Secret Sharing and Non-Shannon Information Inequalities*

Amos Beimel and Ilan Orlov

Dept. of Computer Science, Ben-Gurion University Be'er-Sheva, Israel

Abstract. The known secret-sharing schemes for most access structures are not efficient; even for a one-bit secret the length of the shares in the schemes is $2^{O(n)}$, where n is the number of participants in the access structure. It is a long standing open problem to improve these schemes or prove that they cannot be improved. The best known lower bound is by Csirmaz (J. Cryptology 97), who proved that there exist access structures with n participants such that the size of the share of at least one party is $n/\log n$ times the secret size. Csirmaz's proof uses Shannon information inequalities, which were the only information inequalities known when Csirmaz published his result. On the negative side, Csirmaz proved that by only using Shannon information inequalities one cannot prove a lower bound of $\omega(n)$ on the share size. In the last decade, a sequence of non-Shannon information inequalities were discovered. This raises the hope that these inequalities can help in improving the lower bounds beyond n. However, in this paper we show that all the inequalities known to date cannot prove a lower bound of $\omega(n)$ on the share size.

1 Introduction

A secret-sharing scheme is a mechanism for sharing data among a set of participants such that only pre-defined authorized subsets of participants can reconstruct the data, while any other subset has absolutely no information on the data. The collection of authorized subsets is called an access structure. For example, in a t-out-of-n threshold secret-sharing scheme, the access structure contains all subsets of size at least t. As an interesting "real-world" illustration of this situation: According to *Time Magazine* control of the nuclear weapon in Russia in the early 1990s depended upon a similar "two-out-of-tree" access mechanism, where the three parties were the President, the Defense Minister, and the Defense Ministry. Secret-sharing schemes, introduced by [40, 8, 30], are nowadays used in many cryptographic protocols, e.g., Byzantine agreement [38], secure multiparty computations [6, 14, 17], threshold cryptography [20], access control [36], and attribute-based encryption [27, 43].

An important issue in secret-sharing schemes is the size of the shares distributed to the participants. For most access structures, even the best known

* Partially supported by the Frankel Center for Computer Science at the Ben-Gurion University.

secret-sharing schemes (e.g., [7, 11, 21, 31, 42, 31]) are not efficient; the length of the shares for sharing an ℓ-bit secret is $\ell \cdot 2^{O(n)}$, where n is the number of participants in the access structure. The best lower bound was proved by Csirmaz [18]; he proved that for each n there exists an access structure with n participants such that any secret-sharing scheme with an ℓ-bit secret requires shares of length $\Omega(\ell n/\log n)$. There is a large gap between the upper bounds and the lower bounds. Closing this gap is a major open problem.

The entropy of a random variable, which was introduced by Shannon in the landmark paper [41], is a measure of the amount of uncertainty associated with the value of the random variable. Starting from the works of Karnin et al. [32] and Capocelli et al. [12], the entropy was used to prove lower bounds on the share size in secret sharing schemes [9, 22, 18, 19]. Specifically, Csirmaz's proof [18] uses only Shannon information inequalities, which were the only information inequalities known when Csirmaz published his result (this is true also for all the previous works mentioned above). On the negative side, Csirmaz proved that by using only Shannon information inequalities one cannot prove a lower bound of $\omega(n)$ on the share size. In the last decade, a sequence of non-Shannon information inequalities were discovered. This raises the hope that these inequalities can help in improving the lower bounds beyond n. However, in this paper we show that all the inequalities known to date cannot prove a lower bound of $\omega(n)$ on the share size.

1.1 Related Work

Threshold secret-sharing schemes, in which a subset is authorized iff its size is larger than some threshold, were independently introduced by Shamir [40] and Blakley [8] about thirty years ago. General secret sharing schemes were presented by Ito, Saito, and Nishizeki [30]; they presented a construction of a secret-sharing scheme for every monotone access structure. More efficient schemes for specific access structures were presented in, e.g., [7, 11, 21, 42, 31]. However, even these better constructions are not efficient and, for most access structure, the shares' size is exponential. Lower bounds for secret-sharing schemes were presented in [9, 22, 18, 19]; however, as stated above, there is a big gap between the upper and lower bounds. Super-polynomial lower bounds for *linear* secret-sharing schemes were presented in [1, 26].

In this work, we discuss using information inequalities for proving lower bounds on the share size in secret-sharing schemes. An information inequality is a linear inequality over the entropy of subsets of variables that holds for any random variables (for a formal definition see Section 2.1). For example, $H(X_1) + H(X_2) \geq H(X_1X_2)$ is an information inequality. Many inequalities can be expressed as a linear combination of a single inequality involving the conditional mutual information, namely, $I(X;Y|Z) \geq 0$. Such inequalities are known as Shannon inequalities. It was an open problem for many years if there are information inequalities that are not implied by Shannon inequalities, i.e., if there are non-Shannon inequalities. The first non-Shannon inequality was given by Zhang and Yeung [47]. In the last decade, several additional non-Shannon inequalities were discovered [33, 46, 23, 44]. In particular, an interesting technique for deriving non-Shannon inequalities, called projection, was presented in [44]. Several papers have dealt with the characterization of information inequalities. Chan and Yeung [13] have characterized information inequalities using group-theoretic inequalities. Matúš [34] has proved that there are infinitely many independent information inequalities. Guille et al. [28] have given results concerning the structure of information inequalities and, more specially, results describing the minimal set of information inequalities when all the coefficient are 1 or -1, called Ingleton inequalities.

The information inequality of Zhang and Yeung [47] was used in several areas. It was used by Dougherty, Freiling, and Zeger [24] to prove bounds on the capacity of network coding, by Matúš [35] to prove that a function is not asymptotically entropic, and by Riis [39] to prove bounds on graph entropy of certain graphs. Furthermore, it was used by Beimel, Livne, and Padró [4] to prove lower bounds on the size of shares in secret-sharing schemes; they proved that there is a matroidial access structure – the Vamos access structure – that is not nearly ideal. We observe that this result can be proved using other information inequalities, e.g., the information inequalities of [23]. Furthermore, the information inequalities of [47, 23] can be used to prove that other matroidial access structures are not nearly ideal, e.g., the access structures induced by the matroids AG32r, F8, Q8 (for the definitions of these matroids see [37]).

This paper deals with limitations of the techniques for proving lower bounds on the size of shares in secret-sharing schemes, continuing the work of [3]. Beimel and Franklin [3] considered weakly-private secret-sharing schemes, in which any unauthorized set can never rule-out any secret (however, it might deduce, for example, that one secret is much less likely than other secrets). They show efficient constructions of weakly-private secret-sharing schemes (for large secret domains), implying that to prove lower bounds on the shares' size in secret-sharing schemes one must use the strong privacy requirement of secret-sharing schemes.

1.2 Our Results

In contrast to the success of applying the known information inequalities to proving lower bounds in several areas, we show that they cannot help in proving lower bounds of $\omega(n)$ on the share size in secret-sharing schemes. Let us elaborate on our proof. Csirmaz [18] in 1994 has proven his lower bound by translating the question of proving lower bounds on share size to proving that a certain linear programming instance does not have a small solution. Csirmaz constructed the linear program by using Shannon inequalities, which were the only information inequalities known in 1994. He proved a lower bound of $\Omega(n/\log n)$ times the secret size for an access structure with n parties. Furthermore, all previous lower bounds [32, 12, 9, 22] can be restated using Csirmaz's framework using Shannon inequalities. On the other hand, Csirmaz proved that for every access structure the linear program has a solution in which the objective function has value $O(n)$, implying that his framework cannot prove better lower bounds than $\Omega(n)$.

