On Abelian Secret Sharing: duality and separation

Amir Jafari and Shahram Khazaei

Sharif University of Technology, Tehran, Iran
`{ajafari,shahram.khazaei}@sharif.ir`

May 27, 2019

Abstract. Unlike linear secret sharing, very little is known about abelian secret sharing. In this paper, we present two results on abelian secret sharing. First, we show that the information ratio of access structures (or more generally access functions) remain invariant for the class of abelian schemes with respect to *duality*. Then, we prove that abelian secret sharing schemes are superior to the linear ones.

New techniques and insight are used to achieve both results. Our result on abelian duality is proved using the notion of *Pontryagin duality*. The intuition behind the usefulness of this tool is to work with an equivalent definition of linear secret sharing, which is less prevalent in the literature, to make it possible to extend the result on linear duality to abelian duality.

We develop a new method for proving *lower bound* on the linear information ratio of access structures that can work not only for general linear secret sharing but also for linear schemes on finite fields with a *specific characteristic*. Unlike the common lower bound techniques, which are usually *either* based on rank/information inequalities *or* based on counting/combinatorial-algebraic arguments, our method is linear algebraic in essence. We apply our method to the Fano and non-Fano access structures for the characteristics on which they are not ideal.

We then show in a straightforward way that for their union—a well-known 12-participant access structure—the abelian schemes are superior to the linear ones.

Keywords: Secret sharing · Access structure · Duality · Characteristic-dependent information ratio · Abelian secret sharing .

1 Introduction

A *(total) secret sharing scheme* [Sha79, Bla79, ISN89] is a method that allows a dealer to share a secret among a set of participants such that only certain *qualified* subsets of participants are able to reconstruct the secret. The secret must remain information theoretically hidden from the remaining subsets, called *unqualified*. The collection of all qualified subsets is called an *access structure*, which is supposed to be monotone, i.e., closed under the superset operation.

The notion of *access function* [FHKP17]—a generalization of the definition of an access structure—allows non-total reconstruction of secret by different subsets of participants. This concept has been matured by building on a sequence of previous works [BM84,KOS$^+$93,SRR02,SC02]. An access function is a monotone real function that specifies the percentage of the information on the secret that is obtained by each subset of participants. An access structure corresponds to a *total* access function which allows all-or-nothing recovery of the secret. An access function can be associated to a secret sharing scheme naturally.

The *information ratio* [BS92, BSSV92, Mar93] of a participant in a secret sharing scheme is defined as the ratio of the size of his share and the size of the secret. The information ratio of a secret sharing scheme is the maximum (also sometimes defined as the average) of all participants' information ratios. The information ratio of an access structure is defined as the infimum of the information ratios of all secret sharing schemes that realize it. When we restrict to the class of linear/abelian schemes, we call it the linear/abelian information ratio.

The *dual* of an access structure [JM94] is another access structure whose qualified subsets corresponds to the complement of unqualified subsets of the original access structure. The definition of duality can be extended to access functions in a natural way [FHKP17]. The relation between the information ratio of dual access structures is an open problem, even when the access structure is assumed to be ideal (i.e., those realizable with information ratio one). But it is known to coincide for the class of linear secret sharing schemes [JM94,FHKP17].

Computation of information ratio of access structures has turned out to be a very difficult problem. Despite several important results (which will be discussed next), we still lack powerful tools for proving close-to-optimal lower-bounds and upper-bounds on the information ratio of access structures. As an examples, the exact values of information ratios of several access structures on five [JM96] and six [VD95] participants are still open and the computation of their optimal linear information ratios have very recently been finalized [FKMP18, GK18].

It is simple to construct a secret sharing scheme realizing any access structure on n participants with information ratio 2^n [ISN89], which can be improved to $2^{n-o(n)}$ [BL88]. It is generally believed that the exponential upper bound is tight for most access structures [Bei11]. This upper-bound has been recently reduced in [LV18a] to $2^{(1-\epsilon)n}$ for some small constant $\epsilon > 0$, using a cryptographic primitive called *conditional disclosure of secrets (CDS)* [GIKM00]. This primitive has proved useful for constructing secret sharing schemes in several recent works [BIKK14,BFMP17,LVW17,BKN18], in particular, for special classes of access structures which are extensions of forbidden graph access structures [SS97]. Another method for finding an upper-bound on the information ratio of access structures (especially those on a small number of participants) is the Stinson's *decomposition* method [Sti92] and its variants [vDKST06, SC02, GK18].

A review on known lower bound techniques. There are mainly two different approaches for determining a lower bound on the information ratio of an access structure.

The *first* one is based on the properties of *entropy* of random variables. The so-called *Shannon-type information inequalities*, were first used by Capocelli, De

Santis, Gargano and Vaccaro [CSGV93] due to the connection between Shannon entropies and polymatroids. The method was later refined by Csirmaz [Csi94], using which he could prove his well-known $\Omega(n/\log n)$ lower bound on information ratio. The method was further improved in [BLP08] by taking into account the so-called *non-Shannon-type* information inequities [ZY97] for general secret sharing or *rank inequalities* [Ing71, DFZ09] for linear secret sharing schemes. A recent modification by Farràs, Kaced, Mollеví and Padró [FKMP18] takes advantage of the non-Shannon-type information inequalities implicitly by using the so-called *Ahlswede-Körner* [CK11] and *common information* [DFZ09] properties, for deriving lower bounds on general and abelian secret sharing, respectively.

The *second* method is based on *counting* and *combinatorial-algebraic arguments*, first introduced by Beimel, Gál and Paterson [BGP97], based on the equivalence of secret sharing schemes and *monotone span programs* [KW93]. This method has been mainly applied to *scaler-linear*[1] secret sharing (i.e., when the secret is a single field element) and was refined in [BGK+96, BGW99]. The method was further improved by Gál in [Gál98], based on combinatorial-algebraic ideas of Raz [Raz90], to prove a $\Omega(n^{\log n})$ lower-bound. Building on ideas from [GP03], Gál's lower-bound was later shown in [BBPT14] to hold for *(multi-)linear* secret sharing as well. An exponential lower bound on scaler-linear secret sharing has been recently proved in [PR18] along the same lines. Lower bounds, merely based on counting arguments, have also been applied to the class of forbidden graph access structures [SS97] and their generalization known as uniform access structures [AA18, BKN18, LV18b], respectively, in [BFMP17] and [ABF+19].

We remark that the entropy method finds a lower bound for arbitrarily long secrets but it fails to work for restricted situations (e.g., for a specific secret space size or dimension). However, as discussed above, they have the potential to be applied on linear and abelian schemes. On the other hand, all combinatorial-algebraic (and counting) methods are used for scaler-linear secret sharing schemes (with [BFMP17] being an exception).

1.1 Motivations and contributions

The motivation and contributions of this paper are threefold.

Duality. Duality is a fundamental concept in several mathematical and computer science areas such as linear algebra, group theory, matroids and coding theory. The duality notion for access structures was first introduced by Jackson and Martin in [JM94] and was later extended to access functions by Farràs, Hansen, Kaced and Padró in [FHKP17]. For every *linear* secret sharing scheme there exists a (dual) scheme with the same access function and information ratio [FHKP17] (the case of access structures had already been settled in the initial

[1] In this paper, we allow the secret in linear schemes to contain any arbitrary number of field elements and simply call theme linear. When the secret is a single field element, we call it scaler-linear.

paper). A long standing open problem, with no progress, is if the duality invariance holds for general secret sharing. This problem is even open for the class of ideal access structures. In this paper, we put one step forward and prove that the abelian information ratio of access functions remains invariant with respect to duality.

Characteristic-specific lower bound. Beimel and Weinreb [BW05] have shown that the choice of underlying finite field characteristic may affect the information ratio of an access structure. Their method is combinatorial-algebraic and, in particular, they prove a super-polynomial separation between any two fields with different characteristics for scaler-linear secret sharing[2]. Their result justifies the existence of characteristic-dependent linear rank inequalities, but explicit examples of such inequalities were later demonstrated by Blasiak, Kleinberg and Lubetzky in [BKL11] (see [DFZ15] for a follow-up).

Some remarks follow that justifies our motivation for seeking a new technique. *First*, we were not able to find a non-trivial lower bound on the access structures induced by *Fano* and *non-Fano* matroids—the smallest *characteristic-dependent* access structures—by adding the characteristic-dependent rank inequalities from [BKL11] on seven variables to the corresponding linear program [Met11, PVY13]. The reason for this failure is not surprising; the success of direct use of non-Shannon information inequalities in improving lower bounds has been quite limited [BLP08, Csi09, Met11, PVY13, Gha13]. As mentioned above, the implicit usage of the entropy inequalities has turned out to be much more advantageous when used in improved linear programming techniques [FKMP18]. *Second*, unfortunately, the existence of a notion similar to the Ahlswede-Körner [CK11] or common information [DFZ09] for characteristic-specific linear random variables is unclear. If such a notion is ever found, it can be used similarly in an automated linear program. *Third*, the lower bound method based on combinatorial-algebraic techniques are not suitable for finding lower bound on a specific access structure, even those on a small number of participants.

We provide a new technique, essentially of linear-algebraic nature, which is useful for finding a lower bound not only on the general linear information ratio but also characteristic-specific linear information ratio. Our method is currently useful to be applied to concrete small access structures and it can be easily automated. As an application, we apply our method to the Fano and non-Fano access structures on linear schemes with odd and even characteristics, respectively (they are ideal on the opposite characteristic).

To show the power of our method on general linear secret sharing, we also apply our method to one of the five-participant access structures from [JM96] which had remained open for a long time and was recently resolved using the common information method in [FKMP18].

[2] It is not clear to us if their result can be extended to hold for (multi-)linear secret sharing schemes.

Separation. The first indication of superiority of non-linear schemes (with short secrets) to scaler-linear schemes was provided by Beimel and Ishai [BI01] (see [VV15] for a follow-up) as their result was valid assuming some plausible number-theoretic (or complexity-theoretic) assumption holds true. Later, Beimel and Weinreb [BW05] proved separation between non-linear and scaler-linear secret sharing without relying on any assumption. Recently, such separation has been proved by Liu, Vaikuntanathan and Wee [LVW17], for the class of forbidden graph access structures using their connection to the CDS primitive [GIKM00].

