Conjecturally Superpolynomial Lower Bound for Share Size

Shahram Khazaei

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

Abstract. Information ratio, which measures the maximum/average share size per shared bit, is a criterion of efficiency of a secret sharing scheme. 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 incompetently $\Omega(n/\log n)$. Closing this gap is a long-standing open problem in cryptology.
In this paper, using a technique called *substitution*, we recursively construct a family of access structures having information ratio $n^{\Omega(\frac{\log n}{\log\log n})}$, assuming a well-stated information-theoretic conjecture is true. Our conjecture emerges after introducing the notion of *convec set* for an access structure, a subset of n-dimensional real space. We prove several topological properties about convec sets and raise several open problems.
Key words: secret sharing, general access structure, information ratio, perfect security

1 Introduction

A *secret sharing scheme* [32,8] is a powerful cryptographic tool that allows a dealer to share a secret among a set of n participants such that only certain *qualified* subsets of participants are able to reconstruct the secret. The secret must remain information theoretically hidden from the remaining subsets, called *forbidden*. The collection of all qualified subsets is called an *access structure*, which is supposed to be monotone, i.e., closed under the superset operation. The original definition, known as *threshold* secret sharing, only dealt with access structures that include all subsets of size larger than a certain threshold and the general notion was later introduced in [20].

The *information ratio* [12,9,25] 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., [11,31,33,26,27]), 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 (for example, see [35,21]) is still open while very few cases have been resolved (see [19,17] for two notable examples).

It is known that every access structure on n participants admits a secret sharing scheme with information ratio $2^{\mathrm{O}(n)}$ and it is generally believed that this upper bound is tight for most access structures. See [23] for a recent result towards achieving a lower bound on the portion of access structures with superpolynomial share size. Particularly, it is conjectured (e.g., see [3]) 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 [16] (earlier presented in [14]) and average [15] 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 [22,13] based on *Shannon type information inequalities*, cannot be used to show a superlinear lower bound. This negative result was further strengthened in [7,28] by showing that certain additional *non-Shannon type* information inequalities [38] 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 *linear* secret-sharing schemes, however, the lower bound has recently been shown to be exponential [30], closing the gap with the former superpolynomial lower bound $n^{\Omega(\log n)}$ [1,4].

1.1 Our main result

We take one step towards beating Csirmaz infamous lower bound. We construct a family of access structures having information ratio $n^{\Omega(\frac{\log n}{\log\log n})}$ under some information-theoretic conjecture, called *substitution conjecture* which will be introduced in this paper. A *lifting theorem*, useful for boosting the information ratio of a well-chosen family of access structures, lies at the heart of our improvement. Below, we present a simplified and informal statement of the theorem.

Theorem 1 (Lifting theorem—informal and simplified). *Let $b, t : \mathbb{R}^+ \to \mathbb{R}^+$ be two 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, has a subset of participants of size $b(n_k)$ with minimum total share size $t(n_k)$. Assuming that the function $\frac{\log t(x)}{\log b(x)}$ satisfies some "mild" conditions and assuming the truth of the substitution conjecture, then there exists a family of access structures with average (and consequently maximum) information ratio $n^{\Omega\left(\frac{\log t(n)}{\log b(n)}\right)}$.*

Csirmaz proves his $\Omega(n/\log n)$ lower bound on maximum information ratio, by constructing a family of access structures [16] and exhibiting a subset of participants of size $b(n) = \Theta(\log n)$ with minimum total share size $t(n) = \Omega(n)$. Our (conjecturally) improved $n^{\Omega(\frac{\log n}{\log\log n})}$ lower bound for average/maximum information ratio is achieved by a simple application of the lifting theorem to his family.

1.2 Main ideas

We use three main ideas in this paper:

- **Reintroducing the 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 $\Gamma_3 = \Gamma_1[b \to \Gamma_2] = a(a' + b'c') + (a' + b'c')cd = aa' + ab'c' + a'cd + b'c'cd$. This concept has already been introduced by Martin in [25] and some basic properties of the operation has also been studied. We are interested in the relation between information ratio of the three involved access structures.
- **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 *convec set*, where convec is short for contribution vector [21]. 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 [37] framework for studying the so called *entropy region*.

– **Connecting the two notions via the substitution conjecture.** As we mentioned above, our lifting theorem relies on a conjecture that we refer to as the *substitution conjecture*. This conjecture links the notions of access structure substitution and convec set. In addition to the notion of access structure substitution, a relevant notion of *set substitution* can be defined for two subsets $\mathcal{X}_1 \subset \mathbb{R}^n$ and $\mathcal{X}_2 \subset \mathbb{R}^m$ with respect to some specific coordinate $i \in [n]$, which results in the subset $\mathcal{X}_3 = \mathcal{X}_1[i \to \mathcal{X}_2] \subset \mathbb{R}^{n+m-1}$. The two substitution operations (one on access structures and one on subsets of multi-dimensional real space) seem so coherent leading us to state the substitution conjecture as follows.

  Conjecture 1 (Substitution conjecture) *Let Γ_1 and Γ_2 be two access structures and let $\Gamma_3 = \Gamma_1[p_i \to \Gamma_2]$ for some participant p_i of Γ_1. Let $\mathcal{X}_j$ denote the closure of the convec set of Γ_j for $j = 1, 2, 3$. Then, $\mathcal{X}_1[i \to \mathcal{X}_2] = \mathcal{X}_3$, where index $i \in [n]$ corresponds to the coordinate of the information ratio of participant p_i in $\mathcal{X}_1 \subset \mathbb{R}^n$.*

  Proving the inclusion $\mathcal{X}_3 \subseteq \mathcal{X}_1[i \to \mathcal{X}_2]$ remains challengingly open and the lifting theorem relies only on the truth of this inclusion. Even though the reverse inclusion also remains open, we prove it under a second conjecture called *Uniform Share Distribution (USD) conjecture*. Informally, this conjecture states that, for every access structure, the optimal information ratio is achieved by a secret sharing scheme (or a converging sequence of schemes) with uniform distribution on the shares.

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 technique for access structures and subsets of multi-dimensional real space, as well as the substitution and USD conjectures, are given in Section 4. In Section 5, we prove our lifting theorem after introducing a recursive method for constructing new access structures using the substitution technique. Finally, we conclude the paper in Section 6.

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 [3,29] 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 1, Lemma 1 and Convension 1.

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 $\mathrm{cl}(\mathcal{X})$, is the union of $\mathcal{X}$ with all its limit points. When $\mathrm{cl}(\mathcal{X})$ 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., $\mathrm{cl}(\mathcal{X})\backslash\mathrm{int}(\mathcal{X})$. In this paper, we define the *frontier* of $\mathcal{X}$ as the set $\mathrm{cl}(\mathcal{X})\backslash\mathcal{X}$.

Remark 1 (Frontier vs. boundary) *In the literature the boundary is also referred to as frontier and some authors (for example [36]) even use the term frontier instead of boundary. However, similar to [2], 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

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. The set of all important participants of access structure Γ is denoted by $P(\Gamma)$. 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 $\Gamma = \sum_{A\in\Gamma^-}\prod_{p\in A} p$.

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*. 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 $\boldsymbol{S}_{p_0} = s$.

We say that Π is a secret sharing scheme for Γ, or Π *realizes* Γ, or Γ *admits* Π, when:

a) $\mathrm{H}(\boldsymbol{S}_{p_0} \mid \boldsymbol{S}_A) = 0$, for every qualified set $A \in \Gamma$ and,

b) $\mathrm{H}(\boldsymbol{S}_{p_0} \mid \boldsymbol{S}_B) = \mathrm{H}(\boldsymbol{S}_{p_0})$, for every forbidden set $B \in \Gamma^c$.

where $\boldsymbol{S}_A = (\boldsymbol{S}_p)_{p\in A}$, for a subset $A \subseteq P$.