In the last decade, a sequence of non-Shannon information inequalities were discovered [47, 33, 46, 23, 44]. This gives hope that adding these inequalities to the linear program, one could prove better lower bounds on the share size. However, in this work we show that Csirmaz's solution to the linear program remains valid even after adding all the known information inequalities. That is, all the information inequalities known to date cannot prove lower bounds better than $\Omega(n)$ even if used simultaneously. Our proof that Csirmaz's solution remains valid after adding the new inequalities is much more involved than Csirmaz's proof for Shannon inequalities. We present a brute-force algorithm that checks if Csirmaz's solution remains valid given an information inequality.[1] We executed this algorithm, using a computer program, on all known information inequalities of [47, 33, 46, 23]. For [47, 46, 33, 44], which also give an infinite sequence of information inequalities, we manually executed the algorithm on a symbolic representation of the inequalities. The conclusion is that all the known information inequalities cannot help in proving better lower bounds than $\Omega(n)$.

We end the introduction with a few remarks. First, one cannot interpret our result as suggesting that information inequalities cannot help in improving the lower bounds. To the contrary, the conclusion of our paper is that new information inequalities should be sought. Hopefully, these new information inequalities would not be ruled-out by our algorithm. However, not failing the test in our algorithm is only the first step. Our algorithm only gives a necessary condition for an information inequality to be helpful in proving lower bounds of $\omega(n)$ on the share size. To use new inequalities, one has to prove that for some access structure the linear program with the new inequalities, and possibly with all the known inequalities, has only large solutions.

2 Preliminaries

In this section we review the relevant definitions from information theory and define secret-sharing schemes.

2.1 Basic Definitions from Information Theory and Information Inequalities

In this section, we review the basic concepts of Information Theory used in this paper. For a complete treatment of this subject see, e.g., [16]. All the logarithms here are of base 2.

The *entropy* of a random variable X is $H(X) \stackrel{\text{def}}{=} -\sum_{x,\Pr[X=x]>0} \Pr[X = x] \log \Pr[X = x]$. It can be proved that $0 \leq H(X) \leq \log |\text{supp}(X)|$, where

[1] Our algorithm is highly inefficient. However, most known non-Shannon information inequalities have 4 or 5 variables, thus, executing the computer program returns an answer in a reasonable time (less than a minute).

$|\mathrm{supp}(X)|$ is the size of the support of X (the number of values with probability greater than zero). The upper bound $|\mathrm{supp}(X)|$ is obtained if and only if the distribution of X is uniform and the lower bound is obtained if and only if X is deterministic. Given two random variables X and Y (possibly dependent), the *conditioned entropy* of X given Y is defined as $H(X|Y) \stackrel{\mathrm{def}}{=} H(X,Y) - H(Y)$. From the definition of the conditional entropy, the following properties can be proved: $0 \le H(X|Y) \le H(X)$, where $H(X|Y) = H(X)$ if and only if X and Y are independent, and $H(X|Y) = 0$ if the value of Y completely determines the value of X. The *mutual information* between X and Y is defined as $I(X;Y) \stackrel{\mathrm{def}}{=} H(X) - H(X|Y)$, and the *conditional mutual information* between X and Y given Z is defined as $I(X;Y|Z) \stackrel{\mathrm{def}}{=} H(X|Z) - H(X|Y,Z)$. Entropies, conditional entropies, mutual information, and conditional mutual information are called *Shannon's information measures.*

Let $\{X_i\}_{i\in[m]}$ be a set of m jointly distributed random variables. For any subset I of $[m]$, let $X_I = (X_i)_{i\in I}$.

Definition 1 (Information Inequality). *An* information inequality over m variables is defined by 2^m constants $\{\alpha_A\}_{A\subseteq[m]}$, where $\alpha_A \in \mathbb{R}$, such that $\sum_{A\subseteq[m]} \alpha_A H(X_A) \ge 0$ for every m random variables $X_1,\ldots,X_m$.

For example, $H(X_1) + H(X_2) \ge H(X_1X_2)$ is an information inequality. Many inequalities can be expressed as a linear combination of a single inequality involving the conditional mutual information, namely, $I(X_1;X_2|X_3) \ge 0$ (this inequality can be stated as $H(X_1,X_3)+H(X_2,X_3)-H(X_1,X_2,X_3)-H(X_3) \ge 0$). Such inequalities are known as Shannon-type inequalities. Information inequalities that cannot be deduced from Shannon inequalities are called non-Shannon inequalities. For more background on information inequalities the reader may consult [45].

2.2 Secret Sharing

Definition 2 (Access Structure and Distribution Scheme). *Let $P = \{p_1,\ldots,p_n\}$ be a finite set of parties, and let $p_0 \notin P$ be a special party called* the dealer.*A collection $\mathcal{A} \subseteq 2^P$ is* monotone *if $B \in \mathcal{A}$ and $B \subseteq C$ imply that $C \in \mathcal{A}$. An* access structure *is a monotone collection $\mathcal{A} \subseteq 2^P$ of non-empty subsets of P. Sets in $\mathcal{A}$ are called* authorized*, and sets not in $\mathcal{A}$ are called* unauthorized.

A distribution scheme *$\Sigma = \langle \Pi, \mu\rangle$ with domain of secrets K is a pair, where μ is a probability distribution on some finite set R (the set of random strings) and Π is a mapping from $K \times R$ to a set of n-tuples $K_1 \times K_2 \times \cdots \times K_n$, where K_i is called the* share-domain *of p_i. A dealer distributes a secret $s \in K$ according to Σ by first sampling a string $r \in R$ according to μ, computing a vector of* shares *$\Pi(s,r) = (s_1,\ldots,s_n)$, and privately communicating each share s_i to party p_i.*

We next define secret-sharing schemes using the entropy function. It is convenient to view the secret as the share of the dealer p_0, and for every set $T \subseteq P \cup \{p_0\}$ to consider the vector of shares of T. Any probability distribution on the domain of secrets, together with the distribution scheme Σ, induces, for any $T \subseteq P \cup \{p_0\}$, a probability distribution on the vector of shares of the parties in T. We denote the random variable taking values according to this probability distribution on the vector of shares of T by S_T, and by S the random variable denoting the secret (i.e., $S = S_{\{p_0\}}$).

Definition 3 (Secret-Sharing Scheme). *We say that a distribution scheme is a secret-sharing scheme realizing an access structure $\mathcal{A}$ with respect to a given probability distribution on the secrets, denoted by a random variable S, if the following conditions hold.*

Correctness. *For every authorized set $T \in \mathcal{A}$, the shares of the parties in T determine the secret, i.e., $H(S|S_T) = 0$.*

Privacy. *For every unauthorized set $T \notin \mathcal{A}$, the shares of the parties in T do not disclose any information on the secret, that is, $H(S|S_T) = H(S)$.*

Remark 1. Although the above definition considers a specific distribution on the secrets, Blundo et al. [10] proved that its correctness and privacy are actually independent of this distribution: If a scheme realizes an access structure with respect to one distribution on the secrets, then it realizes the access structure with respect to any distribution with the same support. Furthermore, the above definition is equivalent to the definition of [15, 2, 5], where there is no probability distribution associated with the secrets and it is required that the probability of every vector of shares of an unauthorized set is the same given any secret.

Karnin et al. [32] have showed that for each non-redundant party (that is, a party that appears in at least one minimal authorized set) $H(S_i) \geq H(S)$, which implies that the size of the share of the party is at least the size of the secret.

Notation 1. *We use the following notation for two sets A and $\widehat{A}$. The set $\widehat{A}$ is a subset of $P \cup \{p_0\}$ and the set A is a subset of P, where $A = \widehat{A} \setminus \{p_0\}$, that is, if $p_0 \notin \widehat{A}$, then $A = \widehat{A}$, otherwise A is obtained by removing p_0 from $\widehat{A}$.*

3 Csirmaz Framework for Proving Lower Bounds and Its Limitations

3.1 Csirmaz Framework for Proving Lower Bounds

Csirmaz [18] has proved the best known lower bounds on the size of the shares in secret-sharing schemes. Towards this goal, he presented a framework for proving lower bounds and showed how to implement this framework to prove lower bounds for a specific access structure. The idea of the framework of Csirmaz is to construct a linear program such that lower bounds on the value of the objective function in this program imply lower bounds on the share size. Specifically, given an access structure $\mathcal{A}$ and a secret-sharing scheme realizing it, define the function $f(\widehat{A}) = H(S_{\widehat{A}})/H(S)$ for every $\widehat{A} \subseteq P \cup \{p_0\}$. The correctness and privacy of the secret-sharing scheme can be translated to constrains on the function f. Namely, (1) if $A \in \mathcal{A}$, then $f(A \cup \{p_0\}) = f(A)$, and (2) if $A \notin \mathcal{A}$, then $f(A \cup \{p_0\}) = f(A) + 1$. Proving lower bounds on the size of the shares is equivalent to proving that any n random variables $S_1, \ldots, S_n$ (i.e., shares) satisfying the above equalities imply that $\sum_{i=1}^{n} H(S_i)$ is large.

