafari and Shahram Khazaei. On abelian secret sharing: duality and separation. Cryptology ePrint Archive, Report 2019/575, 2019. `https://eprint.iacr.org/2019/575`.
33. Tarik Kaced. Almost-perfect secret sharing. In *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, July 31 - August 5, 2011*, pages 1603–1607, 2011.
34. Tarik Kaced. *Secret Sharing and Algorithmic Information Theory. (Partage de secret et the'orie algorithmique de l'information)*. PhD thesis, Montpellier 2 University, France, 2012.
35. Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-logarithmic depth lower bounds via the direct sum in communication complexity. *Computational Complexity*, 5(3/4):191–204, 1995.
36. Ehud D. Karnin, J. W. Greene, and Martin E. Hellman. On secret sharing systems. *IEEE Trans. Information Theory*, 29(1):35–41, 1983.
37. Shahram Khazaei. Conjecturally superpolynomial lower bound for share size. Cryptology ePrint Archive, Report 2018/143, 2018. `https://eprint.iacr.org/2018/143`.
38. Pravesh K. Kothari, Raghu Meka, and Prasad Raghavendra. Approximating rectangles by juntas and weakly-exponential lower bounds for LP relaxations of csps. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 590–603, 2017.
39. James R. Lee, Prasad Raghavendra, and David Steurer. Lower bounds on the size of semidefinite programming relaxations. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 567–576, 2015.
40. Qiang Li, Xiang Xue Li, Xue Jia Lai, and Ke Fei Chen. Optimal assignment schemes for general access structures based on linear programming. *Designs, Codes and Cryptography*, 74(3):623–644, 2015.
41. Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 699–708, 2018.
42. Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. *J. Mathematical Cryptology*, 4(2):95–120, 2010.
43. Jaume Martí-Farré, Carles Padró, and Leonor Vázquez. Optimal complexity of secret sharing schemes with four minimal qualified subsets. *Designs, Codes and Cryptography*, 61(2):167–186, 2011.
44. Keith M Martin. New secret sharing schemes from old. *J. Combin. Math. Combin. Comput*, 14:65–77, 1993.
45. Frantisek Matús. Matroid representations by partitions. *Discrete Mathematics*, 203(1-3):169–194, 1999.
46. Frantisek Matús. Two constructions on limits of entropy functions. *IEEE Trans. Information Theory*, 53(1):320–330, 2007.

47. Sebastià Martín Molleví, Carles Padró, and An Yang. Secret sharing, rank inequalities, and information inequalities. *IEEE Trans. Information Theory*, 62(1):599–609, 2016.
48. Carles Padró. Lecture notes in secret sharing. *IACR Cryptology ePrint Archive*, 2012:674, 2012.
49. Toniann Pitassi and Robert Robere. Lifting nullstellensatz to monotone span programs over any field. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 1207–1219, 2018.
50. Ran Raz and Pierre McKenzie. Separation of the monotone NC hierarchy. *Combinatorica*, 19(3):403–435, 1999.
51. Paul D. Seymour. On secret-sharing matroids. *J. Comb. Theory, Ser. B*, 56(1):69–73, 1992.
52. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
53. Yaoyun Shi and Yufan Zhu. Quantum communication complexity of block-composed functions. *Quantum Information & Computation*, 9(5):444–460, 2009.
54. Juriaan Simonis and Alexei E. Ashikhmin. Almost affine codes. *Des. Codes Cryptography*, 14(2):179–197, 1998.
55. Douglas R Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.
56. Hung-Min Sun and Bor-Liang Chen. Weighted decomposition construction for perfect secret sharing schemes. *Computers & Mathematics with Applications*, 43(6):877–887, 2002.
57. Marten Van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6(2):143–169, 1995.
58. Marten Van Dijk, Wen-Ai Jackson, and Keith M Martin. A general decomposition construction for incomplete secret sharing schemes. *Designs, Codes and Cryptography*, 15(3):301–321, 1998.
59. Marten van Dijk, Tom A. M. Kevenaar, Geert Jan Schrijen, and Pim Tuyls. Improved constructions of secret sharing schemes by applying (lambda, omega)-decompositions. *Inf. Process. Lett.*, 99(4):154–157, 2006.
60. Stephen Willard. *General topology*. Courier Corporation, 1970.
61. Raymond W. Yeung. A framework for linear information inequalities. *IEEE Trans. Information Theory*, 43(6):1924–1934, 1997.
62. Zhen Zhang and Raymond W. Yeung. A non-shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory*, 43(6):1982–1986, 1997.

