sciendo

TATRA MOUNTAINS
Mathematical Publications

DOI: 10.2478/tmmp-2019-0008
Tatra Mt. Math. Publ. **73** (2019), 97–108

ON THE INFORMATION RATIO OF GRAPHS WITH MANY LEAVES

Máté Gyarmati — Péter Ligeti

3in Research Group, Faculty of Informatics, Eötvös Loránd University, Budapest, HUNGARY

ABSTRACT. We investigate the information ratio of graph-based secret sharing schemes. This ratio characterizes the efficiency of a scheme measured by the amount of information the participants must remember for each bits in the secret.

We examine the information ratio of several systems based on graphs with many leaves, by proving non-trivial lower and upper bounds for the ratio. On one hand, we apply the so-called entropy method for proving that the lower bound for the information ratio of n-sunlet graphs composed of a 1-factor between the vertices of a cycle C_n and n independent vertices is 2. On the other hand, some symmetric and recursive constructions are given that yield the upper bounds. In particular, we show that the information ratio of every graph composed of a 1-factor between a complete graph K_n and at most 4 independent vertices is smaller than 2.

1. Introduction

1.1. Motivation and notion

In a *secret sharing scheme* some sensitive information—i.e., the secret—is distributed among a finite set of *participants* $\mathcal{P}$ in a system in such a way that only some predefined subsets can recover it from the shared pieces. The distinguished subsets of participants are called *qualified* subsets, the collection of all qualified subsets is called an *access structure*, and denoted by $\mathcal{A}$. Additionally, we suppose that non-qualified subsets cannot learn anything about the secret.

2010 Mathematics Subject Classification: Primary 94A62, 94A60.

Keywords: secret sharing, information ratio, entropy method.

This research has been partially supported by the ÚNKP-17–4 National Excellence Program of the Ministry of Human Capacities, the Lendület program of the Hungarian Academy of Sciences and by the European Union, co-financed by the European Social Fund (EFOP–3.6.2–16-2017–00013, Thematic Fundamental Research Collaborations Grounding Innovation in Informatics and Infocommunications).

Let us note, that we can suppose that $\mathcal{A}$ is monotone, since the access structure can be described by its minimal elements. In this work we examine *graph based schemes*, where the size of the minimal qualified subsets is two. In other words, there is a one-to-one correspondence between the access structure and a graph, where the vertices are indexed by the participants, and a subset A is qualified if there is some edge between the respective vertices.

One interesting quantity related to a secret sharing is the *information ratio* measuring the amount of information the participants have to store related to the size of the secret.

One of the most important and relevant problems in this topic is to prove the exact value or at least some non-trivial bounds for the information ratio of any particular graph-class.

1.2. Related work and our contribution

Secret sharing was first introduced in two independent fundamental papers by Blakley [1] and Shamir [14] based on finite dimensional vector spaces and polynomials over finite fields, respectively. On one hand, the information ratios of several small graphs are determined, like graphs up to six vertices [3,4,11,13,19,20] and of some graphs with at most ten vertices [10,12,15,16,21]. On the other hand, in addition to the case of small graphs, exact values for the information ratios of some general families of graphs are proved as well, like hypercubes and d-dimensional lattices [5], trees [9], recursive constructions [2], special unicyclic graphs [12], graphs with large girth [8] or graphs with large girth and no adjacent vertices of high-degree [7].

The typical method for proving exact information ratios is to give upper and lower bounds that coincide. However, it is hard to predict which bound is harder to prove. To illustrate this phenomenon, we investigate two graph classes with many leaves, in either of them one direction is simple, but the other needs more sophisticated ideas.

Note that different degree 1 neighbors of a given vertex are equivalent from the secret sharing point of view (i.e., the respective participants can get the same share), hence we can suppose that every vertex has at most one leaf.

The first main result is to determine the exact information ratio for a large family of unicyclic graphs for which the lower bound is non-trivial. Let S_n denote the *n-sunlet graph* on $2n$ vertices composed of a cycle C_n and a 1-factor between the vertices of C_n and the remaining independent vertices. (Note that the case of a cycle with less leaves is partially covered in [12].)