These constrains are translated to a linear program using known properties of the entropy function, namely, information inequalities. That is, we get a set of linear inequalities, where we want to minimize $\sum_{i=1}^{n} f(\{p_i\})$.

Csirmaz has constructed an access structure $\mathcal{A}$ that implies a linear program in which $\sum f(\{p_i\}) = \Omega(n^2/\log n)$, thus, for at least one party $f(\{p_i\}) = \Omega(n/\log n)$. This implies that in every secret-sharing scheme realizing $\mathcal{A}$ with an ℓ-bit secret, the share of at least one party is an $\Omega(\ell \cdot n/\log n)$-bit string. We next formally define and describe Csirmaz's framework.

Definition 4. *Given a secret sharing scheme over n parties, define the function* $f : 2^{P \cup \{p_0\}} \to \mathbb{R}$ *as follow:* $f(\widehat{A}) = H(S_{\widehat{A}})/H(S)$ *for every* $\widehat{A} \subseteq P \cup \{p_0\}$.

The properties of the entropy function implies that f is a polymatroid as defined below.

Definition 5. *Let Q be a finite set, and $g : 2^Q \to \mathbb{R}$ be a function assigning real numbers to subsets of Q. The system (Q, g) is a* polymatroid *if g satisfies the following conditions:*

non-negative: $g(A) \geq 0$ *for all* $A \subseteq Q$ *and* $g(\emptyset) = 0$,
monotone: *if* $A \subseteq B \subseteq Q$, *then* $g(A) \leq g(B)$,
submodular: $g(A) + g(B) \geq g(A \cup B) + g(A \cap B)$ *for every* $A, B \subseteq Q$.

Proposition 1 ([25]). *The function f defined in Definition 4 is a polymatroid.*

Combining Proposition 1 and the properties of secret-sharing scheme we get:

Proposition 2. *The function f defined in Definition 4 satisfies the following additional inequalities for every sets $A, B \subseteq P$:*

1. *If* $A \subseteq B, A \notin \mathcal{A}$, *and* $B \in \mathcal{A}$, *then* $f(B) \geq f(A) + 1$,
2. *If* $A \in \mathcal{A}, B \in \mathcal{A}$, *but* $A \cap B \notin \mathcal{A}$, *then* $f(A) + f(B) \geq f(A \cap B) + f(A \cup B) + 1$.

3.2 Limitation of Shannon Inequalities

Csirmaz [18] has proved that using his framework with only Shannon inequalities (which were the only information inequalities known when he published his result) one cannot prove lower bounds better than $\Omega(n)$. That is, his lower bound is the best possible up to a factor of $\log n$ using only Shannon inequalities.

In this section we explain how Csirmaz proved this limitation. Since Csirmaz proved his result in 1994, some non-Shannon information inequalities were discovered. In Section 6 we will show that these inequalities cannot prove better lower bounds than $\Omega(n)$ using Csirmaz's framework.

Theorem 1. *Given any access structure $\mathcal{A}$ on the n-element set P, there is a polymatroid $\widehat{g} : 2^{P\cup\{p_0\}} \to \mathbb{R}$ so that*

1. *For every $A \subseteq P$, $\widehat{g}(A \cup \{p_0\}) = \widehat{g}(A)$ if $A \in \mathcal{A}$ and $\widehat{g}(A \cup \{p_0\}) = \widehat{g}(A) + 1$ if $A \notin \mathcal{A}$.*
2. *$\widehat{g}$ satisfies the conditions of Proposition 2,*
3. *$\widehat{g}(\{p_i\}) \leq n$ for every $p_i \in P$.*

In order to prove this theorem, Csirmaz has defined a polymatroid $\widehat{g}$ that, on one hand, satisfies all the conditions and, on the other hand, $\widehat{g}(\{p_i\}) = n$. In other words, Csirmaz has shown that for every access structure the linear program has a small solution.

Definition 6 (The Csirmaz function). *Let $n \in \mathbb{N}$. Define the* the Csirmaz function $C_n : \{0, \ldots, n\} \to \mathbb{N}$ *as follows*

$$\mathcal{C}_n(k) \overset{def}{=} n + (n-1) + ... + (n-k+1) = nk + \frac{k}{2} - \frac{k^2}{2}.$$

To prove Theorem 1, Csirmaz defined $g : 2^P \to \mathbb{N}$ as $g(A) \overset{\text{def}}{=} \mathcal{C}_n(|A|)$. Next, he extended g to $\widehat{g} : 2^{P\cup\{p_0\}} \to \mathbb{N}$, where for every $A \subseteq P$ he defined $\widehat{g}(A) = g(A)$, and $\widehat{g}(A \cup \{p_0\}) = g(A)$ if $A \in \mathcal{A}$, and $\widehat{g}(A \cup \{p_0\}) = g(A) + 1$ if $A \notin \mathcal{A}$. It can be checked that $\widehat{g}$ satisfies the conditions of the theorem. The Csirmaz function is universal; it is used to construct a polymatroid for every access structure. We next prove that any such universal function is at least as large as the Csirmaz function. This lemma sheds some light why Csirmaz chose this function.

Lemma 1. *Let $y_n : \{0, \ldots, n\} \to \mathbb{R}$ be a function satisfying the following inequalities:*

1. *If $A \subseteq B \subseteq Q$, then $y_n(|B|) \geq y_n(|A|) + 1$ and $y_n(0) = 0$,*
2. *If A and B are subsets of Q such that $A \not\subseteq B$ and $B \not\subseteq A$, then $y_n(|A|) + y_n(|B|) \geq y_n(|A \cap B|) + y_n(|A \cup B|) + 1$.*

The Csirmaz Function $\mathcal{C}_n(k)$ is the minimal function that satisfies these requirements, i.e., for each $1 \leq k \leq n, \mathcal{C}_n(k) \leq y_n(k)$.

Proof. Let A, B be two sets of k elements each that are different in exactly one element. Thus, $|A \cap B| = k-1$ and $|A \cup B| = k+1$. From Item (2) in the lemma, for each $0 \leq k \leq n$

$$y_n(k) - y_n(k-1) \geq y_n(k+1) - y_n(k) + 1.$$

This implies that $y_n(k) - y_n(k-1) \geq y_n(n) - y_n(n-1) + n - k$ for every $0 \leq k \leq n$. By Item (1) in the lemma, $y_n(|B|) \geq y_n(|A|) + 1$. Thus, $y_n(n) - y_n(n-1) \geq 1$. Therefore,

$$y_n(k) - y_n(k-1) \geq n - k + 1. \tag{1}$$

By the requirement in the lemma $y_n(0) = 0$, thus, Inequality (1) with $k = 1$ implies $y_n(1) \geq n = \mathcal{C}_n(1)$. By induction and by (1), $y_n(k) \geq y_n(k-1) + n - k + 1 \geq \mathcal{C}_n(k-1) + n - k + 1 = \mathcal{C}_n(k)$. □

4 When Can Information Inequalities Help?

In this section, we will define when information inequalities can help in improving lower bounds beyond $\Omega(n)$. We start with some notation; using this notation we will define two quantities for an information inequality, Δ and Λ. These quantities are used to define when an information inequality can help.

