Secret Sharing

Qi Chen

December 14, 2015

What is secret sharing?

- A dealer: know the secret S and distribute the shares of S to each party
- A set of n parties $\mathcal{P}_n \triangleq \{p_1, \cdots, p_n\}$: each party owns a share
- Authorized subset of the parties:$B \subset \mathcal{P}_n$ can reconstruct the secret from their shares
- Unauthorized subset of the parties: $T \subset \mathcal{P}_n$ know nothing about the secret from their shares

Applications

- Secure storage
- Secure multiparty computation
- Threshold cryptography
- Byzantine agreement
- Access control
- Private information retrieval
- Atribute-based encryption
- General oblivious transfer
- ...

Access structure

- The collection $\mathcal{A}$ of all authorized subsets is called the access structure of a secret sharing.
- Access structure is monotone, i.e., if $A \subset B$ and $A \in \mathcal{A}$, then $B \in \mathcal{A}$.

Access structure

- The collection $\mathcal{A}$ of all authorized subsets is called the access structure of a secret sharing.
- Access structure is monotone, i.e., if $A \subset B$ and $A \in \mathcal{A}$, then $B \in \mathcal{A}$.

Example

Let $\mathcal{P}_4 = \{p_1, \cdots, p_4\}$. Then

$$\mathcal{A} = \{\{p_1, p_2\}, \{p_2, p_3\}, \{p_3, p_4\}, \{p_1, p_2, p_3\}, \\ \{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}, \{p_1, p_2, p_3, p_4\}\}$$

is an access structure.

Access structure

Collection $\mathcal{A}^*$ of minimal sets in $\mathcal{A}$

- Let $\mathcal{A}^*$ be the collection of minimal sets in $\mathcal{A}$, i.e., $B \in \mathcal{A}^*$ if $B \in \mathcal{A}$ and for any $C \subset B$, $C \notin \mathcal{A}$
- Access structure $\mathcal{A}$ is uniquely determined by $\mathcal{A}^*$

Access structure

Collection $\mathcal{A}^*$ of minimal sets in $\mathcal{A}$

- Let $\mathcal{A}^*$ be the collection of minimal sets in $\mathcal{A}$, i.e., $B \in \mathcal{A}^*$ if $B \in \mathcal{A}$ and for any $C \subset B$, $C \notin \mathcal{A}$
- Access structure $\mathcal{A}$ is uniquely determined by $\mathcal{A}^*$

Example

$$\mathcal{A}^* = \{\{p_1, p_2\}, \{p_2, p_3\}, \{p_3, p_4\}\}$$

Access structure

Collection $\mathcal{A}^*$ of minimal sets in $\mathcal{A}$

- Let $\mathcal{A}^*$ be the collection of minimal sets in $\mathcal{A}$, i.e., $B \in \mathcal{A}^*$ if $B \in \mathcal{A}$ and for any $C \subset B$, $C \notin \mathcal{A}$
- Access structure $\mathcal{A}$ is uniquely determined by $\mathcal{A}^*$

Example

$$\mathcal{A}^* = \{\{p_1, p_2\}, \{p_2, p_3\}, \{p_3, p_4\}\}$$

Remark

- Note that $\mathcal{A}^*$ is a Sperner family on $\mathcal{P}_n$, i.e, a collection of subsets of $\mathcal{P}_n$ such that any two member of the collection does not contain each other.
- Sperner family is counted by Dedekind number which grows very fast with n. This imply the difficulty of secret sharing problem.

Definition by probability

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

Definition by probability

Scheme Σ is a secret-sharing scheme realizing an access structure $\mathcal{A}$ if the following two requirement hold:

1. (**Correctness**) For any $B = \{p_{i_1}, \cdots, p_{i_{|B|}}\} \in \mathcal{A}$, there is a reconstruction function $\mathrm{REC} : K_{i_1} \times \cdots : K_{i_{|B|}} \to K$ such that for any $k \in K$,

$$\Pr[\mathrm{REC}(\Pi(k, r)_B) = k] = 1.$$

2. (**Perfect Privacy**) For any $T \notin \mathcal{A}$, for any $a, b \in K$, and for every possible vector of shares $\langle s_j \rangle_{p_j \in T}$:

$$\Pr[\Pi(a, r)_T = \langle s_j \rangle_{p_j \in T}] = \Pr[\Pi(b, r)_T = \langle s_j \rangle_{p_j \in T}]$$