Theorem 1.1. *For every $n \in \mathbb{N}, n > 1$ the information ratio of the n-sunlet graph S_n is 2.*

On the other hand, we prove the non-trivial upper bound for the information ratio of another family of graphs by using the weighted decomposition method

of S u n and C h e n [19]. Furthermore, we show that in some cases this bound is optimal. Let K_n^l denote a graph on $n+l$ vertices composed of a complete graph K_n on n vertices and a one-factor between any l of its vertices and the remaining l independent vertices (i.e., the leaves). 2 is a trivial upper bound for these graphs. We determine the exact information ratio if l is at most two, and give non-trivial upper bounds strictly smaller than 2 in the case of $l \leq 4$.

Theorem 1.2. *For every $n \in \mathbb{N}^+, l \in \mathbb{N}, l \leq 4, l \leq n$ the information ratio of K_n^l is smaller than 2.*

Particularly, if $l = n$, then this coincides with the cases examined by C s i r m a z [6]. For this graph class, the author showed that there is no linear secret sharing construction that matches the lower bound given by the entropy method. It was showed that for $n = 2$, $n = 3$ the lower bound is strictly less than 2.

2. Results on the information ratio of graphs with many leaves

2.1. Definitions and methods

Let a finite set $\mathcal{P}$ be called the set of participants and let $\mathcal{A} \subseteq 2^{\mathcal{P}}$ be an increasing monotone set of subsets called access structure containing the qualified subsets. For a given access structure, we can define a secret sharing related to this set-system:

Definition 2.1. A *perfect secret sharing* $\mathcal{S}$ realizing the access structure $\mathcal{A}$ is a collection of random variables ξ_i for every $i \in \mathcal{P}$ and ξ_s with a joint distribution such that

(i) if $A \in \mathcal{A}$, then $\{\xi_i : i \in A\}$ determines ξ_s;

(ii) if $A \notin \mathcal{A}$, then $\{\xi_i : i \in A\}$ is independent of ξ_s.

Note that, as a consequence of the monotonicity of $\mathcal{A}$, the minimal elements are able to describe the whole access structure. In this paper we investigate a special case, in which the size of every minimal qualified subset is two. In this case a graph $G = (V, E)$ can describe $\mathcal{A}$ with $V = \mathcal{P}$ and $E = \min \mathcal{A}$. For the sake of simplicity, we use the notation uv for an edge $\{u, v\}$.

The efficiency of a given secret sharing scheme is characterized by the size of the largest share the participants store related to the size of the secret. This quantity is called information ratio. The size of a discrete random variable ξ is traditionally measured by its *Shannon entropy*, denoted by $H(\xi)$. The precise definition is the following:

Definition 2.2. Let G be a graph describing the access structure $\mathcal{A}$. Then the information ratio of the graph G is

$$\sigma(G) = \inf_{\mathcal{S}} \max_{i \in \mathcal{P}} \frac{H(\xi_i)}{H(\xi_s)},$$

where the infimum is taken over all perfect schemes $\mathcal{S}$ realizing $\mathcal{A}$.

The most frequently used method for proving lower bounds for the information ratio is the so-called *entropy method* introduced by Blundo et al. [3]. The method is based on some basic properties of the Shannon entropy and the secret sharing and can be summarized in the following way. For every subset A of the participants let the following define real-valued function f:

$$f(A) = \frac{H(\{\xi_i : i \in A\})}{H(\xi_s)}. \tag{1}$$

By this notation, the information ratio is the maximal value in $\{f(i) \ : \ i \in \mathcal{P}\}$. Using the standard properties of the entropy function, it is easy to show that the following so-called *Shannon inequalities* hold for all subsets of the participants:

Remark 1 (Shannon inequalities)**.** Let $f : 2^{\mathcal{P}} \longrightarrow \mathbb{R}$ be a function defined by 1. Then for every $A, B \subseteq \mathcal{P}$:

(a) $f(\emptyset) = 0$, and in general $f(A) \geq 0$ (positivity);
(b) if $A \subseteq B \subseteq V$, then $f(A) \leq f(B)$ (monotonicity);
(c) $f(A) + f(B) \geq f(A \cap B) + f(A \cup B)$ (submodularity);
(d) if $A \subseteq B$, A is an independent set and B is not, then $f(A) + 1 \leq f(B)$ (strong monotonicity);
(e) if neither A nor B is independent but $A \cap B$ is so, then $f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$ (strong submodularity).

