Secret sharing on large girth graphs

Laszlo Csirmaz Peter Ligeti

Eotvos Lorand University, Department of Computeralgebra
Alfred Renyi Institute of Mathematics, Hungarian Academy of Sciences

June 18, 2019

Outline

1. Introduction
   - Secret Sharing
   - Graph Secret Sharing
   - Efficiency

2. Method
   - Definitions: complexity
   - Graph Example:
   - Main problem:

Outline

1. Introduction
   - Secret Sharing
   - Graph Secret Sharing
   - Efficiency
2. Method
   - Definitions: complexity
   - Graph Example:
   - Main problem:

Secret Sharing

Secret Sharing Scheme (Shamir 79)

- Secret: s
- Participants: $P = \{P_1, ..., P_n\}$
- Shares: $\{s_1, ..., s_n\}$
- Access Structure: $\mathcal{A} \subseteq 2^P$

Correctness: Every authorized set $B \in \mathcal{A}$ can recover s.
Privacy: Any unauthorized set $B \notin \mathcal{A}$ cannot learn anything about s.

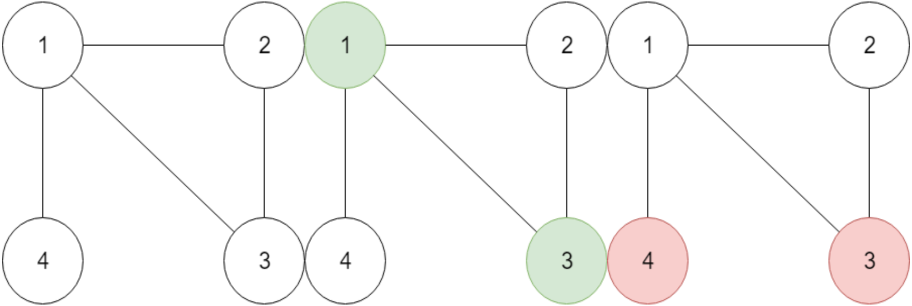
(t,n) Threshold schemes

- Participants: $P = \{P_1, ..., P_n\}$
- Access Structure: $\mathcal{A} = \{A \subseteq P : |A| \geq t\}$

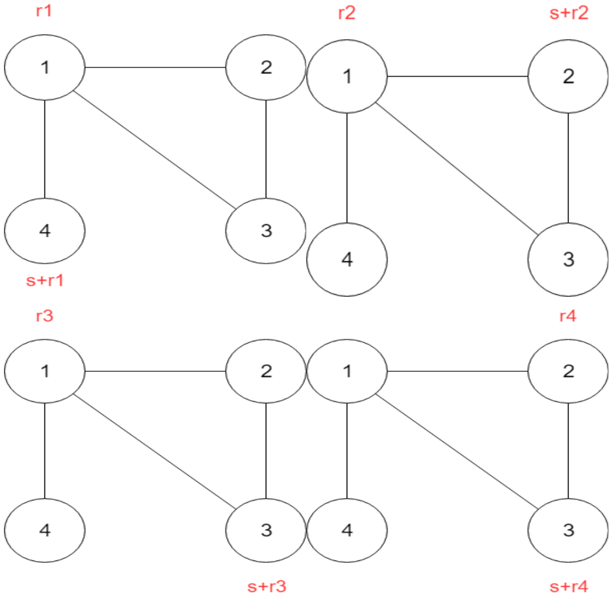
Outline

Graph Secret Sharing Scheme

- Participants: The participants are the vertices of a graph G =(V, E)
- Access Structure: A set of participants is qualified if there is an edge $e \in E$ with endpoints in this set.