The *information ratio* of participant $p_i \in P$ is defined as $\sigma_i = \mathrm{H}(\boldsymbol{S}_{p_i})/\mathrm{H}(\boldsymbol{S}_{p_0})$. The *convec* of Π (where convec is abbreviation for *contribution vector* [21]) is defined and denoted by $\boldsymbol{\sigma}(\Pi) = (\sigma_i)_{i\in[n]}$. A secret sharing scheme Π is called ideal if $\boldsymbol{\sigma}(\Pi) = \mathbf{1}$.

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 $\max\big(\boldsymbol{\sigma}(\Pi)\big)$ (resp. $\frac{1}{n}\|\boldsymbol{\sigma}(\Pi)\|$) over all secret sharing schemes Π realizing Γ.

We close this section by introducing a lemma by Blundo *et. al.* [10] and a convention regarding our notation.

Lemma 1 ([10]). *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 $A \in \Gamma^c$.*

Convention 1 *We assume that all participants of all access structures are important. For such access structures, the information ratio of each participant is at least one [22,13]. Also, we assume that our access structures do not contain singleton sets; that is, no participant is qualified on its own. Consequently, when the distribution on the secret changes, the distribution on each individual's share does not change (see Lemma 1).*

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

For our convenience, we provide the following definition.

Definition 2 (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 $[\boldsymbol{a}, \infty) \subseteq \mathcal{X}$.*

3.1 Basic properties of convec sets

In this section we provide three lemmas about the properties of convec sets, which will be of use in later sections. The first one follows from the well-known result of [22,13], stating that each (important) participant's share size is not smaller than the secret itself. The second one says that the convec sets have the shifted orthant inclusion property. The last one states that the convec sets remain unchanged if we restrict ourselves to secret sharing schemes with uniform secret distribution.

Lemma 2 (A trivial superset for convec sets). *We have $\Sigma(\Gamma) \subseteq [\mathbf{1}, \infty)$, for any access structure Γ.*

Lemma 3 (Shifted orthant inclusion property of convec sets). *For any access structure Γ, the set $\Sigma(\Gamma)$ has the shifted orthant inclusion property.*

Proof. Let $\boldsymbol{a} \in \Sigma(\Gamma)$. 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 $\boldsymbol{\sigma}(\Pi) = \boldsymbol{a}$, it is easy to construct a secret sharing scheme Π' for Γ with $\boldsymbol{\sigma}(\Pi') = \boldsymbol{a}'$; 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 $\boldsymbol{\sigma}(\Pi') = \boldsymbol{a}'$; hence, $\boldsymbol{a}' \in \Sigma(\Gamma)$. □

Lemma 4 (Uniform secret invariance property of convec sets). *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.

By Lemma 1 (see also Convention 1), 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 $p \in P$.

Consequently, $\boldsymbol{a}'' = \boldsymbol{\sigma}(\Pi'') = \frac{\mathrm{H}(\boldsymbol{S}_{p_0})}{\mathrm{H}(\boldsymbol{S}''_{p_0})}\boldsymbol{a} \preceq \boldsymbol{a}$; that is, $\boldsymbol{a} \in [\boldsymbol{a}'', \infty)$. We can then construct Π', realizing Γ with $\boldsymbol{\sigma}(\Pi') = \boldsymbol{a}$, from Π'' similar to the proof of the shifted orthant inclusion property (Lemma 3), by increasing each participant's share size, without changing secret distribution. □

3.2 On interiors of convec sets

In this section, we prove a proposition, showing that the interiors of convec sets are convex. First, we present two lemmas, and then the proposition.

Lemma 5 (Closure convexity of convec sets). *The convec set of any access structure is a set with a convex closure.*

Proof. Let Γ be an access structure on participant set P. Equivalently, we prove the following claim. For every real number $x \in [0,1]$, and every pair of vectors $\boldsymbol{a}, \boldsymbol{b} \in \mathrm{cl}(\Sigma(\Gamma))$, there is a sequence $\{\Pi_j\}$ of secret sharing schemes such that: 1) each Π_j realizes Γ, 2) the sequence $\{\boldsymbol{\sigma}(\Pi_j)\}$ converges to $x\boldsymbol{a} + (1-x)\boldsymbol{b}$.

It is sufficient to prove the claim for convecs $\boldsymbol{a}, \boldsymbol{b} \in \Sigma(\Gamma)$. Let $\Pi_{\mathrm{a}} = \big(\boldsymbol{A}_p\big)_{p \in P \cup \{p_0\}}$ and $\Pi_{\mathrm{b}} = \big(\boldsymbol{B}_p\big)_{p \in P \cup \{p_0\}}$ be secret sharing schemes realizing Γ with convecs $\boldsymbol{a}$ and $\boldsymbol{b}$, respectively. For each j, we construct a secret sharing Π_j satisfying the required properties.

Assume that $x = c/d$ is rational, the secret random variables $\boldsymbol{A}_{p_0}$ and $\boldsymbol{B}_{p_0}$ are both uniform, and $|\mathrm{supp}(\boldsymbol{A}_{p_0})| = |\mathrm{supp}(\boldsymbol{B}_{p_0})|$. In this situation, Π_j can be simply constructed by Stinson's λ-decomposition technique [34] by using c instances of Π_{a} and $d-c$ instances of Π_{b} (i.e., $\lambda = d$). It is easy to remove the uniform distribution assumption on the secret, thanks to Lemma 1, and extend this argument to the case where the ratio $y = \mathrm{H}(\boldsymbol{A}_{p_0})/\mathrm{H}(\boldsymbol{B}_{p_0})$ is rational. The remaining part of the proof is devoted to handle the general case.

Let $\{x_j\}, \{y_j\}$ be two sequences of non-negative rational numbers respectively converging to x and y. Let $x_j = c_j/d_j$ and $y_j = e_j/f_j$ where c_j, d_j, e_j, f_j are non-negative integers. The secret sharing scheme $\Pi_j = \big(\boldsymbol{S}_p\big)_{p \in P \cup \{p_0\}}$ is constructed as follows. Consider a matrix of random variables with $f_j c_j + e_j(d_j - c_j)$ rows and $|P| + 1$ columns. Each column is labeled with an element of $P \cup \{p_0\}$ and all rows are independent random variables. The top $f_j c_j$ rows are identically distributed as Π_{a} and the bottom $e_j(d_j - c_j)$ rows are identically distributed as Π_{b}. For each $p \in P \cup \{p_0\}$, the random variable $\boldsymbol{S}_p$ is defined to be the column with label p. It is

easy to see that Π_j realizes Γ. We continue to show that $\boldsymbol{\sigma}(\Pi_j)$ converges to $x\boldsymbol{a} + (1-x)\boldsymbol{b}$. By independence of the random variables, we have $\mathrm{H}(\boldsymbol{S}_p) = f_j c_j \mathrm{H}(\boldsymbol{A}_p) + e_j(d_j - c_j)\mathrm{H}(\boldsymbol{B}_p)$, for every $p \in P \cup \{p_0\}$. Therefore,

$$\begin{aligned}\frac{\mathrm{H}(\boldsymbol{S}_p)}{\mathrm{H}(\boldsymbol{S}_{p_0})} &= \frac{f_j c_j \mathrm{H}(\boldsymbol{A}_p) + e_j(d_j - c_j)\mathrm{H}(\boldsymbol{B}_p)}{f_j c_j \mathrm{H}(\boldsymbol{A}_{p_0}) + e_j(d_j - c_j)\mathrm{H}(\boldsymbol{B}_{p_0})} \\ &= \frac{x_j}{x_j + (1-x_j)y_j/y}\frac{\mathrm{H}(\boldsymbol{A}_p)}{\mathrm{H}(\boldsymbol{A}_{p_0})} + \frac{(1-x_j)}{x_j y/y_j + (1-x_j)}\frac{\mathrm{H}(\boldsymbol{B}_p)}{\mathrm{H}(\boldsymbol{B}_{p_0})} \ .\end{aligned}$$

or more compactly,

$$\boldsymbol{\sigma}(\Pi_j) = \frac{x_j}{x_j + (1-x_j)y_j/y}\boldsymbol{a} + \frac{(1-x_j)}{x_j y/y_j + (1-x_j)}\boldsymbol{b} \ ,$$

which clearly converges to $x\boldsymbol{a} + (1-x)\boldsymbol{b}$, concluding the claim. □

