Emirhan Gürpınar

Bounds on guessing numbers and secret sharing combining information theory methods

Kybernetika, Vol. 60 (2024), No. 5, 553–575

Persistent URL: http://dml.cz/dmlcz/152714

KYBERNETIKA — VOLUME *60* (2024), NUMBER 5, PAGES 553–575

BOUNDS ON GUESSING NUMBERS AND SECRET SHARING COMBINING INFORMATION THEORY METHODS

Emirhan Gürpinar

This paper is on developing some computer-assisted proof methods involving non-classical inequalities for Shannon entropy.

Two areas of the applications of information inequalities are studied: Secret sharing schemes and hat guessing games. In the former a random secret value is transformed into shares distributed among several participants in such a way that only the qualified groups of participants can recover the secret value. In the latter each participant is assigned a hat colour and they try to guess theirs while seeing only some of the others'. The aim is to maximize the probability that every player guesses correctly, the optimal probability depends on the underlying sight graph. We use for both problems the method of non-Shannon-type information inequalities going back to Z. Zhang and R. W. Yeung. We employ the linear programming technique that allows to apply new information inequalities indirectly, without even writing them down explicitly. To reduce the complexity of the problems of linear programming involved in the bounds we extensively use symmetry considerations. Using these tools, we improve lower bounds on the ratio of key size to secret size for the former problem and an upper bound for one of the ten vertex graphs related to an open question by Riis for the latter problem.

Keywords: Shannon entropy, non-Shannon-type information inequalities, secret sharing, linear programming, symmetries, copy lemma, entropy region, guessing games, network coding, multiple unicast, information theory, Shannon inequalities

Classification: 94A05, 94A15, 94A17, 94A62

1. INTRODUCTION

The aim of this paper is to show how the techniques of computer-assisted proofs for information inequalities (for the Shannon entropy) can be used in various applications. Each ingredient of our approach has already been known, but we argue that a properly chosen combination of these methods is quite powerful, to the point that we can improve several previously known bounds. We apply the techniques to two targets: we prove lower bounds for the efficiency of *secret sharing schemes* (for several specific access structures) and upper bounds for *hat guessing games*. Our new bounds are proven using heavy computations and it seems that the same results would be very hard to achieve

DOI: 10.14736/kyb-2024-5-0553

manually, without a computer. Our main goal is to show the efficiency of the right combination of technical tools; this is why we have deliberately chosen problems (in secret sharing and in hat-guessing games) that were already studied earlier by other researchers, so that we can compare our results with previously known bounds.

We go on with a brief review of the fields of secret sharing and hat guessing games in which we apply our techniques.

The notion of secret sharing introduced by Shamir [30] and Blakley [6], is nowadays pretty standard in cryptography. In what follows the motivation and the basic definition of secret sharing is recalled.

Imagine that we want to share a secret between some participants in such a way that

- some coalitions (subsets of participants), the *authorized* ones, can reconstruct the secret combining their shares;
- the other coalitions are not qualified, they get no information about the secret.

One can easily imagine practical situations when such a tool is useful, and Shamir's famous secret sharing scheme deals with the case when all sufficiently large groups (at least t participants for some threshold t) are authorized while small groups with less than t participants are not. Given the description of the authorized coalitions for a set of participants, we want to find how small the maximal share size can be made, with respect to the size of the secret. In general this is an open problem, thus we look for lower bounds on this quantity as frequently done in the literature. Such questions are of interest in their own right. Also, they can be used as benchmarks for the techniques based on information inequalities.

In this article we study several particular access structures. We improve some previously known lower bounds for their information ratios. The previously known bounds were obtained using the Ahlswede–Körner (AK) lemma in [15]. We use a different technique – the general version of the *copy lemma* [36] combined with symmetry considerations. For every given access structure, we reduce the question of the information ratio to a linear problem (of very large size) and then use linear programming solvers to obtain a lower bound for this information ratio. Our results on secret sharing are summarized in Theorem 4.2 and compared with the previously known bounds in Table 2.

The *hat guessing games* is a family of recreational mathematics problems [33], some variants of which are known to be connected to coding theory [28]. Each player gets a hat of some colour (invisible to them) and has to guess this colour (knowing only the colours of the hats they see). There are many versions of these games [8, 19]. We consider a version introduced by Riis in [26, 27] as it is connected with some other interesting problems. In this version the visibility (who can see whose hats) is determined by a graph named the sight graph. The challenge is to maximize the probability that each player guesses their hat colour correctly. No communication between players is allowed during the game, but a strategy can be agreed upon before the game.

This problem for an arbitrary graph remains open. Moreover there exists a specific graph with 10 vertices for which the question is open (the single smallest such undirected graph). We improve the upper bound on the probability of 'correct guessing' for this graph. Our main result here is given in Theorem 5.2 and compared with the previously known bound in Section 5.

To bound the quantities that arise in both of these problems (secret sharing and hat guessing games), we use a combination of several techniques. To prove the bounds, we use non-classical inequalities for entropy (non-Shannon-type inequalities). We derive the necessary inequalities with the *copy lemma*. More precisely, we use these new inequalities indirectly, without writing them explicitly. To this end, we combine the copy lemma with the linear programming approach. To decrease the complexity of the linear program and improve the results we use symmetry considerations (the symmetries of the authorized coalitions for problems of secret sharing and the symmetries of the sight graphs for the hat guessing games). Each of these techniques has already been known. However their combination proves to be so efficient that we improve some known bounds for these problems. Our improved bounds are given in the Results sections (in Section 4.2 and Section 5.2).

In the next section we give preliminaries and explain the context in more detail. In Section 3 we discuss symmetries. In the following sections we formulate more precisely the particular problems on which we apply our method.

2. PRELIMINARIES

2.1. Entropy region

Definition 2.1. (Entropy Vector) Let $X = (X_i)_{i\in[\![1,n]\!]}$[1] be a sequence of jointly distributed random variables with a finite range. We denote by h_X the vector, the coordinates of which are the values of Shannon entropy for all sub-tuples of X. This vector is called the *entropy vector* (also known as *the entropy profile*) of X. Note that it consists of $2^n - 1$ real components $h_I = H((X_i)_{i\in I})$[2] for each $\varnothing \neq I \subseteq [\![1, n]\!]$, so it is in $\mathbb{R}^{2^n-1}$.

Definition 2.2. (Entropy Region) For $n > 0$, the set of all entropy vectors of dimension 2^n-1 (for every distribution of n-tuples of random variables) is called the *entropy region*. Following [36], we use the notation $\Gamma^*_n \subset \mathbb{R}^{2^n-1}$ for it.

Definition 2.3. (Almost Entropic) The closure of Γ^*_n is noted $\overline{\Gamma^*_n}$, and its elements are called *almost entropic* vectors. Any non-strict inequality that is satisfied by all elements of Γ^*_n is also satisfied by all elements of $\overline{\Gamma^*_n}$ by limit.

Remark 2.4. $\overline{\Gamma^*_n}$ is a convex cone [35]. In particular it is invariant under multiplication by a non-negative scalar in $\mathbb{R}_+$.

So $\overline{\Gamma^*_n}$ is defined solely by the linear inequalities satisfied by Γ^*_n.
The characterization of Γ^*_n and that of its closure are open problems.

2.2. Information Inequalities for entropy

Definition 2.5. (Information Inequality) An *information inequality* for entropy is a linear inequality for the entropy quantities of jointly distributed random variables with real coefficients.

