Tatracrypt 2007

Exact bound on tree based secret sharing schemes

László Csirmaz

CEU, Budapest

Joint work with
Gábor Tardos, Rényi Institute

Definition A *Perfect Secret Sharing Scheme* $\mathcal{S}$ on the vertices V of a graph G is a joint distribution

$$\{\xi_v : v \in V\} \text{ (shares) and } \xi_s \text{ (secret)}$$

such that

- each edge (v, w) can recover the secret, i.e. ξ_v and ξ_w determines uniquely ξ_s,
- if $A \subseteq V$ is independent, then $\{\xi_v : v \in A$ and ξ_s are independent.

Definition $\mathsf{H}(\xi)$ is the Shannon entropy of ξ;

$$\mathcal{S}(v) \overset{\text{def}}{=} \frac{\mathsf{H}(\xi_v)}{\mathsf{H}(\xi_s)} = \text{how many bits } \mathcal{S} \text{ assigns to } v \text{ for each bit in } s.$$

Definition The *worst case information rate*

$$\mathsf{R}(G) \stackrel{\text{def}}{=} \min_{\text{scheme } \mathcal{S}} \max_{v \in V} \mathcal{S}(v)$$

(i.e. at least that much information someone must remember)

Claim $\mathsf{R}(G) \geq 1$ if G is not empty. In fact, $\mathcal{S}(v) \geq 1$ for each non-isolated vertex.

Theorem

$\mathsf{R}(G) = 1$ for the complete graph K_n (Shamir)

$\mathsf{R}(G) \leq \frac{1}{2}(\text{ max degree } +1)$ (Stinson)

$\mathsf{R}(G) \leq \dfrac{cn}{\log n}$ for all graphs on n vertices (Erdős–Pyber)

$\mathsf{R}(G) \geq \log_2 n$ for some graph on n vertices (Csirmaz, van Dijk, Capocelli et al)

Known exact information rate for certain graphs

- R(star) $=1$ (folklore)
- paths, cycles (Stinson):

R$(P_1) =$ R$(P_2) = 1$, R$(P_k) = 1.5$ otherwise;

R$(C_3) =$ R$(C_4) = 1$, R$(C_k) = 1.5$ otherwise

- all graphs on ≤ 5 vertices (Stinson, van Dijk, Santis)
- some graphs on 6 vertices
- specially constructed large graphs (van Dijk, Santis),

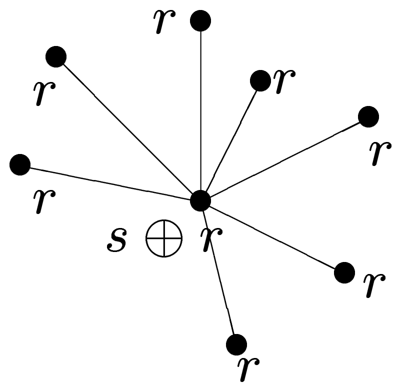
  e.g. R$(\{0,1\}^d) = d/2$ (Csirmaz)

Theorem (Csirmaz – Tardos, 2006) *The exact information rate for all trees.*

Upper Bounds

Claim R(star) ≤ 1.

Proof secret $s \in \{0, 1\}$,
random $r \in \{0, 1\}$

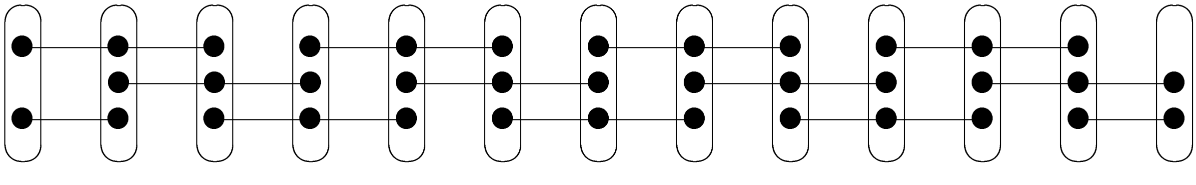


Theorem (Stinson): *$G_i \subseteq G$, $\mathcal{S}_i$ is a scheme on G_i assigning $\mathcal{S}_i(v)$ bits to $v \in V$. Each edge is covered $\geq k$ times. Then for some scheme $\mathcal{S}$ on G,*