Simonis and Ashikhmin have shown that (multi-)linear secret sharing is more powerful than the scaler-linear secret sharing [SA98] by studying the access structure induced by the Non-Pappus matroid (see [BBPT14] for stronger results). Applebaum and Arkis [AA18] have further discussed the power of amortization in secret sharing.

To the best of our knowledge, there is no result that shows non-linear secret sharing schemes are more powerful than (multi-)linear ones; nor, any result comparing abelian schemes with linear or non-abelian ones. We prove that abelian schemes outperform (multi-)linear schemes and provide some evidence that non-abelian schemes are more powerful than abelian ones.

We study the $\mathcal{F}+\mathcal{N}$ access structure—a 12-participant access structure which is the sum (union) of the Fano ($\mathcal{F}$) and non-Fano ($\mathcal{N}$) access structures—introduced independently by Matús [Mat07] and Beimel-Livne [BL08]. The information ratio of this access structure is 1, without addmiting an ideal scheme; but, the exact value of its linear information ratio is unknown. We remark that even though the earlier results show that this access structure does not admit an ideal linear scheme, they do not refute that its linear information ratio might be one. Our results on the characteristic-specific linear information ratio of the Fano and non-Fano access structures readily determine the optimal linear information ratio of $\mathcal{F}+\mathcal{N}$ (max$=4/3$ and average$=41/36$). Additionally, we provide an upper bound on its abelian information ratio (max$\leqslant 7/6$ and average$\leqslant 41/36$), proving separation between linear and abelian (and consequently non-linear) secret sharing schemes.

Currently, the best known technique for finding a non-trivial lower bound on the abelian information ratio of a given (small) access structure is to use the common information property [FHKP17] in an automated linear program. Unfortunately, computers are rather useless to work for $\mathcal{F}+\mathcal{N}$ due to the huge size of the linear program. Nevertheless, clever manual calculations my be a more appropriate tool in this case. Therefore, it remains open if our abelian upper-bound is tight. But we conjecture that the abelian information ratio of $\mathcal{F}+\mathcal{N}$ is strictly greater than one. If true, superiority of non-abelian schemes to abelian ones is verified.

1.2 A technical overview on our approach

In this section, we provide an informal description of ideas used in this paper.

Working with a convenient definition of linear schemes. A linear secret sharing can equivalently be described in terms of linear maps over a finite field [Bri89, Kot84], linear codes [Mas93, MS81] or multi-target monotone span programs [KW93, Bei11]. The latter one, essentially defines a secret sharing scheme as a *collection of vector spaces*[3]. We find this simple definition a convenient abstraction to work with for the same reason that vector spaces furnish an abstract and coordinate-free way of dealing with different objects.

To summarize, we simply define a linear secret sharing on a set P of participants as a collection $(T_i)_{i\in\{0\}\cup P}$ of subspaces of a vector space T of finite dimension over some finite field, where T_0 is the secret subspace and T_i is the share subspace of participant $i \in P$. We then explain how this spaces can be used to introduce a secret sharing scheme, i.e., a vector of jointly distributed random variables $(\boldsymbol{S}_i)_{i\in Q}$, where $Q = P \cup \{0\}$. Let T^* denote the dual space of T. The maps $\mu_i : T^* \to T_i^*$ defined by $\alpha \to \alpha|_{T_i}$ and the uniform probability distribution $\boldsymbol{T}^*$ on T^* induce a random vector $(\boldsymbol{S}_i)_{i\in Q} = \big(\mu_i(\boldsymbol{T}^*)\big)_{i\in Q}$

The value of the access function of a secret sharing scheme on a subset $A \subseteq P$, denoted by $\Phi(A)$, is the normalized amount of information gained by the participant set A about the secret. One can verify that for every $A \subseteq P$, we have $\Phi(A) = \dim(T_A \cap T_0)/\dim T_0$ where $T_A = \sum_{i\in A} T_i$. It is also easy to see that the information ratio of participant $i \in P$ is $\dim(T_i)/\dim(T_0)$.

An alternative description of linear duality of [FHKP17]. The proof of the duality of linear secret sharing schemes in [FHKP17] is based on the definition of linear schemes as a collection of linear maps. In the following, we provide an alternative description based on the definition as a collection of vector spaces in a way that it can be easily extended to secret sharing based on abelian groups. Consider the vector subspace $C \subseteq \prod_{i\in Q} T_i$ formed by the vectors $(x_i)_{i\in Q} \in \prod_{i\in Q} T_i$ satisfying $\sum_{i\in Q} x_i = 0$. The uniform probability distribution on C and the projections $C \to T_i$ define a random vector $(\boldsymbol{S}_i^*)_{i\in Q}$. It is not difficult to check that the linear secret sharing scheme determined by $(\boldsymbol{S}_i^*)_{i\in Q}$ coincides with the dual of the linear secret sharing scheme given by $(\boldsymbol{S}_i)_{i\in Q}$; that is, they have the same information ratio and their access functions are dual of each other. In particular, its access function is $\Phi^*(A) = 1 - \Phi(P\backslash A)$, which is the definition of the dual of an access function [FHKP17].

Abelian schemes, Pontryagin dual and Abelian duality. The definition of a linear scheme as a collection of subspaces of some vector space may justify to define an abelian scheme as a collection of subgroups of some abelian group. Using the notion of Pontryagin duality, we will show that this definition is equivalent to a more natural definition based on *group-characterizable random variables* [Cha07] whose main groups are abelian. See Section 3 for details.

The Pontryagin dual of an abelian group G, denoted by $\widehat{G}$, is the group of all homomorphism from G to $\mathbb{C}^*$, the multiplicative group of non-zero complex

[3] This has been explicitly mentioned in the introduction of [KW93], but another definition mentioned in the body of the paper has been exclusively used in the literature.

numbers. This notion also plays a crucial role in extending the linear duality of secret sharing schemes in a straightforward way.

A collection $(G_i)_{i\in Q}$ of subgroups of an abelian group G induces an (abelian) secret sharing scheme just as in the linear case, except that the vector space duality is replaced with Pontryagin duality. More precisely, the maps $\widehat{G} \to \widehat{G_i}$ defined by $\alpha \to \alpha|_{G_i}$ and the uniform probability distribution on $\widehat{G}$ define a random vector $(\boldsymbol{S}_i)_{i\in Q}$. It is easy to show that the information ratio of participant $i \in P$ and the value of access function on a subset $A \subseteq P$ of participants are $\log|G_i|/\log|G_0|$ and $\Phi(A) = \log|G_A \cap G_0|/\log|G_0|$, respectively, where $G_A = \sum_{i\in A} G_i$.

Consider now the subgroup $C \subseteq \prod_{i\in Q} G_i$ whose elements are the vectors $(x_i)_{i\in Q} \in \prod_{i\in Q} G_i$ satisfying $\sum_{i\in Q} x_i = 0$. As before, the uniform probability distribution on C and the projections $C \to G_i$ define a random vector $(\boldsymbol{S}_i^*)_{i\in Q}$. Using the isomorphism theorems, one can prove that the secret sharing schemes defined by those two random vectors are dual of each other; that is, they have the same information ratio and their access functions are dual of each other. Details are given in Section 4.

Our lower bound technique. Let $(T_i)_{i\in Q}$ be a linear secret sharing for a given access structure. We show that for every minimal qualified subset $A \subseteq P$, and every participant $i \in A$, there is a subspace V_i^A of T_i of dimension equal to $\dim T_0$ (i.e., the secret dimension), such that it is a *minimal subspace*; that is, no smaller subspace can recover the whole secret together with other parities corresponding subspaces (i.e., $\{T_i\}_{i\in A-\{i\}}$). Now if a participant $i \in P$ belongs to several minimal qualified subsets, one has several such subspaces of T_i. If one can show that the intersection of these subspaces is small, then it is concluded that the subspace T_i must have a big dimension. Our idea is to consider a collection of these intersections of subspaces associated to different minimal qualified sets and to use certain notions from linear algebra to show that the sum of dimensions of these intersections has a non-trivial upper bound. To do this, often the characteristic of the underlying finite field plays a crucial role. See Section 5 for details.

1.3 Paper organization

In Section 2, we present the required preliminaries and introduce our notation. In Section 3, we study the group-characterizable secret sharing schemes and their connection to the linear and abelian ones. Section 4 presents the duality of abelian schemes. In Section 5, we introduce our new lower-bound technique and apply it to three access structures. In Section 6, we discuss separation between linear and abelian secret sharing. Finally, we conclude the paper in Section 7.

2 Secret sharing schemes

In this section, we provide the basic background along with some notations and conventions. We refer the reader to Beimel's survey [Bei11] on secret sharing.

We assume that the reader is comfortable with basic concepts from group theory and linear algebra.

General notations. We use random variables and distributions interchangeably and use boldface characters for them. All random variables are discrete in this paper. The Shannon entropy of a random variable $\boldsymbol{X}$ is denoted by $\mathrm{H}(\boldsymbol{X})$, and the mutual information of random variables $\boldsymbol{X}, \boldsymbol{Y}$, denoted by $\mathrm{I}(\boldsymbol{X} : \boldsymbol{Y})$. For a positive integer m, we use $[m]$ to represent the set $\{1, \ldots, m\}$. Throughout the paper, $P = \{p_1, \ldots, p_n\}$ stands for a finite set of *participants*. A distinguished participant $p_0 \notin P$ is called *dealer* and we notate $Q = P \cup \{p_0\}$. Unless otherwise stated, we identify the participant p_i with its index i; i.e., $Q = \{0, 1, \ldots, n\}$. The set of positive integers and real numbers are respectively denoted by $\mathbb{N}$ and $\mathbb{R}$. All logarithms are to the base two. The closure of a topological set $\mathcal{X}$ is denoted by $\overline{\mathcal{X}}$, defined as the union of $\mathcal{X}$ with all its limit points.

Definition 2.1 (Access structure) *A non-empty subset $\Gamma \subseteq 2^P$, with $\varnothing \notin \Gamma$, is called an* access structure *on P if it is* monotone*; that is, $A \subseteq B \subseteq P$ and $A \in \Gamma$ imply that that $B \in \Gamma$.*

A subset $A \subseteq P$ is called *qualified* if $A \in \Gamma$; otherwise, it is called *unqualified*. A qualified subset is called *minimal* if none of its proper subsets is qualified.