[1]The traditional notation $[\![1, n]\!]$ to denote the set $\{1, 2, \dots n\}$ of integers from 1 to n, is used throughout the article.

[2]The Shannon entropy of a random variable X is denoted as $H(X)$ throughout the article.

By definition of Γ_n^*, the *information inequalities* for n random variables are exactly the linear inequalities for $2^n - 1$ coordinates that are true for all vectors in Γ_n^*.

The first universally true information inequalities were given in the seminal paper [31] by Shannon.

Definition 2.6. (Shannon and Shannon-type inequalities) Let us denote $(X_i)_{i\in I}$ by X_I in short. The inequalities of the form

$$I(X_I : X_J|X_K) \geq 0$$

[3] are called *Shannon inequalities*. They can be expanded as

$$H(X_{I\cup K}) + H(X_{J\cup K}) \geq H(X_{I\cup J\cup K}) + H(X_K).$$

The inequalities that are linear combinations with positive coefficients of Shannon inequalities are called *Shannon-type (classical) inequalities*.

The set of vectors with $2^n - 1$ coordinates (not necessarily entropic) satisfying all classical inequalities is noted Γ_n.

Note that $\Gamma_n^* \subset \overline{\Gamma_n^*} \subset \Gamma_n$, that Γ_n^* is closed under addition and that $\overline{\Gamma_n^*}$ is a convex cone [35].

Definition 2.7. (Elemental Information Inequalities) Let $X_1, \dots X_n$ be random variables. The inequalities of the form

$$I(X_i : X_j|X_K) \geq 0$$

where $i \neq j$ and $K \subseteq [\![1, n]\!] \setminus \{i, j\}$ or $i = j$ and $K = [\![1, n]\!] \setminus \{i\}$ are called *elemental information inequalities* or shortly *elemental inequalities*.

Fact 2.8. Elemental inequalities for n variables imply all Shannon inequalities for n variables by linear combinations with positive coefficients, see [34, Chapter 13].

Remark 2.9. There are $\binom{n}{2}2^{n-2} + n$ elemental inequalities for n variables.

2.3. How to prove an information inequality

Consider a Shannon-type inequality, i. e. a linear combination of Shannon inequalities. Here the situation is simple: for a given number n of random variables (or strings) we have $2^n - 1$ entropic quantities and can write down all the Shannon inequalities for these quantities. Then we want to know whether the inequality in question is a non-negative linear combination of Shannon inequalities. This is a classical question of linear programming, a linear program solver finds out whether it is true or not. One should have in mind, however, that the dimension of the linear program grows exponentially in n, so the linear program could be quite large. There are cases which could be checked

[3] The mutual information of two random variables X and Y is denoted $I(X : Y)$ throughout the article. If Z is another random variable, $I(X : Y|Z)$ denotes the conditional mutual information of X and Y given Z.

by hand, and quite soon we bump into a system of linear inequalities that is inaccessible even for computer programs. To make it smaller, we can use dependencies between Shannon inequalities for different tuples and omit some inequalities that can be derived from the elemental ones.

Let $I_i(X_1, \dots X_n)$ be linear combinations of entropies of subsets of $\{X_1, \dots X_n\}$ for $i \in \mathcal{I}$. Statements of the form

$$\wedge_{i\in\mathcal{I}} I_i(X_1, \dots X_n) \geq 0 \implies I(X_1, \dots X_n) \geq 0$$

are called conditional or constraint inequalities. They often appear in applications. The same technique of linear programming can be applied by adding the conditions

$$I_i(X_1, \dots X_n) \geq 0, i \in \mathcal{I}$$

to the linear program.

In this way we can derive the Shannon-type inequalities starting from Shannon inequalities. Of course, we may as well add some known non-Shannon-type inequalities to the list of inequalities that we combine.

To get and prove non-Shannon-type inequalities, the most common tool is the *copy lemma* that we are going to formulate now. Let us split all the random variables $X_1, \dots X_n$ into two groups $A_1, \dots A_k$ and $B_1, \dots B_\ell$ (in an arbitrary way). We can assume that $A_1, \dots A_k$ are sampled first according to their marginal distribution and then $B_1, \dots B_\ell$ are sampled according to their conditional distribution. In this way we get the same distribution $A_1, \dots A_k, B_1, \dots B_\ell$, so nothing new is obtained yet. But we can, for the same values of $A_1, \dots A_k$, consider another independent sample ('twins') $B'_1, \dots B'_\ell$ using the same conditional distribution. Then, instead of $k + \ell$ variables $A_1, \dots A_k, B_1, \dots B_\ell$ that we started with, we get a joint distribution for $k+2\ell$ variables

$$A_1, \dots A_k,\ B_1, \dots B_\ell,\ B'_1, \dots B'_\ell$$

that have the following properties:

- the distribution of $A_1, \dots A_k, B_1, \dots B_\ell$ is the same as before;
- the distribution of $A_1, \dots A_k, B'_1, \dots B'_\ell$ is the same as for $A_1, \dots A_k, B_1, \dots B_\ell$;
- the tuples $B_1, \dots B_\ell$ and $B'_1, \dots B'_\ell$ are independent given $A_1, \dots A_k$.

Formally we state the copy lemma in the following two forms. X below corresponds to $A_1, \dots A_k$ above. Y and Z correspond to a partition of $B_1, \dots, B_\ell$, such that we discard the duplicates of Y but keep those of Z. This discarding is useful for not increasing the number of total variables of the linear program we use.

Lemma 2.10. (Copy Lemma [36, 12]) Let X, Y, Z be three jointly distributed random vectors.

1. There exists a random vector Z' such that
   - X, Z and X, Z' are identically distributed,

- Z' and Y, Z are independent given X.

2. There exists a random vector Z' such that
   - every sub-vector of X, Z has the same entropy as the sub-vector of X, Z' that consist of the same coordinates,
   - $I(Z' : Y, Z|X) = 0$.

Z' is called a ***Y-copy of Z over X*** or simply ***Y-copy of*** Z when X consist of all the other variables (when 'all variables' are clear from the context).

Item 1 above is the probabilistic statement, which implies the entropic statement item 2. We use the latter in our applications.

Now we can use linear programming to derive consequences of all the Shannon inequalities for all variables (X, Y, Z, Z') and the equalities that are guaranteed by our constructions. Zhang and Yeung [36] discovered that this way *we get new inequalities that include only original variables* X, Y, Z. By 'new', we mean inequalities that are non-Shannon-type, i.e. they are not linear combinations of Shannon inequalities for original variables. Then these new inequalities can be used explicitly, by adding them to the list of Shannon inequalities, or implicitly.

We also extensively use the symmetries of the problem, which guarantee that an optimal solution can be found among the symmetric ones. This helps to reduce the dimension of the linear program and let the solver work faster.

We discuss these tricks in detail in the corresponding sections.

2.4. Preliminaries of secret sharing

Secret sharing was independently introduced by Blakley [6] and Shamir [30]. These original papers studied a class of secret sharing schemes which are now called *threshold schemes*. A more general definition of secret sharing was introduced by Ito, Saito and Nishizeki [18]. One of the relatively recent surveys on the topic is [3], see also the lecture notes [24] for general definitions such as access structures, information ratio and ideal secret sharing.

