# Lower Bounds on the Information Ratio of Linear Secret Sharing Schemes

Carles Padró

Nanyang Technological University, Singapore

January 30, 2013

**Abstract**

Superpolynomial lower bounds on the average information ratio of linear secret sharing scheme are presented in this note for the first time. The previously known superpolynomial lower bounds applied only to the average information ratio of linear schemes in which the secret is a single field element. The new bounds are obtained by a simple adaptation of the techniques in those previous works.

**Key words.** Secret sharing, Linear secret sharing schemes, Lower bounds on the information ratio.

## 1 Introduction

In a *secret sharing scheme*, a *secret value* is distributed into *shares* among a set of *participants* in such a way that only the *qualified sets* of participants can recover the secret value, while no information at all on the secret value is provided by the shares from an unqualified set. The qualifed sets form the *access structure* of the scheme. Secret sharing was independently introduced by Shamir [10] and Blakley [4]. The reader is referred to [2] for an up-to-date survey on this topic.

Even though there exists a secret sharing scheme for every access structure [8], all known general constructions are impractical because the size of the shares grows exponentially with the number of participants. The general opinion among the researchers in the area is that this is unavoidable. Nevertheless, the known lower bounds on the size of the shares are far from proving this conjecture. Indeed, the best of the known lower bounds is the one given by Csirmaz [5], who proved that, for every $n$, there exists an access structure on $n$ participants requiring shares of size $\Omega(n/\log n)$ times the size of the secret.

The *information ratio*, respectively *average information ratio*, of a secret sharing scheme is the ratio between the maximum size, respectively average size, of the shares and the size of the secret value. Lower bounds on the (average) information ratio provide lower bounds on the size of the shares. For instance, the lower bound by Csirmaz [5] is a bound on the information ratio.

A secret sharing scheme is *linear* if the secret and the shares are vectors over some finite field and the shares are the values of linear maps on the secret and some random vector. In a linear secret sharing scheme, both the computation of the shares and the reconstruction of the secret value can be efficiently performed if the size of the shares is polynomial on the number of participants. In addition, because of their homomorphic properties, linear schemes are specially

useful for the applications of secret sharing. Moreover, most of the known construction methods provide linear secret sharing schemes.

A special class of linear secret sharing schemes, which are called here *simple*, has been mainly considered in the literature. While in a linear secret sharing scheme over a finite field $\mathbb{F}$ the secret value is a vector in $\mathbb{F}^{m_o}$ for some $m_o \geq 1$, in a *simple* linear secret sharing scheme, the secret value is an element in $\mathbb{F}$ (that is, $m_o = 1$). Simple linear secret sharing schemes are equivalent to the *monotone span programs* introduced by Karchmer and Wigderson [9]. In some works, as for instance [2], "linear secret sharing scheme" applies only to the simple ones while "multi-linear secret sharing scheme" is used when $m_o > 1$.

Differently to the general case, which includes nonlinear schemes, superpolynomial lower bounds on the size of the shares in linear secret sharing schemes have been presented. By counting arguments, for most access structures on $n$ participants, the size of the shares in a linear secret sharing scheme is $2^{\Omega(n)}$, but no explicit families of access structures have been found in this situation. Nevertheless, families of access structures for which the size of the shares in a linear scheme is $n^{\Omega(\log n)}$ have been presented [1, 3, 6, 7]. These are lower bounds on the information ratio of *simple* linear secret sharing schemes, which imply lower bounds on the size of the shares in linear secret sharing schemes [2]. Nevertheless, no superpolynomial lower bounds on the information ratio of linear secret sharing schemes have been given.

In this note, such lower bounds are presented for the first time. They are obtained by adapting in a quite simple way the proof in [7] (as presented in [2]) to non-simple linear secret sharing schemes.

## 2 Linear Secret Sharing Schemes

We present here some definitions and known results about linear secret sharing schemes and also the notation that will be used in the proof of the main result. In particular, Proposition 2.1 is one of the main ingredients in that proof.