Definition 2.2 (Access function [FHKP17]) *A mapping $\Phi : 2^P \to [0, 1]$ is called an* access function *if $\Phi(\varnothing) = 0$ and it is monotone; i.e., $A \subseteq B \subseteq P$ implies that $\Phi(A) \leqslant \Phi(B)$. An access function is called* rational *if $\Phi(A)$ is rational for every subset A and called* total *if $\Phi(A) \in \{0, 1\}$.*

Definition 2.3 (Secret sharing scheme) *A tuple $\Pi = \left(\boldsymbol{S}_i\right)_{i \in Q}$ of jointly distributed random variables, with finite supports, is called a* secret sharing scheme *on participant set P when $\mathrm{H}(\boldsymbol{S}_0) > 0$. The random variable $\boldsymbol{S}_0$ is called the* secret *random variable and its support is called the* secret space*. The random variable $\boldsymbol{S}_i$, for any participant $i \in P$, is called the* share *random variable of the participant i and its support is called his* share space*.*

A secret sharing scheme is used as follows. A dealer samples a tuple $\left(s_i\right)_{i \in Q}$ according to the distribution Π and keep s_0 as the secret for himself. He then privately passes each share s_i to participant $i \in P$.

The most common definition of a linear scheme is based on linear maps, given below. In Section 3.3, we provide an equivalent definition based on its connection to group-characterizable and abelian schemes.

Definition 2.4 (Linear scheme) *A secret sharing scheme $\Pi = (\boldsymbol{S}_i)_{i \in Q}$ is said to be* $\mathbb{F}$-linear (or simply linear) *if there are finite dimensional $\mathbb{F}$-vector spaces E and $(E_i)_{i \in Q}$, and $\mathbb{F}$-linear maps $\mu_i : E \to E_i$, $i \in Q$, such that $\boldsymbol{S}_i = \mu_i(\boldsymbol{E})$, where $\boldsymbol{E}$ is the uniform distribution on E. It is called p-linear if the characteristic of $\mathbb{F}$ is p, a prime.*

Definition 2.5 (Total realization) *We say that a secret sharing* $\big(\boldsymbol{S}_i\big)_{i\in Q}$ *is a* (total) scheme *for* Γ*, or it* (totally) realizes Γ*, if the following two hold:*

> **(Correctness)** $\mathrm{H}(\boldsymbol{S}_0|\boldsymbol{S}_A) = 0$ *for every qualified set* $A \in \Gamma$ *and,*
> **(Privacy)** $\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_B) = 0$ *for every unqualified set* $B \in \Gamma^c$*,*

where $\boldsymbol{S}_A = (\boldsymbol{S}_i)_{i\in A}$ *for a subset* $A \subseteq P$*.*

Definition 2.6 (Access function and convec of a scheme) *The* access function *and the* convec *of a secret sharing scheme* $\Pi = \big(\boldsymbol{S}_i\big)_{i\in Q}$ *are respectively denoted by* Φ_Π *and* $\mathrm{cv}(\Pi)$ *and defined as follows:*

$$\Phi_\Pi(A) = \frac{\mathrm{I}(\boldsymbol{S}_0 : \boldsymbol{S}_A)}{\mathrm{H}(\boldsymbol{S}_0)}\ , \qquad\qquad \mathrm{cv}(\Pi) = \Big(\frac{\mathrm{H}(\boldsymbol{S}_i)}{\mathrm{H}(\boldsymbol{S}_0)}\Big)_{i\in P}\ .$$

Information ratio and convec set. Convec is short for contribution vector [JM96] and a norm on it can be used as a measure of efficiency of a secret sharing scheme. The convec set of an access structure can be defined with respect to a class of secret sharing schemes (e.g., linear, group-characterizable, abelian, etc).

Definition 2.7 (Convec set) *The convec set of an access structure* Γ*, denoted by* $\Sigma(\Gamma)$*, is defined as the set of all convecs of all secret sharing schemes that realize* Γ*. When we restrict to the class* C *of secret sharing schemes, we use the notation* $\Sigma^{\mathrm{C}}(\Gamma)$*.*

The maximum and average information ratios of an access structure Γ on n participants, with respect to the class C of schemes, are respectively defined as:

$$\min\{\max(\boldsymbol{x}) : \boldsymbol{x} \in \overline{\Sigma^{\mathrm{C}}(\Gamma)}\} \qquad \text{and} \qquad \tfrac{1}{n}\min\{\textstyle\sum_{i=1}^n x_i : (x_1,\dots,x_n) \in \overline{\Sigma^{\mathrm{C}}(\Gamma)}\}\ .$$

3 Secret sharing based on groups ad vector spaces

The notion of group-characterizable random variables was introduced by Chan and Yeung in [CY02]. We believe that group-characterizable secret sharing schemes provide an interesting playground for studying non-linear secret sharing schemes. We refer to [**?**] and [KKP19] for some recent results on group-characterizable secret sharing schemes. In this section, we draw a line between, linear, abelian and group-characterizable secret sharing schemes.

3.1 Group-characterizable schemes

Definition 3.1 (Group-characterizable scheme [CY02]) *Let* G *be a finite group, called the* main group*, and* $G_0, G_1, \dots, G_n$ *be subgroups of* G*. We refer to the tuple* $(G : G_0, G_1, \dots, G_n)$ *as a group-characterizable secret sharing scheme if* $|G|/|G_0| \geqslant 2$*.*

For a group-characterizable scheme $\Pi = (G : G_0, G_1, \dots, G_n)$, the uniform probability distribution $\boldsymbol{g}$ on G and the quotient maps $G \to G/G_i$ determine a vector of jointly distributed random variables $(\boldsymbol{S}_i)_{i\in Q}$ by letting $\boldsymbol{S}_i = \boldsymbol{g}G_i$. That is, the support of $\boldsymbol{S}_i$ is the left cosets of G_i in G. More generally, it can be shown that for every $A \subseteq [n]$, the marginal random variable $\boldsymbol{S}_A$ is uniform on its support G/G_A where $G_A = \bigcap_{i\in A} G_i$. It is then easy to verify that

$$\Phi_\Pi(A) = \frac{\log\big(|G|/|G_A * G_0|\big)}{\log\big(|G|/|G_0|\big)}\ , \qquad \mathrm{cv}(\Pi) = \Big(\frac{\log\big(|G|/|G_i|\big)}{\log\big(|G|/|G_0|\big)}\Big)_{i\in[n]}\ . \tag{3.1}$$

3.2 Abelian schemes

A group-characterizable scheme is called *abelian* if its main group is abelian. In this section, using the notion of Pontryagin duality, we prove that this definition is equivalent to the following one, which we will work with in this paper.

Definition 3.2 (Abelian scheme) *A tuple $\Pi = (G; G_0, G_1, \dots, G_n)$ is called an abelian secret sharing scheme if G is a finite abelian group and G_i's are subgroups of G with $|G_0| \geqslant 2$. When there is no confusion, we simply write $\Pi = (G_i)_{i\in Q}$.*

As we will see, the access function and the convec of an abelian scheme $\Pi = (G; G_0, G_1, \dots, G_n)$, are computed as follows:

$$\Phi_\Pi(A) = \frac{\log|G_0 \cap G_A|}{\log|G_0|}\ , \qquad \mathrm{cv}(\Pi) = \Big(\frac{\log|G_i|}{\log|G_0|}\Big)_{i\in[n]}\ , \tag{3.2}$$

where $G_A = \sum_{i\in A} G_i$.

Before showing the equivalence of the two definitions, let us recall the definition of Pontryagin duality.

Definition 3.3 (Pontryagin dual) *The Pontryagin dual of an abelian group G, denoted by $\widehat{G}$, is the group of all homomorphism from G to $\mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of non-zero complex numbers. In other words,*

$$\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*) = \{\alpha : G \to \mathbb{C}^* | \alpha(0) = 1, \alpha(a+b) = \alpha(a)\alpha(b)\}\ .$$

It is well-known that $|\widehat{G}| = |G|$ and in fact $\widehat{G} \cong G$, i.e., $\widehat{G}$ and G are isomorphic.

Equivalence. Let $\Pi = (G; G_0, G_1, \dots, G_n)$ be an abelian scheme w.r.t. Definition 3.2 and define:

$$G_i^\perp = \{\alpha \in \widehat{G} : \alpha(x) = 1 \text{ for every } x \in G_i\}\ .$$

That is, $G_i^\perp$ is the kernel of the restriction map $\widehat{G} \to \widehat{G_i}$ defined by $\alpha \to \alpha|_{G_i}$. Now, the uniform probability distribution $\widehat{\boldsymbol{g}}$ on $\widehat{G}$ and the maps $\mu_i : \widehat{G} \to \widehat{G}/G_i^\perp$ determine a joint distribution $(\boldsymbol{S}_i)_{i\in Q} = \big(\mu_i(\widehat{\boldsymbol{g}})\big)_{i\in Q}$, which we call the secret sharing scheme induced by $\mathit{\Pi}$. Clearly, the group-characterizable scheme $\widehat{\mathit{\Pi}} = (\widehat{G} : G_0^\perp, G_1^\perp, \ldots, G_n^\perp)$ is abelian w.r.t. Definition 3.1 and induces the same distribution. Notice that the same transformation takes $\widehat{\mathit{\Pi}}$ into $\mathit{\Pi}$ isomorphically.

We now show the equivalence of relations (3.1) and (3.2). Since the onto homomorphism $\widehat{G} \to \widehat{G_i}$ defined by $\alpha \to \alpha|_{G_i}$ has kernel $G_i^\perp$, we get an isomorphism

$$\widehat{G}/G_i^\perp \cong \widehat{G_i} \cong G_i \ .$$

Therefore, $|\widehat{G}/G_i^\perp| = |G_i|$, implying $\mathrm{cv}(\widehat{\mathit{\Pi}}) = \mathrm{cv}(\mathit{\Pi})$.

To show the access function equality, we need to show that

$$\frac{\widehat{G}}{G_A^\perp + G_0^\perp} = |G_A \cap G_0| \ ,$$

where $G_A^\perp = \bigcap_{i\in A} G_i^\perp$. By the following easy-to-prove lemma, the kernel of the restriction map $\widehat{G} \to \widehat{G_A \cap G_0}$ is $G_A^\perp + G_0^\perp$. So

$$\frac{\widehat{G}}{G_A^\perp + G_0^\perp} \cong \widehat{G_A \cap G_0} \cong G_A \cap G_0 \ ,$$

which completes the proof.