Definition by entropy

Consider the secret be a random variable S on K, and each share be a random variable S_j on K_j. Then the scheme $\mathbf{S} = (S, S_j)_{p_j \in \mathcal{P}_n}$ is a secret-sharing scheme realizing access structure $\mathcal{A}$ if the following two conditions hold:

1. (**Correctness**) For any $B \in \mathcal{A}$,

$$H(S|S_B) = 0$$

2. (**Perfect Privacy**) For any $T \notin \mathcal{A}$,

$$H(S|S_T) = H(S)$$

Definition by entropy

Consider the secret be a random variable S on K, and each share be a random variable S_j on K_j. Then the scheme $\mathbf{S} = (S, S_j)_{p_j \in \mathcal{P}_n}$ is a secret-sharing scheme realizing access structure $\mathcal{A}$ if the following two conditions hold:

1. (**Correctness**) For any $B \in \mathcal{A}$,

$$H(S|S_B) = 0$$

2. (**Perfect Privacy**) For any $T \notin \mathcal{A}$,

$$H(S|S_T) = H(S)$$

Remark For perfect privacy, the condition can be written as $I(S; S_T) = 0$. If we modify the condition to $I(S; S_T) = a_T$ for some $0 \leq a_T \leq H(S)$, then modified version is called non-perfect secret sharing, while the traditional one is called perfect secret sharing.

Equivalence of two definitions

Theorem

Two definitions of secret sharing are equivalent.

- For any $\Sigma = (\Pi, \mu)$ realizing access structure $\mathcal{A}$, we can construct a random vector $\mathbf{S} = (S, S_j)_{p_j \in \mathcal{P}_n}$ realizing $\mathcal{A}$.
- For any random vector $\mathbf{S} = (S, S_j)_{p_j \in \mathcal{P}_n}$ realizing $\mathcal{A}$, we can accordingly construct a $\Sigma = (\Pi, \mu)$ realizing $\mathcal{A}$

Information ratio

Information ratio by the definition of probability

$$\rho_{\Sigma} \triangleq \frac{\max_{1 \leq j \leq n} \log |K_j|}{\log |K|}$$

Information ratio by the definition of entropy

$$\rho_{\mathbf{S}} \triangleq \frac{\max_{1 \leq j \leq n} H(S_j)}{H(S)}$$

Information ratio

Information ratio by the definition of probability

$$\rho_{\Sigma} \triangleq \frac{\max_{1 \leq j \leq n} \log |K_j|}{\log |K|}$$

Information ratio by the definition of entropy

$$\rho_{\mathbf{S}} \triangleq \frac{\max_{1 \leq j \leq n} H(S_j)}{H(S)}$$

Corollary

$$\rho_{\Sigma} = \rho_{\mathbf{S}}$$

if Σ *corresponds to* $\mathbf{S}$.

The fundamental problem of secret sharing: optimal information ratio

Let $\mathcal{N} = \{s\} \cup \mathcal{P}_n$ and $\Gamma^*_{\mathcal{N}}$ the entropy function region on $\mathcal{N}$. Let $\mathcal{A}$ be an access structure on $\mathcal{P}_n$. Then the optimal information ratio on $\mathcal{A}$ is

$$\rho_{\mathcal{A}} \triangleq \inf_{\mathbf{h} \in \Gamma^*_{\mathcal{N}} \cap \Phi_{\mathcal{A}}} \frac{\max_{1 \le j \le n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where

$$\Phi_{\mathcal{A}} = \{\mathbf{h} : \mathbf{h}(\{s\} \cup B) = \mathbf{h}(B) \quad \forall B \in \mathcal{A}, \\ \mathbf{h}(\{s\} \cup T) = \mathbf{h}(\{s\}) + \mathbf{h}(T) \quad \forall T \notin \mathcal{A}\}$$

Shamir's threshold scheme

For $1 \leq t \leq n$, let $\mathcal{A}_{t,n} = \{A \subset \mathcal{P}_n : |A| \geq t\}$. Then $\mathcal{A}_{t,n}$ is a access structure with threshold t. It can be realised by Shamir's scheme in the following