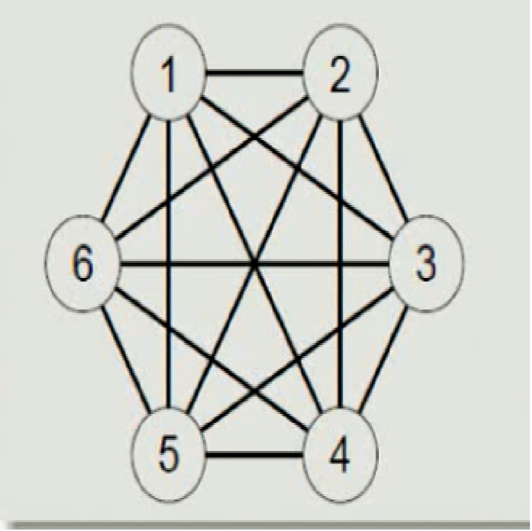
Graph Secret Sharing



All minimal authorized subset are of size 2.
Simple but interesting case
First step of obtaining general results.

The secret s is shared interdependently for every edge.

Graph Threshold Secret Sharing



Clique: It defines threshold access structure of threshold 2.

Outline

1. Introduction
   - Secret Sharing
   - Graph Secret Sharing
   - Efficiency
2. Method
   - Definitions: complexity
   - Graph Example:
   - Main problem:

Efficiency

Efficiency of a secret sharing scheme

- The efficiency of a secret sharing scheme is measured by:
  The ratio between The maximum size of the shares given to any participant and the size of the secret
- Using Shannons entropy to measure the complexity of a secret sharing scheme

Shannons entropy

Shannons entropy

- Shannons entropy measures the amount of uncertainty of a distribution.
- The requirements of secret sharing can be formulized by using entropy.

Shannons entropy

Let random variable X takes values $x_1, ..., x_n$ with probabilities $p_1, ..., p_n$.
The Shannons entropy of X is defined by
$H(X) = -\sum_{i=1}^{n} p(x_i) log(p(x_i)) = -E(log(Pr[x]))$

Outline

Definitions: complexity

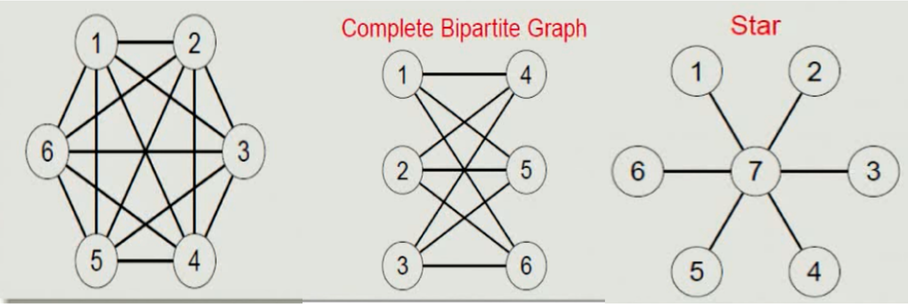
Definitions

- H(.) denotes the Shannon entropy
- Complexity $c(\mathcal{A}) = \inf_{S} \max_{v \in V} \frac{H(\varepsilon_v)}{H(\varepsilon_s)}$
- ideal access structure: when c(A) = 1
- $f : 2^V \to \mathbb{R}^+$ a normalized entropy function
- $f(x) = \frac{H(x)}{H(\varepsilon_s)}$

Outline

1. Introduction
   - Secret Sharing
   - Graph Secret Sharing
   - Efficiency
2. Method
   - Definitions: complexity
   - Graph Example:
   - Main problem:

Graph Example:



Graph Example:

Problem

Characterization of ideal schemes?

- matroid theory elements
- This problem isnt meant for this paper

Problem

Estimation/determination of the complexity for a given system

Sporadic Example:

Theorem (Csirmaz, 09)

Let G = (V, E) be a graph of girth at least 6 and with no adjacent vertices of degree at least 3. Then c(G) $= 2 - \frac{1}{d}$, where d is the maximal degree.

Theorem (Csirmaz, 07)

Let$H_d$be the d-dimensional hypercube. Then c$(H_d) = \frac{d}{2}$

Theorem (Csirmaz, 12)

Let T be a tree, with maximal core of size d. Then c(T) $= 2 - \frac{1}{d}$. A subset of the vertices of a tree is a core if it induces a connected subgraph and for each vertex in the subset one finds a neighbor outside the subset.

