Secret sharing on large girth graphs

László Csirmaz, Péter Ligeti *†

Abstract

Secret sharing is a method for distributing some secret information between a set of participants by giving them some partial knowledge of the secret in a way that only some pre-described coalitions will be able to reconstruct the original secret from the respective parts. We investigate graph based secret sharing schemes and its information ratio, also called *complexity*, measuring the maximal amount of information the vertices has to store. It was conjectured that in large girth graphs, where the interaction between far away nodes is restricted to a single path, this complexity is bounded. This conjecture was supported by several result, most notably by a result of Csirmaz and Ligeti [2] saying that the complexity of graphs with girth at least six and no neighboring high degree vertices is strictly below 2. In this paper we refute the above conjecture.

First, a family of d-regular graphs is defined iteratively such that the complexity of these graphs is the largest possible $(d+1)/2$ allowed by the general bound of Stinson [4]. This part extends earlier results of van Dijk [3] and Blundo et al [1], and uses the so-called *entropy method*.

Second, using combinatorial arguments, we show that these families contain graphs with arbitrary large girth. In particular, we obtain the following purely combinatorial result, which might be interesting on its own: there are d regular graphs G with arbitrary large girth such that any fractional edge-cover of G by stars must cover some vertex $(d+1)/2$ times.

References

1. C. Blundo, A. De Santis, R. De Simone, U. Vaccaro, *Tight bounds on the iformation rate of secret sharing schemes*, Des., Codes and Crypt. **11** (2) (1997) pp. 107–110.

2. L. Csirmaz, P. Ligeti, *On an infinite family of graphs with information ratio* $2-1/k$, Computing **85** (1) (2009) pp. 127–136.

3. M. van Dijk, *On the information rate of persect secret sharing schemes,* Des., Codes and Crypt. **6** (2) (1995) pp. 143–169.

4. D. R. Stinson, *Decomposition construction for secret sharing schemes,* IEEE Trans. on Inf. Theory, **40** (1) (1994) pp. 118–125.

*Central European University, Eötvös Loránd University and Rényi Institute, Budapest
†e-mail: csirmaz@renyi.hu, turul@cs.elte.hu