- Let $K = \mathbb{F}_q$, where $q > n$ is a prime power.
- Let $\alpha_1, \cdots, \alpha_n \in \mathbb{F}_q$ be n distinct non-zero elements known to all parties.
- The dealer uniformly choose $a_1, \cdots, a_{t-1} \in \mathbb{F}_q$ and generate a polynomial $P(x) = k + \sum_{i=1}^{t-1} a_i x^i$.
- The share of p_j is $s_j = P(\alpha_j)$

Shamir's threshold scheme

Correctness

For any $B = \{p_{i_1}, \cdots, p_{i_t}\} \in \mathcal{A}^*_{t,n}$, let

$$Q(x) = \sum_{\ell=1}^{t} s_{i_\ell} \prod_{1 \le j \le t, j \ne \ell} \frac{\alpha_{i_j} - x}{\alpha_{i_j} - \alpha_{i_\ell}}.$$

Note that $Q(\alpha_{i_\ell}) = s_{i_\ell} = P(\alpha_{i_\ell})$ for $1 \le \ell \le t$ which implies that $Q(x) = P(x)$ and $Q(0) = P(0) = k$.

Shamir's threshold scheme

Perfect privacy

For any $T = \{p_{i_1}, \cdots, p_{i_{t-1}}\}$, $t-1$ shares with each secret $a \in \mathbb{F}_q$, uniquely determines a polynomial $P_a(x)$ with $P_a(0) = a$ and $P_a(\alpha_{i_\ell}) = s_{i_\ell}$ for $1 \leq \ell \leq t-1$. Hence

$$\Pr[\Pi(a, r)_T = \langle s_{i_\ell} \rangle_{1 \leq \ell \leq t-1}] = \frac{1}{q^{t-1}}$$

The privacy follows from the probability is the same for every $a \in \mathbb{F}_q$

Shamir's threshold scheme

Perfect privacy

For any $T = \{p_{i_1}, \cdots, p_{i_{t-1}}\}$, $t-1$ shares with each secret $a \in \mathbb{F}_q$, uniquely determines a polynomial $P_a(x)$ with $P_a(0) = a$ and $P_a(\alpha_{i_\ell}) = s_{i_\ell}$ for $1 \leq \ell \leq t-1$. Hence

$$\Pr[\Pi(a, r)_T = \langle s_{i_\ell} \rangle_{1 \leq \ell \leq t-1}] = \frac{1}{q^{t-1}}$$

The privacy follows from the probability is the same for every $a \in \mathbb{F}_q$

Information ratio

- The information ratio is 1 since $K_j = K = \mathbb{F}_q$
- It is the optimal information ratio on the access structure $\mathcal{A}_{t,n}$

Shamir's threshold scheme by entropy

Let $\Gamma_{\mathcal{N}}$ be the polymatroidal region on $\mathcal{N}$. Let $p = \{\{s\}, \mathcal{P}_n\}$ be a partition of $\mathcal{N}$.

Lemma

$$\overline{\Psi_p^*} = \Psi_p$$

where $\Psi_p^* = \Gamma_{\mathcal{N}}^* \cap C_{\mathcal{A}_{t,n}}$, $\Psi_p = \Gamma_{\mathcal{N}} \cap C_{\mathcal{A}_{t,n}}$ *and*

$$\begin{aligned} C_{\mathcal{A}_{t,n}} = \{\mathbf{h} : \ & \mathbf{h}(A) = \mathbf{h}(B), \\ & \mathbf{h}(\{s\} \cup A) = \mathbf{h}(\{s\} \cup B), \\ & \textit{if } |A| = |B| \ \forall A, B \subset \mathcal{P}_n\} \end{aligned}$$

Shamir's threshold scheme by entropy

For simplicity, let $\rho_{t,n} = \rho_{\mathcal{A}_{t,n}}$ and $\Phi_{t,n} = \Phi_{\mathcal{A}_{t,n}}$. Then

$$\rho_{t,n} = \inf_{\mathbf{h} \in \Gamma^*_{\mathcal{N}} \cap \Phi_{t,n}} \frac{\max_{1 \le j \le n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where

$$\Phi_{t,n} = \{\mathbf{h} : \mathbf{h}(\{s\} \cup B) = \mathbf{h}(B) \quad \text{if } |B| \ge t,$$
$$\mathbf{h}(\{s\} \cup B) = \mathbf{h}(\{s\}) + \mathbf{h}(B) \quad \text{if } |B| < t\}$$