Lemma 3.4 *If H_1, H_2 are subgroups of an abelian finite group G, the kernel of the restriction map $\widehat{G} \to \widehat{H_1 \cap H_2}$ is $\widehat{H_1} + \widehat{H_2}$ where $\widehat{H_i}$ is the kernel of the restriction map $\widehat{G} \to \widehat{H_i}$.*

3.3 Linear schemes

In Section 2 (Definition 2.4), we provided a definition of linear schemes based on linear maps. A linear scheme can be simply defined as an abelian scheme whose main group is a vector space. Therefore, we have the following equivalent definition. The group-characterizability of linear random variables has also been mentioned in [Cha07].

Definition 3.5 (Linear scheme) *A tuple $\mathit{\Pi} = (T; T_0, T_1, \ldots, T_n)$ is called a linear secret sharing scheme if T is a finite dimensional vector space over some finite field, T_i is a subspace of T, for each $i \in [n]$, and $\dim T_0 \geqslant 1$. When there is no confusion, we simply write $\mathit{\Pi} = (T_i)_{i\in Q}$.*

By relation (3.2), the access function and convec of a linear scheme $\mathit{\Pi} = (T_i)_{i\in Q}$ are as follows:

$$\mathit{\Phi}_{\mathit{\Pi}}(A) = \frac{\dim(T_0 \cap T_A)}{\dim T_0} \ , \qquad\qquad \mathrm{cv}(\mathit{\Pi}) = \Big(\frac{\dim T_i}{\dim T_0}\Big)_{i\in[n]} \ ,$$

where $T_A = \sum_{i\in A} T_i$.

4 Abelian duality

In this section, we generalize the well-known result of [FHKP17] on duality of linear schemes to the class of abelian schemes. The reader may recall definitions of Pontryagin dual and abelian scheme given in Section 3.2.

Definition 4.1 (Dual of an access function) *Let Φ be an access function on participants set P with $\Phi(P) = 1$. The dual of Φ, denoted by Φ^*, is defined by $\Phi^*(A) = 1 - \Phi(P \backslash A)$, for every $A \subseteq P$. The dual of an access structure Γ, denoted by Γ^*, is defined based on its induced total access function.*

Proposition 4.2 (Abelian duality) *Let $\Pi = (G; G_0, G_1, \ldots, G_n)$ be an abelian scheme that satisfies $G_0 \subseteq \sum_{i=1}^{n} G_i$ (so that $\Phi_\Pi(P) = 1$). Then, there exists an abelian scheme Π^* such that $\Phi_{\Pi^*} = \Phi^*_\Pi$ and $\mathrm{cv}(\Pi^*) = \mathrm{cv}(\Pi)$.*

Proof. We construct an abelian scheme $\Pi^* = (G^*; G^*_0, G^*_1, \ldots, G^*_n)$ such that

1. $|G^*_0| = |G_0|$,
2. $|G^*_i| \leqslant |G_i|$, for every $i \in P$,
3. $\Phi_{\Pi^*}(A) = 1 - \Phi_\Pi(P \backslash A)$, for every $A \subseteq P$.

Therefore, $\mathrm{cv}(\Pi^*) \leqslant \mathrm{cv}(\Pi)$. However, it is easy to tweak the scheme by adding dummy shares (subgroups) so that the convec equality holds.

Consider the subgroup $C \subseteq \prod_{i \in Q} G_i$ whose elements are the vectors $(x_i)_{i \in Q} \in \prod_{i \in Q} G_i$ satisfying $\sum_{i \in Q} x_i = 0$. For every $i \in P$, let C_i be the subgroup of C whose projection on the ith component is zero and define $C_A = \bigcap_{i \in A} C_i$ for $A \subseteq P$.

To define our dual abelian scheme Π^*, we let $G^* = \widehat{C}$ and

$$G^*_i = \{\alpha \in \widehat{C} | \alpha(C_i) = \{1\}\} .$$

It is clear that $G^*_i = \widehat{(C/C_i)}$ since, in general, the subgroup of $\widehat{G}$ that vanishes on a subgroup $H \leqslant G$ is isomorphic to $\widehat{(G/H)}$.

Note that the projection $C \to G_i$ that sends $(x_i)_{i \in Q}$ to x_i is onto for $i = 0$ (since $G_0 \subseteq \sum_{i=1}^{n} G_i$) and its kernel is C_0. So $G_0 \cong C/C_0$. Therefore,

$$|G^*_0| = \left|\widehat{(C/C_0)}\right| = |C/C_0| = |G_0| ,$$

proving (1). Also the projection $C \to G_i$ has kernel C_i so C/C_i is a subgroup of G_i; hence,

$$|G^*_i| = \left|\widehat{(C/C_i)}\right| = |C/C_i| \leqslant |G_i| ,$$

which proves (2).

We claim that

$$G^*_A := \sum_{i \in A} G^*_i = \{\alpha \in \widehat{C} | \alpha(C_A) = \{1\}\} .$$

Notice that $C_A \subseteq C_i$ for all $i \in A$. Therefore, if $\alpha(C_i) = \{1\}$ then $\alpha(C_A) = \{1\}$. So $G_i^* \subseteq \{\alpha \in C^* | \alpha(C_A) = \{1\}\}$ and hence $\sum_{i\in A} G_i^* \subseteq \{\alpha \in C^* | \alpha(C_A) = \{1\}\}$. Conversely, if $\alpha \in \widehat{C}$ and $\alpha(C_A) = \{1\}$, then α, on input $(x_i)_{i\in Q}$, depends only on variables x_i for $i \in A$, i.e., $\alpha(x_0, x_1, \ldots, x_n) = \alpha(y_0, y_1, \ldots, y_n)$, where $y_i = 0$ for $i \notin A$ and $y_i = x_i$ for $i \in A$. Now we have $\alpha(y_1, \ldots, y_n) = \sum_{i\in A} \alpha(0, \ldots, 0, y_i, 0, \ldots, 0)$ and $\alpha(0, \ldots, 0, y_i, 0, \ldots, 0)$ is an element of G_i^* for $i \in A$. Therefore, $\alpha \in \sum_{i\in A} G_i^*$.

It is easy to see that

$$G_0^* \cap G_A^* = \{\alpha \in \widehat{C} | \alpha(C_0 + C_A) = \{1\}\} \cong \left(\widehat{\frac{C}{C_0 + C_A}}\right) \cong \frac{C}{C_0 + C_A} \ .$$

Let $C_0 + C_A \to G_0$ be the projection onto the 0-th component. Then its kernel is C_0 and its image is $G_0 \cap G_{P\setminus A}$; because if $(x_i)_{i\in A} \in C_A$, then $\sum_{i\in A} x_i = 0$ and for every $i \in A$, $x_i = 0$. Therefore $x_0 = -\sum_{i\in P\setminus A} x_i$ and hence $x_0 \in G_{P\setminus A}$. Therefore,

$$\frac{C_0 + C_A}{C_0} \cong G_0 \cap G_{P\setminus A} \ .$$

Finally, (3) is proved as follows:

$$\begin{aligned}
\Phi_{\Pi*}(A) &= \frac{\log |G_0^* \cap G_A^*|}{\log |G_0^*|} \\
&= \frac{\log |C| - \log \left|C_0 + C_A\right|}{\log |C| - \log |C_0|} \\
&= 1 - \frac{\log \left|C_0 + C_A\right| - \log |C_0|}{\log |C| - \log |C_0|} \\
&= 1 - \frac{\log \left|\frac{C_0 + C_A}{C_0}\right|}{\log |G_0|} \\
&= 1 - \frac{\log \left|G_0 \cap G_{P\setminus A}\right|}{\log |G_0|} \\
&= 1 - \Phi_\Pi(P\setminus A) \\
&= \Phi_\Pi^*(A) \ .
\end{aligned}$$

□

5 A new lower bound technique

In this section, we introduce our new technique for finding a lower bound on the (characteristic-dependent) linear information ratio of an access structure. Two linear algebraic lemmas, that we call the *minimal subspace lamma* and the *kernel lemma*, in companion with other concepts from linear algebra lie at the hear of our method.

We apply our method to determine the exact value of the maximum/average linear information ratio of the Fano and non-Fano access structures on odd and even characteristics, respectively. For Fano, we even determine the corresponding convec set precisely.

As another example, we apply our method to one of the five-participant access structures from [JM96] which had remained open for a long time and was recently resolved using the common information method in [FKMP18]. This access structure in characteristic-independent [Bah19] (that is, for every prime p, its p-linear convec set and linear convec set are the same).

5.1 Two useful lemmas

Lemma 5.1 (Minimal subspace lemma) *Let Γ be an access structure on n participants and $A \in \Gamma$ be a minimal qualified set. Let $(T_0, T_1, \ldots, T_n)$ be a linear secret sharing scheme for Γ. Then, there exists a subspace collection $\{V_i\}_{i \in A}$, where $V_i \subseteq T_i$ for each $i \in A$, such that:*

(i) $\dim V_i = \dim T_0$ *for every $i \in A$,*
(ii) $V_k \cap \sum_{i \in A \setminus \{k\}} T_i = \{0\}$ *for every $k \in A$.*
(iii) $T_0 \subseteq \bigoplus_{i \in A} V_i$ *(i.e., every $s \in T_0$ can be uniquely written as $s = \sum_{i \in A} a_i$ where $a_i \in V_i$),*
(iv) the projection of T_0 onto V_i is surjective and injective for every $i \in A$.