Consider a set $P$ of *participants*, together with a special participant $p_o \notin P$ called *dealer*, and take $Q = P \cup \{p_o\}$. An *access structure* $\Gamma$ on $P$ is a monotone increasing family of subsets of $P$, that is, $B \in \Gamma$ if $A \subseteq B \subseteq P$ and $A \in \Gamma$. The members of the access structure are called *qualified sets*. Let $\mathbb{F}$ be a finite field, $V$ and $(E_p)_{p\in Q}$ vector spaces over $\mathbb{F}$, and

$$\pi : V \to \prod_{p\in Q} E_p, \quad x \mapsto (\pi_p(v))_{p\in Q},$$

a linear map such that $\pi_p : V \to E_p$ is surjective for every $p \in Q$. For a set $A \subseteq Q$, we consider $E_A = \prod_{p\in A} E_p$ and the linear map $\pi_A : V \to E_A$ is given by $\pi_A = (\pi_p)_{p\in A}$. In addition, we notate $E_o = E_{p_0}$ and $\pi_o = \pi_{p_o}$. The linear map $\pi$ defines an $\mathbb{F}$-*linear secret sharing scheme* with access structure $\Gamma$ on the set of participants $P$ if the following conditions are satisfied.

1. If $A \in \Gamma$, then $\ker \pi_A \subseteq \ker \pi_o$.
2. If $A \notin \Gamma$, then $V = \ker \pi_o + \ker \pi_A$.

Take $d = \dim V$ and, for $p \in Q$ and $A \subseteq Q$, take $m_p = \dim E_p$ and $m_A = \sum_{p\in A} m_p$. We notate $m = m_Q$ and $m_o = m_{p_o}$. By taking bases of those vector spaces, the linear map $\pi$ can be represented by a $d \times m$ matrix $G$ such that $x\,G = \pi(x)$ for every $v \in V$. The columns of this matrix are indexed by the elements in $K = \{1, \ldots, m\}$, that is $G = (G_k)_{k\in K}$, and there is a map $\psi : K \to Q$ such that, for every $p \in Q$, the $d \times m_p$ matrix $G_p = (G_k)_{\psi(k)=p}$ represents the linear map $\pi_p$. As before, we notate $G_o = G_{p_o}$ and $G_A = (G_k)_{\psi(k)\in A}$ for a set $A \subseteq Q$. Observe

that $G_A$ is a $d \times m_A$ matrix. The same notation will be used for other matrices whose columns are indexed by $K$. The matrix $G$ satisfies the following properties in connection to the access structure $\Gamma$ of the linear secret sharing scheme.

1. If $A \in \Gamma$, then every column of $G_o$ is a linear combination of the columns of $G_A$.
2. If $A \notin \Gamma$, then no nonzero linear combination of the columns of $G_o$ equals a linear combination of the columns of $G_A$.

The *information ratio* and the *average information ratio* of a linear secret sharing scheme are defined, respectively, as

$$\sigma = \frac{\max_{p \in P} \dim E_p}{\dim E_o} = \frac{\max_{p \in P} m_p}{m_o} \quad \text{and} \quad \widetilde{\sigma} = \frac{1}{|P|} \cdot \frac{\sum_{p \in P} \dim E_p}{\dim E_o} = \frac{m_P}{|P| \cdot m_o}$$

**Proposition 2.1.** *The following properties hold for every linear secret sharing scheme and for every $A \subseteq P$.*

1. *If $A \in \Gamma$, then there exists an $m_o \times m$ matrix $H = (H_k)_{k \in K}$ such that $H_o$ is the $m_o \times m_o$ identity matrix, $H_{P \setminus A} = 0$, and $GH^\top = 0$.*
2. *If $A \notin \Gamma$, then there exists an $m_o \times d$ matrix $R$ such that the matrix $RG = S = (S_k)_{k \in K}$ satisfies that $S_o$ is the $m_o \times m_o$ identity matrix and $S_A = 0$.*