Shamir's threshold scheme by entropy

For simplicity, let $\rho_{t,n} = \rho_{\mathcal{A}_{t,n}}$ and $\Phi_{t,n} = \Phi_{\mathcal{A}_{t,n}}$. Then

$$\rho_{t,n} = \inf_{\mathbf{h} \in \Gamma^*_{\mathcal{N}} \cap \Phi_{t,n}} \frac{\max_{1 \le j \le n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where

$$\Phi_{t,n} = \{\mathbf{h} : \mathbf{h}(\{s\} \cup B) = \mathbf{h}(B) \quad \text{if } |B| \ge t,$$
$$\mathbf{h}(\{s\} \cup B) = \mathbf{h}(\{s\}) + \mathbf{h}(B) \quad \text{if } |B| < t\}$$

Theorem

$$\rho_{t,n} = \inf_{\mathbf{h} \in \Psi^*_p \cap \Phi_{t,n}} \frac{\max_{1 \le j \le n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

Shamir's threshold scheme by entropy

Theorem

$$\rho_{t,n} = \min_{\mathbf{h} \in \Psi_p \cap \Phi_{t,n}} \frac{\max_{1 \le j \le n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

The solution is

$$\rho_{t,n} = 1$$

and

$$\arg\min \rho_{t,n} = \{\mathbf{h} : aU_{t,n+1}, a > 0\}$$

Shamir's threshold scheme by entropy

Theorem

$$\rho_{t,n} = \min_{\mathbf{h} \in \Psi_p \cap \Phi_{t,n}} \frac{\max_{1 \le j \le n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

The solution is

$$\rho_{t,n} = 1$$

and

$$\arg\min \rho_{t,n} = \{\mathbf{h} : aU_{t,n+1}, a > 0\}$$

Remark This result can be generalized to non-perfect threshold scheme.

Linear secret-sharing scheme

Definition

A secret-sharing scheme is linear if

- Secret $s \in \mathbb{F}$
- Each ramdom string $r \in R$ is a vector and each entry of r is chosen independent with uniform distribution from $\mathbb{F}$
- Each share s_j is a vector and each entry of s_j is a fixed linear combination of the secret s and the coordinates of the random string r.

Linear secret-sharing scheme

Definition

A secret-sharing scheme is linear if

- Secret $s \in \mathbb{F}$
- Each ramdom string $r \in R$ is a vector and each entry of r is chosen independent with uniform distribution from $\mathbb{F}$
- Each share s_j is a vector and each entry of s_j is a fixed linear combination of the secret s and the coordinates of the random string r.

Shamir's threshold scheme is linear.

Linear secret-sharing scheme

Monotone span program

A monotone span program is a triple $\mathcal{M} = (\mathbb{F}, M, \rho)$, where

- $\mathbb{F}$ is a field,
- M is an $a \times b$ matrix over $\mathbb{F}$
- and $\rho : \{1, \cdots, a\} \to \{p_1, \cdots, p_n\}$ labels each row of M by a party.

Linear secret-sharing scheme

Monotone span program

A monotone span program is a triple $\mathcal{M} = (\mathbb{F}, M, \rho)$, where

- $\mathbb{F}$ is a field,
- M is an $a \times b$ matrix over $\mathbb{F}$
- and $\rho : \{1, \cdots, a\} \to \{p_1, \cdots, p_n\}$ labels each row of M by a party.

Example

Consider the following monotone span program $(\mathbb{F}_{17}, M, \rho)$, where

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \end{bmatrix}$$

and $\rho(1) = \rho(2) = p_2$, $\rho(3) = p_1$ and $\rho(4) = p_4$.

Linear secret-sharing scheme

Monotone span program

- For any $A \subset \mathcal{P}_n$, let M_A denote the sub-matrix obtained by restricting M to the rows labeled by parties in A.
- $\mathcal{M}$ accepts B if the rows of M_B span the vector $\mathbf{e}_1 = (1, 0, \cdots, 0)$.
- $\mathcal{M}$ accepts access structure $\mathcal{A}$ if $\mathcal{M}$ accepts a set B iff $B \in \mathcal{A}$.