Definition 2.11. (Secret Sharing Scheme) We formally define a *secret sharing scheme* for a given access structure with participants $1, \dots n$ as a joint distribution (a tuple of random variables) $(S_0, S_1, \dots S_n)$ satisfying the following conditions for each coalition J:

$$\begin{array}{ll} H(S_0|S_J) = 0, & \text{if } J \text{ is a qualified coalition,} \\ H(S_0|S_J) = H(S_0), & \text{if } J \text{ is not a qualified coalition.} \end{array} \tag{1}$$

The random variable S_0 is called the *secret*, and S_j for $j \in [\![1, n]\!]$ are the *shares* given to each party and S_J is short for $(S_j)_{j \in J}$.

Ito, Saito and Nishizeki proved in [18] that for every access structure there exists a secret sharing scheme.

Fact 2.12. (Ito et al. [18]) Every access structure admits a secret sharing scheme.

Benaloh and Leichter [5] noted that the construction of the proof is a special case of a more general one that starts from the monotone boolean function that describes the access structure.

Currently known lower bounds on information ratio of general access structures are much weaker than ideal secret sharing schemes (such as threshold scheme proposed by Shamir): it was proven by Csirmaz [11] that there exist an n-participant access structure the information ratio of which is at least $n/\log_2 n$, also that Shannon inequalities cannot give a better lower bound than n, see [3] for a discussion.

The common approach to prove a lower bound for the information ratio of a certain access structure is to use the technique of information inequalities. We write down the equalities (1) and all Shannon-type inequalities for the involved random variables and then use linear programming to combine these equalities and inequalities to derive a result

$$\max_i H(S_i) \geq r \cdot H(S_0) \tag{2}$$

for a certain real number r. If we succeed, this means that the information ratio of this access structure is at least r. Such an argument can be found in [9] among others.

This simple scheme can be improved. One can add non-Shannon-type inequalities as well; these additional constraints may help to prove (2) with a larger value of r. Proofs following this scheme can be found, for instance in [4] and [22]. However, we do not follow this scheme and do not explicitly add non-Shannon-type inequalities to our linear program. Instead, we do as follows:

1. We write the conditions (1);

2. instead of looking for non-Shannon-type inequalities for the variables that appear in these conditions, we apply one or several times the copy lemma, thus get some new random variables and some equalities for their entropies;

3. then we write down *only Shannon-type inequalities* but for *all* the involved random variables and then deduce (2) for some specific r.

This type of argument is discussed in [17]. A similar approach (with the AK lemma instead of the copy lemma) was used earlier in [14] and later in [2].

2.5. Preliminaries of hat guessing games

Hat guessing game has been a well known recreational mathematics problem with many variants. In this article we are interested in the variant introduced by Riis [27, 26], which uses some concepts from graph theory. It is connected to the multiple unicast problem in network information theory. This connection, among other similar problems mentioned in [27], the definition of the multiple unicast network problem and the theorem that relates it to guessing number are omitted (see the literature) as they are out of scope of this article. Guessing games also have recent applications in combinatorics (more precisely extremal graph theory and forbidden sub-graphs) by Martin and Rombach [21].

Let $G = (V, E)$ be a finite undirected[4] graph where V is the set of vertices and $E \subseteq V \times V$ the set of edges, note that $(x, y) \in E$ if and only if $(y, x) \in E$ since G is undirected. Note also that all the graphs we consider in this article are loopless. Let $s > 1$ be an integer, and let us denote A_s the set of colours. The game is played on such a graph G called the *sight graph*.

1. At every node $v \in V$ there is a player.
2. Every player is assigned a hat colour s_v from $[\![1, s]\!] = \{1, 2, \dots s\}$ uniformly randomly and independent of the hats of the other players.
3. The edges of the graph show who can see whom, if the vertices x and y are visible from each other, then there is an edge $x \leftrightarrow y$, see Figure 1.
4. The players win as a team if every single one of them guesses their own hat colour correctly and lose otherwise.

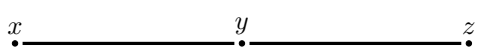

Fig. 1. On the graph above, x and y can see each other, but x and z cannot.

So the players do not compete but cooperate to win. Although they cannot communicate after the game starts (not even hear what another guesses), that is when the hat colours are determined; they can agree on a strategy beforehand and they a priori know G, s and which player is on which vertex. This is shortly called a game on (G, s) or a (G, s)-game. As G is loopless, clearly there is no strategy to win with probability 1. The aim is to maximize the probability of winning. Below we give a formalization of what a strategy is.

Definition 2.13. (Strategy) Let $G = (V, E)$ be the graph on which the game is played with s colours.

A *guessing function* for the player on $x \in V$ is a mapping from $[\![1, s]\!]^{\{y \in V | (x,y) \in E\}}$ to $[\![1, s]\!]$. Intuitively, a guessing function is a table that shows what to guess for every possible configuration of what this player can see. Note that these configurations are equiprobable.

A *strategy* is a family of guessing functions $\mathcal{F} = (f_v)_{v \in V}$ for every vertex of the graph.

Note that there are finitely many guessing functions for a player and thus finitely many strategies for a given (G, s)-game.

In case we want to talk about *random strategy*, we call strategy defined above *deterministic* and define random strategy as probability distribution on deterministic strategies. However, no random strategy can do any better than the best deterministic strategy in terms of probability of winning. Indeed the probability of winning for a random strategy is a weighted average of the probabilities of winning of deterministic strategies. Therefore we only concentrate on deterministic strategies.

[4]For simplicity we restrict ourselves to undirected graphs. This is sufficient as our improvement in this article is on an undirected graph.

Definition 2.14. (Guessing Number) The *guessing number* of a game measures the increase in the probability of correctly guessing the colours when playing with an optimal strategy, compared to a trivial strategy of choosing arbitrary colours as answers. Formally we denote it $gn(G, s)$:

$$gn(G,s) := \max_{\mathcal{F} \text{ strategy}} \log_s \frac{\text{Prob[winning with } \mathcal{F}]}{s^{-|V|}}$$

$$= \max_{\mathcal{F} \text{ str.}} \log_s \left|\{\text{winning config. in } [\![1,s]\!]^V \text{ for } \mathcal{F}\}\right|$$

Remark 2.15. Intuition behind this definition: the guessing number of the graph is k, if a best strategy gives the probability of winning that is s^k times larger compared to the naive strategy where each player chooses an arbitrary colour independently of what hats the neighbours receive. This value is the same as the logarithm on base s of the cardinality of the largest set of configurations on which there is a winning strategy.

Remark 2.16. The guessing number of an acyclic graph is 0 [27, Lemma 3].

Definition 2.17. (Asymptotic Guessing Number, Theorem 3.6 and Definition 3.7 in [10]) The following limit exists.

$$\lim_{s\to\infty} gn(G,s)$$

It is called the *asymptotic guessing number* of G and noted $gn(G)$. In particular, it is equal to $\sup_{s\geq 2} gn(G,s)$.

There is no known efficient algorithm to compute these numbers for a given graph, and for some graphs only upper and lower bounds (that do not match each other) are known.

The lower bounds are proven using fractional clique cover of the graph and the upper bounds using information inequalities see [10, 1]. For (undirected) graphs with less than 10 vertices, the upper bounds given by Shannon-type inequalities match the lower bounds [1] thus the guessing numbers are known.