A Polymatroidal set

In this section, we present a more formal definition of the K-set.

Definition 1 (Polymatroid [22]). *Let Q be a finite set. We say that $\mathcal{S} = (Q, r)$ is a polymatroid with ground set Q and rank function $r : 2^Q \to \mathbb{R}$, when:*

a) $r(\varnothing) = 0$,
b) $r(X) \leqslant r(Y)$, *for every subsets* $X \subseteq Y \subseteq Q$ *(monotonicity),*
c) $r(X) + r(Y) \geqslant r(X \cup Y) + r(X \cap Y)$, *for every subsets* $X, Y \subseteq Q$ *(sub-modularity).*

Definition 2 (Γ-polymatroid [42]). *Let Γ be an access structure on P and $\mathcal{S} = (P \cup \{p_0\}, r)$ be a polymatroid. We say that $\mathcal{S}$ is a* Γ-polymatroid *if it additionally holds that:*

a) $r(A \cup \{p_0\}) = r(p_0)$, *for every qualified set* $A \in \Gamma$ *and,*
b) $r(A \cup \{p_0\}) = r(p_0) + r(A)$, *for every forbidden set* $A \in \Gamma^c$.

Definition 3 (Convec of a polymatroid). *The* convec *of a polymatroid $\mathcal{S} = (P \cup \{p_0\}, r)$ is defined and denoted by* $\mathrm{cv}(\mathcal{S}) = \frac{1}{r(p_0)}(r(p))_{p \in P}$.

Definition 4 (K-set). *The polymatroidal set, or K-set, of an access structure Γ, denoted by $K(\Gamma)$, is defined as the set of all convecs of all Γ-polymatroids.*

B Proof of Proposition 9.3

We first present two lemmas and then the actual proof.

Lemma B.1 *Let $\mathcal{X}_1, \mathcal{X}_2$ and $\mathcal{X}_3$ be subsets of $\mathbb{R}^n, \mathbb{R}^m$, and $\mathbb{R}^{n+m-1}$, respectively, and let $i \in [n]$. Suppose that each $\mathcal{X}_j$, $j = 1, 2, 3$, has the shifted orthant inclusion property and lies in the positive orthant (i.e., $\mathcal{X}_j \subseteq [\mathbf{0}, \infty)$). Then, $\inf_{\mathrm{P}}(\mathcal{X}_1) \Diamond_i \inf_{\mathrm{P}}(\mathcal{X}_2) \subseteq \overline{\mathcal{X}_3}$ implies $\overline{\mathcal{X}_1} \Diamond_i \overline{\mathcal{X}_2} \subseteq \overline{\mathcal{X}_3}$.*

Proof. This direcly follows form the relation $\overline{\mathcal{X}_j} = \bigcup_{\boldsymbol{a} \in \inf_{\mathrm{P}}(\mathcal{X}_j)} [\boldsymbol{a}, \infty)$, $j = 1, 2, 3$.