Lemma 6. *Let $\mathcal{X} \subseteq \mathbb{R}^n$ be a set with a convex closure, having the shifted orthant inclusion property. Then, the interior of $\mathcal{X}$ is convex.*

Proof. We show that $\mathrm{int}(\mathcal{X}) = \mathrm{int}(\mathrm{cl}(\mathcal{X}))$. The claim then follows since the interior of any convex set is convex as well. Obviously, $\mathrm{int}(\mathcal{X}) \subseteq \mathrm{int}(\mathrm{cl}(\mathcal{X}))$. Therefore, it is sufficient to show that $\mathrm{int}(\mathrm{cl}(\mathcal{X})) \subseteq \mathrm{int}(\mathcal{X})$. Let $\boldsymbol{b} \in \mathrm{int}(\mathrm{cl}(\mathcal{X}))$. Equivalently, we show that $\boldsymbol{b} \in \mathrm{int}(\mathcal{X})$. Let $B \subseteq \mathrm{cl}(\mathcal{X})$ be an open ball that contains $\boldsymbol{b}$. Let $\boldsymbol{a} \in B$ be a point which is element-wise strictly smaller than $\boldsymbol{b}$, i.e, $\boldsymbol{a} \prec \boldsymbol{b}$. Since $\boldsymbol{a} \in \mathrm{cl}(\mathcal{X})$, there exists a sequence $\boldsymbol{a}_0, \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots$ of points in $\mathcal{X}$ belonging to the open set $\{\boldsymbol{x} \mid \boldsymbol{x} \prec \boldsymbol{b}\} \cap B$ and converging to $\boldsymbol{a}$. Since $\boldsymbol{a}_0 \in \mathcal{X}$, by the shifted orthant inclusion property of the set, we have $[\boldsymbol{a}_0, \infty) \subset \mathcal{X}$. Clearly, $\{\boldsymbol{x} \mid \boldsymbol{a}_0 \prec \boldsymbol{x}\} \cap B$ is an open convex set that contains $\boldsymbol{b}$ and is completely contained in $\mathcal{X}$. Therefore, $\boldsymbol{b} \in \mathrm{int}(\mathcal{X})$. □

Proposition 1 (Interior convexity of convec sets). *The interior of the convec set of any access structure is convex.*

Proof. Recall the shifted orthant inclusion (Lemma 3) and closure convexity (Lemma 5) properties of convec sets. The claim is then an immediate consequence of Lemma 6. □

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 7 (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 $\Gamma = \Gamma_1 + p\Gamma_2$, where Γ_1, Γ_2 are access structures both on the participant set $P' = P \backslash \{p\}$. More precisely, $\Gamma_1 = \{A \subseteq P' \mid A \in \Gamma\}$ and $\Gamma_2 = \{A \subseteq P' \mid A \notin \Gamma, A \cup \{p\} \in \Gamma\}$. It is well-known that every access structure admits a secret sharing scheme over $\mathbb{Z}_m$ [20]. Let Π_1, Π_2 be, respectively, such secret sharing schemes for Γ_1, Γ_2. 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 $s + r$ to p. Then, we share the randomness r as a secret using the scheme Π_1 and share the secret s using the scheme Π_2. Consequently, every participant in P' receives a share from each of the schemes. Clearly, the resulting scheme realizes Γ and the information ratio of participant p is one. □

Proposition 2 (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. According to Lemma 2, we have $\Sigma(\Gamma) \subseteq [\mathbf{1}, \infty)$. Also, according to Lemma 7, 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 (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 1 (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 $\boldsymbol{a} \in \mathrm{cl}(\mathcal{X})$ is said to be *Pareto-infimal* for $\mathcal{X}$ if it is Pareto-minimal for $\mathrm{cl}(\mathcal{X})$. 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 $\inf_{\mathrm{P}}(\mathcal{X}) = \min_{\mathrm{P}}\big(\mathrm{cl}(\mathcal{X})\big)$.

Definition 4 (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) 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 2. *We have $\mathrm{cl}(\Sigma(\Gamma)) = \bigcup_{\boldsymbol{x} \in \inf_{\mathrm{P}}\left(\Sigma(\Gamma)\right)} [\boldsymbol{x}, \infty)$, 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 2. 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 5 (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., $\boldsymbol{\sigma}(\Pi) \in \min_{\mathrm{P}}\big(\Sigma(\Gamma)\big)$.*

Corollary 3 (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 1 ($\mathcal{P}_3$ access structure) *Consider the graph access structure $\mathcal{P}_3 = ab+bc+cd$, i.e., a path of length 3. It can be shown [13] that $\mathrm{cl}(\Sigma(\mathcal{P}_3))$ 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 [34]) 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 6).*

Example 2 ($\mathcal{F} \cdot \overline{\mathcal{F}}$ access structure) *Beimel-Livne [5,6] and Matús [27] have independently introduced an access structure on 12 participants, which we denote by $\mathcal{F} \cdot \overline{\mathcal{F}}$ (see also Example 3 and Figure 1). In the Sperner system, the minimal representation of $\mathcal{F} \cdot \overline{\mathcal{F}}$ 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

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

derived form Fano and non-Fano matroids, respectively.

Matús [27] has proved that $\mathcal{F}$ (resp. $\overline{\mathcal{F}}$) does not have an ideal scheme when the secret space size is odd (resp. even). The access structure $\mathcal{F} \cdot \overline{\mathcal{F}}$ is called nearly ideal *since while it is not ideal [27], its information ratio is one [5,6]; that is, the all-one vector is Pareto-infimal but not Pareto-minimal. Therefore, $\mathcal{F} \cdot \overline{\mathcal{F}}$ is a NONC access structure and $\mathrm{cl}(\Sigma(\mathcal{F} \cdot \overline{\mathcal{F}})) = [\mathbf{1}, \infty)$. The results of [5,6] can be used to show that $\Sigma(\mathcal{F} \cdot \overline{\mathcal{F}})$ 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 7 can be used to show that $\Sigma(\mathcal{F} \cdot \overline{\mathcal{F}})$ 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 $\Sigma(\mathcal{F} \cdot \overline{\mathcal{F}})$ is unknown to us, and in particular, we do not know if $\mathcal{F} \cdot \overline{\mathcal{F}}$ has any Pareto-minimal convec (see Question 7).*

3.6 Some open problems

Several problems regarding convec sets remain open. 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 1 (Non-ideal closed access structure) *Is there a non-ideal closed access structure?*

More generally, characterizing access structures with respect to Definition 3 seems an interesting question.

Question 2 (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 1).*

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 (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 4 (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 1 and 2) can be proved to be polytopes. It is intriguing to think that this is the case for every access structure.