Let us give a brief sketch of how to reduce the problem of finding an upper bound on the guessing number to a question about entropies and inequalities: Define jointly distributed random variables $(X_v)_{v\in V}$ associated with the vertices of the graph, for the $(G,s)-$game. Each random variable represents the hat colour of the player at vertex v. Let $\mathcal{F}$ be an optimal strategy on (G,s). Instead of considering the independent uniformly random distribution for the colour of each hat, we consider the uniform distributions over all the configurations on which $\mathcal{F}$ wins. In other words, the colour configurations on which $\mathcal{F}$ loses all have probability 0, and those on which $\mathcal{F}$ win are all equiprobable. Two things are special about this distribution.

1. The entropy $H_s((X_v)_{v\in V})$ in base s (using $\log_s$ instead of $\log_2$ in the definition of entropy) of all the variables is the logarithm of the cardinality of the set on which $\mathcal{F}$ wins, i.e. the guessing number by Definition 2.14.

2. In this distributions the colours that are guessed are the same as the actual colours, hence the hat colour of a player is determined by the colours of the hats they see, therefore, $H(X_v|(X_u)_{u\in\to(v)}) = 0$[5].

Proposition 2.18. (As discussed after Theorem V.1 in Baber et al. [1]) Let G be a graph, let us define a random variable X_v for every vertex $v \in V$ as described above, then the optimization problem over random variables (and therefore, their entropies) below gives an upper bound on the guessing number $gn(G, s)$ for any $s \geq 2$, hence for the asymptotic guessing number $gn(G)$.

$$\begin{aligned}&\texttt{Maximize } \mathtt{H}((\mathtt{X_v})_{\mathtt{v\in V}})\\&\texttt{subject to:}\\&\mathtt{H}(\mathtt{X_v}) \leq \mathtt{1}\\&\mathtt{H}(\mathtt{X_v}|(\mathtt{X_u})_{\mathtt{u}\in\to(\mathtt{v})}) = \mathtt{0}\end{aligned}$$

The linear program that we obtain by linear relaxation of this problem (we can add to the list of constraints of this linear program any universally true information inequalities for $(X_v)_{v\in V}$) also gives an upper bound on the asymptotic guessing number.

3. SYMMETRIES

Symmetries of the underlying structures (access structures for secret sharing, sight graphs for guessing games, or other applications for optimization problems on almost entropic vectors) can be exploited in the optimization problems to decrease the complexity of the problem. When combined with the copy lemma, the symmetry constraints force symmetric solutions to our linear programs without the symmetric applications of the copy lemma, thus the use of symmetries may improve the resulting optimal value. From another perspective, by removing the symmetric applications of the copy lemma, which are costly in complexity, the objective value might worsen but symmetry constraints may help decrease the loss.

3.1. Symmetries and Linear Programming

Consider an optimization problem of the following form

$$\begin{array}{c}\max f(v)\\ \text{subject to:}\\ v \in E \subset \mathbb{R}^{2^n-1}\end{array} \tag{3}$$

where $f : \mathbb{R}^{\mathcal{P}([\![1,n]\!])\setminus\varnothing} \to \mathbb{R}$ is a linear form. Then we make the following simple observation.

Lemma 3.1. Suppose

- E is convex,
- there exists a group G which acts on vectors $\mathbb{R}^{2^n-1}$ such that:

[5]From here on, by log we mean $\log_s$.

- E is invariant under G, i.e. for all $u \in E, \sigma \in G$, we have $\sigma \cdot u \in E$,
- f is invariant under G, i.e. for all $u \in E, \sigma \in G$, we have $f(u) = f(\sigma \cdot u)$.

Then we have an optimal solution of (3) invariant under G.

P r o o f . Let $v \in E$ be an optimal solution. Since E is invariant under G, for all $\sigma \in G$, $\sigma \cdot v$ is also in E. Moreover since E is convex, average of these vectors, namely

$$v' = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot v$$

is also in E. By definition v' is symmetric under G. By linearity of f and then by invariance of f under G we have the following:

$$\begin{array}{rcl} f(v') & = & f(\frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot v) \\ & = & \frac{1}{|G|} \sum_{\sigma \in G} f(\sigma \cdot v) \\ & = & \frac{1}{|G|} \sum_{\sigma \in G} f(v) \\ & = & f(v) \end{array}$$

Therefore v' too is an optimal solution of (3). □

We can apply this observation to linear programs for secret sharing and hat guessing games. The set $E \subset \overline{\Gamma_n^*}$ will correspond to particular restrictions that stem from the application (access structure for secret sharing and sight graph for guessing games). Since we know (from the lemma above) that there exists a symmetric solution, we can simply add symmetry constraints in the conditions of the linear program without any loss in the optimal value.

Remark 3.2. In what follows we take E to be an n-dimensional slice of the *closure* of entropy region $\overline{\Gamma^*_{(n+\ell)}}$. Therefore the convexity condition for E, which enable us to apply symmetries, is satisfied.

It is not known whether these operations in the other order, namely first taking a lower-dimensional section of the entropy region and then the closure of this slice, would give a convex set.

Remark 3.3. The general strategy for the applications below involves using one or repeated application(s) of the copy lemma to introduce additional variables (increasing the dimension) and using the symmetry conditions instead of the symmetric versions of the application(s) of the copy lemma (which would be more costly in terms of dimension).

Note that our symmetry conditions only involve equalities of entropies, and that the translation of the statement Z' *is a* $Y-$*copy of* Z into linear equalities for entropy already describes the symmetry by-definition between Z' and Z, unlike the inherent symmetries of the particular problem (underlying structure).

Lemma 3.4. Suppose E can be expressed with linear inequalities and let us consider the following optimization problem on almost entropic points $\overline{\Gamma_n^*}$.

$$\begin{array}{l}\min f(h)\\ \text{subject to:}\\ h \in E\end{array}$$

Then the following linear program gives a lower bound on the above optimization problem.

$$\begin{array}{ll}& \min f(h)\\ & \text{subject to:}\\ \text{(i)} & (h,r) \in \mathbb{R}^{2^{n+\ell}-1}, h \text{ satisfies inequalities that define } E\\ \text{(ii)} & \text{the equalities for entropies which define } \ell \text{ extra}\\ & \text{random variables by one or repeated application(s) of the copy lemma}\\ \text{(iii)} & \text{some information inequalities for } n+\ell \text{ random variables}\end{array}$$

P r o o f . Applying copy lemma and adding information inequalities as extra conditions to the optimization problem does not change its value, since (almost) entropic points already satisfy these conditions. Then loosening the constraints of the obtained problem by removing the 'almost entropic' restriction we obtain indeed the linear program, which hence gives an upper bound to the former.

Note that the information inequalities and the applications of the copy lemma are not (necessarily) redundant conditions for the linear program, unlike what they categorically would be for the optimization problem. □

3.2. Applications of symmetries

The method of reducing an optimization problem for entropies to a linear program was used in [25] and [14] to find lower bounds on the information ratio of an access structure in the context of secret sharing as well as to find upper bounds on the guessing number of sight graphs in the context of hat guessing games in [10] and [1]. Below we combine this approach with symmetries and the applications of the copy lemma as in [17].

Proposition 3.5. Let $(X_1, \dots X_n)$ be random variables associated with an optimization problem the conditions of which are linear inequalities for entropies and f a function expressible as a linear combination of entropies of tuples.

$$\begin{array}{l}\min f(X_1, \dots X_n)\\ \text{subject to:}\\ \text{the inequalities which define the problem}\end{array}$$

Suppose also that G is the symmetry group of the underlying structure of $(X_1, \dots X_n)$ for entropies of tuples. (G acts on vectors by permuting the coordinates $\sigma \cdot (h_{X_I})_{\varnothing \neq I \in [\![1,n]\!]} = (h_{S_{\sigma \cdot I}})_{\varnothing \neq I \in [\![1,n]\!]}$.)