Proof. Let $e_1, \ldots, e_z$ be a basis for T_0. Since $T_0 \subseteq \sum_{i \in A} T_i$, one can write $e_j = \sum_{i \in A} e_{ij}$ for $e_{ij} \in T_i$. We define V_i as the linear span of $e_{i1}, \ldots, e_{iz}$. These vectors are independent because a linear relation $\sum_{j=1}^{z} \lambda_j e_{ij} = 0$ implies that $\sum_{j=1}^{z} \lambda_j e_j$ is expressed inside $\sum_{k \in A \setminus \{i\}} T_k$. But since $A \setminus \{i\}$ is unqualified, it must hold that $\sum_{j=1}^{z} \lambda_j e_j = 0$; i.e., λ_j's are all zero. Hence, $\dim V_i = \dim T_0 = z$ that proves (i). To prove (ii), let $a \in V_k \cap \sum_{i \in A \setminus \{k\}} T_i$. We show that $a = 0$. Write $a = \sum_{j=1}^{z} \lambda_j e_{kj}$ and notice that

$$\begin{aligned} \sum_{j=1}^{z} \lambda_j e_j &= \sum_{j=1}^{z} \sum_{i \in A} \lambda_j e_{ij} \\ &= a + \sum_{j=1}^{z} \sum_{i \in A \setminus \{k\}} \lambda_j e_{ij} \end{aligned} .$$

Since both a and $\sum_{j=1}^{z} \sum_{i \in A \setminus \{k\}} \lambda_j e_{ij}$ belong to $\sum_{i \in A \setminus \{k\}} T_i$, so is $\sum_{j=1}^{z} \lambda_j e_j$. But $A \setminus \{k\}$ is not qualified and hence $\sum_{j=1}^{z} \lambda_j e_j = 0$. So λ_j's are all zero and hence $a = 0$. To prove (iii), it is clear that $T_0 \subseteq \sum_{i \in A} V_i$. But this sum is indeed a direct sum; i.e., $V_k \cap \sum_{i \in A \setminus \{k\}} V_i = \{0\}$ for every $k \in A$, since a stronger statement was proved in (ii). To prove the last statement, since $\dim T_0 = \dim V_i$, we only need to prove that projecting T_0 onto V_i is surjective. Suppose $a \in V_i$ and write $a = \sum_{j=1}^{z} \lambda_j e_{ij}$. Then, the V_i component of $\sum_{j=1}^{z} \lambda_j e_j$ is a, and therefore, its projection onto V_i is a. □

The following corollary can be proved using Shannon inequalities (e.g., refer to [Csi97, Proposition 2.3 (i)]). Here, we present an alternative proof using the minimal subspace lemma (MSL).

Corollary 5.2 *Let Γ be an access structure on n participants and $(T_0, T_1, \ldots, T_n)$ be a linear secret sharing scheme for Γ. Then, for every minimal qualified set $A \in \Gamma$ and every participant $k \in A$, the following inequality holds:*

$$\dim T_k \geqslant \dim T_0 + \dim \big(T_k \cap \sum_{i \in A \setminus \{k\}} T_i\big) .$$

Proof. Let $\{V_i\}_{i\in A}$ be a minimal subspace collection. Clearly, $T_k \cap \sum_{i\in A\setminus\{k\}} T_i$ is a subspace of T_k and so is V_k by the lemma. By Lemma 5.1 (ii), these subspaces are independent. It then follows that

$$\dim T_k \geqslant \dim V_k + \dim \big(T_k \cap \sum_{i\in A\setminus\{k\}} T_i\big) \ .$$

This completes the proof since $\dim V_k = \dim T_0$ by Lemma 5.1 (i). □

Lemma 5.3 (Kernel lemma) *Let $(T_0, T_1, \ldots, T_n)$ be a linear secret sharing scheme for an access structure Γ on n participants. Let $A \in \Gamma$ be a minimal qualified subset and for every participant $i \in A$ let A_i (not necessarily different from A) be a minimal qualified subset that includes i. For the minimal qualified subsets A and A_i, $i \in A$, consider minimal subspace collections $\{V_j\}_{j\in A}$ and $\{V^i_j\}_{j\in A_i}$, respectively. Define the linear map*

$$\phi : T_0 \to \bigoplus_{i\in A} \frac{V_i}{V_i \cap V^i_i} \ ,$$

by sending $s \in T_0$ to its projections on V_i and taking it modulo $V_i \cap V^i_i$ for $i \in A$. That is, if $s = \sum_{i\in A} a_i$ for $a_i \in V_i$, we define

$$\phi(s) = \big([a_i]\big)_{i\in A} \ ,$$

where $[\cdot]$ stands for the class in the corresponding quotient space. Then,

$$\sum_{i\in A} \dim T_i \geqslant (|A| + 1) \dim T_0 - \dim \ker \phi \ .$$

Proof. The linear map ϕ induces a 1-1 linear map $\bar{\phi}$:

$$\bar{\phi} : \frac{T_0}{\ker \phi} \to \bigoplus_{i\in A} \frac{V_i}{V_i \cap V^i_i} \ .$$

Hence,

$$\sum_{i\in A} \dim \frac{V_i}{V_i \cap V^i_i} \geqslant \dim \frac{T_0}{\ker \phi} \ ,$$

or equivalently,

$$\sum_{i\in A} \big(\dim V_i - \dim(V_i \cap V^i_i)\big) \geqslant \dim T_0 - \dim \ker \phi \ .$$

Add $\sum_{i\in A} \dim(V^i_i) = |A| \dim T_0$ —see Lemma 5.1 (i)— to the both sides and simplify to get

$$\sum_{i\in A} \dim(V_i + V^i_i) \geqslant (|A| + 1) \dim T_0 - \dim \ker \phi \ .$$

The claim then follows due to $V_i + V^i_i \subseteq T_i$, which implies $\sum_{i\in A} \dim T_i \geqslant \sum_{i\in A} \dim(V_i + V^i_i)$. □

5.2 Application to Fano

The Fano access structure, denoted by $\mathcal{F}$, is the port of the Fano matroid, with the following minimal qualified subsets

$$\min \mathcal{F} = \{p_1p_4, p_2p_5, p_3p_6, p_1p_2p_3, p_1p_5p_6, p_2p_4p_6, p_3p_4p_5\}.$$

It is ideal on finite fields with even characteristics but it does not admit an ideal scheme if the secret space size is odd [Mat07]. In particular, its p-linear information ratio is unknown for odd characteristics. We use our technique to provide a lower bound on its p-linear convec set for odd p's. Since our lower bound matches the upper-bound found in [Bah19], the boundary of its p-linear convec set is completely determined.

Proposition 5.4 (Fano with odd characteristics) *Let p be an odd prime and $(T_0, T_1, \ldots, T_6)$ be a p-linear secret sharing scheme for the Fano access structure. Then,*

(I) $\dim T_i \geqslant \dim T_0$*, for every* $i \in \{1, \ldots, 6\}$*,*
(II) $\dim T_i + \dim T_j + \dim T_k \geqslant 4 \dim T_0$*, for every size-3 minimal qualified set* $\{i, j, k\}$*.*

Additionally, for any odd p, all extreme points of the polytope described by the above 10 half-planes (after normalization to $\dim T_0$) is realizable by some p-linear scheme. Consequently, the maximum and average p-linear information ratios are both $\frac{4}{3}$.

Proof. The first inequality is trivial and follows by Corollary 5.2. To prove (II), by symmetry, we only prove the inequality for the qualified set $\{1, 2, 3\}$. Let ϕ be the linear map defined in Lemma 5.3 by the minimal qualified sets $A = \{1, 2, 3\}$, $A_1 = \{1, 4\}$, $A_2 = \{2, 5\}$ and $A_3 = \{3, 6\}$ with the corresponding minimal subspace collections $\{V_1, V_2, V_3\}$, $\{V_1', V_4'\}$, $\{V_2', V_5'\}$ and $\{V_3', V_6'\}$. The proposition is proved by showing that $\ker \phi$ is zero, since

$$\dim T_1 + \dim T_2 + \dim T_3 \geqslant 4 \dim T_0 - \dim \ker \phi\ .$$

Suppose $s = a_1 + a_2 + a_3 \in T_0$, where $a_i \in V_i$ for $i = 1, 2, 3$, maps to zero by ϕ; i.e., $\phi(s) = ([a_1], [a_2], [a_3]) = 0$, or equivalently, $a_i \in V_i \cap V_i'$, for $i = 1, 2, 3$.

There are $a_4' \in V_4'$, $a_5' \in V_5'$ and $a_6 \in V_6'$ such that $a_1 + a_4' \in T_0$, $a_2 + a_5' \in T_0$ and $a_3 + a_6' \in T_0$. By subtracting each vector from $s = a_1 + a_2 + a_3 \in T_0$, it then follows that $a_2 + a_3 - a_4' \in T_0$, $a_1 + a_3 - a_5' \in T_0$ and $a_1 + a_2 - a_6' \in T_0$. But since $\{2, 3, 4\}$, $\{1, 3, 5\}$ and $\{1, 2, 6\}$ are unqualified sets, all these vectors must be zero; i.e., $a_4' = a_2 + a_3$, $a_5' = a_1 + a_3$ and $a_6' = a_1 + a_2$. Since the characteristic of the underlying finite field is odd, we have $s = (a_4' + a_5' + a_6')/2$. Since $\{4, 5, 6\}$ is unqualified, it implies that $s = 0$. This shows that $\ker \phi = \{0\}$.

The additional claim follows form [Bah19]. □

5.3 Application to non-Fano

The non-Fano access structure, denoted by $\mathcal{N}$, is the port of the non-Fano matroid, with the following minimal qualified sets

$$\min \mathcal{N} = \{p_1p_4, p_2p_5, p_3p_6, p_1p_2p_3, p_1p_5p_6, p_2p_4p_6, p_3p_4p_5, p_4p_5p_6\} \ .$$

That is, $\min \mathcal{N} = \min \mathcal{F} \cup \{p_4p_5p_6\}$. It is ideal on finite fields with odd characteristics but it does not admit an ideal scheme if the secret space size is even [Mat07].

We use our technique to find a lower bound on its linear convec set over finite fields with even characteristic. Unlike, the case of Fano, our lower bound does not match the upper-bound reported in [Bah19]. Nevertheless, the exact value of the maximum and average 2-linear information ratios are determined.

Proposition 5.5 (Non-Fano with even characteristic) *Let $(T_0, T_1, \ldots, T_6)$ be a linear secret sharing scheme for the non-Fano access structure on a finite field with even characteristic. Then,*

(I) $\dim T_i \geqslant \dim T_0$*, for every* $i \in \{1, \ldots, 6\}$*,*
(II) $\dim T_1 + \dim T_2 + \dim T_3 + \dim T_i \geqslant 5 \dim T_0$*, for every* $i = 4, 5, 6$*,*
(III) $\dim T_4 + \dim T_5 + \dim T_6 \geqslant 4 \dim T_0$*,*
(IV) $\dim T_i + 2\dim T_j + \dim T_k \geqslant 5 \dim T_0$*, for every triple* $(i, j, k) = (1, 5, 6)$*,* $(1, 6, 5)$*,* $(2, 4, 6)$*,* $(2, 6, 4)$*,* $(3, 4, 5)$*,* $(3, 5, 4)$*.*

Additionally, the maximum and average 2-linear information ratios are $\frac{4}{3}$ and $\frac{23}{18}$, respectively.