Question 5 (Non-polytope convec sets) *Is there an access structure such that its convec set is not a polytope?*

Finally, concerning Examples 1 and 2, we present two more specific questions in the following.

Question 6 (Convec set of $\mathcal{P}_3$) *Following Example 1, 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 7 (Convec set of $\mathcal{F} \cdot \overline{\mathcal{F}}$) *Following Example 2, determine the set $\Sigma(\mathcal{F} \cdot \overline{\mathcal{F}})$. Is it a convex set? Does it have any Pareto-minimal convec?*

Note that a positive answer to Question 6 leads to a positive answer to Question 1, while a negative answer partially answers Question 3 (i.e., there exists non-convex NONC access structures).

4 Substitution technique

In this section, we describe different notions of *substitution* for real vectors, subsets of the real space and access structures. We then propose a conjecture, referred to as the *substitution conjecture* that relates the latter two substitution operations. A second conjecture, called *Uniform Share Distribution (USD)*, is also presented, under which the substitution conjecture is partially proved. More precisely, the substitution conjecture is a statement about equality of two sets. If the USD conjecture holds, then we will show that one set includes the other one.

4.1 Vector/Subset substitution

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 ith element has been substituted with $x_i\boldsymbol{y}$, is denoted by $\boldsymbol{x}[i \to \boldsymbol{y}]$; that is,

$$\boldsymbol{x}[i \to \boldsymbol{y}] = (x_1, \ldots, x_{i-1}, x_i y_1, \ldots, x_i y_m, x_{i+1}, \ldots, x_n) \ .$$

Let $\mathcal{X} \subseteq \mathbb{R}^n$ and $\mathcal{Y} \subseteq \mathbb{R}^m$ be two arbitrary sets. For every $i \in [n]$, we define the set $\mathcal{X}[i \to \mathcal{Y}] \subseteq \mathbb{R}^{n+m-1}$ as follows:

$$\mathcal{X}[i \to \mathcal{Y}] = \{\boldsymbol{x}[i \to \boldsymbol{y}] \mid (\boldsymbol{x}, \boldsymbol{y}) \in \mathcal{X} \times \mathcal{Y}\} \ .$$

4.2 Access structure substitution

Let Γ_1 and Γ_2 be two access structures, respectively on (not necessarily disjoint) participant sets P and Q, and let $p_i \in P$. We refer to $\Gamma_3 = \Gamma_1[p_i \to \Gamma_2]$ as the access structure in which the participant p_i has been substituted with Γ_2, in the following sense. In the Sperner representation of Γ_1, we replace p_i with Γ_2 and then expand and simplify the expression naturally. This concept has already been introduced by Martin in [25] and some basic properties of the resulting access structure has been also studied. More precisely, the participant set of Γ_3 is $P(\Gamma_3) = P_{-i} \cup Q$, where $P_{-i} = P \backslash \{p_i\}$, and for every $A \subseteq P(\Gamma_3)$ we have:

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

Example 3 (Access structure substitution) *Let $\Gamma_1 = ab+ac+bc$ and $\Gamma_2 = a+cd+ce+f$. We then have $\Gamma_1[c \to \Gamma_2] = ab+a(a+cd+ce+f)+b(a+cd+ce+f) = a+bcd+bce+bf$. As another example, let $\Gamma = ab$ and $\mathcal{F}, \overline{\mathcal{F}}, \mathcal{F} \cdot \overline{\mathcal{F}}$ be as in Example 2. Then, $\Gamma[a \to \mathcal{F}][b \to \overline{\mathcal{F}}] = \mathcal{F} \cdot \overline{\mathcal{F}}$. See Figure 1.*

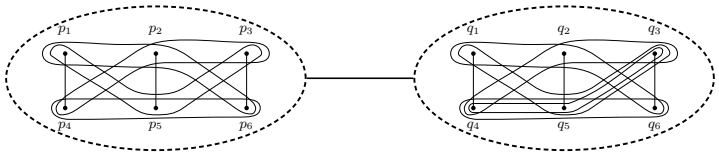


Fig. 1: The access structure $\mathcal{F} \cdot \overline{\mathcal{F}} = \Gamma[a \to \mathcal{F}][b \to \overline{\mathcal{F}}]$ where $\Gamma = ab$ (see Example 3). Also, it can be viewed as $\mathcal{F} \cdot \overline{\mathcal{F}} = \Gamma[p_7 \to \mathcal{F}]$ where $\Gamma = \mathcal{F} \cdot p_7$ (see Remark 2). See Example 2 for descriptions of $\mathcal{F}, \overline{\mathcal{F}}$ and $\mathcal{F} \cdot \overline{\mathcal{F}}$.

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

$$\begin{aligned} \mathcal{B} &= \{B \mid B \subseteq P_{-i} \wedge B \in \Gamma_1\} \ , \\ \mathcal{C} &= \{C \mid C \subseteq P_{-i} \wedge C \in \Gamma_1^c \wedge Cp_i \in \Gamma_1\} \ , \\ \mathcal{D} &= \{D \mid D \subseteq P_{-i} \wedge Dp_i \in \Gamma_1^c\} \ . \end{aligned} \tag{1}$$

It is then easy to verify that:

$$\Gamma_3 = \{BA \mid B \in \mathcal{B} \wedge A \subseteq Q\} \ \cup \{CK \mid C \in \mathcal{C} \wedge K \in \Gamma_2\} \ , \tag{2}$$

and

$$\Gamma_3^c = \{CJ \mid C \in \mathcal{C} \wedge J \in \Gamma_2^c\} \cup \{DA \mid D \in \mathcal{D} \wedge A \subseteq Q\} \ . \tag{3}$$

4.3 The substitution conjecture

Consider two access structures with disjoint participant sets and denote the closure of their convec sets by $\mathcal{X}_1$ and $\mathcal{X}_2$. Substitute the second access structure for some participant in the first one to get a third access structure, with convec set closure $\mathcal{X}_3$. We conjecture that $\mathcal{X}_1[i \to \mathcal{X}_2] = \mathcal{X}_3$, where i corresponds to the coordinate of the substituted participant in $\mathcal{X}_1$. Below we present a formal statement of this conjecture.

Conjecture 2 (Substitution conjecture) *Let Γ_1 and Γ_2 be two access structures on disjoint participant sets. Let $p_i \in P(\Gamma_1)$ and define $\Gamma_3 = \Gamma_1[p_i \to \Gamma_2]$. Let $\mathcal{X}_j = \mathrm{cl}(\Sigma(\Gamma_j))$, for $j = 1, 2, 3$ and let index $i \in [n]$ correspond to the coordinate of participant p_i in $\mathcal{X}_1 \subseteq \mathbb{R}^n$. Then, $\mathcal{X}_3 = \mathcal{X}_1[i \to \mathcal{X}_2]$; that is,*

I. $\mathcal{X}_1[i \to \mathcal{X}_2] \subseteq \mathcal{X}_3$,
II. $\mathcal{X}_3 \subseteq \mathcal{X}_1[i \to \mathcal{X}_2]$.