Let us extend the distribution by adding ℓ random variables $X_{n+1}, \dots X_{n+\ell}$ using one or repeated applications of the copy lemma as in Lemma 3.4. The linear program

described below provides a lower bound on the initial optimization problem:

$\min f(X_1, \dots X_n)$
subject to:
(i) the inequalities which define the problem
(ii) the equalities for entropies that define each of the random variables $X_{n+1}, \dots X_{n+\ell}$ as a copy of other variables (with smaller indices), obtained using the copy lemma
(iii) classical information inequalities for $X_1, \dots X_{n+\ell}$
(iv) the symmetry constraints for entropies of tuples of $X_i, i \in [\![1, n]\!]$ under the symmetry group G

P r o o f. The proposition follows from Lemma 3.4, which justifies the constraints (ii) and (iii), and Lemma 3.1 which justifies the constraint (iv). □

We have already presented in (1) the equalities which define the access structure for secret sharing. An additional normalization condition $H(S_0) = 1$ where S_0 is the secret suffices to make the information ratio $\max_i \frac{H(S_i)}{H(S_0)}$ expressible in linear terms with inequalities as $\min x$ with $x \geq H(S_i),\ i = 1, \dots n$.

Corollary 3.6. The following linear program provides a lower bound on the information ratio of an access structure $\mathcal{A}$.

$\min x$
subject to:
(i) $x \geq h_{S_i}$ for every $i \in [\![1, n]\!]$
(i)' the equalities (1) for the entropies of tuples of $S_0, \dots S_n$ which define the access structure $\mathcal{A}$
(i)" $h_{S_0} = 1$ normalization
(ii) the equalities for entropies that define each of the random variables $S_{n+1}, \dots S_{n+\ell}$ as a copy of other variables (with smaller indices), obtained using the copy lemma
(iii) classical information inequalities for $S_0, \dots S_{n+\ell}$
(iv) the symmetry constraints on the variables $S_i, i \in [\![1, n]\!]$ under the symmetry group of the access structure $\mathcal{A}$

The set of constraints 1 for the access structure $\mathcal{A}$ is indeed invariant under the symmetry group $G = Aut(\mathcal{A})$ by definition, the other constraints and the objective function too.

See the appendix for the symmetry groups of the access structures we study in this work.

Applying Proposition 3.5 to the optimization problem in Proposition 2.18, we get the following corollary.

Corollary 3.7. Let $G = (V, E)$ be a sight graph with n vertices and $X_1, \dots X_n$ the associated random variables as in [10]. The linear program described below provides a lower bound on the asymptotic guessing number of G.

$\max h_{X_{[\![1,n]\!]}}$
subject to:
(i) $h_{X_i} \leq 1$ for every $i \in [\![1,n]\!]$
(i)' $h_{\{X_i, X_j|(j,i)\in E\}} - h_{\{X_j|(j,i)\in E\}} = 0$ for each $i \in [\![1,n]\!]$
(ii) the equalities for entropies that define each of the random variables $X_{n+1}, \dots X_{n+\ell}$ as a copy of other variables (with smaller indices), obtained using the copy lemma
(iii) classical information inequalities for $X_1, \dots X_{n+\ell}$
(iv) the symmetry constraints on the variables $X_i, i \in [\![1,n]\!]$ under the symmetry group of the sight graph G

Remark 3.8. In [1] non-Shannon-type inequalities were added to such a linear program instead of item (ii) (the copy lemma constraints).

4. SECRET SHARING

There is a large class of access structures called *linear access structures* (also known as *vector space access structure*) that are ideal. Let us give their definition.

Definition 4.1. An access strucure is called *linear* if the secret and the participants $1, \dots n$ can be associated respectively to some vectors $v_0, v_1, \dots v_n$ in a vector space such that a coalition I is

- a qualified coalition if $v_0 \in Vect((v_i)_{i\in I})$, that is v_0 belongs to the linear subspace span by the set of vectors V_i for $i \in I$,
- not qualified otherwise.

Note that, in particular, threshold access structures are linear: we can take a vector space of dimension equal to the threshold t. Then choose vectors associated to participants one by one such that any t of them are independent. This can be done by choosing the field large enough[6].

There is a more general class of access structures, based on matroids. See [23] for a detailed introduction to matroids and [11] for a brief discussion of matroid and polymatroid structures in secret sharing. In this text, we are only interested in connected matroids, more particularly *matroid ports* ([29]) and *matroid port access structures* (see [13], [14] and [15] for the definition, an excellent overview and why they are interesting, as well as [7] and [20]).

4.1. Access structures from matroids

Let us give a simple way to obtain some matroids: Let E be a set, if we choose some vector space and a vector v_e for each $e \in E$ and then declare a subset of E to be *independent* when the corresponding vectors are linearly independent, this gives us a matroid. Matroids that can be obtained this way are called *linearly representable*.

[6]If the field has k elements, the vector space has k^t elements. Suppose we have chosen n vectors so far, this can forbid no more than $\binom{n}{t-1}k^{t-1}$ choices for the next vector. Thus $k > \binom{n}{t-1}$ suffices.

The matroids with a ground set E of cardinality 7 or less, as well as those with a ground set of cardinality 8 and rank different than 4, are all known to be *linearly representable* [16]. There exists 940 non-isomorphic matroids of rank 4 on 8 points (see [23]). There exist matroids with a ground set of cardinality 8 and rank 4 that are not linearly representable, and the first known such example among them is the Vámos matroid ([32], [23, Proposition 2.2.26]).

Below we discuss seven other matroids (Table 1) with a ground set of cardinality 8 and rank 4 which are not linearly representable.

Acccess Structure	List of Minimal Authorized Sets
$\mathcal{A}$	123, 145, 167, 246, 257, 347, 356, 1247
$\mathcal{A}^*$	123, 145, 167, 246, 257, 347, 1356, 2356, 3456, 3567
$\mathcal{F}$	123, 145, 167, 246, 257, 347, 356, 1247, 1256
$\mathcal{F}^*$	123, 145, 167, 246, 257, 1347, 1356, 2347, 2356, 3456, 3457, 3467, 3567
$\widehat{\mathcal{F}}$	123, 145, 167, 246, 257, 347, 1256, 1356, 2356, 3456, 3567
$\mathcal{Q}$	123, 145, 167, 246, 257, 347, 1247, 1256, 1356, 2356, 3456, 3567
$\mathcal{Q}^*$	123, 145, 167, 246, 257, 1247, 1347, 1356, 2347, 2356, 3456, 3457, 3467, 3567

Tab. 1. Access structures.

Access structure	previously known lower bound based on AK lemma [15]	bounds we prove using symmetries	weaker bounds we can prove without symmetries
$\mathcal{A}$	$9/8 = 1.125$	$57/50 = 1.14$	$135/119 = 1.134\ldots$
$\mathcal{A}^*$	$33/29 = 1.137\ldots$	$52/45 = 1.1\overline{5}$	$33/29 = 1.137\ldots$
$\mathcal{F}$	$9/8 = 1.125$	$17/15 = 1.1\overline{3}$	$26/23 = 1.130\ldots$
$\mathcal{F}^*$	$42/37 = 1.\overline{135}$	$8/7 = 1.142\ldots$	$42/37 = 1.\overline{135}$
$\widehat{\mathcal{F}}$	$42/37 = 1.\overline{135}$	$23/20 = 1.15$	$42/37 = 1.\overline{135}$
$\mathcal{Q}$	$9/8 = 1.125$	$17/15 = 1.1\overline{3}$	$17/15 = 1.1\overline{3}$
$\mathcal{Q}^*$	$33/29 = 1.137\ldots$	$8/7 = 1.142\ldots$	$33/29 = 1.137\ldots$

Tab. 2. The access structures of which we have improved lower bounds on the information ratio.

