Secret sharing on large girth graphs

László Csirmaz, **Péter Ligeti**

Eötvös Loránd University, Department of Computeralgebra;
Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences

Mathematical Methods for Cryptography
Svolvær – Lofoten 2017

Overview

1. Motivation
   - Secret sharing et al.
   - Examples
   - Problems

2. Methods
   - Definitions
   - Entropy method
   - Constructions

Informal definitions

Secret sharing

- distribute some pieces of a secret data between participants
- only the „good guys” can recover the secret from the parts
- good coalitions describe the system

Complexity

- measures the efficiency of a system
- the amount of information, the participants has to remember
- ideal schemes have complexity 1

Examples

All-or-nothing

- one qualified set only $\Leftrightarrow$ everybody together
- $s \in_R \{0, 1\}, s_i \in_R \{0, 1\}$ such that $\sum s_i = s$

Threshold schemes

- qualified sets $\Leftrightarrow$ coalitions of size $\geq k$
- Shamir '79 (Lagrange interpolation)
- Blakley '79 (vector spaces)

Graph-based schemes

- participants $\Leftrightarrow$ vertices
- vertex set is qualified $\Leftrightarrow$ spanning any edges

Problems

Problem

Characterization of ideal schemes

- matroid theory elements
- this maze isn't meant for this talk

Problem

Estimation/determination of the complexity for a given system

- we focus on this one...

Examples

All-or-nothing

- one qualified set only $\Leftrightarrow$ everybody together
- $s \in_R \{0,1\}, s_i \in_R \{0,1\}$ such that $\sum s_i = s$
- complexity is 1

Threshold schemes

- qualified sets $\Leftrightarrow$ coalitions of size $\geq k$
- Shamir '79 (Lagrange interpolation)
- Blakley '79 (vector spaces)
- complexity is 1

Graph examples

Sporadic examples

- ideal $\Leftrightarrow$ complete (multipartite) $\Leftrightarrow$ 2-threshold
- small graphs (van Dijk '97, ..., Harsányi, LP '17, ...)
- recursive family of d-regular graphs with complexity $(d+1)/2$ (van Dijk and Blundo et al. '95)

Theorem (Csirmaz '07)

Let $\mathcal{H}_d$ be the d-dimensional hypercube. Then $\mathbf{c}(\mathcal{H}_d) = \frac{d}{2}$.

Graph examples

Theorem (Csirmaz, LP '09)

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

Theorem (Csirmaz, Tardos '12)

Let T be a tree, with maximal core of size d. Then $c(T) = 2 - \frac{1}{d}$.

Main problem

Problem

Does there exist large girth graphs with large complexity?

Hints

- 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)

Definitions: secret sharing scheme

Definition

- *participants: a finite set P*
- *access structure: $\mathcal{A} \subseteq 2^P$, elements of $\mathcal{A}$: qualified subsets*
- *perfect secret sharing realizing $\mathcal{A}$ is $\xi_1, \xi_2, \ldots, \xi_{|P|}, \xi_s$ i.d.:*
  - (i) $A \in \mathcal{A} \Rightarrow \{\xi_a : a \in A\}$ *determines* ξ_s
  - (ii) $B \notin \mathcal{A} \Rightarrow \{\xi_b : b \in B\}$ *is independent of* ξ_s

Definitions: complexity

Definition

- $\mathbf{H}(.)$ *denotes the Shannon entropy*
- *complexity*:

$$\mathbf{c}(\mathcal{A}) = \inf_{\mathcal{S}} \max_{v \in V} \frac{\mathbf{H}(\xi_v)}{\mathbf{H}(\xi_s)}$$

- *ideal access structure: when* $\mathbf{c}(\mathcal{A}) = 1$
- $f : 2^V \mapsto \mathbb{R}^+$ *a normalized entropy function*
- $f(x) = \frac{\mathbf{H}(x)}{\mathbf{H}(\xi_s)}$

General lower bounds for the complexity

Theorem (Entropy method, Blundo et al. '95)

Let $f : 2^V \mapsto \mathbb{R}^+$ be a function such that:

- *f is monotone and submodular; moreover $f(\emptyset) = 0$;*
- *$f(A) + 1 \leq f(B)$ 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.

How to use

- huge LP problem, solvable for small examples only
- reduce the number of inequalities, e.g.:

Lemma

For any normalized entropy function f on G_d:

$$\sum_{v \in G_d} f(v) - f(G_d) \geq \frac{d}{2}\,|G_d| - 1.$$

... several lemmas are coming ...

Theorem

For every graph $G_d \in \mathcal{G}_d$

$$\mathbf{c}(G_d) \geq \frac{d+1}{2}.$$

General upper bounds for the complexity

- 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 $\mathbf{c}(G) \leq \frac{v}{e}$.

Corollary (Stinson's bound '94)

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

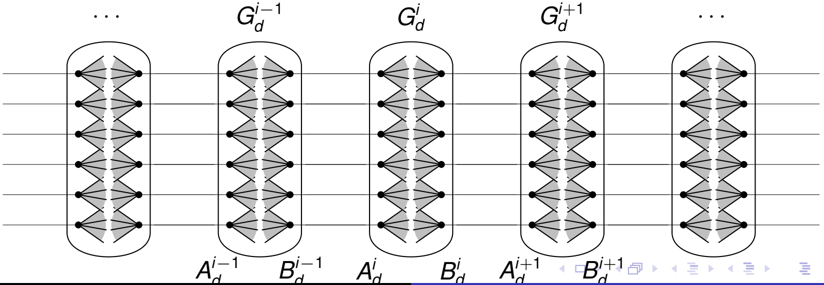
Corollary (Erdős, Pyber '97)

$\mathbf{c}(G) \leq c\frac{n}{\log n}$ *(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 G_d
- G_{d+1} : add an (arbitrary) 1-factor between B_d^i and A_d^{i+1} for all i



The graph family $\mathcal{G}_d$

Definition

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

Claim

Every G_d is a d-regular bipartite graph with, and hence $\mathbf{c}(G_d) \leq (d+1)/2$ by Stinson's bound.

Theorem

For every graph $G_d \in \mathcal{G}_d$

$$\mathbf{c}(G_d) = \frac{d+1}{2}.$$

The main problem was...

Problem

Does there exist large girth graphs with large complexity?

Theorem

For every graph $G_d \in \mathcal{G}_d$

$$\mathbf{c}(G_d) = \frac{d+1}{2}.$$

Lemma

$\mathcal{G}_d$ contains graphs of girth g if

$$N_d \approx 12 \cdot 2^{36\, g\, N_{d-1}}.$$

Open problem

d-regular graph with girth $> g \Rightarrow |V| \geq d^g$.

Thank You for Your Attention!