Linear secret-sharing scheme

Monotone span program

- For any $A \subset \mathcal{P}_n$, let M_A denote the sub-matrix obtained by restricting M to the rows labeled by parties in A.
- $\mathcal{M}$ accepts B if the rows of M_B span the vector $\mathbf{e}_1 = (1, 0, \cdots, 0)$.
- $\mathcal{M}$ accepts access structure $\mathcal{A}$ if $\mathcal{M}$ accepts a set B iff $B \in \mathcal{A}$.

Example

Consider $B = \{p_1, p_2\}$ and $T = \{p_1, p_3\}$. Then

$$M_B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix} \text{ and } M_T = \begin{bmatrix} 1 & 3 & 9 \\ 1 & 4 & 16 \end{bmatrix}.$$

It can be checked $\mathcal{M}_B$ spans $\mathbf{e}_1$ but $\mathcal{M}_T$ does not. We can check further that $\mathcal{A}^* = \{\{p_1, p_2\}, \{p_2, p_3\}\}$.

Linear secret-sharing scheme

Theorem

Let $\mathcal{M} = (\mathbb{F}, M, \rho)$ be a monotone span program accepting an access structure $\mathcal{A}$, where $\mathbb{F}$ is a finite field and for every j there a_j rows of M labeled by p_j. Then, there is a linear secret-sharing scheme realizing $\mathcal{A}$ such that the share of party p_j is a vector in $\mathbb{F}^{a_j}$. The information ratio of the resulting scheme is $\max_{1 \leq j \leq n} a_j$.

Linear secret-sharing scheme

Theorem

Let $\mathcal{M} = (\mathbb{F}, M, \rho)$ be a monotone span program accepting an access structure $\mathcal{A}$, where $\mathbb{F}$ is a finite field and for every j there a_j rows of M labeled by p_j. Then, there is a linear secret-sharing scheme realizing $\mathcal{A}$ such that the share of party p_j is a vector in $\mathbb{F}^{a_j}$. The information ratio of the resulting scheme is $\max_{1 \le j \le n} a_j$.

Theorem

Let $\Gamma^{\mathrm{L}}_{\mathcal{N}}$ be the region bounded by Shannon-type information inequalities and linear rank inequalities over $\mathcal{N}$. Then the optimal information ratio of linear scheme on $\mathcal{A}$ is

$$\rho_{\mathcal{A}} \triangleq \inf_{\mathbf{h} \in \Gamma^{\mathrm{L}}_{\mathcal{N}} \cap \Phi_{\mathcal{A}}} \frac{\max_{1 \le j \le n} \mathbf{h}(\{p_j\})}{\mathbf{h}(\{s\})}$$

where $\Phi_{\mathcal{A}}$ is defined as above.

Lower bounds on the information ratio

Theorem

Let p_j be a non-redundant party in $\mathcal{A}$ and let Σ be any secret-sharing scheme realizing $\mathcal{A}$, then

$$|K_j| \geq |K|$$

which implies that $\rho_{\mathcal{A}} \geq 1$ for any $\mathcal{A}$.

Lower bounds on the information ratio

Theorem

Let p_j be a non-redundant party in $\mathcal{A}$ and let Σ be any secret-sharing scheme realizing $\mathcal{A}$, then

$$|K_j| \geq |K|$$

which implies that $\rho_{\mathcal{A}} \geq 1$ for any $\mathcal{A}$.

Ideal secrete-sharing scheme

For a secret-sharing scheme, if its information ratio is 1, it is called an ideal secret-sharing scheme.

Csirmaz's lower bound

Csirmaz's access structure

We define access structure $\mathcal{A}_n$ by its minimal set $\mathcal{A}_n^*$.

- Let k be the largest integer such that $2^k + k - 1 \leq n$.
- Let $B = \{p_1, \cdots, p_{2^k-1}\}$ and define $B_0 = \emptyset$ and $B_i = \{p_1, \cdots, p_i\}$ for $1 \leq i \leq 2^k - 1$.
- Let $A = \{p_{2^k}, \cdots, p_{2^k+k-1}\}$, and $A = A_0, A_1, \cdots, A_{2^k-1} = \emptyset$ be all the subsets of A such that if $i < i'$, then $A_i \not\subset A_{i'}$.
- Define $U_i = A_i \cup B_i$ for $0 \leq i \leq 2^k - 1$.

