Secret Sharing on Infinite Structures

Laszlo Csirmaz

Central European University
Renyi Institute

January 25, 2010

Contents

A case study: infinite 2-threshold scheme

Requirements

1. each share is independent of the secret
2. any two shares determine the secret

A case study: infinite 2-threshold scheme

Requirements

1. each share is independent of the secret
2. any two shares determine the secret

Algebra (Shamir):

1. shares are values along a line
2. the field $\mathbb{F}$ should be infinite
3. the scheme is determined by the *distribution* of the lines
4. no translation invariant distribution exists $\ddot\frown$

A case study: infinite 2-threshold scheme

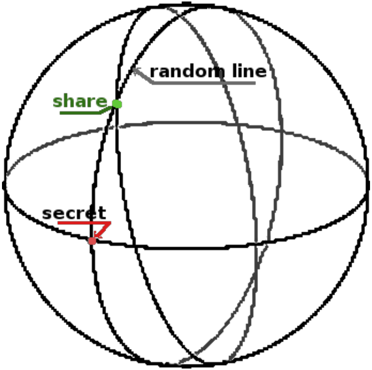
Requirements

1. each share is independent of the secret
2. any two shares determine the secret

Geometry (Blaklay & Swanson):

1. shares are points along a line the projective plane
2. we have a homogeneous uniform distribution $\ddot\smile$
3. there is a duality between lines and points
4. no independence between share and secret $\ddot\frown$

The projective plane



Given the share, the random line is uniform, but the secret is *not*.

Solution (G. Tardos)

- the *secret* is $s \in (0, 0.5)$
- *participants* are real numbers between 0 and 0.5
- R is a uniform random number in $[0, 1]$
- if x is a participant, his share is $xs + R \pmod 1$

1. Clearly, x's share is *independent* of the secret.
2. To *recover* the secret from x's and y's share compute

$$(xs + R) - (ys + R) = (x - y)s \pmod 1.$$

As $-0.5 < (x - y)s < 0.5$, the exact value can be computed from this mod 1 value.

Problem: generalize this for other threshold schemes.

Contents

Examples for ramp schemes

1. Participant i receives uniform and random $r_i \in [0,1]$; the secret is $s = \sum_i r_i 2^{-i}$.
   This is an *all-or-nothing* ramp scheme: even if one participant is missing, the rest does not have full information on s.
2. Participant i receives either 0 or 1 such that the sequence $\{r_i\}$ is eventually constant. The secret is the limit of the sequence.
   In this ramp scheme every infinite subset can recover the secret, and no finite subset has full information (assign probabilities properly).
3. Participants are indexed by real numbers between 0 and 1. Choose a measurable function f on $[0,1]$ with $\int f = 0$ or 1, and assign the share $f(x)$ to x.
   Every set of measure 1 can recover the secret, and sets of measure < 1 have no full information.

Contents

Formal definitions

Definition (Secret Sharing)

Given the set P of participants, a *secret sharing* is a collection of random variables $\{\xi_i : i \in P\} \cup \{\xi_s\}$ with a joint distribution.

Definition (Perfect Secret Sharing)

Given an upward closed access structure $\mathcal{A}$, $\mathcal{S}$ is *perfect* if

1. if A is qualified, then $\{\xi_i : i \in A\}$ determines ξ_s,
2. if A is *not* qualified, then $\{\xi_i : i \in A\}$ is independent of ξ_s.

Definition (Ramp Secret Sharing)

$\mathcal{S}$ is *ramp scheme* if instead of 2 we have

3. if A is not qualified, then $\{\xi_i : i \in A\}$ does not determine ξ_s.

Existence of Perfect SSS – a negative result

Theorem (Ito, Saito, Nishizeki (87); Banaloh, Leichter (88))

If P is finite, then every access structure on P can be realised. □

Existence of Perfect SSS – a negative result

Theorem (Ito, Saito, Nishizeki (87); Banaloh, Leichter (88))

If P is finite, then every access structure on P can be realised. □

Fact (Probability theory)

If A is countable and ξ_s is independent of every finite subset of $\{\xi_i : i \in A\}$, then it is independent from the whole collection. □

Corollary

Suppose P is countably infinite. Then **no** *perfect secret sharing scheme exists for $\mathcal{A} = \{A \subseteq P : A \text{ is infinite}\}$.* □

Existence of Perfect SSS – a positive results

Theorem

Suppose $\mathcal{A}$ is generated by finite sets. Then there is a perfect secret sharing scheme realizing $\mathcal{A}$.

Proof.

The secret s is a single bit. Write s as the sum of independent random bits for each minimal qualified set. Assign each participant all bits from the set she is in. $\square$

Existence of Perfect SSS – a positive results

Theorem

Suppose $\mathcal{A}$ is generated by finite sets. Then there is a perfect secret sharing scheme realizing $\mathcal{A}$.

Proof.