Now, the goal is to prove that for *any* real-valued function f satisfying properties (a)–(e), for some participant i, $f(i) \geq r$. Since functions coming from secret sharing schemes also satisfy these properties, the information ratio is also at least r. The drawback of this general method is that the LP problem arising from all the Shannon inequalities is ill-conditioned, hence one needs to observe some symmetries or structural properties in order to reduce the size of the problem.

Every secret sharing construction yields an upper bound for the information ratio. More specifically, every covering of the graph G with arbitrary graphs yields an upper bound as a consequence of the pioneering work of Stinson [18]. In particular, if the covering uses only complete multipartite graphs, and every vertex is covered by at most p graphs and every edge is covered by at least

e graphs then $\sigma(G) \leq \frac{p}{e}$. Sun and Chen [19] generalized this technique for weighted graphs. A weighted graph G is a graph with the weight function

$$w_G : E \mapsto \mathbb{Z}.$$

We can define secret sharing in weighted graphs. w_G is the number of different secrets, and participants corresponding to an e edge can recover $w_G(e)$ secrets out of the w_G secrets.

As an example, consider the following weighted graph G_w with seven vertices $V = \{u, v, w, s, x, y, z\}$, and nine edges $E = \{uv, uw, us, vw, vs, ws, ux, vy, wz\}$. The weight of uv, and vw are two, and all the other weights are one, see Figure 1

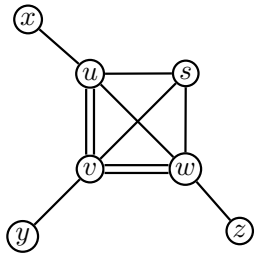


FIGURE 1. The weighted graph G_w on seven vertices.

In a weighted secret sharing we have not just one but w_G secrets. Each pair of participants can recover $w_G(e)$ secrets if they are adjacent, and the independent sets have no information about any of the secrets.

DEFINITION 2.3. A weighted secret sharing $\mathcal{S}$ realizing a graph G is a collection of random variables $\xi_1, \xi_2, \ldots, \xi_{|P|}, \xi_{s_1}, \ldots, \xi_{s_{w_G}}$ with joint distribution such that

(i) If $uv \in E(G)$, then $\{\xi_u, \xi_v\}$ determine $w_G(e)$ secrets out of the $W(G)$ secrets $\{\xi_{s_1}, \ldots, \xi_{s_{w_G}}\}$.

(ii) If B is independent, then $\{\xi_b : b \in B\}$ is independent of $\{\xi_{s_1}, \ldots, \xi_{s_{w_G}}\}$.

Furthermore, we will suppose that the entropies of the secrets are equal, i.e., $H(\xi_{s_1}) = \cdots = H(\xi_{s_{w_G}})$. The *weighted information ratio of a participant* v in a weighted secret sharing realizing graph G is $R_v = H(\xi_v)/H(\xi_{s_1})$.

We construct a weighted secret sharing on the above graph G_w. Let $\mathbb{F}$ be a finite field. Let $s_1, s_2 \in \mathbb{F}$ be two different secrets and $r_1, r_2, r_3 \in \mathbb{F}$ be three random field elements. The shares of the participants are the following:

Participant	u	v	w	s	x	y	z
Shares	$r_1 + s_1$, $r_2 + r_3$	$r_2 + s_2$, r_1, r_3	$r_3 + s_1$, $r_1 + r_2$	$r_1 + r_2 + r_3$	r_1	r_2	r_3

It is easy to check, that for all $e \in E$, the participants corresponding to e can recover $w_G(e)$ secrets, and independent vertex sets have no information about the secrets.