Remark 2 *We remark that a variant of the substitution conjecture in which we let $\mathcal{X}_i = \Sigma(\Gamma_i)$ is not valid. Towards constructing a counter example, let $\mathcal{F}, \overline{\mathcal{F}}, \mathcal{F} \cdot \overline{\mathcal{F}}$ be as in Example 2. Let $\Gamma_1 = \mathcal{F} \cdot p_7$ and $\Gamma_2 = \overline{\mathcal{F}}$ and hence $\Gamma_3 = \Gamma_1[p_7 \to \Gamma_2] = \mathcal{F} \cdot \overline{\mathcal{F}}$. The access structures Γ_1 and Γ_2 are both ideal, respectively on 7 and 6 participants. Therefore, $\mathcal{X}_1[7 \to \mathcal{X}_2] = [\mathbf{1}, \infty)$, but $[\mathbf{1}, \infty) \notin \mathcal{X}_3$ as we saw in Example 2.*

Proving or refuting the inclusion of Part II of the substitution conjecture seems challenging and is not addressed further in this paper. Even though the reverse inclusion (Part I of the substitution conjecture) also remains open, we are able to prove its correctness assuming the truth of another conjecture, discussed in the next section.

4.4 The uniform share distribution conjecture

This section is devoted to proving the Part I of the substitution conjecture assuming the truth of the USD conjecture, stated bellow. We will need two lemmas in the course of proving our claim (Proposition 3).

Conjecture 3 (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 $\{\boldsymbol{\sigma}(\Pi_j)\}_{j\in\mathbb{N}}$ 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 3 (USD conjecture and secret distribution) *As a consequence of Lemma 1, it can be shown that the USD conjecture is equivalent to a seemingly weaker version of the conjecture in which we remove the fourth requirement. This fact justifies our selected running title for the conjecture.*

Remark 4 (USD conjecture and information ratio variants) *Two different flavors of information ratio can be found in the literature [12,9,25]. One is defined based on the ratio between 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 share space size and the secret space size. Consequently, the information ratio of an access structure Γ can be defined in two different ways, which we denote by $\sigma_e(\Gamma)$ and $\sigma_s(\Gamma)$ with respective to these two flavors of information ratio ('e' stands for entropy and 's' stands for size). It is known that $\sigma_s(\Gamma) \geqslant \sigma_e(\Gamma)$; e.g., see [3] (Section 5.2). The USD conjecture implies that $\sigma_s(\Gamma) = \sigma_e(\Gamma)$, for any access structure Γ.*

Lemma 8. *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, $\inf_{\mathrm{P}}(\mathcal{X}_1)[i \to \inf_{\mathrm{P}}(\mathcal{X}_2)] \subseteq \mathrm{cl}(\mathcal{X}_3)$ implies $\mathrm{cl}(\mathcal{X}_1)[i \to \mathrm{cl}(\mathcal{X}_2)] \subseteq \mathrm{cl}(\mathcal{X}_3)$.*

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

Lemma 9. *Let Γ_1 and Γ_2 be two access structures on disjoint participant sets. Let $p_i \in P(\Gamma_1)$ and define $\Gamma_3 = \Gamma_1[p_i \to \Gamma_2]$. 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 $\boldsymbol{\sigma}(\Pi_1) = \boldsymbol{x}$ and $\boldsymbol{\sigma}(\Pi_2) = \boldsymbol{y}$. 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 $\{\boldsymbol{\sigma}(\Pi_3^j)\}_{j \in \mathbb{N}}$ converges to $\boldsymbol{x}[i \to \boldsymbol{y}]$ when j goes to infinity.

Here, index $i \in [n]$ corresponds to the coordinate of participant p_i, where $n = |P(\Gamma_1)|$.

Proof. Let us first introduce the notation $k \times \Pi$, where $\Pi = (\boldsymbol{X}_1, \ldots, \boldsymbol{X}_\lambda)$ is a vector of random variables. Let $\Pi_1, \ldots, \Pi_k$ be independent random variables and identically distributed as Π and let $\Pi_j = (\boldsymbol{X}_1^j, \ldots, \boldsymbol{X}_\lambda^j)$, for $j = 1, \ldots, k$. We define $k \times \Pi = (\boldsymbol{Y}_1, \ldots, \boldsymbol{Y}_\lambda)$ where $\boldsymbol{Y}_i = (\boldsymbol{X}_i^1, \ldots, \boldsymbol{X}_i^k)$ for $i = 1, \ldots, \lambda$.

Let $P(\Gamma_1) = P$ and $P(\Gamma_2) = Q$. Denote $\Pi_1 = (\boldsymbol{S}_p)_{p \in P \cup \{p_0\}}$ and $\Pi_2 = (\boldsymbol{S}_q)_{q \in Q \cup \{q_0\}}$. Let $N = |\mathrm{supp}(\boldsymbol{S}_{p_i})|$ and $M = |\mathrm{supp}(\boldsymbol{S}_{q_0})|$ and, without loss of generality, suppose that $N \leqslant M$; Otherwise, if $M < N$, we can replace Π_2 with $k \times \Pi_2$, where $k = \lceil N/M \rceil$. Note that $k \times \Pi_2$ is still a secret sharing scheme, with uniform shares and secret, realizing Γ_2 with $\boldsymbol{\sigma}(k \times \Pi_2) = \boldsymbol{y}$.

For every $j \in \mathbb{N}$, define $\alpha_j = \lfloor \frac{j \log M}{\log N} \rfloor$ and let $\alpha_j \times \Pi_1 = (\boldsymbol{S}_p^j)_{p \in P \cup \{p_0\}}$ 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 $|\mathrm{supp}(\boldsymbol{S}_{p_i}^j)| = N^{\alpha_j}$, $|\mathrm{supp}(\boldsymbol{S}_{q_0}^j)| = M^j$ 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 $P_{-i} = P \backslash \{p_i\}$ and $P(\Gamma_3) = T$, where $T = P_{-i} \cup Q$. To generate a sample $(s_t)_{t \in T \cup \{t_0\}}$ according to Π_3^j, we first generate a sample $(s_p)_{p \in P \cup \{p_0\}}$ according to $\alpha_j \times \Pi_1$. We let $s_{t_0} = s_{p_0}$, that is, the same secret is used. Each participant $p \in P_{-i}$ (as a participant of $P(\Gamma_3)$) receives s_p as his share, which is trivially distributed according to $\boldsymbol{S}_p^j$. 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 1, is distributed as $\boldsymbol{S}_q^j$. Clearly, the scheme Π_3^j realizes Γ_3 and its convec is:

$$\boldsymbol{\sigma}(\Pi_3^j) = \boldsymbol{x}[i \to \frac{\mathrm{H}(\boldsymbol{S}_{q_0}^j)}{\mathrm{H}(\boldsymbol{S}_{p_i}^j)} \boldsymbol{y}] \ .$$

Since $\mathrm{H}(\boldsymbol{S}^j_{q_0}) = j \log M$ and $\mathrm{H}(\boldsymbol{S}^j_{p_i}) = \alpha_j \log N$, it follows that $\frac{\mathrm{H}(\boldsymbol{S}^j_{q_0})}{\mathrm{H}(\boldsymbol{S}^j_{p_i})}$ $(= \frac{j \log M}{\alpha_j \log N})$ converges to one. Consequently, $\boldsymbol{\sigma}(\Pi^j_3)$ converges to $\boldsymbol{x}[i \to \boldsymbol{y}]$. □

Proposition 3 (USD conjecture ⇒ Part I of the substitution conjecture). *The USD conjecture (Conjecture 3) implies the Part I of the substitution conjecture (Conjecture 2).*

Proof. According to Lemma 8, it is sufficient to prove that $\inf_{\mathrm{P}}\big(\Sigma(\Gamma_1)\big)[i \to \inf_{\mathrm{P}}\big(\Sigma(\Gamma_2)\big)] \subseteq \mathcal{X}_3$.