$$\mathcal{S}(v) \leq \frac{1}{k} \sum_i \mathcal{S}_i(v) \qquad \blacksquare$$

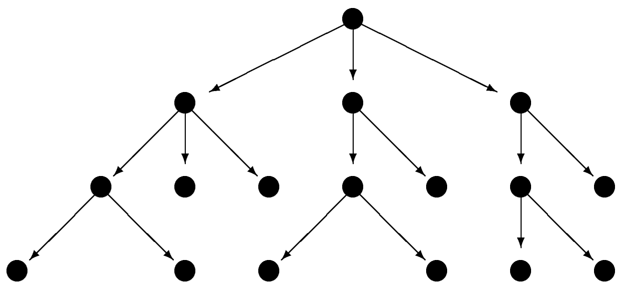
Corollary R(path) ≤ 1.5

Proof Each edge is covered twice, each vertex gets 2 or 3 bits:

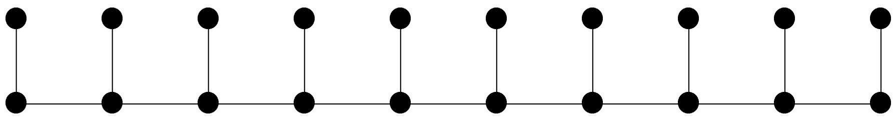


Observation *For each tree T,* R$(T) \leq 2$.

Proof each edge is covered, each vertex gets ≤ 2 bits.

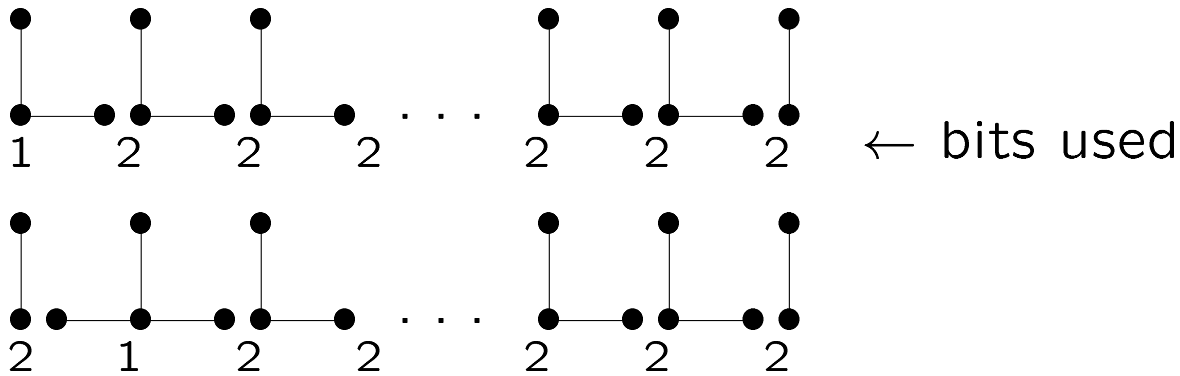


Theorem For the comb of width k:



$$\mathrm{R}(\mathrm{comb}_k) \leq 2 - 1/k.$$

Proof Summing up all k sharings, all edges are covered k times, and $2k-1$ bits are assigned to all bottom nodes.



Lower Bounds

Reminder: $\mathsf{H}(A) =$ entropy of $\{\xi_v : v \in A\}$

Use known linear inequalities for the entropy, in particular: $I(X;Y|Z) \geq 0$.

Typically the lower bound is an LP problem.