The secret s is a single bit. Write s as the sum of independent random bits for each minimal qualified set. Assign each participant all bits from the set she is in. $\square$

Theorem (G. Tardos)

Suppose P is countable, and $\mathcal{A}$ is generated by finite sets. Then there is a perfect SSS for a single bit of secret so that everyone remembers finitely many bits only. $\square$

Reduction

Theorem

For any $\mathcal{A}$, there exists a perfect (ramp) SSS realizing $\mathcal{A}$ iff there is one where the secret is a single bit. $\square$

Definitions

- P is the set of participants
- X_i for $i \in P$ is the set of shares of i
- $X = \prod_i X_i$, Ω is a σ-algebra on X
- for $A \subseteq P$, $X_A = \prod_{i \in A} X_i$
- μ, ν are a probability measures on X, i.e. $\mu(X) = \nu(X) = 1$
- μ_A is the marginal measure on X_A, i.e. $\mu_A(E) = \mu(E \times X_{P-A})$
- $\mu \perp \nu$ if $X = U \cup^* V$ with $\mu(U) = \nu(V) = 0$

Existence of Perfect Secret Sharing Scheme

Let P be the set of participants, $\mathcal{A}$ be an access structure. The existence of a *perfect* SSS realizing $\mathcal{A}$ is equivalent to the following

Problem

Find sets X_i for $i \in P$, a σ-algebra Ω on the set $X = \prod_{i \in P} X_i$ and two probability measures μ and ν on Ω such that

- *when $A \subseteq P$ is unqualified, then $\mu_A = \nu_A$,*
- *when $A \subseteq P$ is qualified, then $\mu_A \perp \nu_A$ (they are mutually singular)*

Existence of Ramp Secret Sharing Scheme

Let P be the set of participants, $\mathcal{A}$ be an access structure. The existence of a *ramp* SSS realizing $\mathcal{A}$ is equivalent to the following

Problem

Find sets X_i for $i \in P$, a σ-algebra Ω on the set $X = \prod_{i\in P} X_i$ and two probability measures μ and ν on Ω such that

- *when $A \subseteq P$ is unqualified, then μ_A and ν_A have the same null sets,*
- *when $A \subseteq P$ is qualified, then $\mu_A \perp \nu_A$ (they are mutually singular)*

Open Problems

Problem

Define secret sharing for more than countably many participants.

Problem (Compactness for Perfect Schemes)

Suppose $\mathcal{A}$ is upward closed, and for each subset $N \subseteq P$, if all finite subsets of N are **not** *qualified, then nor is N (i.e., $N \notin \mathcal{A}$). Does there then exist a* **perfect** *scheme realizing $\mathcal{A}$?*

Problem (Existence of ramp schemes)

Does there exist a **ramp** *scheme for every access structure?*
Does there exist a ramp scheme for every access structures on **countably many** *participants?*

Contents

Complexity of infinite structures

In this section all structures are perfect, and have finitely generated qualified subsets.

Definition (Finitely spanned substructure)

$\Gamma' \prec \Gamma$ if $P' \subset P$, P' is finite, and
$A \subseteq P'$ is qualified in Γ' $\iff$ A is qualified in Γ

Claim

If Γ is finite and $\Gamma' \prec \Gamma$, then $\sigma(\Gamma') \leq \sigma(\Gamma)$. □

Definition (Complexity of Infinite Structures)

The complexity of Γ, denoted as $\sigma(\Gamma)$ is the sup of the complexity of its finitely spanned substructures:

$$\sigma(\Gamma) = \sup\{\sigma(\Gamma') \; : \Gamma' \prec \Gamma\}.$$

Theorem (Decomposition theorem a lá Stinson)

Let $\Gamma_i \subseteq \Gamma$ be a collection of substructures, and assume that every Γ-qualified set is qualified in at least k of the substructures. For each participant $p \in P$ define $\sigma_i(p) = 0$ if $p \notin \Gamma_i$, and $\sigma_i(p) = \sigma(\Gamma_i)$ otherwise. Then

$$\sigma(\Gamma) \leq \sup_{p \in P} \frac{\sum_i \sigma_i(p)}{k} .$$

Proof.

Let $\Gamma' \prec \Gamma$, then $\sigma(\Gamma')$ can be upper bounded by the right hand side by Stinson's decomposition theorem. $\square$

Problem

If $\mathcal{S}_i$ realizes Γ_i with complexity $\leq \sigma_i$, can you construct an $\mathcal{S}$ realizing Γ with complexity $\leq \sigma$?

Contents

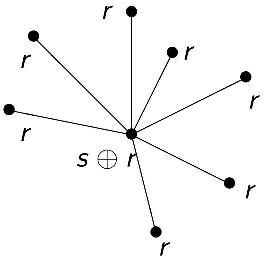
Stars

Fact

$\sigma(K_\infty) = 1.$ □

Fact

$\sigma(star) = 1$ □



Corollary

If the degree of G is $\leq d$, then $\sigma(G) \leq (d+1)/2$.

Proof.