*Proof.* The first statement is proved by taking into account that every column of $G_o$ is a linear combination of the columns of $G_A$ if $A \in \Gamma$. If $A \notin \Gamma$, then $V = \ker \pi_o + \ker \pi_A$, and hence there exist $m_o$ vectors $v_1, \ldots, v_{m_o} \in \ker \pi_A$ such that $\{\pi_o(v_1), \ldots, \pi_o(v_{m_o})\}$ is a basis of $E_o$. Let $R'$ be the $m_o \times d$ matrix whose rows are the coordinates of the vectors $v_1, \ldots, v_{m_o}$. Then $R'M = S' = (S'_k)_{k \in K}$ is such that $S'_o$ is invertible and $S'_A = 0$. Clearly, the proof is concluded by taking $R = (S'_o)^{-1} R'$. □

# 3 The Bound

The main result in this note, Theorem 3.4, is proved in this section by adapting the proof by Gál and Pudlák [7], as presented in [2], of the same result for simple linear secret sharing schemes. The adaptation is based on Proposition 2.1 and the following technical result, whose proof is straightforward.

**Lemma 3.1.** *Let $D$ be an $\ell \times t$ $\{0,1\}$-matrix. Let $\widehat{D}$ be the $m_o\ell \times m_o t$ matrix that is obtained from $D$ by replacing every entry equal to 1 with the $m_o \times m_o$ identity matrix and every entry equal to 0 with the $m_o \times m_o$ zero matrix. Then $\operatorname{rank}_{\mathbb{F}} \widehat{D} \geq m_o \operatorname{rank}_{\mathbb{F}} D$ for every field $\mathbb{F}$.*

Let $\Gamma$ be an access structure on $P$. A family $\mathcal{C} = (C_{j0}, C_{j1})_{j \in J}$ of pairs of subsets of $P$ satisfies the *unique intersection property* for $\Gamma$ if the following conditions are satisfied.

1. $P \setminus (C_{j0} \cup C_{j1}) \notin \Gamma$ for every $j \in J$.
2. $B \cap C_{j0} = \emptyset$ or $B \cap C_{j1} = \emptyset$ for every $j \in J$ and $B \in \min \Gamma$.

Observe that $B \cap (C_{j0} \cup C_{j1}) \neq \emptyset$ if $B \in \min \Gamma$, and hence every minimal qualified set has nonempty intersection with exactly one of the sets $C_{j0}, C_{j1}$. Let $(B_i)_{i \in I}$ be the family of minimal qualified subsets of $\Gamma$. Consider the matrix $D = D(\Gamma, \mathcal{C}) = (D_{ij})_{(i,j) \in I \times J}$ defined by $D_{ij} = 0$ if $B_i \cap C_{j0} \neq \emptyset$ and $D_{ij} = 1$ if $B_i \cap C_{j1} \neq \emptyset$. The following result is proved in [2, 7].

**Proposition 3.2.** *For every $n$, there exists an access structure $\Gamma$ on $n$ participants that admits a family $\mathcal{C}$ with the unique intersection property such that $\operatorname{rank}_{\mathbb{F}} D(\Gamma, \mathcal{C})$ is $n^{\Omega(\log n)}$ for every field $\mathbb{F}$.*

For $m_o \geq 1$, consider the block matrix $\widehat{D} = \widehat{D}(\Gamma, \mathcal{C}, m_o) = (\widehat{D}_{ij})_{(i,j)\in I\times J}$ such that $\widehat{D}_{ij}$ is the $m_o \times m_o$ identity matrix if $D_{ij} = 1$ and $\widehat{D}_{ij}$ is the $m_o \times m_o$ zero matrix if $D_{ij} = 0$. By Lemma 3.1, $\operatorname{rank}_{\mathbb{F}} \widehat{D} \geq m_o \operatorname{rank}_{\mathbb{F}} D$ for every field $\mathbb{F}$.

**Proposition 3.3.** *Let $\Gamma$ be an access structure on a set of participants $P$ and $\mathcal{C}$ a family satisfying the unique intersection property for $\Gamma$. Take $D = D(\Gamma, \mathcal{C})$. Then, for every finite field $\mathbb{F}$, the average information ratio of every $\mathbb{F}$-linear secret sharing scheme with access structure $\Gamma$ is at least $(\operatorname{rank}_{\mathbb{F}} D)/|P|$.*

*Proof.* Put $\min \Gamma = (B_i)_{i\in I}$ and $\mathcal{C} = (C_{j0}, C_{j1})_{j\in J}$. Consider an $\mathbb{F}$-linear secret sharing scheme, represented by a matrix $G$. For $j \in J$, take $A_j = P \setminus (C_{j0} \cup C_{j1})$. By Proposition 2.1, the following properties hold.