A graph decomposition for weighted graphs can be generalized in the following way

Definition 2.4. Let $G = (V, E)$ be a graph. A λ-weighted decomposition of G consists of a collection of weighted graphs $\{G_1, ldots, G_k\}$ such that the following requirements are satisfied:

(1) G_i is a subgraph of G for $1 \leq i \leq k$.
(2) For each $e \in E$, there exist $s, i_1, \ldots, i_s \in \mathbb{Z}^+$ with $1 \leq i_1 < \cdots < i_s \leq k$ such that $\sum_{j=1}^{s} w_{G_{i_j}}(e) \geq \lambda$.

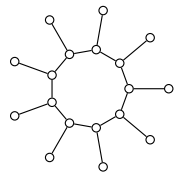
We will use the following generalization of the decomposition theorem of Stinson for weighted secret sharing schemes:

Theorem 2.5 (Weighted decomposition theorem, Sun and Chen 2002)**.** *Let G be a graph of access structure on n participants, and suppose that $\{G_1, \ldots, G_t\}$ is a λ-weighted decomposition of G. Assume that for each weighted graph G_i there exists a perfect secret sharing scheme with weighted information ratio $R_{v,i}$ for each $v \in V$. Then there exists a perfect secret sharing scheme S for G with information ratio*

$$\sigma_S(G) = \max_{v \in V} \sum_{i=1}^{t} \frac{R_{v,i}}{\lambda}.$$

2.2. n-sunlet graphs

Let C_n denote the cycle of length n and let S_n denote the n-sunlet graph on $2n$ vertices composed of a cycle C_n and a 1-factor between the vertices of the cycle and the remaining independent vertices. See the following example of the 9-sunlet graph S_9 as an illustration:



Solving the LP of the entropy method gives 2 as a lower bound for S_4. We prove that the information ratio is 2 for S_n if $n \geq 4$.

Theorem 2.6. *$\sigma(S_n) = 2$ for every $n \in \mathbb{N}, n \geq 4$.*

Proof. To prove the statement, we have to prove that 2 is both the upper and the lower bound. First we prove the upper bound. We give a graph covering of S_n with complete bipartite graphs, such that all edges ate covered once and all

vertices are covered at most twice. Let $u_1, \ldots, u_n$ denote the vertices of the cycle of S_n and $v_1, \ldots, v_n$ denote the leaf vertices such that u_i and v_i are adjacent.

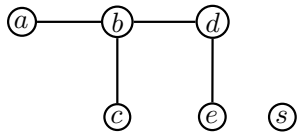
Cover the vertex set $\{u_i, u_{i+1}, v_{i+1}\}$ with a path of length two for all $1 \leq i \leq n$ (i.e., with special complete bipartite graphs). It is easy to see that all edges are covered exactly once, the vertices of the cycle are covered twice and the leaf vertices are covered once.

Let us note, that it is easy to construct a covering yielding the same upper bound for any unicycle graphs, i.e., graphs containing only one cycle.

To prove the lower bound we use the entropy method. First, a simple argument for a small subgraph of S_n is needed:

Lemma 2.7. *Let f be a real valued function satisfying the Shannon inequalities, and let G be the graph on vertices $\{a, b, c, d, e, s\}$ and edges $\{ab, bc, bd, de\}$. Then $f(ab) + f(ds) + f(c) + \geq f(ac) + f(s) + 4$.*

P r o o f. We will use the appropriate combination of the Shannon inequalities described in 1. We present the respective graph here to facilitate the check of the properties



