Charles University in Prague
Faculty of Mathematics and Physics
Katedra algebry

Generalized Ideal Secret-sharing Schemes and Matroids

Author: Jaroslav Kotil

27.11.2010 somewhere far, far away...

Intro

Our goal:

- Classify ideal perfect SSS.

How?

- Consider only perfect SSS.
- Axiomatic approach to SSS's, which enables us to study combinatorial and probabilistic ideal SSS's from a unified point of view.
- We will establish the relationship between ideal SSS's and matroids.

What is what...

- perfect SSS - nonallowed coalitions of participants cannot get any additional information on the possible value of the secret
- ideal SSS - the "size" of the secret is not less then the "size" of the share provided to any parcipant

Models of SSS:

- Probabilistic model
- Combinatorial model

Probabilistic model

- $\mathbb{S}_0, \mathbb{S}_1, \ldots, \mathbb{S}_n$ and probability distribution P on their Cartesian product $\mathbb{S} = \mathbb{S}_0 \times \mathbb{S}_1 \times \ldots \times \mathbb{S}_n$
- set Γ of subsets of the set $\{1, \ldots, n\}$ - access structure
- pair $(P, \mathbb{S})$ is called a perfect probabilistic SSS realizing the access structure Γ if the following properties hold:
  - $P(S_0 = c_0 | S_i = c_i, i \in A) \in 0, 1$ if $A \in \Gamma$,
  - $P(S_0 = c_0 | S_i = c_i, i \in A) = P(S_0 = c_0)$ if $A \notin \Gamma$,
- or equivalently in the language of entropy
  - $H(S_i, i \cup 0) = H(S_i, i \in A) + \delta_\Gamma(A) H(S_0)$, where $\delta_\Gamma(A) = 0$ if $A \in \Gamma$, and $A \notin \Gamma$ otherwise

Combinatorial model

- call $V \subset \mathbb{S}$ the "code" of a combinatorial SSS, and call it's codewords "sharing rules"
- V_B the code obtained from V by deleting columns whose numbers are not contained in $B \subset \{0, 1, \ldots, n\}$
- $\|W\|$ denote the number of distinct codewords of a code W
- $h_q(W) = \log_q \|W\|$
- say that a code $V \subset \mathbb{S}$ generates a perfect combinatorial SSS if $\|V_{A\cup 0}\| = \|V_A\| \times \|V_0\|^{\delta_\Gamma(A)}$, or equivalently, if $h_q(V_{A\cup 0}) = h_q(V_A) + \delta_\Gamma(A) h_q(V_0)$, where $\delta_\Gamma(A) = 0$ if $A \in \Gamma$, and $A \notin \Gamma$ otherwise

Essential elements

- $x \in \{1, \ldots, n\}$ is called essential if there exists a set A such that $x \cup A \in \Gamma$, but $A \notin \Gamma$, i.e. there is a set $C \in \Gamma_{min}$ that contains the element x, where Γ_{min} consists of all minimal sets of Γ
- consider a set X consisting of all essential elements, $\Gamma_X = \{A : A \subseteq X, A \in \Gamma\}$.
- we can suppose that all elements of Γ are essential

Ideal SSS's

- for perfect probabilistic SSS holds $H(S_i) \geq H(S_0)$ for all i
- ideal if holds $H(S_i) = H(S_0)$ for all i
- for perfect combinatorial SSS holds $|S_i| \geq |S_0|$ for all i
- ideal if holds $|S_i| = |S_0|$ for all i

Matroid and its rank function - for the forgetful ones

A matroid is a finite set X and a collection I of subsets of X, which are called independent sets, for which holds:

- $\emptyset \in I$
- if $A \in I$ and $B \subset A$, then $B \in I$
- if $A, B \in I$ and $|A| = |B| + 1$, then there exists $a \in A \setminus B$ such that $a \cup B \in I$

Rank function $r(A)$ defined as the maximal cardinality of the independent subset $B \subseteq A$. Only independent sets satisfy the condition $r(A) = |A|$. Rank function properties:

- $r(A) \in \mathbb{Z}$, $r(\emptyset) = 0$
- $r(A) \leq r(A \cup b) \leq r(A) + 1$
- if $r(A \cup b) = r(A \cup c) = r(A)$, then $r(A \cup b \cup c) = r(A)$

Axiomatic approach to SSS's

We want to prove $H(A) := \frac{H(S_i, i \in A)}{H(S_0)}$, and $h_q(A) := h_q(V_A)$, where $q = |S_0|$ have properties of rank function, i.e. from a matroid.
Problem for uniform proof - H is submodular, i.e.

$$H(A \cup B) + H(A \cap B) \leq H(A) + H(B),$$

whereas h is not always so.
Example:
$V = \{(0,0,0), (1,0,0), (0,1,0), (1,1,0), (1,1,1)\}$.
Put $A = \{0,2\}, B = \{1,2\}$. Then
$\|V_A\| = 3, \|V_B\| = 3, \|V_{A \cup B}\| = 5, \|V_{A \cap B}\| = 2$, submodularity does not hold because $3 \times 3 < 5 \times 2$.

Lets weak them!