Proof. The first inequality is trivial and follows by Corollary 5.2. Proofs of (II)-(IV) are based on the kernel lemma (Lemma 5.3).

Proof of (II). By symmetry, we prove the inequality for $i = 4$. Let ϕ be the linear map defined in Lemma 5.3 by the minimal qualified sets $A = \{1, 2, 3\}$, $A_1 = \{1, 4\}$, $A_2 = \{2, 5\}$ and $A_3 = \{3, 6\}$ with the corresponding subspace collections $\{V_1, V_2, V_3\}$, $\{V_1', V_4'\}$, $\{V_2', V_5'\}$ and $\{V_3', V_6'\}$. Since we have,

$$\dim T_1 + \dim T_2 + \dim T_3 \geqslant 4 \dim T_0 - \dim \ker \phi \ ,$$

it is enough to show that

$$\dim T_4 \geqslant \dim T_0 + \dim \ker \phi \ .$$

By Corollary 5.2, for the minimal qualified set $\{4, 5, 6\}$, we have

$$\dim T_4 \geqslant \dim T_0 + \dim(T_4 \cap (T_5 + T_6)) \ .$$

Therefore, it is enough to construct a 1-1 map from $\ker \phi$ into $T_4 \cap (T_5 + T_6)$. This implies that $\dim(T_4 \cap (T_5 + T_6)) \geqslant \dim \ker \phi$, which completes the proof. We construct the 1-1 map from $\ker \phi$ into $T_4 \cap (T_5 + T_6)$ by associating a unique $a_4' \in T_4 \cap (T_5 + T_6)$ to every $s \in \ker \phi$. Suppose $s = a_1 + a_2 + a_3 \in T_0$, where

$a_i \in V_i$ for $i = 1,2,3$, maps to zero by ϕ; i.e.; $a_i \in V_i \cap V'_i$ for $i = 1,2,3$. Therefore, one can find $a'_4 \in V'_4$, $a'_5 \in V'_5$ and $a'_6 \in V'_6$ such that $a_1 + a'_4 \in T_0$, $a_2 + a'_5 \in T_0$ and $a_3 + a'_6 \in T_0$. If we add each of these three vectors separately to $s = a_1 + a_2 + a_3 \in T_0$, we get $a_2 + a_3 + a'_4 \in T_0$, $a_1 + a_3 + a'_5 \in T_0$ and $a_1+a_2+a'_6 \in T_0$ (recall the characteristic is even). Now all these vectors need to be zero since $\{2,3,4\}$, $\{1,3,5\}$ and $\{1,2,6\}$ are unqualified sets; hence, $a'_4 = a_2+a_3$, $a'_5 = a_1+a_3$ and $a'_6 = a_1+a_2$. It follows that $a'_4 = a'_5+a'_6$ and, hence, it belongs to $T_4 \cap (T_5+T_6)$. So we have defined a 1-1 map from $\ker\phi$ into $T_4 \cap (T_5+T_6)$ by sending s to a'_4. The 1-1 ness of this map follows from the uniqueness of $a'_4 \in V'_4$ such that $a_1 + a'_4 \in T_0$; see Lemma 5.1 (iv).

Proof of (III). The proof is similar to that of Proposition 5.4. Let ϕ be the linear map defined in Lemma 5.3 by the minimal qualified sets $A = \{4,5,6\}$, $A_4 = \{1,4\}$, $A_5 = \{2,5\}$ and $A_6 = \{3,6\}$ with the corresponding subspace collections $\{V_4,V_5,V_6\}$, $\{V'_1,V'_4\}$, $\{V'_2,V'_5\}$ and $\{V'_3,V'_6\}$. It is enough to show that $\ker\phi$ is zero because

$$\dim T_3 + \dim T_4 + \dim T_5 \geqslant 4\dim T_0 - \dim\ker\phi\ .$$

Suppose $s = a_4+a_5+a_6 \in T_0$, where $a_i \in V_i$ for $i = 4,5,6$, is in the kernel of ϕ; i.e.; $a_i \in V_i \cap V'_i$ for $i = 4,5,6$. We can find $a'_i \in V'_i$, for $i = 1,2,3$, such that $a'_1 + a_4 \in T_0$, $a'_2 + a_5 \in T_0$ and $a'_3 + a_6 \in T_0$. By adding the sum of the first two vectors to $s = a_4 + a_5 + a_6 \in T_0$, it follows that $a'_1 + a'_2 + a_6 \in T_0$ (characteristic is even). But since $\{1,2,6\}$ is unqualified, the resulting vector must be zero; i.e., $a_6 = a'_1+a'_2$. Similarly, $a_4 = a'_2+a'_3$ and $a_5 = a'_1+a'_3$. Hence $s = a_4+a_5+a_6 = 0$. This shows that $\ker\phi = \{0\}$.

Proof of (IV). By symmetry, we prove the inequality only for the triple $(i,j,k) = (1,5,6)$. Let ϕ be the linear map defined in Lemma 5.3 by the minimal qualified sets $A = \{1,5,6\}$, $A_1 = \{1,4\}$, $A_5 = \{2,5\}$ and $A_6 = \{3,6\}$ with the corresponding minimal subspace collections $\{V_1,V_5,V_6\}$, $\{V'_1,V'_4\}$, $\{V'_2,V'_5\}$ and $\{V'_3,V'_6\}$. The proof continues similar to that of (I). It is enough to show that

$$\dim T_5 \geqslant \dim T_0 + \dim\ker\phi\ ,$$

because

$$\dim T_1 + \dim T_5 + \dim T_6 \geqslant 4\dim T_0 - \dim\ker\phi\ .$$

Since $\{4,5,6\}$ is a minimal qualified set, by Corollary 5.2, we have

$$\dim T_5 \geqslant \dim T_0 + \dim(T_5 \cap (T_4+T_6))\ .$$

Therefore, to complete the proof, it is enough to construct a 1-1 map from $\ker\phi$ into $T_5 \cap (T_4+T_6)$. Suppose $s = a_1 + a_5 + a_6 \in T_0$ for $i = 1,5,6$, where $a_i \in V_i$, maps to zero by ϕ; i.e.; $a_i \in V_i \cap V'_i$ for $i = 1,5,6$. Our map sends s to a_5. The uniqueness of this choice follows from Lemma 5.1 (iv). It remains to prove that $a_5 \in T_5 \cap (T_4+T_6)$. It is enough to show that $a_5 \in T_4+T_6$ since clearly $a_5 \in T_5$. Find $a'_i \in V'_i$, for $i = 2,3,4$ such that $a_1 + a'_4 \in T_0$, $a'_2 + a_5 \in T_0$ and $a'_3+a_6 \in T_0$. By adding the second vector, the third one and the sum of the three vectors to $s = a_1 + a_5 + a_6 \in T_0$, it respectively follows that $a_1 + a'_2 + a_6 \in T_0$,

$a_1 + a'_3 + a_5 \in T_0$ and $a'_2 + a'_3 + a'_4 \in T_0$ (characteristic is even). But all these vectors must be zero since $\{1,2,6\}$, $\{1,3,5\}$ and $\{2,3,4\}$ are unqualified sets. Hence $a_5 = a_1 + a'_3 = (a'_2 + a_6) + (a'_2 + a'_4) = a'_4 + a_6 \in T_4 + T_6$.

The claim on the information ratio follows by [Bah19]; see Remark 5.6. □

Remark 5.6 (Tightness) *It is easy to verify that the polytope described by the 16 half-planes mentioned in Proposition 5.5 has 13 extreme points in total which are symmetries of* $(2,1,1,2,1,1)$, $(1,1,1,2,2,2)$, $(2,1,1,1,2,2)$, $(\frac{3}{2},1,1,\frac{3}{2},\frac{3}{2},\frac{3}{2})$, $(\frac{5}{3},1,1,\frac{4}{3},\frac{4}{3},\frac{4}{3})$ *(a normalization to* $\dim T_0$ *is considered). All except the last one have been realized in [Bah19]. Even though this is enough to determine the exact value of the maximum and average information ratios, the* 2*-linear convec set remains unknown. If one proves the following additional inequalities, it shows that the upper-bound reported in [Bah19] is tight:*

$$\begin{gathered}\dim T_i + \dim T_j + \dim T_k + \dim T_\ell \geqslant 5 \dim T_0 \ , \\ (i,j,k,\ell) \in \big\{(1,5,6,2),(1,5,6,3),(2,4,6,1), \\ (2,4,6,3),(3,4,5,1),(3,4,5,2)\big\} \ . \end{gathered} \tag{5.1}$$

5.4 Application to a five-participant access structure

To show the power of our method for the case of characteristic-independent information ratio, we apply it to the access structures Γ_{73} [JM96] on five-participants, with the following minimal qualified sets

$$\min \Gamma_{73} = \{p_1p_2, p_1p_3, p_2p_4, p_3p_5, p_1p_4p_5\} \ .$$

The information ratio of this access structure is still unknown. Its linear information ratio was also open for a long time, but it has been recently computed using the common information method in [FKMP18], for which a matching upper-bound was also provided. We determine the linear convec set (closure) of this access structure completely.

Its linear convec set is independent of characteristic and is given by the following set of inequalities:

(I) $\dim T_i \geqslant \dim T_0$, for every $i \in \{1,\ldots,5\}$,
(II) $\dim T_i + \dim T_j \geqslant 3 \dim T_0$, for every $(i,j) \in \{(1,2),(1,3),(2,4),(3,5)\}$,
(III) $\dim T_1 + \dim T_4 + \dim T_5 \geqslant 4 \dim T_0$,
(IV) $\dim T_1 + \dim T_i + \dim T_4 + \dim T_5 \geqslant 6 \dim T_0$, for $i = 2, 3$,
(V) $\dim T_1 + \dim T_2 + \dim T_3 \geqslant 5 \dim T_0$,

In [Bah19], it has been shown that all extreme points (convecs) of the polytope specified by the above 13 half-planes are realizable by some linear scheme for every arbitrary (non-zero) field characteristic.