Note that the assumptions of the strong monotonicity property are fulfilled twice, hence we get:

$$f(acdes) \geq f(aces) + 1,$$

$$f(abcds) \geq f(acds) + 1.$$

On the other hand, from the strong submodularity for two subsets of vertices, we get:

$$f(abcs) + f(bds) \geq f(bs) + f(abcds) + 1,$$

$$f(ab) + f(bc) \geq f(b) + f(abc) + 1.$$

Finally, four instances of the submodularity property give

$$f(acds) + f(aces) \geq f(acs) + f(acdes),$$

$$f(abc) + f(acs) \geq f(ac) + f(abcs),$$

$$f(bs) + f(ds) \geq f(s) + f(bds),$$

$$f(b) + f(c) \geq f(bc).$$

The addition of the above eight inequalities gives the statement of the lemma. □

Second, by applying Lemma 2.7 for vertices $u_i, u_{i+1}, v_{i+1}, u_{i+2}, v_{i+2}, v_{i+3}$, we get:

$$f(u_iu_{i+1}) + f(u_{i+2}v_{i+3}) + f(v_{i+1}) \geq f(u_iv_{i+1}) + f(v_{i+3}) + 4.$$

The sum of the inequalities for all $1 \leq i \leq n$ yields:

$$\sum f(u_iu_{i+1}) + \sum f(u_iv_{i+1}) + \sum f(v_i) \geq \sum f(u_iv_{i+1}) + \sum f(v_i) + 4n,$$

$$\sum f(u_iu_{i+1}) \geq 4n.$$

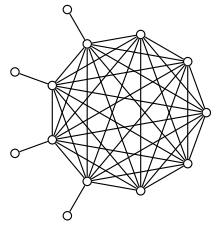
Using the fact that $f(u_i) + f(u_{i+1}) \geq f(u_iu_{i+1})$, we get:

$$2\sum f(u_i) \geq 4n.$$

So there exists a vertex u_i such that $f(u_i) \geq 2$, which completes the proof. □

2.3. Weighted graphs

Let K_n^l denote a graph on $n + l$ vertices composed of a complete graph on n vertices and a one-factor between any l of its vertices and the remaining l independent vertices. Consider K_9^4 as a simple example:

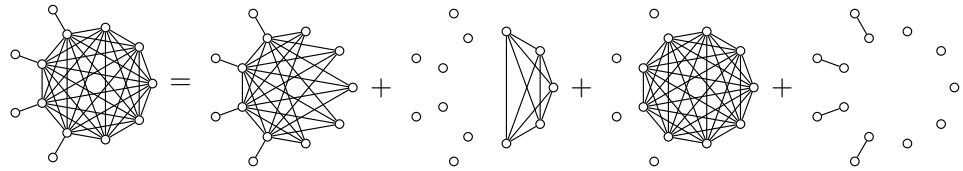


Prior to the main theorem of this section, we present a general result, which is interesting on its own:

Lemma 2.8. *Let G be the graph K_{l+1}^l for $l \geq 1$. If $\sigma(G) \leq c$, then $\sigma(K_n^l) \leq c/2 + 1$ for $n \geq l + 2$.*

Proof. Using the optimal secret sharing scheme of K_{l+1}^l with information ratio c we will construct a secret sharing for K_n^l with information ratio $c/2 + 1$.

Construct a graph G_1 with $n + l$ vertices. Start with a K_{l+1}^l, let w be the vertex of degree l. Add $n-l-1$ distinct samples of w to the graph. G_2 is a K_{n-l} on the $n-l$ samples of w. G_3 is a K_n on the vertices of degree at least l, and G_4 is a 1-factor between the leaves and the vertices of the original K_{l+1}^l. K_n^l can be covered with G_1, G_2, G_3 and G_4 such that each edge is covered exactly twice, see the following illustration of the decomposition:



It is easy to check that if we use the optimal secret sharing for G_1, G_2, G_3, G_4, then the leaves are covered twice, and all the other vertices are covered $c+2$ times. Hence the information ratio for K_n^l is at most $c/2+1$. □

Remark 2. A simple consequence of Lemma 2.8 is that if the information ratio is smaller than 2 for K_{l+1}^l, then it is smaller than two for K_n^l if $n \geq l$.

Theorem 2.9. *$\sigma(K_n^l) < 2$ for every $n, l \in \mathbb{N}, l \leq 4, l \leq n$.*

Proof. We can prove different bounds for different values of the parameter l . For $l = 0$ we get the case of complete graphs having information ratio equal to 1. The case $l \geq 1$ is detailed in several lemmas.