Example: For $G = \overset{a}{\bullet}\!-\!\!-\!\!-\!\overset{b}{\bullet}\!-\!\!-\!\!-\!\overset{c}{\bullet}\!-\!\!-\!\!-\!\overset{d}{\bullet}$ we have $\mathsf{H}(b) + \mathsf{H}(c) \geq \mathsf{H}(bc) \geq 3\,\mathsf{H}(s)$ as:

$$
\begin{array}{rcl}
\mathsf{H}(abcd) & \geq & \mathsf{H}(ad) + \mathsf{H}(s) \\
\mathsf{H}(ad) + \mathsf{H}(ac) & \geq & \mathsf{H}(acd) + \mathsf{H}(a) \\
\mathsf{H}(acd) + \mathsf{H}(abc) & \geq & \mathsf{H}(abcd) + \mathsf{H}(ac) + \mathsf{H}(s) \\
\mathsf{H}(ab) + \mathsf{H}(bc) & \geq & \mathsf{H}(abc) + \mathsf{H}(b) + \mathsf{H}(s) \\
\mathsf{H}(a) + \mathsf{H}(b) & \geq & \mathsf{H}(ab)
\end{array}
$$

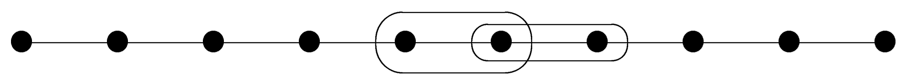
Does not necessarily work: not all polymatroids are entropy-representable (Matuš)

Definition A *core* C of G is a connected subset of the vertices such that each vertex in C has a heighbour (in G) outside if C.

For each tree the maximal core size can be found in $O(n^2)$ steps.

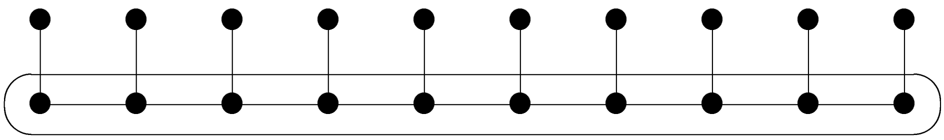
Theorem (Csirmaz–Tardos) *Let G be a tree, and let k be the size of the maximal core in G. Then the information rate* $\mathrm{R}(G) = 2 - 1/k$.

Example Path of length at least 3:



has maximal core size 2, $\mathrm{R}(\text{path}) = 2 - 1/2$.

For the comb, the bottom nodes form a core of size k, thus $\mathsf{R}(\mathrm{comb}_k) = 2 - 1/k$



Proof The Lower bound uses information theoretic machinery. Let C be a core in G, then (assuming $\mathsf{H}(s) = 1$)

$$\sum_{v \in C} \mathsf{H}(v) \geq \mathsf{H}(C) + |C| - 2. \tag{1}$$

(1) follows from the connectedness of C. Now

$$\mathsf{H}(C) \geq |C| + 1, \tag{2}$$

as each vertex in C is connected to a member in a large independent set. Summing these

$$\sum_{v \in C} \mathsf{H}(v) \geq 2|C| - 1,$$

i.e. for at least one $v \in C$, $\mathsf{H}(v) \geq 2 - 1/|C|$.

The upper bound comes from a multiple covering of the edges by stars. Let k be the size of the largest core in G. Then there exists a collection of stars (as subgraphs of G) such that

- each vertex is covered exactly k times,
- no vertex is contained in more than $2k - 1$ of these stars.

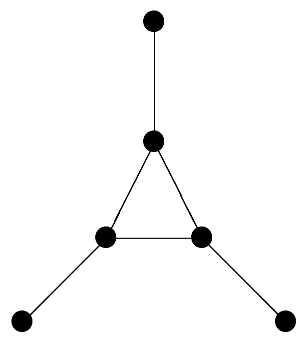
Such a covering can be constructed in $O(n^3)$ steps.

Using Stinson's construction, we can construct the required perfect secret sharing scheme with rate $2 - 1/k$. ∎

Problems for further research

when Stinson's construction does not help ...

The rate of this graph is 7/4. The best construction from covering it by stars yields a scheme with rate 2.



Determine the rate of the graph on $2n$ vertices, where each vertex of a complete graph on n vertices is matched to an independent set of size n. (The above graph is the special case for $n = 3$). The lower bound is $2 - 1/2^{n-1}$, and for $n > 3$ only construction with rate 2 is known.

Finally, and most importantly, is there any graph where the lower bound given by the entropy method cannot be achieved?