We focus on a few access structures whose study was initiated in [15] (as they are among smallest non-linear matroids). All these access structures have some nice geomet-

ric interpretation, so do the matroids of which they are ports. In [15], they are named after the matroids $AG(3,2)'$ (faces, diagonal planes and a twisted plane of a cube), F_8 and Q_8 (faces and five of the six diagonal planes of a cube) from the appendix of [23], from which they are derived. We follow their notation. As usual, each access structure can be defined by its minimal authorized coalitions, see Table 1.

The ultimate goal of this line of research is to find the information ratio for each of these access structures (and study the connection of information ratio with the combinatorial properties of matroids). This goal was not achieved in [15], nor is it in our work. However, we take a new step in this direction and improve the known lower bound for the information ratio of these access structures.

4.2. Results

We improve the lower bounds for the seven access structures.

Theorem 4.2. The information ratios of $\mathcal{A}$, $\mathcal{A}^*$, $\mathcal{F}$, $\mathcal{F}^*$, $\widehat{\mathcal{F}}$, $\mathcal{Q}$ and $\mathcal{Q}^*$ are $57/50 = 1.14$, $52/45 = 1.1\overline{5}$, $17/15 = 1.1\overline{3}$, $8/7 = 1.142\ldots$, $23/20 = 1.15$, $17/15 = 1.1\overline{3}$ and $8/7 = 1.142\ldots$ respectively. In the column 3 of Table 2 we show these are lower bounds on the information ratio.

Proof. For each of the seven access structures we construct a linear program as in Corollary 3.6. In this linear program we use auxiliary random variables with one or two applications of the copy lemma inspired from the applications of the AK lemma in [15]. We also add the constraints to express for each access structure the symmetry conditions (see Section 3.2 and the appendix).

We use the following applications of the copy lemma to create four additional variables for each access structure. To denote a copy of X, we use X' in the first application of the copy lemma, X'' in the second copy step etc. and $X^{(i)}$ in the i^{th}:

- $\mathcal{A}$: we introduce new variables (S'_0, S'_3, S'_4, S'_7) as a copy of (S_0, S_3, S_4, S_7).
- $\mathcal{A}^*$: we introduce (S'_0, S'_3) as a (S_5, S_6)-copy of (S_0, S_3) and then another pair (S''_1, S''_2) as a (S_0, S'_0, S_3, S'_3)-copy of (S_1, S_2).
- $\mathcal{F}$: we introduce new variables (S'_0, S'_2, S'_4, S'_6) as a copy of (S_0, S_2, S_4, S_6).
- $\mathcal{F}^*$: we introduce (S'_0, S'_4) as a (S_3, S_7)-copy of (S_0, S_4) and then (S''_1, S''_4) as a (S_0, S'_0, S'_4, S_5)-copy of (S_1, S_4).
- $\widehat{\mathcal{F}}$: we introduce (S'_0, S'_4) as a (S_2, S_6)-copy of (S_0, S_4) and then (S''_1, S''_4) as a (S_0, S'_0, S'_4, S_5)-copy of (S_1, S_4).
- $\mathcal{Q}$: we introduce (T', V') as a (S_0, S_2, S_4, S_6)-copy of (T, V) over (S_1, S_3, S_5, S_7) and then (T'', V'') as a $(S_0, S_2, S_4, S_6, T', V')$-copy of (T, V) over (S_1, S_3, S_5, S_7), where $T = (S_0, S_4)$ and $V = (S_2, S_6)$.
- $\mathcal{Q}^*$: we introduce a (S'_0, S'_4) as a (S_3, S_7)-copy of S_0, S_4 and (S''_1, S''_5) as a (S_0, S'_0, S_4, S'_4)-copy of (S_1, S_5).

For comparison, in column 4 of Table 2, we show the weaker bound (strictly except for Q) that can be proven with the same use of the copy lemma but without symmetry conditions. □

5. HAT-GUESSING GAMES

We discussed hat guessing games in the preliminaries section2.5, here we show our results. Our main result is on an undirected graph called R^- with 10 vertices. The best known lower bound on its guessing number is $^{20}/_3 = 6.\bar{6}$ and the previously known best upper bound was $^{59767}/_{8929} = 6.693\ldots$. We get an upper bound $^{1847}/_{276} = 6.6920\ldots$ ($\approxeq 6.692028986$). The other result is to use our tools to get another proof of a known lower bound (for R^L, a directed graph) from [1].

For the lower bounds on asymptotic guessing number using fractional clique cover number (definition just below) see [10] by Christofides and Markström.

Definition 5.1. (Fractional Clique Cover Number) Let $G = (V, E)$ be a graph and K be the set of its cliques. A fractional clique cover is a weighting $w : K \to [0, 1]$ of cliques such that, for every vertex $v \in V$, the sum of weights of the cliques it belongs to is 1. Formally

$$\forall v \in V, \sum_{\substack{k \in K \\ v \in k}} w(k) = 1.$$

Among all fractional clique covers, one that minimizes the sum of all weights defines the *fractional clique partition number* of G:

$$cp_f(G) = \min_{w \text{ fractional clique cover}} \sum_{k \in K} w(k)$$

5.1. Upper bounds on guessing number via entropy

In [10], upper bounds on the asymptotic guessing numbers of some graphs were proven with the help of Shannon-type information inequalities (the proofs are traditional, without use of computer). In [1] this method was extended: the authors explicitly used the formalism of linear programming and the assistance of a computer; these proofs involved non-Shannon-type inequalities.

In [10] it was conjectured (Conjecture 6.4) that the asymptotic guessing number of a graph G with n vertices is always equal to $n - cp_f(G)$.[7] The authors of [1] wanted to check this conjecture for graphs with small number of vertices. They used the method of Proposition 2.18 firstly with only Shannon-type inequalities and compared the upper bound given by this method to the lower bound given by the fractional clique cover on all (undirected) graphs with 9 or less vertices. They found that the bounds match (they performed the verification numerically, using floating point arithmetic). On graphs with 10 vertices they found only 2 graphs (up to isomorphism) for which the lower and upper bounds do not match, called R and R^-. The graph $R-$ is given in Figure 2 which is obtained from R by removing the edge $9 \leftrightarrow 10$ from it.

[7] The authors use the notation $\chi_f(\overline{G})$ instead of $cp_f(G)$, since the chromatic number of the complement is clique cover number of G.

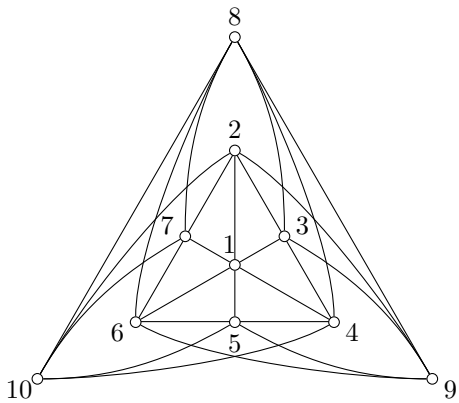

Fig. 2. The graph R^-.