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 $\boldsymbol{x}[i \to \boldsymbol{y}] \in \mathrm{cl}(\Sigma(\Gamma_3))$. To prove this, we show that there exists a sequence $\{\Pi^{j,k}_3\}_{(j,k)\in\mathbb{N}\times\mathbb{N}}$ of secret sharing schemes such that:

(1') $\Pi^{j,k}_3$ realizes Γ_3, for every $j, k \in \mathbb{N}$,
(2') the sequence $\{\boldsymbol{\sigma}(\Pi^{j,k}_3)\}$ converges to $\boldsymbol{x}[i \to \boldsymbol{y}]$ when j, k both go to infinity.

Assuming that the USD conjecture is true, there exists a sequence $\{\Pi^k_1\}_{k\in\mathbb{N}}$ (resp. $\{\Pi^k_2\}_{k\in\mathbb{N}}$) of secret sharing schemes, with uniform distributions on secrets and individual shares, realizing Γ_1 (resp. Γ_2), such that the sequences $\{\boldsymbol{x}_k\}_{k\in\mathbb{N}} = \{\boldsymbol{\sigma}(\Pi^k_1)\}_{k\in\mathbb{N}}$ (resp. $\{\boldsymbol{y}_k\}_{k\in\mathbb{N}} = \{\boldsymbol{\sigma}(\Pi^k_2)\}_{k\in\mathbb{N}}$) converge to $\boldsymbol{x}$ (resp. $\boldsymbol{y}$).

Consequently, for each $k \in \mathbb{N}$, according to Lemma 9, there exists a sequence $\{\Pi^{j,k}_3\}_{j\in\mathbb{N}}$ of secret sharing schemes such that:

(1") $\Pi^{j,k}_3$ realizes Γ_3, for every $j \in \mathbb{N}$,
(2") the sequence $\{\boldsymbol{\sigma}(\Pi^{j,k}_3)\}_{j\in\mathbb{N}}$ converges to $\boldsymbol{x}_k[i \to \boldsymbol{y}_k]$ when j goes to infinity.

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

5 Conjecturally improving Csirmaz lower bound

The aim of this section is to, assuming the Part II of the substitution conjecture is true, construct a family of access structures with information ratio $n^{\Omega(\frac{\log n}{\log\log n})}$, beating Csirmaz $\Omega(n/\log n)$ lower bound. Our candidate family is recursively constructed from a carefully selected access structure Γ on participant set Q and a well-chosen subset $I \subseteq Q$.

Below, we introduce a definition and some notations. We define our recursive procedure for constructing a family of access structures in Section 5.1. We will then present a *lifting theorem* in Section 5.2. As we will see in Section 5.3, direct application of this theorem leads to our superpolynomial $n^{\Omega(\frac{\log n}{\log\log n})}$ lower bound for information ratio. We discuss possible improvements of our bound in Section 5.4.

Definition 6 (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 $\tilde{\sigma}_{\mathcal{F}}(n) = g(n)$, 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 $\sigma_{\mathcal{F}}(n)$.*

Notation. In Section 4, we introduced the notation $\boldsymbol{x}[i \to \boldsymbol{x}']$ and $\Gamma[p \to \Gamma']$ for vectors and access structures for *single* element substitution. In this section, we use the notation $\boldsymbol{x}[(i_1, \ldots, i_\lambda) \to (\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_\lambda)]$ and $\Gamma[(p_1, \ldots, p_\lambda) \to (\Gamma'_1, \ldots, \Gamma'_\lambda)]$ for *multiple* elements substitution. We do not bother to provide a formal definition.

Remark 5 *It is easy to see that a variant of the substitution conjecture with multiple elements substitution is equivalent with the single element substitution description as stated in Conjecture 2.*

5.1 The family $\mathcal{F}_{\Gamma,I}$ of access structures

Let Γ and Γ' be two access structures on participant sets Q and Q', respectively, and let $I \subseteq Q$. We assume that Q and $I \times Q'$ are disjoint; the reason for this assumption will be clear in a moment. We first define the access structure $\Gamma[I \to \Gamma']$.

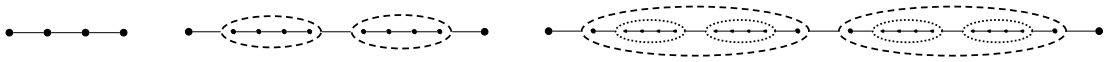
Informally, $\Gamma[I \to \Gamma']$ is an access structure obtained by substituting an instance of Γ' for every participant of I in Γ, where the participant sets of all involved $|I| + 1$ access structures are assumed to be disjoint.

More formally, for every $p \in I$, let $Q'_p = \{p\} \times Q'$ and define the access structure Γ'_p on Q'_p as $\Gamma'_p = \{\{p\} \times A \mid A \in \Gamma'\}$. Note that Γ'_p's are all isomorphic with Γ' and they all have disjoint participant sets, also disjoint form Q. Let $I = \{p_1, \ldots, p_\lambda\}$. We then define $\Gamma[I \to \Gamma'] = \Gamma[(p_1, \ldots, p_\lambda) \to (\Gamma'_{p_1}, \ldots, \Gamma'_{p_\lambda})]$.

Corollary 4. $|P(\Gamma[I \to \Gamma'])| = |Q| + |I|(|Q'| - 1)$.

The family $\mathcal{F}_{\Gamma,I} = \{\Gamma_m\}_{m \in \mathbb{N}}$ of access structures is then recursively defined as $\Gamma_m = \Gamma[I \to \Gamma_{m-1}]$, where $\Gamma_1 = \Gamma$.

Example 4 *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) $\Gamma_2 = \mathcal{P}_3[I \to \Gamma_1]$ (c) $\Gamma_3 = \mathcal{P}_3[I \to \Gamma_2]$

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

5.2 The lifting theorem

In this section, we present a lifting theorem, useful for boosting the information ratio of a family of access structures under some conditions. First, we provide a definition and a key lemma. Then, we present a second definition before stating our lifting theorem.

Definition 7 ((B,T)-access structure). *Let $B \in \mathbb{N}$, $T \in \mathbb{R}^+$ and Γ be an access structure. We call Γ a (B,T)-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 $\sum_{p \in I} \sigma_p \geqslant T$.*

Lemma 10 (Key lemma). *Let Γ be a (B,T)-access structure on participant set Q and let $I \subseteq Q$ 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. $|P(\Gamma_m)| = (|Q| - 1)(1 + B + \ldots + B^{m-1}) + 1$,
II. $\|\boldsymbol{x}\| \geqslant T^m$ *for every* $\boldsymbol{x} \in \mathrm{cl}(\Sigma(\Gamma_m))$, *assuming that the Part II of the substitution conjecture (Conjecture 2) is true.*

Proof. The first claim can be proved by an easy induction on m and using Corollary 4.