Lemma B.2 *Let Γ_1 and Γ_2 be two access structures on disjoint participant sets. Let $p_i \in P(\Gamma_1)$ and define $\Gamma_3 = \Gamma_1 \Diamond_{p_i} \Gamma_2$. Let Π_1 and Π_2 be two secret sharing schemes, each with uniform distribution on the secret and each individual share, respectively realizing Γ_1 and Γ_2, with $\mathrm{cv}(\Pi_1) = \boldsymbol{x}$ and $\mathrm{cv}(\Pi_2) = \boldsymbol{y}$. Then, there exists a sequence $\{\Pi_3^j\}_{j \in \mathbb{N}}$ of secret sharing schemes such that:*

(1) Π_3^j realizes Γ_3, for every $j \in \mathbb{N}$,
(2) the sequence $\{\mathrm{cv}(\Pi_3^j)\}_{j \in \mathbb{N}}$ converges to $\boldsymbol{x} \Diamond_{p_i} \boldsymbol{y}$ when j goes to infinity.

Proof. Let us first introduce the notation $k \times \Pi$, where Π is a secret sharing scheme with secret space $\mathcal{S}$. The secret space of $k \times \Pi$ is $\mathcal{S}^k$ and to share a secret $(s_1, \ldots, s_k)$ using $k \times \Pi$, each s_i is shared among participants using an independent instance of Π. Consequently, every participant receives a share for each s_i.

Let $P(\Gamma_1) = P$ and $P(\Gamma_2) = Q$. Denote $\Pi_1 = (\boldsymbol{S}_{p_i})_{p_i \in P \cup \{p_0\}}$ and $\Pi_2 = (\boldsymbol{S}_q)_{q \in Q \cup \{q_0\}}$. Let $\mathcal{S}_{p_i} = \mathrm{supp}(\boldsymbol{S}_{p_i})$ and $\mathcal{S}_{q_0} = \mathrm{supp}(\boldsymbol{S}_{q_0})$ and, without loss of generality, suppose that $|\mathcal{S}_{p_i}| \leqslant |\mathcal{S}_{q_0}|$.

For every $j \in \mathbb{N}$, define $\alpha_j = \lfloor \frac{j \log |\mathcal{S}_{q_0}|}{\log |\mathcal{S}_{p_i}|} \rfloor$ and let $\alpha_j \times \Pi_1 = (\boldsymbol{S}_{p_i}^j)_{p_i \in P \cup \{p_0\}}$ and $j \times \Pi_2 = (\boldsymbol{S}_q^j)_{q \in P \cup \{q_0\}}$. Note that $|\mathrm{supp}(\boldsymbol{S}_{p_i}^j)| \leqslant |\mathrm{supp}(\boldsymbol{S}_{q_0}^j)|$, since $|\mathrm{supp}(\boldsymbol{S}_{p_i}^j)| = |\mathcal{S}_{p_i}|^{\alpha_j}$, $|\mathrm{supp}(\boldsymbol{S}_{q_0}^j)| = |\mathcal{S}_{q_0}|^j$ and $\alpha_j \geqslant 1$. Therefore, there exists an injection $g : \mathrm{supp}(\boldsymbol{S}_{p_i}^j) \to \mathrm{supp}(\boldsymbol{S}_{q_0}^j)$.

For each $j \in \mathbb{N}$, we construct the secret sharing scheme Π_3^j, satisfying (1) and (2), as follows.

Let $P_{-p} = P \backslash \{p_i\}$ and $P(\Gamma_3) = T$, where $T = P_{-p} \cup Q$. To generate a sample $(s_t)_{t \in T \cup \{t_0\}}$ according to Π_3^j, we first generate a sample $(s_{p_i})_{p_i \in P \cup \{p_0\}}$ according to $\alpha_j \times \Pi_1$. We let $s_{t_0} = s_{p_0}$, that is, the same secret is used. Each participant $p_i \in P_{-p}$ (as a participant of $P(\Gamma_3)$) receives s_p as his share, which is trivially distributed according to $\boldsymbol{S}_{p_i}^j$. Then, $g(s_{p_i})$ is shared using the scheme $j \times \Pi_2$ to produce the shares $(s_q)_{q \in Q}$. Each participant $q \in Q$ (as a participant of $P(\Gamma_3)$) receives s_q as his share, which according to Lemma 2.2, is distributed as $\boldsymbol{S}_q^j$, assuming that Γ_2 does not contain singleton sets; that is, no participant is qualified on its own (it is easy to remove this assumption and we leave it to the reader). Clearly, the scheme Π_3^j realizes Γ_3 and its convec is:

$$\mathrm{cv}(\Pi_3^j) = \boldsymbol{x} \Diamond_{p_i} \Big(\frac{\mathrm{H}(\boldsymbol{S}_{q_0}^j)}{\mathrm{H}(\boldsymbol{S}_{p_i}^j)} \boldsymbol{y} \Big) \ .$$

Since $\mathrm{H}(\boldsymbol{S}_{q_0}^j) = j \log |\mathcal{S}_{q_0}|$ and $\mathrm{H}(\boldsymbol{S}_{p_i}^j) = \alpha_j \log |\mathcal{S}_{p_i}|$, it follows that $\frac{\mathrm{H}(\boldsymbol{S}_{q_0}^j)}{\mathrm{H}(\boldsymbol{S}_{p_i}^j)}$ $(= \frac{j \log |\mathcal{S}_{q_0}|}{\alpha_j \log |\mathcal{S}_{p_i}|})$ converges to one. Consequently, $\mathrm{cv}(\Pi_3^j)$ converges to $\boldsymbol{x} \Diamond_{p_i} \boldsymbol{y}$. □

Proof (Proof of Proposition 9.3). By Lemma B.1, it is sufficient to prove that

$$\inf_{\mathrm{P}}\big(\Sigma(\Gamma_1)\big) \Diamond_{p_i} \inf_{\mathrm{P}}\big(\Sigma(\Gamma_2)\big) \subseteq \overline{\Sigma(\Gamma_1 \Diamond_{p_i} \Gamma_2)} \ .$$

Equivalently, we prove that for every $\boldsymbol{x} \in \inf_{\mathrm{P}}\big(\Sigma(\Gamma_1)\big)$ and $\boldsymbol{y} \in \inf_{\mathrm{P}}\big(\Sigma(\Gamma_2)\big)$ it holds that $\boldsymbol{x} \Diamond_{p_i} \boldsymbol{y} \in \overline{\Sigma(\Gamma_1 \Diamond_{p_i} \Gamma_2)}$. To prove this, we show that there exists a sequence $\{\Pi_3^{j,k}\}_{(j,k) \in \mathbb{N} \times \mathbb{N}}$ of secret sharing schemes such that:

(1') $\Pi_3^{j,k}$ realizes $\Gamma_3 = \Gamma_1 \Diamond_{p_i} \Gamma_2$, for every $j, k \in \mathbb{N}$,
(2') the sequence $\{\mathrm{cv}(\Pi_3^{j,k})\}$ converges to $\boldsymbol{x} \Diamond_{p_i} \boldsymbol{y}$ when j, k both go to infinity.

Assuming that the USD conjecture is true, there exists a sequence $\{\Pi_1^k\}_{k\in\mathbb{N}}$ (resp. $\{\Pi_2^k\}_{k\in\mathbb{N}}$) of secret sharing schemes, with uniform distributions on secrets and individual shares, realizing Γ_1 (resp. Γ_2), such that the sequences $\{\boldsymbol{x}_k\}_{k\in\mathbb{N}} = \{\mathrm{cv}(\Pi_1^k)\}_{k\in\mathbb{N}}$ (resp. $\{\boldsymbol{y}_k\}_{k\in\mathbb{N}} = \{\mathrm{cv}(\Pi_2^k)\}_{k\in\mathbb{N}}$) converge to $\boldsymbol{x}$ (resp. $\boldsymbol{y}$).