Notation 2. *Let $A_1, \ldots, A_m$ be m (not necessarily disjoint) sets. For $I \subseteq [m]$, denote $A_I = \bigcup_{i \in I} A_i$.*

Let $\sum_{I \subseteq [m]} \alpha_I H(X_I) \geq 0$ be an information inequality. Given an access structure $\mathcal{A}$, we fix some secret-sharing scheme realizing it. Therefore, the function $f(\widehat{A}) = H(S_{\widehat{A}})/H(S)$ where $\widehat{A} \subseteq P \cup \{p_0\}$ is well defined. Then, for every sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$, the following inequality is valid $\sum_{I \subseteq [m]} \alpha_I f(\widehat{A}_I) \geq 0$. Recall that for every $1 \leq i \leq m$, we defined $A_i = \widehat{A}_i \setminus \{p_0\}$. Using this notation, $f(\widehat{A}_I) = f(A_I) + 1$ if $p_0 \in \widehat{A}_I$ and $A_I \notin \mathcal{A}$, otherwise, $f(\widehat{A}_I) = f(A_I)$.

Definition 7. *For an information inequality $\sum_{I \subseteq [m]} \alpha_I H(X_I) \geq 0$, an access structure $\mathcal{A}$, and sets $\widehat{A}_1, \ldots, \widehat{A}_m$, define Δ as $\Delta \stackrel{def}{=} -\sum_{I : p_0 \in \widehat{A}_I; A_I \notin \mathcal{A}} \alpha_I$.*

Claim 1. *Let $\widehat{A}_1, \ldots, \widehat{A}_m$ be m sets, $\sum_{I \subseteq [m]} \alpha_I H(X_I) \geq 0$ be an information inequality, and $\mathcal{A}$ be an access structure. Then, $\sum_{I \subseteq [m]} \alpha_I f(A_I) \geq \Delta$.*

Proof. Applying the rules $f(\widehat{A}_I) = f(A_I)$ if $p_0 \notin \widehat{A}_I$ or $A_I \in \mathcal{A}$, and $f(\widehat{A}_I) = f(A_I) + 1$ otherwise, the inequality $\sum_{I \subseteq [m]} \alpha_I f(\widehat{A}_I) \geq 0$ implies

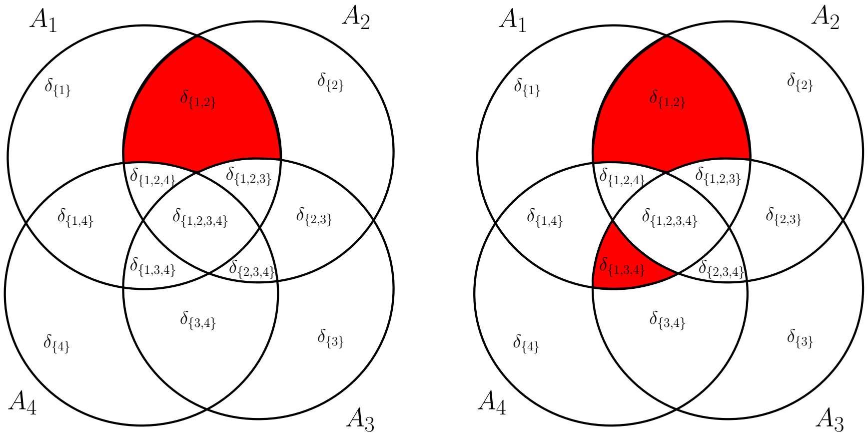
$$\begin{aligned}\sum_{I \subseteq [m]} \alpha_I f(\widehat{A}_I) &= \sum_{I \,:\, p_0 \notin \widehat{A}_I \vee A_I \in \mathcal{A}} \alpha_I f(A_I) + \sum_{I \,:\, p_0 \in \widehat{A}_I \wedge A_I \notin \mathcal{A}} \alpha_I (f(A_I) + 1) \\ &= \sum_{I \subseteq [m]} \alpha_I f(A_I) - \Delta \geq 0. \qquad \square\end{aligned}$$

Observe that Δ can be negative, positive, or equal to zero, but, as we will see later, the information inequality can be useful only when $\Delta > 0$.

Definition 8. *Let $\sum_{I \subseteq [m]} \alpha_I H(X_I) \geq 0$ be an information inequality. For sets $A_1, \ldots, A_m \subseteq P$ define Λ as $\Lambda \stackrel{def}{=} \sum_{I \subseteq [m]} \alpha_I \mathcal{C}_n(|A_I|)$.*

For every $I \subseteq [m]$, the size $|A_I|$ depends on some of the sizes of the intersections between the sets $A_1, \ldots, A_m$. Therefore, we define additional notation in order to represent these intersections. For an illustration of this notation see Fig. 1.

Notation 3. *Let $A_1, \ldots, A_m$ be m (not necessarily disjoint) sets. Denote $\delta_I \stackrel{def}{=} \bigcap_{i \in I} A_i \setminus \bigcup_{i \notin I} A_{\{i\}}$ and $t_I \stackrel{def}{=} |\delta_I|$ for $I \subseteq [m]$. In addition, for $\mathcal{I} \subseteq 2^{[m]}$, denote $\delta_{\mathcal{I}} \stackrel{def}{=} \bigcup_{I \in \mathcal{I}} \delta_I$.*



(a) $\delta_{\{1,2\}} = (A_1 \cap A_2) \setminus (A_3 \cup A_4)$. (b) $\delta_{\{\{1,2\},\{1,3,4\}\}} = \delta_{\{1,2\}} \cup \delta_{\{1,3,4\}}$.

Fig. 1. An illustration of Notation 3 for $m = 4$. For clarity of the illustration, we assume that $\delta_{\{2,4\}} = \delta_{\{1,3\}} = \emptyset$.

Observation 1. $\delta_J \subseteq A_i$ if and only if $i \in J$, that is, $A_i = \cup_{i \in J} \delta_J$ and $A_I = \cup_{i \in I} A_i = \cup_{I \cap J \neq \emptyset} \delta_J$.

Csirmaz has suggested a specific function defined in Definition 6 in order to show the limitations of Shannon information inequalities. We will prove in Lemma 4 that any information inequality remains valid after plugging in the Csirmaz function. That is, if $\sum_{I \subseteq [m]} \alpha_I H(X_I) \geq 0$ is an information inequality, then $\sum_{I \subseteq [m]} \alpha_I \mathcal{C}_n(|A_I|) \geq 0$. So, our only hope is that Δ is "big" for some sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ and the corresponding sets $A_1, \ldots, A_m \subseteq P$, but, $\Lambda = \sum_{I \subseteq [m]} \alpha_I \mathcal{C}_n(|A_I|)$ is negative (or "small"). If this condition does not hold, then the inequality cannot help.

Definition 9. *We say that an information inequality* $\sum_{I \subseteq [m]} \alpha_I H(X_I) \geq 0$ can at most γ-help *if $\Delta \leq \gamma \Lambda$ for every sets $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ and for every access structure $\mathcal{A}$, where $\Delta = -\sum_{I : p_0 \in \widehat{A}_I ; A_I \notin \mathcal{A}} \alpha_I$ and $\Lambda = \sum_{I \subseteq [m]} \alpha_I \mathcal{C}_n(|A_I|)$.*

Theorem 2. *Let $\gamma > 0$ be a constant. Consider a collection of information inequalities, where each information inequality in the collection can at most γ-help. Then, this collection of information inequalities cannot help improving the lower bounds beyond γn even if all inequalities are used simultaneously.*

Proof. Consider an access structure $\mathcal{A}$ and the "huge" linear program obtained for this access structure by applying each information inequality to every choice of subsets of the parties. We take the polymatroid $g(A_I) = \gamma \mathcal{C}_n(|A_I|)$, and we get a solution that satisfies each inequality in the program, where $g(\{p_i\}) = \gamma n$. $\square$

When dealing with a finite collection of information inequalities, one can use a rougher notion than an information inequality that can at most γ-help.