We continue to prove the second claim, also, by induction on m. The base case, $m = 1$, trivially holds. Assuming that the claim holds for $m \in \mathbb{N}$, we show that it holds as well for

$m+1$; that is, $\|\boldsymbol{x}'\| \geqslant T^{m+1}$ for every $\boldsymbol{x}' \in \mathrm{cl}(\Sigma(\Gamma_{m+1}))$. Let $I = \{p_{i_1}, \ldots, p_{i_\lambda}\}$. By Part II of the substitution conjecture (see also Remark 5), there exists convecs $\boldsymbol{x} \in \mathrm{cl}(\Sigma(\Gamma))$ and $\boldsymbol{x}_{p_{i_1}}, \ldots, \boldsymbol{x}_{p_{i_\lambda}} \in \mathrm{cl}(\Sigma(\Gamma_m))$ such that

$$\boldsymbol{x}' = \boldsymbol{x}[(i_1, \ldots, i_\lambda) \to (\boldsymbol{x}_{p_{i_1}}, \ldots, \boldsymbol{x}_{p_{i_\lambda}})] \ .$$

Note that, by the induction hypothesis, $\|\boldsymbol{x}_p\| \geqslant T^m$, for every $p \in I$. Let $\boldsymbol{x} = (\sigma_p)_{p \in Q}$ and recall that, by assumption, $\sum_{p \in I} \sigma_p \geqslant T$. Consequently,

$$\begin{aligned} \|\boldsymbol{x}'\| &= \textstyle\sum_{p \in Q \setminus I} \sigma_p + \sum_{p \in I} \big(\sigma_p \|\boldsymbol{x}_p\|\big) \\ &\geqslant \textstyle\sum_{p \in I} \big(\sigma_p T^m\big) \\ &= T^m \textstyle\sum_{p \in I} \sigma_p \\ &\geqslant T^{m+1} \ . \end{aligned}$$

□

Corollary 5 (Simple lifting). *Assume that the Part II of the substitution conjecture (Conjecture 2) is true. If there exist a (B,T)-access structure with $B \geqslant 2$, then there exists a family of access structures with average (and consequently maximum) information ratio $\Omega\big(n^{\log_B(T/B)}\big)$.*

Proof. The condition $B \geqslant 2$ implies $T \geqslant 2$. Consequently, from Lemma 10, it follows that $n = |P(\Gamma_m)| \leqslant |Q|B^m$ and $\|\boldsymbol{x}\| \geqslant T^m \geqslant T^{\log_B(n/|Q|)} = \Omega\big(n^{\log_B T}\big)$. Hence, $\tilde{\sigma}(\Gamma_m) = \Omega\big(n^{\log_B(T/B)}\big)$.

□

Definition 8 ($\big(b(n), t(n)\big)$-family of access structures). *Let $b, t : \mathbb{R}^+ \to \mathbb{R}^+$ be two 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 $(b(n), t(n))$-family if, for every $k \in \mathbb{N}$, Γ_k is a $\big(b(n_k), t(n_k)\big)$-access structure. That is, there exists a subset $I_k \subseteq P(\Gamma_k)$ of size $|I_k| = b(n_k)$ with minimum total information ratio $t(n_k)$.*

Theorem 2 (Lifting theorem). *Assume that the Part II of the substitution conjecture (Conjecture 2) is true. Let $b, t : \mathbb{R}^+ \to \mathbb{R}^+$ be two functions such that $b(x) \geqslant 2$ and $f(x) = \frac{\log t(x)}{\log b(x)}$ is increasing. If there exists a $\big(b(n), t(n)\big)$-family of access structures, then, for any $0 < \epsilon < \frac{1}{2}$, there exists a family of access structures with total share size at least $n^{(1-2\epsilon)\frac{\log t(n^\epsilon)}{\log b(n^\epsilon)}}$. 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 the average (and consequently maximum) information ratio of the family is $n^{\Omega\left(\frac{\log t(n)}{\log b(n)}\right)}$.*

Proof. Let $\mathcal{F} = \{\Gamma_k\}_{k \in \mathbb{N}}$ be the $\big(b(n), t(n)\big)$-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 10 for the family $\mathcal{F}_{\Gamma_k, I_k} = \{\Gamma_{k,m}\}_{m \in \mathbb{N}}$. We have $|Q| = n_k$, $B = b(n_k)$ and $T = t(n_k)$. 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 10 (Part I), our choice for m_k and taking into account that $2 \leqslant b(n_k) \leqslant n_k$, we have:

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

Also, by Part II of Lemma 10, for every $\boldsymbol{x} \in \mathrm{cl}(\Sigma(\Gamma'_k))$, we have

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

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

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

proving the first part of the claim.

Consequently, $\tilde{\sigma}_{\mathcal{F}'}(n) \geqslant n^{(1-2\epsilon)\frac{\log t(n^\epsilon)}{\log b(n^\epsilon)}-1}$ and the additional condition $\frac{\log t(x)}{\log b(x)} = \omega(1)$ implies that $\tilde{\sigma}_{\mathcal{F}'}(n) = n^{\Omega\left(\frac{\log t(n^\epsilon)}{\log b(n^\epsilon)}\right)}$. The remaining part of the claim is a corollary of Lemma 11 (Part I), given below. □

For proving the final claim of Theorem 2, we only relied on the Part I of Lemma 11. 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 11. *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, $m = \left\lceil \frac{\log\log M - \log\log x}{\log\epsilon} \right\rceil + 1$.

It is easy to prove by induction that $f(x) \leqslant \alpha^m f\left(x^{\epsilon^m}\right)$. 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 $f\left(x^{\epsilon^m}\right) \leqslant T$, 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 $f(x) = 2^{2^{\lceil\log\log x\rceil}}$ 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.

□

5.3 Applications of the lifting theorem

The following examples are direct applications of our lifting theorem, respectively, leading to $n^{\Omega(\log\log n)}$ and $n^{\Omega(\frac{\log n}{\log\log n})}$ lower bounds for information ratio.

Example 5 (A $n^{\Omega(\log\log n)}$ lower bound) *For any integer $d \geqslant 2$, Csirmaz has studied the access structure $\mathcal{C}_d$, called d-dimensional cube [18], with 2^d participants. For any $I \subseteq P(\mathcal{C}_d)$, Csirmaz has shown that for every $(\sigma_p)_{p\in P(\mathcal{C}_d)} \in \Sigma(\mathcal{C}_d)$, it holds that $\sum_{p\in I}\sigma_p \geqslant \frac{d}{2}|I|$. If we let $|I| = 2$, it can be seen that $\{\mathcal{C}_d\}$ is a $(2, \Theta(\log n))$-family. The lifting theorem then guarantees a family of access structures with average/maximum information ratio $n^{\Omega(\log\log n)}$, assuming the truth of Part II of the substitution conjecture.*

Example 6 (A $n^{\Omega(\frac{\log n}{\log\log n})}$ lower bound) *For any integer $k \geqslant 2$, Csirmaz [16] has constructed an access structure $\mathcal{A}_k$ with $2^k + k - 2$ participants. Csirmaz has proved that the maximum information ratio of the family $\{\mathcal{A}_k\}$ is $\Omega(n/\log n)$. To show this, he has exhibited a subset $I \subseteq P(\mathcal{A}_k)$ of size k such that for every $(\sigma_p)_{p\in P(\mathcal{A}_k)} \in \Sigma(\mathcal{A}_k)$ it holds that $\sum_{p\in I}\sigma_p \geqslant 2^k - 1$. That is, $\{\mathcal{A}_k\}$ is a $\big(\Theta(\log n), \Omega(n)\big)$-family. Consequently, our lifting theorem promisses a family of access structures with average/maximum information ratio $n^{\Omega(\frac{\log n}{\log\log n})}$, provided that the Part II of the substitution conjecture is true.*

5.4 How could we do better?

The lifting theorem boosts the maximum information ratio $\Omega(t(n)/b(n))$, of a $(b(n), t(n))$-family of access structures, into an average (and consequently maximum) information ratio $n^{\Omega\left(\frac{\log t(n)}{\log b(n)}\right)}$, assuming some mild conditions on $\frac{\log t(x)}{\log b(x)}$ and the truth of Part II of the substitution conjecture. We achieved our ultimate lower bound $n^{\Omega(\frac{\log n}{\log\log n})}$ for information ratio using Csirmaz $\big(\Theta(\log n), \Omega(n)\big)$-family [16] of access structures (Example 6).