Inequalities (I)-(IV) can be derived using Shanon-type information inequalities. The first two can also be derived using our MSL (minimum subspace lemma) technique, but we were not able to derive (IV). Inequality (V) can be derived using the common information method of [FKMP18]. Below, we derive it using the MSL method. First, we present two lemmas. The first one is easily proved by induction. We only prove the second one.

Lemma 5.7 (Intersection lemma) *Given subspaces $T_1, \ldots, T_m$ of T, we have*

$$(m-1)\dim T \geqslant \sum_{i=1}^{m} \dim T_i - \dim \bigcap_{i=1}^{m} T_i \ .$$

Notation. Use a compact notation for set union, that is, AB stands for $A \cup B$ and iA for $\{i\} \cup A$. For a minimal qualified set A, denote a minimal subspace collection by $\{V_i^A\}_{i \in A}$. For a subset $B \subseteq P$, notate $V_B^A = \sum_{i \in B} V_i^A$.

Lemma 5.8 (Embedding lemma) *Let Γ be an access structure. For every $i = 1, \ldots, m$, assume that aA_i is a minimal qualified subset of Γ but A_1A_i is not qualified. Then we have a 1-1 mapping:*

$$V_a^{aA_1} \cap \ldots \cap V_a^{aA_m} \hookrightarrow V_{A_1}^{aA_1} \cap \ldots \cap V_{A_m}^{aA_m} \ .$$

Proof. If $x \in V_a^{aA_1} \cap \ldots \cap V_a^{aA_m}$ there are $x_1 \in V_{A_1}^{aA_1}, \ldots, x_m \in V_{A_1}^{aA_m}$ such that $x + x_1, \ldots, x + x_m \in T_0$. Therefore, $x_i - x_1 \in T_0$ for for every $i = 1, \ldots, m$. But by assumption, A_1A_i is not qualified, so $x_i = x_1$ for all $i = 1, \ldots, m$. Therefore, we have a 1-1 map from the left side to the right side. □

Proof of (V). By Lemma 5.7, we have

$$\dim T_2 \geqslant 2\dim T_0 - d_2, \text{ where } d_2 = \dim\left(V_2^{21} \cap V_2^{24}\right) , \tag{5.2}$$

and

$$\dim T_3 \geqslant 2\dim T_0 - d_3, \text{ where } d_3 = \dim\left(V_3^{31} \cap V_3^{35}\right) . \tag{5.3}$$

Since 14 and 15 are not qualified, by Lemma 5.8, we have the following embeddings:

$$V_2^{21} \cap V_2^{24} \hookrightarrow V_1^{21} \cap V_4^{24} \ ,$$
$$V_3^{31} \cap V_3^{35} \hookrightarrow V_1^{31} \cap V_5^{35} \ .$$

If we show that the following three subspaces are independent,

$$V_1^{21} \cap V_4^{24}, \quad V_1^{31} \cap V_5^{35}, \quad V_1^{145}$$

then we have

$$\dim T_1 \geqslant \dim T_0 + d_2 + d_3 \ . \tag{5.4}$$

By adding (5.2), (5.3) and (5.4), Inequality (V) is proved.

If $x \in V_1^{21} \cap V_4^{24} \cap V_1^{31} \cap V_5^{35}$, then there is $y \in V_2^{24}$ such that $x + y \in T_0$. But $x \in V_5^{35}$ and 25 is not qualified, so $x = 0$. Now assume that

$$x \in \Big(\big(V_1^{21} \cap V_4^{24}\big) + \big(V_1^{31} \cap V_5^{35}\big)\Big) \cap V_1^{145} \ .$$

Then $x \in (T_4 + T_5) \cap V_1^{145}$. So there are $y \in V_4^{145}$ and $z \in V_5^{145}$ such that $x+y+z \in T_0$. But $x \in T_4+T_5$ and 45 is not qualified, so $x = 0$ (also $y = z = 0$).

6 Separation

In this section, we prove that abelian secret sharing schemes are more powerful than the linear schemes. To this end, we determine the exact value of the maximum/average linear information ratio of the access structure $\mathcal{F}+\mathcal{N}$, a well-known 12-participant access structure which is the union of Fano and non-Fano access structures [BL08, Mat07]. We also compute an upper-bound on its abelian information ratio. This access structure is known to be nearly ideal but non-ideal [BL08, Mat07]; i.e., $\mathbf{1} \in \overline{\Sigma(\mathcal{F}+\mathcal{N})}$) but $\mathbf{1} \notin \Sigma(\mathcal{F}+\mathcal{N})$).

Let us use the notation $\Sigma^{\mathrm{L}}(\Gamma)$, $\Sigma^{p}(\Gamma)$ and $\Sigma^{\mathrm{ABL}}(\Gamma)$, respectively, for the linear, p-linear, and abelian convec set of an access structure Γ.

Similar to the Σ-set, the Σ^p-set and Σ^{ABL}-set of every access structure can be shown to be a set with convex closure. The Σ^{L}-sets of most access structures have convex closures too. Our results of Section 5 shows that the closure of the linear convec set of $\mathcal{F}+\mathcal{N}$ is not convex, but union of two convex sets, since in general we have:

$$\Sigma^{\mathrm{L}}(\Gamma) = \bigcup_{p:\text{prime}} \Sigma^{p}(\Gamma) \ .$$

Notice that the p-linear convec set of $\mathcal{F}+\mathcal{N}$ is

$$\Sigma^{p}(\mathcal{F}+\mathcal{N}) = \Big(\Sigma^{p}(\mathcal{F}) \oplus [\mathbf{1},\infty)\Big) \cup \Big([\mathbf{1},\infty) \oplus \Sigma^{p}(\mathcal{N})\Big),$$

where, for $\mathcal{X} \subseteq \mathbb{R}^n$ and $\mathcal{Y} \subseteq \mathbb{R}^m$, the set $\mathcal{X} \oplus \mathcal{Y} \subseteq \mathbb{R}^{m+n}$ is defined as follows

$$\mathcal{X} \oplus \mathcal{Y} = \{(x,y) \mid x \in \mathcal{X} \wedge y \in \mathcal{Y}\} \ .$$

The results of previous section (Proposition 5.4 and Proposition 5.5) determine a lower and upperbound for the linear convec set of $\mathcal{F}+\mathcal{N}$. However, the optimal values of the maximum and average linear information ratios are determined (max=4/3 and average= 41/36). The following proposition, which is easy to prove, provides an upper-bound on the abelian information ratio of $\mathcal{F}+\mathcal{N}$ (max=7/6 and average= 41/36). Refer to Table 1 for a summary of our results.

Proposition 6.1 (Linear convex-hull inclusion) *The closure of the abelian convec set of every access structure includes the closure of the convex hull of its linear convec set.*

We wonder if there exists an access structure for which the convex-hull inclusion is proper. If there is no such an access structure, our upper-bounds on the maximum and average abelian information ratios are exact, showing superiority of non-abelian schemes to the abelian ones.

Separation between non-abelian and abelian secret sharing may also be proved by finding a nontrivial lower bound on the abelian information ratio of $\mathcal{F}+\mathcal{N}$, which we conjecture to be strictly greater than one. Currently, the best known technique for computing a non-trivial lower bound on the abelian information ratio is to solve a linear program based on the common information property [FHKP17] by a computer. Unfortunately, computers can not help in the case of $\mathcal{F}+\mathcal{N}$ due to the huge size of the linear program (the variant discussed in the conclusion of [FHKP17] based on a feasible solution of the dual linear program is not applicable either). Nevertheless, clever manual calculations may be a more appropriate tool in this case.

		information ratio	
access structure	class	max	average
$\mathcal{F}$	linear (odd)	4/3	4/3
$\mathcal{N}$	linear (even)	4/3	23/18
$\mathcal{F}+\mathcal{N}$	linear	4/3	41/36
	abelian	$\leqslant 7/6$	$\leqslant 41/36$

Table 1: Upper and lower bounds on the information ratios of the Fano ($\mathcal{F}$), non-Fano ($\mathcal{N}$) and their union ($\mathcal{F}+\mathcal{N}$) access structure, with respect to different classes of schemes.

7 Conclusion

We introduced a new technique which is useful for finding a lower bound not only on the (general) linear information ratio but also characteristic-specific linear information ratio of access structures. Our method is currently useful to be applied to concrete small access structure and it can be easily automated.

We applied our method to the Fano and non-Fano access structures whose information ratios depend on the characteristic of the underlying finite filed, and also on a five participant access structure whose linear information ratio is characteristic-independent.

We then used our result in a straightforward way to prove superiority of abelian schemes to the linear ones. Additionally, we proved that a well-known result about the duality of linear schemes can be extended to the abelian ones.

It is an interesting question to study separation and duality with respect to other classes of group-characterizable-based secret sharing schemes. Unfortunately, very little is known about such schemes and they have not taken that much attention from the crypto community. We refer to [JK19] and [KKP19] for some recent results.

Below, we suggest some problems for future.

Q1. Prove or refute the following statement: the closure of the abelian convec set of every access structure is the same as the closure of the convex hull of its linear convec set.
Q2. Determine a non-trivial lower bound on the abelian information ratio of $\mathcal{F}+\mathcal{N}$ (see Section 6).
Q3. Prove or refute Inequality (5.1) for the non-Fano access structure.
Q4. Prove Inequality (IV) for Γ_{73} using the MSL method (see Section 5.4).

Probably, the best way to handle Q2 is to apply the common information method [FKMP18] manually on $\mathcal{F}+\mathcal{N}$ in a clever way. Here is another direction for tackling the problem. The common information method does not take the size of subgroups into account. What we need is a technique for finding a lower bound on the abelian information ratio of an access structure (e.g., the Fano or non-Fano), for the case where the order of secret subgroup is even or odd. Indeed, this would be a generalization of our characteristic-dependent lower bound method.

References

AA18. Benny Applebaum and Barak Arkis. On the power of amortization in secret sharing: d-uniform secret sharing and CDS with constant information rate. In *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part I*, pages 317–344, 2018.

ABF+19. Benny Applebaum, Amos Beimel, Oriol Farràs, Oded Nir, and Naty Peter. Secret-sharing schemes for general and uniform access structures. *IACR Cryptology ePrint Archive*, 2019:231, 2019.

Bah19. Sorush Bahariyan. A systematic approach for determining the linear convec set of small access structures (in persian). Master's thesis, Sharif University of Technology, 2019.