Definition 10. *We say that an information inequality* $\sum_{I\subseteq[m]} \alpha_I H(X_I) \geq 0$ cannot help *(in improving the lower bounds beyond $\Omega(n)$) if for every sets* $\widehat{A}_1, \ldots, \widehat{A}_m \subseteq P \cup \{p_0\}$ *and for every access structure $\mathcal{A}$, if $\Delta > 0$ then $\Lambda > 0$.*

Observation 2. Let $\sum_{I\subseteq[m]} \alpha_I H(X_I) \geq 0$ be an information inequality that cannot help. Observe that $\Delta = -\sum_{I:p_0\in\widehat{A}_I;A_I\notin\mathcal{A}} \alpha_I \geq -\sum_{I:p_0\in\widehat{A}_I;A_I\notin\mathcal{A};\alpha_I<0} \alpha_I$. In addition, using Lemma 3 (proved later), if $\Lambda > 0$ then there exists a constant $\beta > 0$ that depends only on the coefficients of the information inequality (and, therefore, independent of the access structure and the number of parties in the access structure) such that $\Lambda \geq \beta$.[2] Thus, the information inequality can at most γ-help for some constant $\gamma > 0$. If we consider a *finite* collection of information inequalities, such that each inequality in the collection cannot help, then there is a constant $\gamma > 0$ such that each inequality in the collection can at most γ-help, and we can apply Theorem 2. Therefore, when dealing with a finite collection of information inequalities, we will check that each inequality in the collection cannot help; this is easier than calculating the maximal γ for each inequality.

5 Examples of Information Inequalities that Cannot Help

In this section, we demonstrate our method for proving that an information inequality cannot help by considering two example. First, we will demonstrate the calculations and the technique that we will use later on a simple Shannon inequality with two random variables. The fact that this inequality cannot help follows from Csirmaz's proof that using only Shannon inequalities one cannot prove better lower bounds. We reprove this result in order to supply a simple example of our method.

We consider the inequality $f(\widehat{A}_1) + f(\widehat{A}_2) \geq f(\widehat{A}_1 \cup \widehat{A}_2) + f(\widehat{A}_1 \cap \widehat{A}_2)$ for two sets $\widehat{A}_1, \widehat{A}_2 \subseteq P \cup \{p_0\}$. This inequality follows from the fact that the conditional mutual information is non-negative. We should calculate $\Lambda = \mathcal{C}_n(|A_1|) + \mathcal{C}_n(|A_2|) - \mathcal{C}_n(|A_1 \cup A_2|) - \mathcal{C}_n(|A_1 \cap A_2|)$. By Obseration 1, $|A_1| = t_1 + t_{1,2}$, $|A_2| = t_2 + t_{1,2}$, $|A_1 \cup A_2| = t_1 + t_{1,2} + t_2$, and $|A_1 \cap A_2| = t_{1,2}$.[3] Furthermore, $n = t_1 + t_{1,2} + t_2$. Therefore, for every $A_1, A_2 \subseteq P$

$$
\begin{aligned}
&\mathcal{C}_n(|A_1|) + \mathcal{C}_n(|A_2|) - \mathcal{C}_n(|A_1 \cup A_2|) - \mathcal{C}_n(|A_1 \cap A_2|) \\
&\quad = (t_1 + t_{1,2}) \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_1 + t_{1,2})}{2} \right] \\
&\qquad + (t_2 + t_{1,2}) \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_2 + t_{1,2})}{2} \right] \\
&\qquad - (t_1 + t_{1,2} + t_2) \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_1 + t_{1,2} + t_2)}{2} \right] \\
&\qquad - t_{1,2} \left[(t_1 + t_{1,2} + t_2) + \frac{1}{2} - \frac{(t_{1,2})}{2} \right] \quad = \quad t_1 t_2.
\end{aligned}
$$

[2] The value of β can be calculated by assigning $t_I = 1$ whenever $t_I > 0$.

[3] For simplicity of our notation, in the rest of the paper we sometimes write $t_{1,2}$ instead of $t_{\{1,2\}}$ (and similarly for other sets).

Assume that $p_0 \in \widehat{A}_1, \widehat{A}_2$. Thus, $p_0 \in \widehat{A}_1 \cup \widehat{A}_2, \widehat{A}_1 \cap \widehat{A}_2$. Before calculating Δ we have to decide which sets are in the access structure. If $A_1 \cup A_2 \notin \mathcal{A}$, then also $A_1, A_2, A_1 \cap A_2 \notin \mathcal{A}$. Thus, $f(A_1 \cup \{p_0\}) = f(A_1)+1$, $f(A_2 \cup \{p_0\}) = f(A_2)+1$, $f(A_1 \cup A_2 \cup \{p_0\}) = f(A_1 \cup A_2) + 1$, and $f(A_1 \cap A_2 \cup \{p_0\}) = f(A_1 \cap A_2) + 1$. Therefore, $\Delta = 0$ and the inequality cannot help using these selections. However, if $A_1, A_2 \in \mathcal{A}$, but $A_1 \cap A_2 \notin \mathcal{A}$, then $f(A_1 \cup \{p_0\}) = f(A_1)$, $f(A_2 \cup \{p_0\}) = f(A_2)$, $f(A_1 \cup A_2 \cup \{p_0\}) = f(A_1 \cup A_2)$, and $f((A_1 \cap A_2) \cup \{p_0\}) = f(A_1 \cap A_2) + 1$. Therefore, $\Delta = 1 > 0$ as needed. But the selection of $A_1, A_2 \in \mathcal{A}$ and $A_1 \cap A_2 \notin \mathcal{A}$ implies $A_1 \setminus (A_1 \cap A_2), A_2 \setminus (A_1 \cap A_2) \neq \emptyset$ which means that $t_1 > 0$ and $t_2 > 0$, thus, $\Lambda = t_1 \cdot t_2 \geq 1 > 0$ as well. In other words using these selections the inequality cannot help. Moreover, every other set of selections cannot help to achieve $\Delta > 0$ while $\Lambda = 0$.

To conclude, given an information inequality we want $\Delta > 0$ while $\Lambda = 0$. By different choices of which sets are in the access structure and which sets contain the dealer we get different values of Δ. We want choices that maximize Δ. However, notice that by choosing, for example, $A_1 \in \mathcal{A}$ while $A_2 \notin \mathcal{A}$, we must have that $A_1 \setminus A_2 \neq \emptyset$. Thus, the choices of which sets are in the access structure force that certain sets are non-empty, which might imply that $\Lambda > 0$.

5.1 The Zhang and Yeung Information Inequality Cannot Help

We next consider the Zhang and Yeung information inequality [47] – the first Non-Shannon inequality that was discovered – and prove that this inequality cannot help in proving lower bounds of $\omega(n)$.

Theorem 3 (The Zhang and Yeung Information Inequality [47, Theorem 3]). *For every four discrete random variables X_1, X_2, X_3, and X_4 the following inequality holds:*

$$\begin{aligned} &3\left[H(X_3X_4) + H(X_2X_4) + H(X_2X_3)\right] + H(X_1X_3) + H(X_1X_2) - H(X_4) \\ &- 2\left[H(X_3) + H(X_2)\right] - H(X_1X_4) - 4H(X_2X_3X_4) - H(X_1X_2X_3) \geq 0. \quad (2) \end{aligned}$$

For every secret-sharing scheme and for every four sets $\widehat{A}_1, \widehat{A}_2, \widehat{A}_3, \widehat{A}_4 \subseteq P \cup \{p_0\}$ we can consider the random variables $X_i = S_{\widehat{A}_i}$ for $i = 1, \ldots, 4$. Thus,

$$\begin{aligned} &3\left[f(\widehat{A}_3\widehat{A}_4) + f(\widehat{A}_2\widehat{A}_4) + f(\widehat{A}_2\widehat{A}_3)\right] + f(\widehat{A}_1\widehat{A}_3) + f(\widehat{A}_1\widehat{A}_2) - f(\widehat{A}_4) \\ &- 2\left[f(\widehat{A}_3) - f(\widehat{A}_2)\right] - f(\widehat{A}_1\widehat{A}_4) - 4f(\widehat{A}_2\widehat{A}_3\widehat{A}_4) - f(\widehat{A}_1\widehat{A}_2\widehat{A}_3) \geq 0. \quad (3) \end{aligned}$$