Consider a real-valued function $f(A)$ defined on subsets of the set $\{0, 1, \ldots, n\}$ satisfying

- $f(\emptyset) = 0$
- $f(A) \leq f(B)$ if $A \subset B$
- $f(A \cup B) \leq f(A) + f(B)$

We call a function f perfect if for any set A, $f(A \cup 0) = f(A) + \delta_f(A) f(0)$, where $\delta_f(A) \in \{0, 1\}$. We say that the function f realizes the access structure Γ perfectly if $f(A \cup 0) = f(A) + \delta_\Gamma(A) f(0)$. It is possible if and only if f is perfect, and there is only one such structure for a given function f, which is $\Gamma_f = \{A : f(A \cup 0) = f(A)\}$.

Key definition

- For any point p and any set A the hold: $f(A) \leq f(p \cup A) \leq f(A) + f(p)$.
- We say that a point p is f-nonseparable from a set A if $f(p \cup A) = f(A)$, and that a point p is strongly f-separable from a set A if $f(p \cup A) = f(A) + f(p)$.
- Perfectness of the function f means that for any set A, the point 0 is always either nonseparable from it or strongly separable.
- We will consider from now on only perfect functions.

Finally some Lemmas!

Lemma

If the point 0 is strongly separable from a set A but is nonseparable from a set $A \cup p$, then $f(A \cup p) \geq f(A) + f(0)$ and $f(p) \geq f(0)$.

call f a perfect realization of an access structure Γ ideal if $f(p) = f(0)$ for all $p \in \{1, \ldots, n\}$. Normalizing the function f, we assume without loss of generality that $f(p) = 1$ for all $p \in \{1, \ldots, n\}$. Consider only such realizations.

Lemma

If a point a is strongly separable from a set A but the point a is nonseparable from a set $A \cup b$, then the point b is strongly separable from the set A and is nonseparable from the set $A \cup a$.

Last restriction and our definition

- Lets impose the last restriction on a function f
  - (a) if a point p is nonseparable from a set A and $A \subset B$, then the point p is nonseparable from the set B
  - (b) if a point p is strongly separable from a set A and $B \subset A$, then the point p is strongly separable from the set B
- It hold for h, H.

Definition

A function f defined on the set of all subsets of the set $\{0, 1, \ldots, n\}$ is called a generalized ideal SSS realizing an access structure Γ if it satisfies

- f is real-valued function
- f realizes the access structure Γ perfectly
- f is ideal
- f holds the properties (a) and (b)

Few properties of separability

Lemma

If for any $b \in B$ the point b is strongly separable from a set $A \cup B \setminus b$, then $f(A' \cup B) = f(A') + |B|$ for any $A' \subset A$.

Lemma

If a point a is nonseparable from a set $A \cup b$ and a point b is nonseparable from a set B, then the point a is nonseparable from the set $A \cup B$.

Lemma

If the point 0 is strongly separable from a set B but the point 0 is nonseparable from a set $A \cup B$, then there exists a point $a \in A$ which is nonseparable from a set $0 \cup B \cup A \setminus a$.

We enter finals

Corollary

If the point a is nonseparable from the set A, then there exists a point $a \in A$ which is nonseparable from the set $0 \cup A \setminus a$

Theorem

Any generalized ideal SSS is an integer-valued function.

Proof:
Let A be a set of minimal cardinality for which the statement is not valid. There are 2 cases:

- The point 0 is nonseparable from a set A, i.e. $A \in \Gamma$. There is a point a which is nonseparable from a set $0 \cup A \setminus a$. Hence $f(A) = f(0 \cup A) = f(0 \cup A \setminus a) = f(A \setminus a) + \delta$, $\delta \in \{0, 1\}$ and $f(A)$ is an integer.

...to be continued...

- the point 0 is strongly separable from a set A. Consider sets B such that the point 0 is strongly separable from the set B but nonseparable from a set $A \cup B$. Choose one of the sets B of minimal possible cardinality and denote it by B_0. Then $\exists a \in A$ which is nonseparable from a set $0 \cup B_0 \cup A \setminus a$. Otherhand the point 0 is nonseparable from a set $B_0 \cup A \setminus$, so we get that a is nonseparable from a set $B_0 \cup A \setminus a$. By the definition of B_0, the point 0 is nonseparable from a set $A \cup B_0$ and is strongly separable from a set $A \cup B_0 \setminus b$ for all $b \in B_0$. Then any point b is strongly separable from $A \cup B_0 \setminus b$. So we have $f(A \cup B_0) = f(A) + |B_0|$ and $f(B_0 \cup A \setminus a) = f(A \setminus a) + |B_0|$. So $f(A) = f(A \setminus a)$ and $f(A \setminus a)$ is an integer number according to the minimality of the set A.

We enter finals

Theorem

For every generalized ideal SSS f realizing an access structure Γ, the independent sets defined by the condition $f(a) = |A|$ form a connected matroid on the set $\{0, 1, \ldots, n\}$. All circuits of this matroid which contain the point 0 are of the form $0 \cup A$, where $A \in \Gamma_{min}$.

Conclusion

- No difference between combinatorial and probabilistic ideal SSS's.
- Therefore, we can simply speak about ideal SSS's.
- We can realize generalized ideal SSS by a connected matroid.

That's All Folks!

Thank you for your attention!