Cover G by stars: every edge is covered twice, every vertex gets $\leq d+1$ bits. □

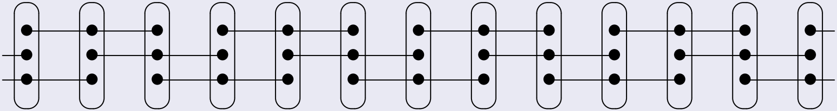
Infinite path

Theorem

$\sigma(P_\infty) = 3/2.$

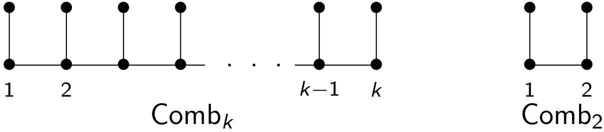
Proof.

Cover the path as follows:



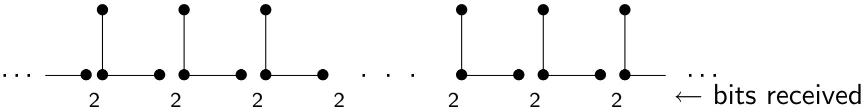
Every edge is covered twice, and every node receives 3 bits. $\square$

Comb



Theorem (L.Cs)

For $k \geq 2$, $\sigma(Comb_k) = 2 - 1/k$. $\square$



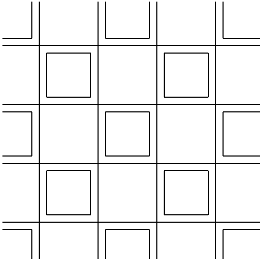
Corollary

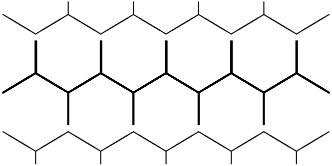
$\sigma(Comb_\infty) = 2$, *consequently* $Comb_\infty$ *is* **not** *local.*

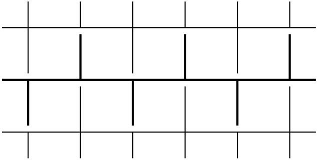
Lattices

Theorem (L.Cs)

$\sigma(\mathit{Honeycomb}) = 2,$
$\sigma(2\text{-}\mathit{lattice}) = 2,$
$\sigma(d\text{-}\mathit{lattice}) = d.$





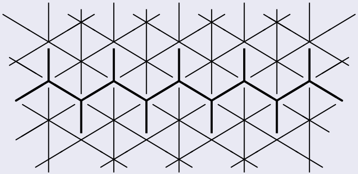


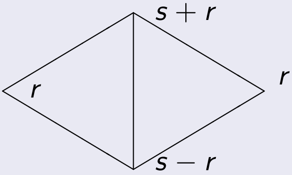
Lattices

Theorem

$2 \leq \sigma(\textit{triangle lattice}) \leq 12/5$

Proof.





$\square$

Problem

$\sigma(\textit{triangle lattice}) = ?$

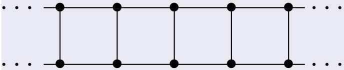
Ladder – 1

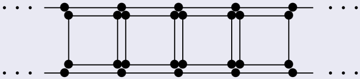
Theorem

$\sigma(Ladder) = 7/4$

Proof.

The cover on the left hand side gives the upper bound 7/4.





Using Shannon inequalities, $\kappa = 7/4$ for this graph (pentagonal prism):

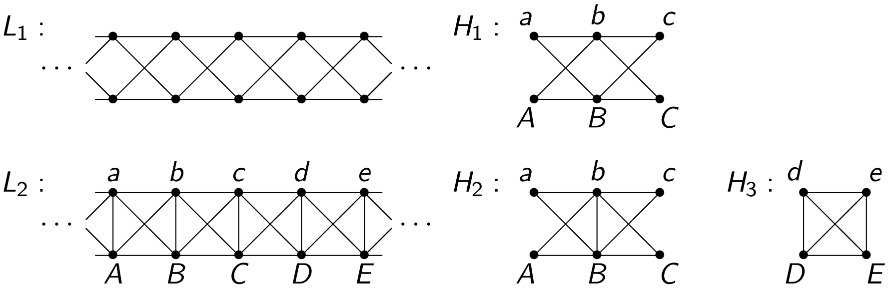
$$\begin{array}{ccccccccccccc} - & a & - & b & - & c & - & d & - & e & - & a & - \\ & | & & | & & | & & | & & | & & | & \\ - & A & - & B & - & C & - & D & - & E & - & A & - \end{array}$$

$\square$

Ladder – 2

Theorem

$\sigma(L_1) = 3/2$, $\sigma(L_2) = 5/3$

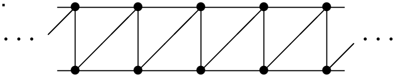


Ladder – 3

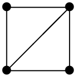
Theorem

$7/4 \le \sigma(L_3) \le 11/6.$

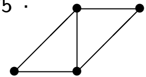
L_3 :



H_4 :



H_5 :



Problem

Find the exact value of $\sigma(L_3)$.

Thank you for your attention