By choosing which sets contain the dealer and which sets are in the access structure we get different values of Δ. We next apply the Csirmaz function on Inequality (3). We use the same process described above on each one of the terms of (3). After simplifications, we get the following polynomial Λ, which is a multivariate polynomial whose variables are $\{t_I : I \subseteq [m]\}$.

$$\begin{aligned}
&\frac{\overbrace{t_{1,2,3}+t_{1,2,3}^2}}{2} + t_1 t_{1,2,3} + t_{1,2}t_{1,2,3} + \overbrace{t_{1,2,4}+t_{1,2,4}^2} + 2t_1t_{1,2,4} + 2t_{1,2}t_{1,2,4} + t_{1,2}t_{1,3} \\
&+ t_{1,2,3}t_{1,3} + \overbrace{t_{1,3,4}+t_{1,3,4}^2} + 2t_1t_{1,3,4} + 2t_{1,3}t_{1,3,4} + \frac{\overbrace{t_{1,4}+t_{1,4}^2}}{2} + t_1t_{1,4} + 2t_{1,2}t_{1,4} \\
&+ 2t_{1,2,4}t_{1,4} + 2t_{1,3}t_{1,4} + t_{1,3,4}t_{1,4} + t_{1,2,3}t_2 + 2t_{1,2,4}t_2 + t_{1,3}t_2 + 2t_{1,4}t_2 + t_{1,2}t_{2,3} \\
&+ \overbrace{t_{2,3}+t_{2,3}^2} + t_1t_{2,3} + t_{1,2,3}t_{2,3} + t_{1,3}t_{2,3} + 2t_2t_{2,3} + \frac{\overbrace{t_{2,4}+t_{2,4}^2}}{2} + 2t_1t_{2,4} + t_2t_{2,4} \\
&+ 2t_{1,2}t_{2,4} + 2t_{1,2,4}t_{2,4} + 2t_{1,4}t_{2,4} + t_{1,2}t_3 + t_{1,2,3}t_3 + 2t_{1,3,4}t_3 + 2t_{1,4}t_3 + 2t_2t_3 \\
&+ 2t_{2,3}t_3 + \frac{\overbrace{t_{3,4}+t_{3,4}^2}}{2} + 2t_1t_{3,4} + 2t_{1,3}t_{3,4} + 2t_{1,3,4}t_{3,4} + 2t_{1,4}t_{3,4} + t_3t_{3,4} + +t_1t_4 \\
&+ 2t_{1,2}t_4 + 2t_{1,2,4}t_4 + 2t_{1,3}t_4 + 2t_{1,3,4}t_4 + t_{1,4}t_4 + t_2t_4 + t_{2,4}t_4 + t_3t_4 + t_{3,4}t_4.
\end{aligned}$$

After applying the Csirmaz function we get a polynomial of degree 2 such that all its coefficients are non-negative. We are looking for the following situation: $\Lambda = 0$ while $\Delta > 0$. Since all coefficients are non-negative and $t_I \geq 0$ for every $I \subseteq [m]$, the value of Λ is zero if every monomial in Λ is zero. In particular, every term $\beta \cdot t_I$ or $\beta \cdot t_I^2$ in Λ has to be equal to zero. If the coefficient β is positive, then $t_I = 0$ must hold. Thus, $t_{1,2,3} = t_{1,2,4} = t_{1,3,4} = t_{1,4} = t_{2,3} = t_{2,4} = t_{3,4} = 0$. Let Λ' be the polynomial after setting these variables to be zero, that is,

$$\Lambda' = t_{1,2}t_{1,3} + t_{1,3}t_2 + t_{1,2}t_3 + 2t_2t_3 + t_1t_4 + 2t_{1,2}t_4 + 2t_{1,3}t_4 + t_2t_4 + t_3t_4.$$

The polynomial Λ' should be zero, therefore, in the inequality above one of the variables (i.e., set size) in each monomial has to be zero (e.g., $t_{1,2} = 0$ or $t_{1,3} = 0$).

We use a brute-force algorithm for checking if it is possible that $\Delta > 0$ while $\Lambda = 0$. We have two decisions to make:

- For each $i \in \{1, \ldots, 4\}$ we should decide if $p_0 \in \widehat{A}_i$ or not.
- We have to decide which sets are in the access structure. Specifically, for each $I \subseteq [m]$ such that $\alpha_I \neq 0$ in the information inequality, we need to decide whether $A_I \notin \mathcal{A}$ or $A_I \in \mathcal{A}$. These decisions should be consistent with the constrains that some sets δ_J are of size zero.

Example 1. Assume that A_4 is the only minimal set in the in the access structure. Thus, the sets that are in the access structure are exactly those that include A_4. We add the dealer to $\widehat{A}_2$ and do not add it to any other set. After committing to these decisions we compute Δ as specified in Definition 7, $\Delta = -\sum_{2 \in I, 4 \notin I} \alpha_I = -(3 + 1 - 2 - 1) = -1 < 0$. Thus, these decisions cannot help.

Example 2. Assume that $A_{\{1,2\}}$ and $A_{\{2,3\}}$ are the only minimal sets in the in the access structure. This means that the sets that are in the access structure are exactly those that include $A_{\{1,2\}}$ or $A_{\{2,3\}}$. For example, $A_{\{1,2,3\}} \in \mathcal{A}$. We also add the dealer to every $\widehat{A}_i$, $1 \leq i \leq 4$. After committing to these two decisions we compute $\Delta = -\sum_{\{1,2\}\not\subseteq I \wedge \{1,3\}\not\subseteq I} \alpha_I = -(3+3+3-1-2-2-1-4) = 1 > 0$. Observe that $\Delta > 0$ as needed. But, $A_{\{1,2\}} \in \mathcal{A}$ while $A_{\{1,3\}} \notin \mathcal{A}$. This means that $A_{\{1,2\}} \setminus A_{\{1,3\}} = \delta_{\{\{2\},\{2,4\}\}} \neq \emptyset$. However, we have set $t_{2,4} = 0$, thus, $t_2 \neq 0$. In a similar way, $A_{\{2,3,4\}} \in \mathcal{A}$ while $A_{\{2,3\}} \notin \mathcal{A}$. This means that $A_{\{2,3,4\}} \setminus A_{\{2,3\}} = \delta_{\{\{4\},\{1,4\}\}} \neq \emptyset$. However, we have set $t_{1,4} = 0$, thus, $t_4 \neq 0$. Combining these two constraints we get $t_2 \cdot t_4 > 0$, which implies $\Lambda > 0$. Thus, as before, these decisions cannot help.

We have written a computer program that checks all the possibilities for including the dealer in the sets and for which sets are in the access structure. The computer program showed that for each possible combination either $\Delta \leq 0$ or $\Lambda > 0$ (or both). This means that the Csirmaz function is still a solution to the linear program and this inequality cannot help.

6 All Known Information Inequalities Cannot Help

In this section we describe an algorithm that checks if an information inequality cannot help. We executed this algorithm on all known information inequalities, except for two infinite collections of inequalities, and verified that they cannot help. Thereafter, we consider the two known infinite collections of information inequalities and show that they can at most γ-help for some constant $\gamma > 0$. Before presenting these results, we show how to compute the polynomial Λ efficiently and analyze its properties.

6.1 Properties of the Polynomial Λ

For every information inequality $\sum_{I\subseteq[m]} \alpha_I H(X_I) \geq 0$ and for every sets $A_1, \ldots, A_m$ we consider the quantity $\Lambda = \sum_{I\subseteq[m]} \alpha_I \mathcal{C}_n(|A_I|)$. By Obseration 1, $|A_I| = \sum_{I\cap J\neq\emptyset} t_J$. Thus, we consider $\Lambda = \sum_{I\subseteq[m]} \alpha_I \mathcal{C}_n(\sum_{I\cap J\neq\emptyset} t_J)$ as a polynomial in the variables $\{t_J\}_{J\subseteq[m]}$. We start with proving a property of information inequalities that we use in the analysis of our algorithm.