Outline

1. Introduction
   - Secret Sharing
   - Graph Secret Sharing
   - Efficiency
2. Method
   - Definitions: complexity
   - Graph Example:
   - Main problem:

main problem:

Problem

Does there exist large girth graphs with large complexity?

- recursive family of d-regular graphs of girth 6 with complexity $(d+1)/2$ (van Dijk and Blundo et al. 95)
- d-dimensional hypercube (girth 4) with complexity $d/2$ (Csirmaz 07)
- graphs of girth at least 6 with no adjacent vertices of degree at least 3 and complexity 2-1/d (Csirmaz, LP 09)
- trees (girth 0) with complexity 2-1/d. (Csirmaz, Tardos 12)

Lower bounds for the complexity:

Entropy method (Blundo, 95)

- $f : 2^V \to \mathbb{R}^+$ a normalized entropy function, such that:
- f is monotone and submodular; moreover f(Ø) = 0;
- f(A) + 1 $\leq$ f(B) if A $\subset$ B, A is independent and B is not (strict monotonicity)
- f(AC) + f(BC) $\geq$ f(C) + f(ABC) + 1 if C is empty or independent, AC and BC are qualified (strict submodularity).
- If for any such function f we have f(v) $\geq \alpha$ for some vertex v of G, then the complexity of G is at least α.

upper bounds for the complexity :

Only solvable for small examples as huge LP problem.

Theorem

- For any normalized entropy function f on Gd :

$$H(X) = -\sum_{v \in G_d} f(v) - f(G_d) \geq \frac{d}{2}|G_d| - 1$$

- For every graph Gd $\in \mathcal{G}_d$:

$$c(Gd) \geq \frac{d+1}{2}$$

Constructions:

Theorem (Stinson,94)

Let G = (V, E) covered by ideal graphs such that every vertex is contained in at most v and every edge is contained in at least e such graphs. Then c(G)$\leq \frac{v}{e}$.

Corollary (Stinson,94)

c(G)$\leq \frac{d+1}{2}$, d is the maximal degree (covering with stars).

Corollary (Pyber, 97)

c(G)$\leq c\frac{n}{log n}$, d is the maximal degree (covering with complete bipartite graphs)).

The graph family $\mathcal{G}_d$:

Recursive construction

- $G_2 = (A_2, B_2)$ is the cycle of even length
- $G_d = (A_d, B_d)$ has been constructed, take several copies of Gd
- G_{d+1} : add an (arbitrary) 1-factor between B_d^i and A_d^{i+1} for all i

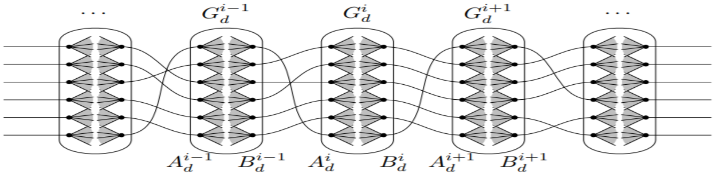


Figure 1: Structure of the graph G_{d+1}

The graph family $\mathcal{G}_d$:

Definition

$\mathcal{G}_d$ consists of all graphs G_d constructed this way

Claim

Every Gd is a d -regular bipartite graph with, and hence $c(G_d) \leq \frac{(d+1)}{2}$ by Stinsons bound

Theorem

For every graph $G_d \in \mathcal{G}_d$:
$c(G_d) = \frac{d+1}{2}$

Summary

- Using the entropy method, it was shown that the general upper bound $(d+1)/2$ on the complexity of graph based secret sharing schemes, known as Stinsons bound, is tight for a large class of inductively defined d-regular bipartite graphs.
- This result refutes the widely believed conjecture that large girth graphs have bounded complexity due to the exponentially diminishing interaction between the shares assigned to the vertices.