The fractional clique cover number for R and R^- are both $^{10}/_3 = 3.\overline{3}$, which implies the lower bound $10 - {}^{10}/_3 = {}^{20}/_3 = 6.\overline{6}$ by [10].

The guessing number of R is proven to be $\frac{27}{4} = 6.75$ in [1] by an upper bound using Shannon-type inequalities and the construction of a strategy.

The best upper bound for R^- found in [1] using the non-Shannon-type inequalities from [12] is $^{59767}/_{8929} = 6.693\ldots$.

In [1], the authors looked for an undirected graph such that the guessing number can be increased by adding one directed edge. They could not find such an example, and this motivated the question whether making a vertex 'Superman' (visible by all others) by adding directed edges increases the guessing number. This led to the definition of the graph R^S which is just as R up to three outgoing edges from the vertex 1 to vertices 8, 9 and 10. The guessing number of R^S is found to be $^{27}/_4 = 6.75$.

Another question on guessing games on graphs: are there any graphs where the guessing number changes when the direction of all of its edges are reversed? This question has been motivated by the connection of guessing games with information networks (and the natural question of reversibility of networks). The authors of [1] looked at the candidates R^S and its reverse R^L in which 1 is a 'Luthor' vertex (sees all other vertices). A better lower bound for R^L than its fractional clique cover number is given by the guessing number $^{27}/_4$ of R. The best upper bound they found on R^L is $^{359}/_{53} = 6.773\ldots$ using the non-Shannon-type inequalities from [12].

5.2. Our results

Using Corollary 3.7 we improve the upper bound on R^- and give an alternative proof of the previously known bound on R^L. For both of these graphs, the asymptotic guessing numbers remain unknown. See the appendix for the symmetry groups.

We get the following linear program and upper bounds for $gn(R^-)$, thus improve the bound given in [1].

Theorem 5.2. For the above defined graph R^-,

$$gn(R^-) \leq {}^{1847}/_{276} = 6.6920\ldots.$$

P r o o f. We construct a linear program as in Corollary 2.18 with the following constraints.

1. The following applications of the copy lemma:
   (a) X_2' be a X_3-copy of X_2;
   (b)
   - (X_4'', X_5'') be a X_{10}-copy of (X_4, X_5) over $X_1, X_2, X_3, X_6, X_7, X_8, X_9$,
   - and X_7''' be a (X_4'', X_5, X_{10})-copy of X_7 over $X_1, X_2, X_3, X_4, X_5'', X_6, X_8, X_9$;

   (c)
   - (X_6'''', X_7'''') be a copy of (X_6, X_7) over $X_1, X_2, X_3, X_4, X_5, X_8, X_9, X_{10}$,
   - and X_8'''' be a (X_7, X_7'''')-copy of X_8 over $X_1, X_2, X_3, X_4, X_5, X_6, X_6'''', X_9, X_{10}$;
2. the elemental inequalities for the following sets of random variables
   - those that appear in the copy step in the item 1a above: $X_1, X_2, X_2', X_3, X_4, X_5, X_6, X_7, X_8, X_9, X_{10}$,
   - those that appear in the copy steps of the item 1b above: $X_1, X_2, X_3, X_4, X_4'', X_5, X_5'', X_6, X_7, X_7''', X_8, X_9, X_{10}$,
   - those that appear in the copy steps of the item 1c above: $X_1, X_2, X_3, X_4, X_5, X_6, X_6'''', X_7, X_7'''', X_8, X_8'''', X_9, X_{10}$;
3. the symmetry constraints.

The optimal value of this linear program is ${}^{1847}/_{276} \approxeq 6.692028986$, which proves the claim. □

We confirm the upper bound proven in [1].

Theorem 5.3. For the graph R^L defined above,

$$gn(R^L) \leq {}^{359}/_{53} = 6.7735849\ldots.$$

P r o o f. We construct a linear program as in the previous proof. We use the following constraints.

1. The following applications of the copy lemma:
   (a)
   - (X_4', X_5') be a copy of (X_4, X_5),
   - X_5'' be a (X_1, X_4, X_4')-copy of X_5,
   - and X_1''' be a (X_4, X_4')-copy of X_1;

(b) • (X_2'''', X_7'''') be a copy of (X_2, X_7) over $X_1, X_3, X_4, X_5, X_6, X_8, X_9, X_{10}$,
• and X_1'''' be a (X_7, X_7'''')-copy of X_1 over $X_2, X_2'''', X_3, X_4, X_5, X_6, X_8, X_9, X_{10}$;

2. the elemental inequalities for the following sets of random variables
   - $X_1, X_1''', X_2, X_3, X_4, X_4', X_5, X_5', X_5'', X_6, X_7, X_8, X_9, X_{10}$
   - $X_1, X_1'''''', X_2, X_2'''', X_3, X_4, X_5, X_6, X_7, X_7'''', X_8, X_9, X_{10}$;
3. the symmetry constraints.

The optimal value of this linear program confirms the upper bound $\leq {}^{359}/_{53} \approxeq 6.773584906$. □

Remark 5.4. Note that in the linear programs constructed in the proofs above, unlike those in secret sharing, we did not take all the elemental information inequalities for all the combinations of old and new random variables. For example there is no Shannon-type inequality involving both X_2' and X_4'' in the first linear program and none involving both X_4' and X_2'''' in the second. The reason is that the number of elemental inequalities involving all possible combinations of random variables is enormous. If we included all these constraints in the linear program, the computational complexity of the problem would increase so much that the existing linear program solvers (for our computers) could not handle it. Our choice of the sets of variables for which we write elemental information inequalities follows from the applications of the copy lemma: a copy variable used in order to define another copy variable is put in the same set as the latter.

6. CONCLUSION

In this paper we studied the application of computer-assisted proofs involving non-Shannon-type inequalities. Though each separate ingredient used in our construction was known earlier, the resulting combination proved to be surprisingly efficient.

We improved lower bounds for the information ratio of the access structures on Table 1 based on rank-4 8-point not-linearly-representable matroids. We believe that the used method is quite strong and it might be interesting to extend to the other instances of the problem of secret sharing.

We also improved the upper bound for the single smallest undirected graph, the asymptotic guessing number of which is unknown, namely R^-. Not only our bound improves upon the previous one, but also the fraction is simpler (i. e. the denominator is smaller). Note that there is no evidence that the obtained number is the exact guessing number for this graph, a finer analysis may improve our upper bound.

7. ACKNOWLEDGEMENT

I thank Andrei Romashchenko for his reading, suggestions, feedback and motivating me to finish this article. This work was partly funded by FLITTLA project (ANR-21-CE48-0023). I also thank the reviewers for their comments and suggestions as well as the editor for her patience.

(Received October 16, 2023)

REFERENCES

[1] R. Baber, D. Christofides, A. N. Dang, E. R. Vaughan, and S. A. Riis: Graph guessing games and non-Shannon information inequalities. IEEE Trans. Inform. Theory *63* (2016), 7, 4257–4267. DOI:10.1109/TIT.2016.2628819

[2] M. Bamiloshin, A. Ben-Efraim, O. Farras, and C. Padro: Common information, matroid representation, and secret sharing for matroid ports. Designs Codes Cryptogr. *89* (2021), 1, 143–166. DOI:10.1007/s10623-020-00811-1

[3] A. Beimel: Secret-sharing schemes: A survey. In: International Conference on Coding and Cryptology, Springer 2011, pp. 11–46.