- For every $i \in I$, there exists a matrix $H^i = (H^i_k)_{k\in K}$ such that $H^i_o$ is the $m_o \times m_o$ identity matrix, $H_{P\setminus B_i} = 0$, and $G(H^i)^\top = 0$.
- For every $j \in J$, there exists an $m_o \times d$ matrix $R^j$ such that the matrix $R^j G = S^j = (S^j_k)_{k\in K}$ satisfies that $S^j_o$ is the $m_o \times m_o$ identity matrix and $S^j_{A_j} = 0$.

Then $S^j(H^i)^\top = R^j G(H^i)^\top = 0$, and hence $S^j_P(H^i_P)^\top = -I_{m_o}$ for every $i \in I$ and $j \in J$, where $I_{m_o}$ is the $m_o \times m_o$ identity matrix. For every $j \in J$, consider the matrix $T^j$ defined by $T^j_{C_{j0}} = 0$ and $T^j_{Q\setminus C_{j0}} = -S^j_{Q\setminus C_{j0}}$. Then $T^j_P(H^i_P)^\top = 0$ if $B_j \cap C_{j0} \neq \emptyset$ and $T^j_P(H^i_P)^\top = I_{m_o}$ if $B_j \cap C_{j1} \neq \emptyset$. We can assume that $I = \{1, \ldots, \ell\}$ and $J = \{1, \ldots, t\}$. Consider the block matrices

$$T = \begin{pmatrix} T^1_P \\ \vdots \\ T^\ell_P \end{pmatrix} \quad \text{and} \quad H = \begin{pmatrix} H^1_P \\ \vdots \\ H^t_P \end{pmatrix}$$

Clearly, $TH^\top = \widehat{D} = \widehat{D}(\Gamma, \mathcal{C}, m_o)$. Since $T$ has $m_P$ columns, $m_P \geq \operatorname{rank}_{\mathbb{F}} \widehat{D} \geq m_o \operatorname{rank}_{\mathbb{F}} D$ and the proof is concluded. □

Finally, the main result is obtained by combining Propositions 3.2 and 3.3.

**Theorem 3.4.** *For every $n$ there exists an access structure on $n$ participants such that, for every finite field $\mathbb{F}$, the average information rate of every $\mathbb{F}$-linear secret sharing scheme for $\Gamma$ is $n^{\Omega(\log n)}$.*

## Acknowledgements

The author's work was supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.

## References

[1] L. Babai, A. Gál, A. Wigderson. Superpolynomial lower bounds for monotone span programs. *Combinatorica* **19** (1999) 301–319.

[2] A. Beimel. Secret-Sharing Schemes: A Survey. *Coding and Cryptology, Third International Workshop, IWCC 2011, Lecture Notes in Comput. Sci.* **6639** (2011) 11–46.

[3] A. Beimel, A. Gál, M. Paterson. Lower bounds for monotone span programs. *Comput. Complexity* **6** (1997) 29–45.

[4] G. R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings.*, **48** (1979) 313–317.

[5] L. Csirmaz. The size of a share must be large. *J. Cryptology* **10** (1997) 223–231.

[6] A. Gál. A characterization of span program size and improved lower bounds for monotone span programs. *Comput. Complexity* **10** (2001) 277–296.

[7] A. Gál, P. Pudlák. A note on monotone complexity and the rank of matrices *Inform. Process. Lett.* **87** (2003) 321-326.

[8] M. Ito, A. Saito, T. Nishizeki. Secret sharing scheme realizing any access structure. *Proc. IEEE Globecom'87.*, (1987) 99–102.

[9] M. Karchmer and A. Wigderson. On span programs. *Proceedings of the Eighth Annual Structure in Complexity Theory Conference*, 102–111, 1993.

[10] A. Shamir. How to share a secret. *Commun. of the ACM*, **22** (1979) pp. 612–613.