BBPT14. Amos Beimel, Aner Ben-Efraim, Carles Padró, and Ilya Tyomkin. Multi-linear secret-sharing schemes. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 394–418, 2014.

Bei11. Amos Beimel. Secret-sharing schemes: A survey. In *Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China, May 30-June 3, 2011. Proceedings*, pages 11–46, 2011.

BFMP17. Amos Beimel, Oriol Farràs, Yuval Mintz, and Naty Peter. Linear secret-sharing schemes for forbidden graph access structures. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part II*, pages 394–423, 2017.

BGK+96. László Babai, Anna Gál, János Kollár, Lajos Rónyai, Tibor Szabó, and Avi Wigderson. Extremal bipartite graphs and superpolynomial lower bounds for monotone span programs. In *STOC*, pages 603–611, 1996.

BGP97. Amos Beimel, Anna Gál, and Mike Paterson. Lower bounds for monotone span programs. *Computational Complexity*, 6(1):29–45, 1997.

BGW99. László Babai, Anna Gál, and Avi Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica*, 19(3):301–319, 1999.

BI01. Amos Beimel and Yuval Ishai. On the power of nonlinear secret-sharing. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity, Chicago, Illinois, USA, June 18-21, 2001*, pages 188–202, 2001.

BIKK14. Amos Beimel, Yuval Ishai, Ranjit Kumaresan, and Eyal Kushilevitz. On the cryptographic complexity of the worst functions. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 317–342, 2014.

BKL11. Anna Blasiak, Robert Kleinberg, and Eyal Lubetzky. Lexicographic products and the power of non-linear network coding. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 609–618, 2011.

BKN18. Amos Beimel, Eyal Kushilevitz, and Pnina Nissim. The complexity of multiparty PSM protocols and related models. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, pages 287–318, 2018.

BL88. Josh Cohen Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. In *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, pages 27–35, 1988.

BL08. Amos Beimel and Noam Livne. On matroids and nonideal secret sharing. *IEEE Trans. Information Theory*, 54(6):2626–2643, 2008.

Bla79. George Robert Blakley. Safeguarding cryptographic keys. *Proc. of the National Computer Conference1979*, 48:313–317, 1979.

BLP08. Amos Beimel, Noam Livne, and Carles Padró. Matroids can be far from ideal secret sharing. In *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008.*, pages 194–212, 2008.

BM84. George Robert Blakley and Catherine Meadows. Security of ramp schemes. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 242–268. Springer, 1984.

Bri89. Ernest F. Brickell. Some ideal secret sharing schemes. In *Advances in Cryptology - EUROCRYPT '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium, April 10-13, 1989, Proceedings*, pages 468–475, 1989.

BS92. Ernest F. Brickell and Douglas R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *J. Cryptology*, 5(3):153–166, 1992.

BSSV92. Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, and Ugo Vaccaro. Graph decompositions and secret sharing schemes. In *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*, pages 1–24, 1992.

BW05. Amos Beimel and Enav Weinreb. Separating the power of monotone span programs over different fields. *SIAM J. Comput.*, 34(5):1196–1215, 2005.

Cha07. Terence H. Chan. Group characterizable entropy functions. In *IEEE International Symposium on Information Theory, ISIT 2007, Nice, France, June 24-29, 2007*, pages 506–510, 2007.

CK11. Imre Csiszar and János Körner. *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

CSGV93. Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, and Ugo Vaccaro. On the size of shares for secret sharing schemes. *J. Cryptology*, 6(3):157–167, 1993.

Csi94. László Csirmaz. The size of a share must be large. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, pages 13–22, 1994.

Csi97. László Csirmaz. The size of a share must be large. *J. Cryptology*, 10(4):223–231, 1997.

Csi09. László Csirmaz. An impossibility result on graph secret sharing. *Des. Codes Cryptography*, 53(3):195–209, 2009.

CY02. Terence H. Chan and Raymond W. Yeung. On a relation between information inequalities and group theory. *IEEE Trans. Information Theory*, 48(7):1992–1995, 2002.

DFZ09. Randall Dougherty, Christopher F. Freiling, and Kenneth Zeger. Linear rank inequalities on five or more variables. *CoRR*, abs/0910.0284, 2009.

DFZ15. Randall Dougherty, Eric Freiling, and Kenneth Zeger. Characteristic-dependent linear rank inequalities with applications to network coding. *IEEE Trans. Information Theory*, 61(5):2510–2530, 2015.

FHKP17. Oriol Farràs, Torben Brandt Hansen, Tarik Kaced, and Carles Padró. On the information ratio of non-perfect secret sharing schemes. *Algorithmica*, 79(4):987–1013, 2017.

FKMP18. Oriol Farràs, Tarik Kaced, Sebastià Martín Molleví, and Carles Padró. Improving the linear programming technique in the search for lower bounds in secret sharing. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 597–621, 2018.

Gál98. Anna Gál. A characterization of span program size and improved lower bounds for monotone span programs. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 429–437, 1998.

Gha13. Motahhareh Gharahi. *On the Complexity of Perfect Secret Sharing Schemes (in Persian)*. PhD thesis, Iran University of Science and Technology, 2013.

GIKM00. Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. *J. Comput. Syst. Sci.*, 60(3):592–629, 2000.

GK18. Motahhareh Gharahi and Shahram Khazaei. Optimal linear secret sharing schemes for graph access structures on six participants. *Theoretical Computer Science*, 2018.

GP03. Anna Gál and Pavel Pudlák. A note on monotone complexity and the rank of matrices. *Inf. Process. Lett.*, 87(6):321–326, 2003.

Ing71. Aubrey W Ingleton. Representation of matroids. *Combinatorial mathematics and its applications*, 23, 1971.

ISN89. Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret sharing scheme realizing general access structure. *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, 72(9):56–64, 1989.

JK19. Amir Jafari and Shahram Khazaei. On relaxed security notions for secret sharing. *IACR Cryptology ePrint Archive*, 2019:??, 2019.

JM94. Wen-Ai Jackson and Keith M. Martin. Geometric secret sharing schemes and their duals. *Des. Codes Cryptography*, 4(1):83–95, 1994.

JM96. Wen-Ai Jackson and Keith M Martin. Perfect secret sharing schemes on five participants. *Designs, Codes and Cryptography*, 9(3):267–286, 1996.

KKP19. Reza Kaboli, Shahram Khazaei, and Maghsoud Parviz. Group-homomorphic secret sharing schemes are group-characterizable with normal subgroups. *IACR Cryptology ePrint Archive*, 2019:??, 2019.

KOS+93. Kaoru Kurosawa, Koji Okada, Keiichi Sakano, Wakaha Ogata, and Shigeo Tsujii. Nonperfect secret sharing schemes and matroids. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 126–141, 1993.

Kot84. Suresh C. Kothari. Generalized linear threshold scheme. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 231–241, 1984.

KW93. Mauricio Karchmer and Avi Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*, pages 102–111, 1993.

LV18a. Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 699–708, 2018.

LV18b. Tianren Liu and Vinod Vaikuntanathan. Breaking the circuit-size barrier in secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 699–708, 2018.

LVW17. Tianren Liu, Vinod Vaikuntanathan, and Hoeteck Wee. Conditional disclosure of secrets via non-linear reconstruction. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part I*, pages 758–790, 2017.

Mar93. Keith M Martin. New secret sharing schemes from old. *J. Combin. Math. Combin. Comput*, 14:65–77, 1993.

Mas93. James L Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279. Citeseer, 1993.

Mat07. Frantisek Matús. Two constructions on limits of entropy functions. *IEEE Trans. Information Theory*, 53(1):320–330, 2007.

Met11. Jessica Ruth Metcalf-Burton. Improved upper bounds for the information rates of the secret sharing schemes induced by the vámos matroid. *Discrete Mathematics*, 311(8-9):651–662, 2011.

MS81. Robert J. McEliece and Dilip V. Sarwate. On sharing secrets and reed-solomon codes. *Commun. ACM*, 24(9):583–584, 1981.

PR18. Toniann Pitassi and Robert Robere. Lifting nullstellensatz to monotone span programs over any field. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018, Los Angeles, CA, USA, June 25-29, 2018*, pages 1207–1219, 2018.

PVY13. Carles Padró, Leonor Vázquez, and An Yang. Finding lower bounds on the complexity of secret sharing schemes by linear programming. *Discrete Applied Mathematics*, 161(7-8):1072–1084, 2013.

Raz90. Alexander A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Combinatorica*, 10(1):81–93, 1990.

SA98. Juriaan Simonis and Alexei E. Ashikhmin. Almost affine codes. *Des. Codes Cryptography*, 14(2):179–197, 1998.

SC02. Hung-Min Sun and Bor-Liang Chen. Weighted decomposition construction for perfect secret sharing schemes. *Computers & Mathematics with Applications*, 43(6):877–887, 2002.

Sha79. Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

SRR02. K. Srinathan, N. Tharani Rajan, and C. Pandu Rangan. Non-perfect secret sharing over general access structures. In *Progress in Cryptology - INDOCRYPT 2002, Third International Conference on Cryptology in India, Hyderabad, India, December 16-18, 2002*, pages 409–421, 2002.

SS97. Hung-Min Sun and Shiuh-Pyng Shieh. Secret sharing in graph-based prohibited structures. In *Proceedings IEEE INFOCOM '97, The Conference on Computer Communications, Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Driving the Information Revolution, Kobe, Japan, April 7-12, 1997*, pages 718–724, 1997.

Sti92. Douglas R. Stinson. An explication of secret sharing schemes. *Des. Codes Cryptography*, 2(4):357–390, 1992.

VD95. Marten Van Dijk. On the information rate of perfect secret sharing schemes. *Designs, Codes and Cryptography*, 6(2):143–169, 1995.

vDKST06. Marten van Dijk, Tom Kevenaar, Geert-Jan Schrijen, and Pim Tuyls. Improved constructions of secret sharing schemes by applying (λ, ω)-decompositions. *Information processing letters*, 99(4):154–157, 2006.

VV15. Vinod Vaikuntanathan and Prashant Nalini Vasudevan. Secret sharing and statistical zero knowledge. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, pages 656–680, 2015.

ZY97. Zhen Zhang and Raymond W. Yeung. A non-shannon-type conditional inequality of information quantities. *IEEE Trans. Information Theory*, 43(6):1982–1986, 1997.