Consequently, for each $k \in \mathbb{N}$, according to Lemma B.2, there exists a sequence $\{\Pi_3^{j,k}\}_{j\in\mathbb{N}}$ of secret sharing schemes such that:

(1") $\Pi_3^{j,k}$ realizes $\Gamma_3 = \Gamma_1 \Diamond_{p_i} \Gamma_2$, for every $j \in \mathbb{N}$,
(2") the sequence $\{\mathrm{cv}(\Pi_3^{j,k})\}_{j\in\mathbb{N}}$ converges to $\boldsymbol{x}_k \Diamond_{p_i} \boldsymbol{y}_k$ when j goes to infinity.

Therefore, (1') and (2') also hold, finishing the proof. □

C USD cojecture for quasi-total security

Even though it remains open if the USD conjecture holds true for the total security or even the statistical relaxation, in this section we prove that it holds true for another relaxation called quasi-total security defined by Kaced in [33,34].

We first present two definitions and then define the notion of quasi-total secret sharing and quasi-total convec set.

Definition C.1 (Convec-converging family of schemes) *A sequence $\mathcal{F} = \{\Pi_k\}_{k\in\mathbb{N}}$ of secret sharing schemes on participants set P is called a* convec-converging family of schemes *if i) the entropy of secret does not vanish; i.e., $\mathrm{H}(\boldsymbol{S}_0^k) = \Omega(1)$ and, ii) the sequence $\{\mathrm{cv}(\Pi_k)\}_{k\in\mathbb{N}}$ is converging. The convec of the convec-converging family $\mathcal{F}$ is defined as*

$$\mathrm{cv}(\mathcal{F}) = \lim_{k\to\infty} \mathrm{cv}(\Pi_k) \ .$$

Definition C.2 (Access function of a secret sharing scheme [23]) *The* access function *of a secret sharing scheme $\Pi = \big(\boldsymbol{S}_i\big)_{i\in P\cup\{p_0\}}$ is a a (monotone) mapping $\Phi_\Pi : 2^P \to [0,1]$ defined as follows:*

$$\Phi_\Pi : A \to \frac{\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A)}{\mathrm{H}(\boldsymbol{S}_0)} \ .$$

Definition C.3 (Quasi-total realization) *Let Γ be an access structure on P and $\mathcal{F} = \{\Pi_k\}_{k\in\mathbb{N}}$ be a convec-converging family of secret sharing schemes. We say that $\mathcal{F}$ is a quasi-total family for Γ if $\lim_{k\to\infty} \Phi_{\Pi_k} = \Phi_\Gamma$, where $\Phi_\Gamma : 2^P \to \{0,1\}$ is a (monotone) mapping defined as $\Phi_\Gamma(A) = 1 \iff A \in \Gamma$.*

Definition C.4 (Quasi-total convec sets) *The quasi-total convec set of an access structure Γ, denoted by $\Sigma_{\mathrm{qt}}(\Gamma)$, is defined as the set of all convecs of all quasi-total families for Γ. When we restrict ourselves to the class $\mathcal{C}$ of secret sharing schemes, we use the notation $\Sigma_{\mathrm{qt}}^{\mathrm{C}}$.*

Notice that unlike the total security, the quasi-total convec sets are closed. We are interested in the quasi-total convec set for the restricted class of group-characterizable secret sharing schemes, denoted by $\Sigma_{\mathrm{qt}}^{\mathrm{G}}$.

Definition C.5 (Group-characterizable scheme) *A secret sharing scheme $\Pi = \big(\boldsymbol{S}_p\big)_{p\in P\cup\{p_0\}}$ is said to be* group-characterizable *if there exists a finite group G and subgroups G_p's of G such that, for every $p \in P \cup \{p_0\}$, we have $\boldsymbol{S}_p = \boldsymbol{X}G_p$ where $\boldsymbol{X}$ is a uniform random variable with support G and $\boldsymbol{X}G_p$ is a random variable whose support is the left cosets of G_p.*

For the case of total security, it remains open if the inclusion $\overline{\Sigma^{\mathrm{G}}(\Gamma)} \subseteq \overline{\Sigma(\Gamma)}$ is proper for some access structure Γ. The following theorem, whose proof follows from a well-known theorem by Chan and Yeung in [16], asserts that the answer is negative for quasi-total security; that is group-characterizable schemes are "complete" for this security notion.