Lemma 2. *Let $\sum_I \alpha_I H(X_I) \geq 0$ be an information inequality. Then, for every $J \subseteq [m]$, $\sum_{I\cap J\neq\emptyset} \alpha_I \geq 0$.*

Proof. Define a random variable Y which is uniformly distributed in $\{0,1\}$; in particular $H(Y) = 1$. Now define $X_1, \ldots, X_m$, where $X_j = Y$ iff $j \in J$ and $X_j = 0$ otherwise (that is, in the latter case X_j is a deterministic variable whose entropy is 0). This implies that $H(X_I) = 1$ iff $I \cap J \neq \emptyset$ and $H(X_I) = 0$ otherwise. Since the information inequality holds for every random variables, the lemma follows. □

Lemma 3. *For every information inequality the polynomial Λ is a multivariate polynomial with total degree 2. Furthermore, the coefficient of every monomial in Λ is non-negative and can be efficiently calculated from the information inequality (without applying the Csirmaz function).*

Proof. The fact that the polynomial Λ is a multivariate polynomial with total degree 2 can be deduced from the structure of the Csirmaz function (see Definition 6), that is, Λ is a sum of polynomials $\mathcal{C}_n(|A_I|) = \mathcal{C}_n(\sum_{I\cap J\neq\emptyset} t_J)$, where $\mathcal{C}_n(k)$ is polynomial of degree 2. Next, we compute the coefficients of Λ. Recall that $n = \sum_{I\subseteq[m]} t_I$.

$$\begin{aligned}
\Lambda = \sum_{I\subseteq[m]} \alpha_I \mathcal{C}_n(|A_I|) &= \sum_{I\subseteq[m]} \alpha_I \left[n\,|A_I| + \frac{|A_I|}{2} - \frac{|A_I|^2}{2} \right] \\
&= \sum_{I\subseteq[m]} \alpha_I \left(\sum_{J:I\cap J\neq\emptyset} t_J + \sum_{J:I\cap J=\emptyset} t_J \right) \left(\sum_{J:I\cap J\neq\emptyset} t_J \right) + \sum_{I\subseteq[m]} \alpha_I \frac{\sum_{J:I\cap J\neq\emptyset} t_J}{2} \\
&\quad - \sum_{I\subseteq[m]} \alpha_I \frac{\left(\sum_{J:I\cap J\neq\emptyset} t_J\right)^2}{2} \\
&= \sum_{I\subseteq[m]} \alpha_I \left(\frac{\sum_{J:I\cap J\neq\emptyset} t_J + \left(\sum_{J:I\cap J\neq\emptyset} t_J\right)^2}{2} + \sum_{J:I\cap J\neq\emptyset} t_J \cdot \sum_{J:I\cap J=\emptyset} t_J \right).
\end{aligned}$$

We can now compute the coefficients of the monomials of the polynomial Λ:

1. βt_J: In this case $\beta = \frac{\sum_{I\cap J\neq\emptyset} \alpha_I}{2}$, i.e., the sum of the coefficients of sets that include δ_J. By Lemma 2 this sum is non negative.
2. βt_J^2: In this case $\beta = \frac{\sum_{I\cap J\neq\emptyset} \alpha_I}{2}$, again, this is the sum of the coefficients of sets that include δ_J.
3. $\beta t_J t_K$: In this case $\beta = \sum_{I\,:\,I\cap(J\cup K)\neq\emptyset} \alpha_I$. That is, β is the sum of coefficients of sets that include at least one of t_J and t_K, and by Lemma 2, $\beta \geq 0$. □

As all the coefficients in Λ are non-negative and all the values of t_I are non-negative, its value is always non-negative. That is,

Lemma 4. *Let $\sum_{I\subseteq[m]} \alpha_I H(X_I) \geq 0$ be an information inequality. Then, for every sets $A_1, \ldots, A_m \subseteq P$, $\sum_{I\subseteq[m]} \alpha_I C_n(|A_I|) \geq 0$.*

6.2 An Algorithm for Checking If an Information Inequality Cannot Help

We next present the algorithm that checks if an information inequality cannot help. The algorithm is a brute-force algorithm that checks, for each possible choice of adding the dealer or not adding the dealer to each set A_i and for each possible choice $A_I \in \mathcal{A}$ or $A_I \notin \mathcal{A}$ for each $I \subseteq [m]$, if $\Delta > 0$ while it is possible that $\Lambda = 0$. To check if Λ can equal 0 under some a specific choice, we check for each choice $t_I = 0$ and $t_I > 0$ for each $I \subseteq [m]$ if (1) $\Lambda = 0$ under this choice,

Input : An information inequality $\sum_{A\subseteq[m]} \alpha_A H(X_A) \geq 0$.
Output: "NO" if the information inequality cannot help, "YES" otherwise.

1 *Calculate the polynomial Λ using Lemma 3*;
2 **foreach** *monomial in Λ of the form βt_J where $\beta \neq 0$* **do** set $t_J = 0$;
3 Let Λ' be the resulting polynomial after setting these variables.;
4 **foreach** *choice of setting $A_I \in \mathcal{A}$ or $A_I \notin \mathcal{A}$ for each $\alpha_I \neq 0$ in the information inequality* **do**
    `/* If there are` q `terms with non-zero coefficient in` $\sum_{I\subseteq[m]} \alpha_I H(X_I) \geq 0$`, there are` 2^q `combinations. */`
5   **foreach** *choice of setting $p_0 \in \widehat{A}_i$ or $p_0 \notin \widehat{A}_i$ for every $1 \leq i \leq m$* **do**
        `/* There are` 2^m `combinations. */`
6   Calculate $\Delta = -\sum_{I:p_0\in\widehat{A}_I;A_I\notin\mathcal{A}} \alpha_I$;
7   **if** $\Delta \leq 0$ **then** go to (5);
        `/* Check if it is possible that` $\Lambda = 0$`: */`
8   **foreach** *choice of setting $t_I = 0$ or $t_I > 0$ for every $I \subseteq [m]$* **do**
            `/* There are` 2^{2^m} `such combinations. */`
9   **foreach** *monomial $\beta t_J t_K$ in Λ', where $\beta \neq 0$* **do**
10   **if** *$t_J > 0$ and $t_K > 0$ in the current explored combination* **then** go to (8);
11   **end**
12   **foreach** *I, J where $\alpha_I \neq 0$ and $\alpha_J \neq 0$ in the information inequality $\sum_{I\subseteq[m]} \alpha_I H(X_I) \geq 0$* **do**
13   **if** *in the current explored combination $A_I \in \mathcal{A}, A_J \notin \mathcal{A}$, and there is no $K \subseteq [m]$ such that $I \cap K \neq \emptyset, J \cap K = \emptyset$, and $t_K > 0$ in the current explored combination* **then** go to (8);
14   **end**
15   **return** *"YES"*
16   **end**
17   **end**
18 **end**
19 **return** *"NO"*

Algorithm 1: A brute-force algorithm that checks if an information inequality cannot help.

and (2) this choice is consistent with the choice of sets that are in the access structure. The algorithm is formally described in Algorithm 1.

We have executed Algorithm 1 on the following non-Shannon inequalities:

- The first Non-Shannon inequality with four variables that was discovered by Zhang and Yeung in [47].
- The six Non-Shannon inequalities with four variables and anther one with five variables in [23].
- The five Non-Shannon inequalities with four variables in [44].
- The inequality of Ingleton in [29].[4]

[4] The inequality of Ingleton [29] holds only for linear-algebraic spaces.

For each of these inequalities the result is the same – the information inequality cannot help in proving lower bounds of $\omega(n)$.

Remark 2. The algorithm written above is not efficient. However, for our purpose – checking information inequalities with four or five variables – the algorithm is good enough. To be precise, the running of the computer program executing the algorithm takes less than a minute even for an information inequality of [23] that contains five variables. All other inequalities contain 4 variables and the running time is better.

Remark 3. Our algorithm gives a necessary condition for an information inequality to be helpful. We do not know of an information inequality that fulfills this necessary condition. We do have an example of a potential inequality that satisfies it: $H(X_1X_2)+H(X_1X_3)+H(X_2X_3)+H(X_4) \leq H(X_1X_2X_3)+H(X_1)+H(X_2)+H(X_3X_4)$. We stress that we do not know if this is an information inequality. It does satisfy Lemma 2 and some stronger conditions for being an information inequality.