Then $\mathcal{A}_n^* = \{U_i : 0 \leq i \leq 2^k - 1\}$.

Csirmaz's lower bound

Csirmaz's access structure

We define access structure $\mathcal{A}_n$ by its minimal set $\mathcal{A}_n^*$.

- Let k be the largest integer such that $2^k + k - 1 \leq n$.
- Let $B = \{p_1, \cdots, p_{2^k-1}\}$ and define $B_0 = \emptyset$ and $B_i = \{p_1, \cdots, p_i\}$ for $1 \leq i \leq 2^k - 1$.
- Let $A = \{p_{2^k}, \cdots, p_{2^k+k-1}\}$, and $A = A_0, A_1, \cdots, A_{2^k-1} = \emptyset$ be all the subsets of A such that if $i < i'$, then $A_i \not\subset A_{i'}$.
- Define $U_i = A_i \cup B_i$ for $0 \leq i \leq 2^k - 1$.

Then $\mathcal{A}_n^* = \{U_i : 0 \leq i \leq 2^k - 1\}$.

Theorem

The information ratio of secret-sharing scheme realizing access structure constructed above is $\Omega(n/\log n)$.

Csirmaz's lower bound

Lemma

For every $0 \leq i \leq 2^k - 2$,

$$H(B_i \cup A) - H(B_i) \geq H(B_{i+1}) - H(B_{i+1}) + H(S)$$

Csirmaz's lower bound

Lemma

For every $0 \leq i \leq 2^k - 2$,

$$H(B_i \cup A) - H(B_i) \geq H(B_{i+1}) - H(B_{i+1}) + H(S)$$

Proof sketch of Theorem

$$\begin{aligned}
\sum_{p_j \in A} H(\{p_j\}) &\geq H(A) \\
&\geq H(B_0 \cup A) - H(B_0) \\
&\geq H(B_{2^k-1} \cup A) - H(B_{2^k-1}) + (2^k - 1)H(S) \\
&= \Omega(n)H(S).
\end{aligned}$$

This implies that $H(\{p_j\}) = \Omega(n/\log n)H(S)$ for at least one p_j. $\square$

Csirmaz's lower bound

Lemma

For every $0 \leq i \leq 2^k - 2$,

$$H(B_i \cup A) - H(B_i) \geq H(B_{i+1}) - H(B_{i+1}) + H(S)$$

Proof sketch of Theorem

$$\begin{aligned}\sum_{p_j \in A} H(\{p_j\}) &\geq H(A) \\ &\geq H(B_0 \cup A) - H(B_0) \\ &\geq H(B_{2^k-1} \cup A) - H(B_{2^k-1}) + (2^k - 1)H(S) \\ &= \Omega(n)H(S).\end{aligned}$$

This implies that $H(\{p_j\}) = \Omega(n/\log n)H(S)$ for at least one p_j. $\square$

Remark Both Lemma and the inequalities in the proof sketch are Shannon-type.

Lower bounds for linear secret sharing

Theorem

For any n, there exists an access structure $\mathcal{A}_n$ sucht that every monotone span program over any field accepting it has size $n^{\Omega(\log n)}$.

Limitations of known techniques for lower bounds

- No better lower bound is found since Csirmaz's lower bound in 1994
- Shannon-type information inequalities can not help to improve the bound
- All information inequalities with less than 6 random variables can not help to improve the bound

Open problems

Question 1

Prove or disprove that there exists an access structure such that the information ratio of every secret-sharing scheme realizing it is $2^{\Omega(n)}$.

Question 2

Prove or disprove that there exists an access structure such that the information ratio of every secret-sharing scheme realizing it with domain $\{0,1\}$ is super-polynomial in n.

Question 3

Prove that there exists an explicit access structure such that the information ratio of every linear secret-sharing scheme realizing it is $2^{\Omega(n)}$.

Bibiography


A. Beilmel, "Secret-sharing schemes: a survey," *Coding and cryptology*, 2011-Springer.


Q. Chen and R. W. Yeung, "Partition-Symmetrical Entropy Functions," submitted to *IEEE Trans. Info. Theory*.

Discussion

What can we do?

Thank you!