Proposition C.6 ($\boldsymbol{\Sigma^{\mathrm{G}}_{\mathrm{qt}} = \Sigma_{\mathrm{qt}}}$) *Group characterizable schemes are complete for quasi-total security. That is for every access structure Γ, it holds that $\Sigma^{\mathrm{G}}_{\mathrm{qt}}(\Gamma) = \Sigma_{\mathrm{qt}}(\Gamma)$.*

Proof. The Chan-Yeung's theorem [16, Theorem 4.1] is about random variables and can be stated for secret sharing schemes as follows: for every scheme $\Pi = (\boldsymbol{S}_i)_{i\in P\cup\{p_0\}}$, there exists a sequence $\{\Pi_k\}$ of group-characterizable schemes, with $\Pi_k = (\boldsymbol{S}^k_i)_{i\in P\cup\{p_0\}}$, such that for every $A \subseteq P \cup \{p_0\}$ it holds that $\lim_{k\to\infty} \frac{1}{k}\mathrm{H}(\boldsymbol{S}^k_A) = \mathrm{H}(\boldsymbol{S}_A)$. It then follows that $\lim_{k\to\infty} \mathrm{cv}(\Pi_k) = \mathrm{cv}(\Pi)$ and $\lim_{k\to\infty} \Phi(\Pi_k) = \Phi(\Pi)$.

Now we return to the proof of our theorem. Let Γ be an access structure and $\boldsymbol{\sigma} \in \Sigma_{\mathrm{qt}}(\Gamma)$. We need to show that $\boldsymbol{\sigma} \in \Sigma^{\mathrm{G}}_{\mathrm{qt}}(\Gamma)$. Let $\mathcal{F} = \{\Pi_m\}_{m\in\mathbb{N}}$ be a quasi-total family for Γ with $\mathrm{cv}(\mathcal{F}) = \boldsymbol{\sigma}$. Therefore, by Chan-Yeung's theorem, for each scheme Π_m, there exists a a sequence $\{\Pi_{k,m}\}$ of group-characterizable schemes such that $\lim_{k\to\infty} \mathrm{cv}(\Pi_{k,m}) = \mathrm{cv}(\Pi_m)$ and $\lim_{k\to\infty} \Phi(\Pi_{k,m}) = \Phi(\Pi_m)$. It is then easy to see that the family $\mathcal{F}' = \{\Pi_{j,j}\}$ of group-characterizable schemes satisfies $\mathrm{cv}(\mathcal{F}') = \lim_{j\to\infty} \mathrm{cv}(\Pi_{j,j}) = \mathrm{cv}(\mathcal{F})$ and $\lim_{k\to\infty} \Phi_{\Pi_{j,j}} = \Phi_\Gamma$; that is, $\boldsymbol{\sigma} \in \Sigma^{\mathrm{G}}_{\mathrm{qt}}(\Gamma)$. □

Even though the USD conjecture was left open in the case of total security, the following is an immediate corollary of Proposition C.6, since the distribution of secret is uniform for group-characterizable schemes by definition.

Corollary C.7 (USD & quasi-total) *The USD conjecture holds for the quasi-total security.*

It can be shown that statistical security implies quasi-total security [**?**]. The total security also trivially implies the statistical security; i.e., $\overline{\Sigma(\Gamma)} \subseteq \Sigma_{\mathrm{s}}(\Gamma \subseteq \Sigma_{\mathrm{qt}}(\Gamma)$. It is open if all convec sets coincide. In particular, it remains open if the USD conjecture holds for total and statistical security notions.

Question C.8 (USD & total/statistical) *Prove or refute if the USD conjecture holds for the total or statistical security notions.*