6.3 Dealing with the Known Infinite Collections of Information Inequalities

There are a few examples for infinite sequences of Non-Shannon inequalities. The first infinite sequence of Non-Shannon inequalities was discovered by Zhang and Yeung in [47]; they show for every $n \in \mathbb{N}$ an information inequality with n variables. A sequence of Non-Shannon information inequalities generalizing the result of [47] appears in [33, 46]. Finally, an infinite sequence of Non-Shannon information inequalities with four variables was given in [44].

In [44] there is a symbolic inequality with four variables, where some of the coefficients are a function of a parameter s. This inequality is an information inequality for every assignment $s \in \mathbb{N}^+$. For example, for $s = 2$ it yields the Zhang and Yeung information inequality [47]. For this symbolic information inequality, we computed the symbolic polynomial Λ and proved that there is a constant $\gamma > 0$ such that for every $s \in \mathbb{N}^+$ the information inequality with parameter s can at most γ-help. We used a similar technique to deal with the infinite sequence presented in [46] that is more general than the infinite sequences presented in [47, 33]. For these sequences the result is that there is a constant $\gamma > 0$ such that every inequality in the sequence can at most γ-help.

Using Theorem 2 we conclude that all the known information inequalities cannot help in proving lower bounds of $\omega(n)$ on the size of the shares in secret-sharing schemes.

Theorem 4. *The information inequalities of [29, 47, 33, 46, 23, 44] cannot help in proving lower bounds of $\omega(n)$ even if they are used simultaneously.*

Acknowledgment. We thank the anonymous TCC referees for valuable comments.

References

[1] L. Babai, A. Gál, and A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.
[2] A. Beimel and B. Chor. Universally ideal secret sharing schemes. *IEEE Trans. on Info. Theory*, 40(3):786–794, 1994.
[3] A. Beimel and M. Franklin. Weakly-private secret sharing schemes. In S. Vadhan, editor, *TCC 2007*, volume 4392 of *LNCS*, pages 253–272. Springer-Verlag, 2007.
[4] A. Beimel, N. Livne, and C. Padró. Matroids can be far from ideal secret sharing. In *TCC 2008*, volume 4948 of *LNCS*, pages 194–212, 2008.
[5] M. Bellare and P. Rogaway. Robust computational secret sharing and a unified account of classical secret-sharing goals. In *14th CCS*, pages 172–184, 2007.
[6] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computations. In *20th STOC*, pages 1–10, 1988.
[7] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. In *CRYPTO '88*, volume 403 of *LNCS*, pages 27–35. Springer-Verlag, 1990.
[8] G. R. Blakley. Safeguarding cryptographic keys. In *Proc. of the 1979 AFIPS National Computer Conference*, pages 313–317, 1979.
[9] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro. On the information rate of secret sharing schemes. *Theoretical Computer Science*, 154(2):283–306, 1996.
[10] C. Blundo, A. De Santis, and U. Vaccaro. On secret sharing schemes. *Inform. Process. Lett.*, 65(1):25–32, 1998.
[11] E. F. Brickell. Some ideal secret sharing schemes. *Journal of Combin. Math. and Combin. Comput.*, 6:105–113, 1989.
[12] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro. On the size of shares for secret sharing schemes. *J. of Cryptology*, 6(3):157–168, 1993.
[13] T. H. Chan and R. W. Yeung. On a relation between information inequalities and group theory. *IEEE Trans. on Info. Theory*, 48(7):1992–1995, 2002.
[14] D. Chaum, C. Crépeau, and I. Damgård. Multiparty unconditionally secure protocols. In *20th STOC*, pages 11–19, 1988.
[15] B. Chor and E. Kushilevitz. Secret sharing over infinite domains. *J. of Cryptology*, 6(2):87–96, 1993.
[16] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley & Sons, 1991.
[17] R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 316–334. Springer-Verlag, 2000.
[18] L. Csirmaz. The size of a share must be large. In A. De Santis, editor, *EUROCRYPT '94*, volume 950 of *LNCS*, pages 13–22. Springer-Verlag, 1995.
[19] L. Csirmaz. The dealer's random bits in perfect secret sharing schemes. *Studia Sci. Math. Hungar.*, 32(3–4):429–437, 1996.
[20] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In *CRYPTO '91*, volume 576 of *LNCS*, pages 457–469. Springer-Verlag, 1992.
[21] M. van Dijk. A linear construction of perfect secret sharing schemes. In *EUROCRYPT '94*, volume 950 of *LNCS*, pages 23–34. Springer-Verlag, 1995.
[22] M. van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6:143–169, 1995.
[23] R. Dougherty, C. Freiling, and K. Zeger. Six new non-Shannon information inequalities. In *ISIT 2006*, pages 233–236, 2006.

[24] R. Dougherty, C. Freiling, and K. Zeger. Networks, matroids, and non-Shannon information inequalities. *IEEE Trans. on Info. Theory*, 53(6):1949–1969, 2007.

[25] S. Fujishige. Polymatroidal dependence structure of a set of random variables. *Information and Control*, 39(1–3):55–72, 1978.

[26] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Computational Complexity*, 10(4):277–296, 2002.

[27] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th CCS*, pages 89–98, 2006.

[28] L. Guille, T. H. Chan, and A. Grant. The minimal set of Ingleton inequalities. Technical Report 0802.2574, arxiv.org, 2008. `http://arxiv.org/abs/0802.2574`.

[29] A. W. Ingleton. Conditions for representability and transversability of matroids. In *Proc. Fr. Br. Conf 1970*, pages 62–67. Springer-Verlag, 1971.

[30] M. Ito, A. Saito, and T. Nishizeki. Secret sharing schemes realizing general access structure. In *Globecom 87*, pages 99–102, 1987.

[31] M. Karchmer and A. Wigderson. On span programs. In *Proc. of the 8th IEEE Structure in Complexity Theory*, pages 102–111, 1993.

[32] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Info. Theory*, 29(1):35–41, 1983.

[33] K. Makarychev, Y. Makarychev, A. Romashchenko, and N. Vereshchagin. A new class of non-Shannon type inequalities for entropies. *Communications in Information and Systems*, 2(2):147–166, 2002.

[34] F. Matúš. Infinitely many information inequalities. In *IEEE International Symposium on Information Theory 2007*, pages 41–44, 2007.

[35] F. Matúš. Two constructions on limits of entropy functions. *IEEE Trans. on Info. Theory*, 53(1):320–330, 2007.

[36] M. Naor and A. Wool. Access control and signatures via quorum secret sharing. *IEEE Transactions on Parallel and Distributed Systems*, 9(1):909–922, 1998.

[37] J. G. Oxley. *Matroid Theory*. Oxford University Press, 1992.

[38] M. O. Rabin. Randomized Byzantine generals. In *Proc. of the 24th IEEE Symp. on Foundations of Computer Science*, pages 403–409, 1983.

[39] S. Riis. Graph entropy, network coding and guessing games. Technical Report 0711.4175, arxiv.org, 2007. `http://arxiv.org/abs/0711.4175`.

[40] A. Shamir. How to share a secret. *Comm. of the ACM*, 22:612–613, 1979.

[41] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[42] G. J. Simmons, W. Jackson, and K. M. Martin. The geometry of shared secret schemes. *Bulletin of the ICA*, 1:71–88, 1991.

[43] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Technical Report 2008/290, Cryptology ePrint Archive, 2008. `http://eprint.iacr.org/`.

[44] W. Xu, J. Wang, and J. Sun. A projection method for derivation of non-Shannon-type information inequalities. In *ISIT 2008*, pages 2116–2120, 2008.

[45] R. W. Yeung. *A First Course in Information Theory*. Springer, 2006.

[46] Z. Zhang. On a new non-Shannon type information inequality. *Communications in Information and Systems*, 3(1):47–60, 2003.

[47] Z. Zhang and R. W. Yeung. On characterization of entropy function via information inequalities. *IEEE Trans. on Info. Theory*, 44(4):1440–1452, 1998.