# On infinite families of graphs with information rate $2 - \frac{1}{k}$

Péter Ligeti, Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences;
Eötvös Loránd University, ELTECRYPT Research Group

Joint work with László Csirmaz

In this paper we consider the secret sharing problem on special access structures with minimal qualified subsets of size two, i.e. secret sharing on graphs. This means that the participants are the vertices of the graph and the qualified subsets are the subsets of $V(G)$ spanning at most one edge. The information rate of a graph $G$ is denoted by $\rho(G)$ and is defined as the ratio of the greatest size of the shares a vertex have to remember and of the size of the secret.

Since the determination of the *exact* information rate is a non-trivial problem even for small graphs (i.e. for $V(G) = 6$), every construction can be of particular interest. A nice example is due to Csirmaz and Tardos [4] claiming that the information rate of every finite tree $T$ is $2 - \frac{1}{k}$ for some $k \in \mathbb{N}$. An interested reader can find further constructions of graphs with exact information rate in [1], [2], [3], [5].

In this paper we present other large families of graphs of arbitrary size with information rate $2 - \frac{1}{k}$ by proving upper and lower bounds for $\rho(G)$ that coincide.

As a consequence of the pioneering work of Stinson [6] every covering of the graph $G$ with arbitrary graphs yields an upper bound for the information rate, i.e. if there is a covering with graphs such that every vertex is covered by at most $p$ graphs and every edge is covered by at least $e$ graphs then $\rho(G) \leq \frac{p}{e}$.

The first main result of the paper is to construct such a covering for arbitrary graph in the special case of the covering with stars (i.e. with graphs having all but on vertex of degree one). To this end we use polyhedral combinatorics point of view by rephrasing the covering assumptions as a linear programming (LP) problem. The size of the arising LP problem is linear in the number of edges of the graph, hence it can be solved even for large graphs, furthermore the star-covering can be read out from the optimal solution of the LP easily.

The only known method for proving lower bound for the information rate is the well-known *entropy method*. The essence of this method is to prove that *any* real-valued function $f$ satisfy some properties of the entropy function the largest value of $f$ on the vertices is at least $l$. Then, as functions coming from secret sharing schemes also satisfies these properties, conclude, that $\rho(G) \geq l$. Unfortunately the size of the LP problem arising from these entropy-inequalities can be too large to solve it even in the case of few vertices. Hence one needs to reduce the number of the inequalities by identifying some adequate structural properties of the graph.

The second main result of the present paper is to observe such a structural property for recursively defined graph-classes.

**Theorem.** *Let $G$ be an arbitrary graph and denote by $d_i$ the degree of the $i$th vertex of this graph. Then for the graph $G'$ arising from $G$ by replacing all of the edges of $G$ by a path of length at most two the following lower bound holds:*

$$\rho(G') \geq 2 - \frac{1}{\max_i d_i}.$$

With the help of the above two main tools one can get a large family of graphs where the two bounds coincide (note that every graph having no two adjacent nodes of degree at most three can be considered as a $G'$ in the theorem). Here we present two simple examples:

**Example** *Let $C_m^+$ denote the cycle of length $2m \geq 6$ with a chord replacing with a path of length at least two between two vertices of distance $m$. Then $\rho(C_m^+) = \frac{5}{3}$.*

**Example** *Let $K_n^{m+}$ denote the graph arising from the complete graph on $n \geq 4$ vertices replacing all of its edges with a path of length $m \geq 2$. Then $\rho(K_n^{m+}) = 2 - \frac{1}{n-1}$.*

There is no known graph with exact information rate less than two but not $2 - \frac{1}{k}$. Both all the previous results and the presented new graph-families suggest the following:

**Conjecture.** *If a graph $G$ has information rate $1 < \rho(G) < 2$, then $\rho(G) = 2 - \frac{1}{k}$ for some $k \in \mathbb{N}$.*

## References


[1] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, *Graph decomposition and secret sharing schemes*, Journal of Cryptology **8** (1995), 39–64.

[2] C. Blundo, A. De Santis, R. D. Simone and U. Vaccaro, *Tight bounds on the information rate of secret sharing schemes*, Journal of Cryptology **11** (1997), 107–110.

[3] L. Csirmaz, *Secret sharing on the d-dimensional cube*, Manuscript (2005).

[4] L. Csirmaz and G. Tardos, *Exact bounds on tree based secret sharing schemes*, Tatracrypt 2007, Slovakia (2007).

[5] A. Shamir, *How to share a secret*, Communications of the ACM, **22** (1979), 612–613.

[6] D. R. Stinson, *Decompostion construction for secret sharing schemes*, IEEE Transactions on Information Theory **40** (1994), 118–125.