[4] A. Beimel, N. Livne, and Carles Padro: Matroids can be far from ideal secret sharing. In: Theory of Cryptography Conference, Springer 2008, pp. 194–212.

[5] J. Benaloh and J. Leichter: Generalized secret sharing and monotone functions. In: Conference on the Theory and Application of Cryptography, Springer 1988, pp. 27–35.

[6] G. R. Blakley: Safeguarding cryptographic keys. In: Managing Requirements Knowledge, International Workshop, IEEE Computer Society 1979, pp. 313–313.

[7] E. F. Brickell and D. M. Davenport: On the classification of ideal secret sharing schemes. J. Cryptology *4* (1991), 2, 123–134. DOI:10.1007/BF00196772

[8] S. Butler, M. T. Hajiaghayi, R. D. Kleinberg, and T. Leighton: Hat guessing games. SIAM Rev. *51* (2009), 2, 399–413. DOI:10.1137/080743470

[9] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro: On the size of shares for secret sharing schemes. J. Cryptology *6* (1993), 3, 157–167. DOI:10.1007/BF00198463

[10] D. Christofides and K. Markstr: The guessing number of undirected graphs. Electr. J. Combin. (2011), 192–192.

[11] L. Csirmaz: The size of a share must be large. J. Cryptology *10* (1997), 4, 223–231. DOI:10.1007/s001459900029

[12] R. Dougherty, Ch. Freiling, and K. Zeger: Non-Shannon information inequalities in four random variables. In: arXiv preprint arXiv:1104.3602 (2011).

[13] O. Farras: Secret sharing schemes for ports of matroids of rank 3. Kybernetika *56* (2020), 5, 903–915. DOI:10.1134/S1022795420080116

[14] O. Farras, T. Kaced, S. Martin, and C. Padro: Improving the linear programming technique in the search for lower bounds in secret sharing. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer 2018, pp. 597–621.

[15] O. Farras, Tarik Kaced, S. Martin, and C. Padro: Improving the linear programming technique in the search for lower bounds in secret sharing. IEEE Trans. Inform. Theor *66* (2020), 11, 7088–7100. DOI:10.1109/TIT.2020.3005706

[16] J. C. Fournier: epresentation sur un Corps d Ordre. In: Theorie des Matroides, Springer 1971, pp. 50–61.

[17] E. Gurpinar and A. Romashchenko: How to use undiscovered information inequalities: Direct applications of the copy lemma. In: IEEE International Symposium on Information Theory (ISIT), IEEE 2019, pp. 1377–1381.

[18] M. Ito, A. Saito, and T. Nishizeki: Secret sharing scheme realizing general access structure. In: Electronics and Communications in Japan (Part III: Fundamental Electronic Science). Japanese Publ. *72* (1989), 9, 56–64. DOI:10.1080/10371398908522079

[19] T. Ma, X. Sun, and H. Yu: A new variation of hat guessing games. In: International Computing and Combinatorics Conference, Springer 2011, pp. 616–626.

[20] J. Martín-Farras and C. Padro: VOn secret sharing schemes, matroids and polymatroids. J. Math. Cryptol. *4* (2010), 2, 95–120.

[21] J. Martin and P. Rombach: Guessing Numbers and Extremal Graph Theory. In: arXiv preprint arXiv:1104.3602, 2020.

[22] J. R. Metcalf-Burton: Improved upper bounds for the information rates of the secret sharing schemes induced by the Vamos matroid. Discr. Math. *311* (2011), 8–9, 651–662. DOI:10.1016/j.disc.2011.01.003

[23] J. Oxley: Matroid Theory. Second edition. Oxford University Press, 2011.

[24] C. Padro: Lecture notes in secret sharing. In: Cryptology ePrint Archive 2012.

[25] C. Padro, L. Vazquez, and A. Yang: Finding lower bounds on the complexity of secret sharing schemes by linear programming. Discrete Appl. Math. *161* (2013), 7–8, 1072–1084. DOI:10.1016/j.dam.2012.10.020

[26] S. Riis: Information flows, graphs and their guessing numbers. In: Electr. J. Combinator. (2007), R44–R44.

[27] S. Riis: Utilising public information in network coding. General Theory Inform. Transfer Combinator. *4123* (2006), 866–897.

[28] S. Robinson: Why mathematicians now care about their hat color. In: The New York Times, Science Times Section, page D *5* (2001).

[29] P. D. Seymour: A forbidden minor characterization of matroid ports. The Quarterly J. Math. *27* (1976), 4, 407–413. DOI:10.1093/qmath/27.4.407

[30] A. Shamir: How to share a secret. Commun. ACM *22* (1979), 11, 612–613. DOI:10.1145/359168.359176

[31] C. E. Shannon: A mathematical theory of communication. Bell Syst. Techn. J. *27* (1948), 3, 379–423. DOI:10.1002/j.1538-7305.1948.tb01338.x

[32] P. Vamos: On the representation of independence structures. Unpublished manuscript, 1968.

[33] P. Winkler: Games people don't play. 2002.

[34] R. Wai-Ho Yeung: A first Course in Information Theory. Springer Science and Business Media, 2002.

[35] Z. Zhang and R. Wai-Ho Yeung: A non-Shannon-type conditional inequality of information quantities. IEEE Trans. Inform. Theory *43* (1997), 6, 1982–1986.

[36] Z. Zhang and R. Wai-Ho Yeung: On characterization of entropy function via information inequalities. IEEE Trans. Inform. Theory *44* (1998), 4, 1440–1452.

Emirhan Gürpınar,
e-mail: emirhangurpinar@mailfence.com

APPENDICES

A. Symmetry groups of access structures

To find the symmetry constraints to be written in item (iv) of the Corollary 3.6, one needs to find the symmetries of the access structures under consideration, so here we give the symmetry groups of the access structures we previously described.

The reader can check manually or by computer since the structures are small.

- $\mathcal{A}, \mathcal{A}^*$: $\langle (12)(56), (14)(36), (17)(35) \rangle$
- $\mathcal{F}, \mathcal{F}^*$: $\langle (12)(4576), (46)(57) \rangle$
- $\mathcal{Q}, \widehat{\mathcal{F}}, \mathcal{Q}^*$: $\langle (12)(47), (12)(56) \rangle$

B. Symmetry groups of sight graphs

The reader can check the symmetry groups by analysing the blocks or by brute-force since the graphs are small.

The symmetry group of R^- is generated by two permutations: $\sigma = (18)(2\ 10\ 5\ 9)(3746)$ and $\tau = (25)(36)(47)$. $Aut(R^-) = \langle \sigma, \tau \rangle$.

$$Aut(R^-) = \langle (18)(2\ 10\ 5\ 9)(3746), (25)(36)(47) \rangle$$

The symmetry group of R^L is same as that of R, namely

$$Aut(R^L) = \langle (25)(36)(47), (26)(35)(8\ 10), (24)(57)(89) \rangle.$$

C. A certificate of $^{1847}/_{276}$ bound

The 1920 inequalities with their respective non-zero coefficients derived from the rational solution of the shortened linear program, which has optimal value $\frac{1847}{276}$ can be downloaded from:

`https://archive.org/details/anx-c-rmns-1847ovr-276crtfcte`.