One way to ameliorate our bound is to find a $\big((\log n)^{o(1)}, n^{\Theta(1)}\big)$-family of access structures which, by our lifting theorem, leads to an improved lower bound for the information ratio. We Remark that Csirmaz has shown that, by merely using the Shannon information inequalities [22,13], the best that one can achieve is $t(n) \leqslant nb(n)$; see the proof of Theorem 3.5 in [16]. Beimel and Orlov [7] have shown that even by incorporating the so-called non-Shannon information inequalities [38] with four or five variables, unknown at time of publication of [16], the negative result of Csirmaz still is valid; see [28] for a follow-up. We conclude that the best lower bound that may be achieved by lifting an access structure constructed using similar methods is $n^{\Omega(\log n)}$. Fortunately, there is still some hope to get close to this bound using known techniques. The point is that, for $0 < c < 1$, it is conceivable to find a $\big((\log n)^{o(1)}, \Omega(n^c)\big)$-family, since it does not violate the Csirmaz negative result. Note that even though the maximum information ratio of such (hypothetical) access structures is uncompetitive with Csirmaz lower bound, they improve our lower bound when lifted.

Another way to enhance our bound is to lift a $\big(n^{o(1)}, n^{\Omega(\frac{\log n}{\log\log n})}\big)$-family, leading to an improved lower bound for the information ratio. Notice the family that we have constructed is (conjecturally) a $\big(n, n^{\Omega(\frac{\log n}{\log\log n})}\big)$-family. Constructing a $\big(n^{o(1)}, n^{\Omega(\frac{\log n}{\log\log n})}\big)$-family might be possible by modified notions of recursion or other means.

6 Conclusion

The crypto community lacks suitable approaches for constructing complex, yet analyzable, access structures. We believe that the substitution technique, originally introduced by Martin in [25] and further developed in this paper, is an initiation in this direction.

The introduced notion of convec set leaves several problems unanswered. Apart from the intriguing substitution conjecture, a list of suggested open problems were discussed in Section 3.6. Solving any of these questions may change our understanding of secret sharing schemes.

Additionally, proving/refuting the USD conjecture is left for future. Fortunately, if this conjecture turns out to be false, our lifting theorem —Theorem 2, which is useful for amplifying the information ratio of a family of access structures— will not be affected.

Our best lower bound for share size is achieved by applying our lifting theorem to Csirmaz [14,16] family of access structures. Another line for future research would be to seek alternative families that result in better bounds; see Section 5.4 for further discussion.

The concept of convec set is an initiation for studying other sets associated to access structures, which are probably easier to comprehend. For an access structure Γ, the convec set $\Sigma(\Gamma)$ conveys much more information than the parameter $\sigma(\Gamma)$ (and its tilde version). One can naturally define the *linear* and *polymatroid* convex sets $\Lambda(\Gamma)$ and $K(\Gamma)$, which are natural extensions of the parameters $\lambda(\Gamma)$ and $\kappa(\Gamma)$ (and their tilde version), introduced in [24]. Studying the properties of these sets is left for future.

Last but not least, our statement of the substitution conjecture is given for two access structures with disjoint participant sets. It is unclear what to expect when the participant sets are not disjoint.

Acknowledgment. The proof of Lemma 11 is due to Morteza Fotouhi.

References

1. László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.
2. William F. Basener. *Topology and Its Applications (1. ed.)*. John Wiley & Sons, 2006.
3. Amos Beimel. Secret-sharing schemes: A survey. In Yeow Meng Chee, Zhenbo Guo, San Ling, Fengjing Shao, Yuansheng Tang, Huaxiong Wang, and Chaoping Xing, editors, *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, volume 6639 of *Lecture Notes in Computer Science*, pages 11–46. Springer, 2011.
4. Amos Beimel, Anna Gál, and Mike Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997.
5. Amos Beimel and Noam Livne. On matroids and non-ideal secret sharing. In *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, pages 482–501, 2006.
6. Amos Beimel and Noam Livne. On matroids and nonideal secret sharing. *IEEE Trans. Information Theory*, 54(6):2626–2643, 2008.
7. Amos Beimel and Ilan Orlov. Secret sharing and non-shannon information inequalities. *IEEE Trans. Information Theory*, 57(9):5634–5649, 2011.
8. George Robert Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference1979*, 48:313–317, 1979.
9. Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, and Ugo Vaccaro. Graph decompositions and secret sharing schemes. In Rainer A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*, volume 658 of *Lecture Notes in Computer Science*, pages 1–24. Springer, 1992.

10. Carlo Blundo, Alfredo De Santis, and Ugo Vaccaro. On secret sharing schemes. *Inf. Process. Lett.*, 65(1):25–32, 1998.
11. Ernest F. Brickell and Daniel M. Davenport. On the classification of ideal secret sharing schemes. *J. Cryptology*, 4(2):123–134, 1991.
12. 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.
13. 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.
14. László Csirmaz. The size of a share must be large. In Alfredo De Santis, editor, *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 13–22. Springer, 1994.
15. László Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar*, 32(4):429–437, 1996.
16. László Csirmaz. The size of a share must be large. *J. Cryptology*, 10(4):223–231, 1997.
17. László Csirmaz. Secret sharing on the d-dimensional cube. *Designs, Codes and Cryptography*, 74(3):719–729, 2015.
18. László Csirmaz. Secret sharing on the d-dimensional cube. *Des. Codes Cryptography*, 74(3):719–729, 2015.
19. László Csirmaz and Gábor Tardos. Optimal information rate of secret sharing schemes on trees. *IEEE Trans. Information Theory*, 59(4):2527–2530, 2013.
20. 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.
21. Wen-Ai Jackson and Keith M Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9(3):267–286, 1996.
22. Ehud D. Karnin, J. W. Greene, and Martin E. Hellman. On secret sharing systems. *IEEE Trans. Information Theory*, 29(1):35–41, 1983.
23. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Towards breaking the exponential barrier for general secret sharing. Cryptology ePrint Archive, Report 2017/1062, 2017. `https://eprint.iacr.org/2017/1062`.
24. Jaume Martí-Farré and Carles Padró. On secret sharing schemes, matroids and polymatroids. *J. Mathematical Cryptology*, 4(2):95–120, 2010.
25. Keith M Martin. New secret sharing schemes from old. *J. Combin. Math. Combin. Comput*, 14:65–77, 1993.
26. Frantisek Matús. Matroid representations by partitions. *Discrete Mathematics*, 203(1-3):169–194, 1999.
27. Frantisek Matús. Two constructions on limits of entropy functions. *IEEE Trans. Information Theory*, 53(1):320–330, 2007.
28. Sebastià Martín Molleví, Carles Padró, and An Yang. Secret sharing, rank inequalities, and information inequalities. *IEEE Trans. Information Theory*, 62(1):599–609, 2016.
29. Carles Padró. Lecture notes in secret sharing. *IACR Cryptology ePrint Archive*, 2012:674, 2012.
30. Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A. Cook. Exponential lower bounds for monotone span programs. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 406–415, 2016.
31. Paul D. Seymour. On secret-sharing matroids. *J. Comb. Theory, Ser. B*, 56(1):69–73, 1992.
32. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.
33. Juriaan Simonis and Alexei E. Ashikhmin. Almost affine codes. *Des. Codes Cryptography*, 14(2):179–197, 1998.
34. Douglas R Stinson. Decomposition constructions for secret-sharing schemes. *IEEE Transactions on Information Theory*, 40(1):118–125, 1994.
35. Marten Van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6(2):143–169, 1995.

36. Stephen Willard. *General topology*. Courier Corporation, 1970.
37. Raymond W. Yeung. A framework for linear information inequalities. *IEEE Trans. Information Theory*, 43(6):1924–1934, 1997.
38. Zhen Zhang and Raymond W. Yeung. A non-shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory*, 43(6):1982–1986, 1997.