Lemma 2.10. *$\sigma(K_n^1) = 3/2$ for every $n \geq 3$.*

Proof. The information ratio of K_3^1 is $3/2$, and K_n^1 contains K_3^1 as an induced subgraphs, hence $\sigma(K_n^1) \geq 3/2$. The information ratio of K_2^1 is 1, and Lemma 2.8 gives a secret sharing scheme with information ratio $1/2 + 1 = 3/2$. □

Lemma 2.11. *$\sigma(K_2^2) = \sigma(K_3^2) = 3/2$, and $\sigma(K_n^2) = 7/4$ if $n \geq 4$.*

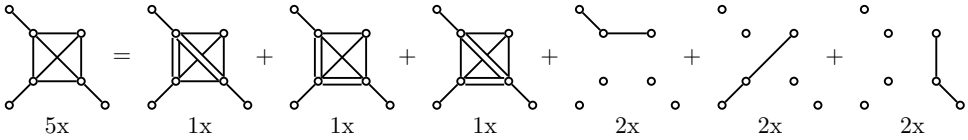
Proof. The case of $K_{3,2}$ was solved by Stinson [17]. Solving the LP problem, we get that $\sigma(K_4^2) = 7/4$, which gives the lower bound $7/4$ for K_n^2 $n \geq 4$.

Using the fact that the information ratio of K_3^2 is $3/2$, Lemma 2.8 proves that for $n \geq 4$, $\sigma(K_n^2) \leq (3/2)/2 + 1 = 7/4$ which gives the upper bound. □

Lemma 2.12. *$\sigma(K_3^3) = 7/4$, $7/4 \leq \sigma(G_4^3) \leq 9/5$, $9/5 \leq \sigma(K_n^3) \leq 19/10$ if $n \geq 5$.*

Proof. Sun and Chen [19] showed that $\sigma(K_3^3) = 7/4$. Solving the LP problem, we get the lower bounds $\sigma(K_4^3) \geq 7/4$, and $\sigma(K_n^3) \geq 9/5$, $n \geq 5$.

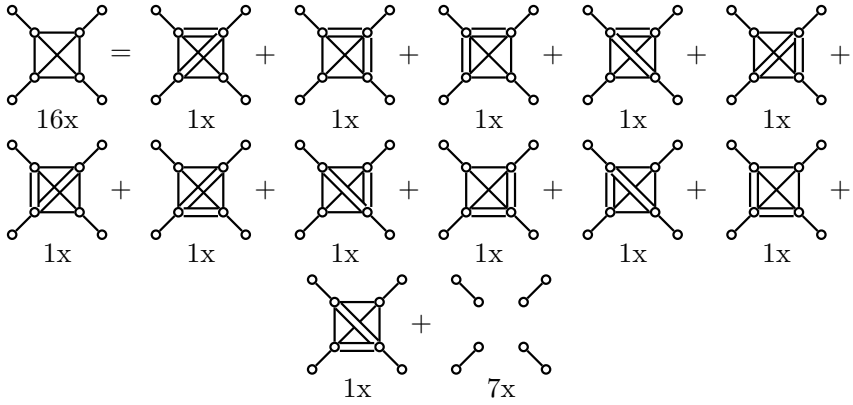
Let the vertex set and the edge set of K_4^3 be $V = \{u, v, w, s, x, y, z\}$, and $E = \{uv, uw, us, vw, vs, ws, ux, vy, wz\}$, respectively. We give a 5-weighted decomposition of K_4^3. G_1, G_2, G_3 are three slightly different samples of the weighted graph G_w, such that the 2-weighted edges are $\{uv, uw\}$, $\{uv, vw\}$ and $\{uw, vw\}$, respectively. The other graphs in the weighted decomposition are just stars with two edges: $\{ux, us\}$, $\{vy, vs\}$, $\{wz, ws\}$, two of each of them, see the following figure as an illustration of the decomposition:



It is easy to see, that this is a 5-weighed decomposition of G_4^3 indeed. If we use the weighted secret sharing scheme on G_w we have shown before, and the optimal secret sharing schemes for the stars, then the weighted information ratios in the weighted decomposition for u, v, w are $3, 2, 2, 2, 0, 0$, for s are $1, 1, 1, 2, 2, 2$, and for x, y, z are $1, 1, 1, 2, 0, 0$ in some order. Then by the weighted decomposition theorem there exists a secret sharing on K_4^3 with information ratio $9/5$. □

Lemma 2.13. *$15/8 \leq \sigma(K_4^4) \leq 31/16$, $15/8 \leq \sigma(K_5^4) \leq 49/25$, and $31/16 \leq \sigma(K_n^4) \leq 99/50$ if $n \geq 6$.*

P r o o f. Solving the LP problems in the entropy method gives the lower bounds $15/8 \leq \sigma(K_4^4)$, $15/8 \leq \sigma(K_5^4)$ and $31/16 \leq \sigma(K_n^4)$ for $n \geq 6$. Let $K_4^4 = (V, E)$, with $V = \{u, v, w, s, x, y, z, t\}$, and $E = \{uv, uw, us, vw, vs, ws, ux, vy, wz, st\}$. We give a 16-weighted decomposition of K_4^4. Consider all twelve different weighted subgraphs of K_4^4 isomorphic to G_w, and the edges ux, vy, wz, st, 7 of each of them.



It is easy to check that both the edges of the K_4 and the leaf edges are covered 16 times. The weighted graphs cover the leaves 9 times, and the vertices of the K_4 24 times, hence all the vertices are covered at most 31 times. This proves that $31/16$ is an upper bound indeed.

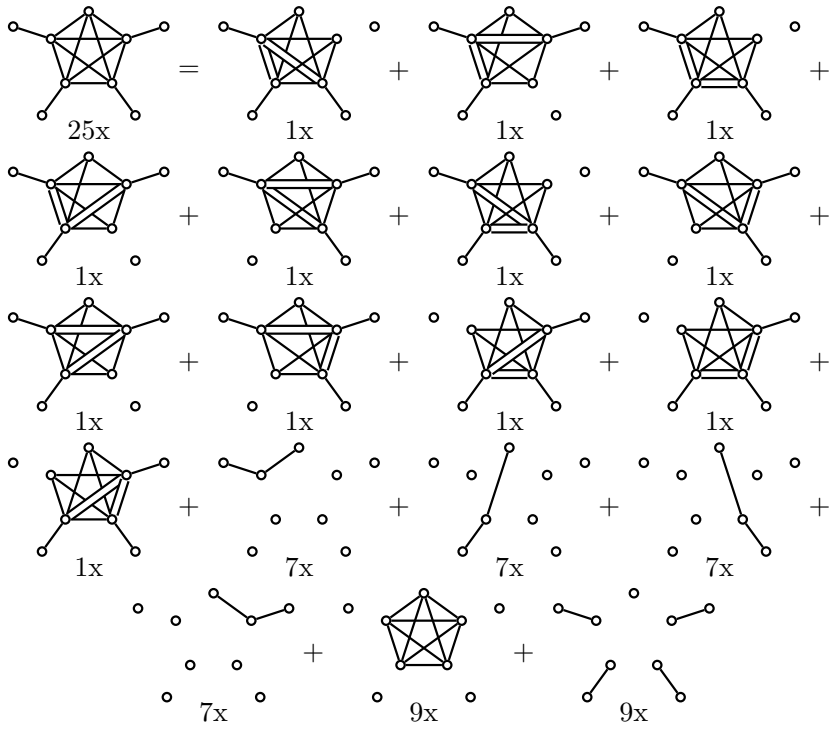
A similar but more complicated construction gives the upper bound $49/25$ for K_5^4, the construction can be found in Appendix A. Lemma 2.8 proves that $99/50$ is an upper bound for K_n^4, $n \geq 6$. □

Lemmas 2.10, 2.11, 2.12 and 2.13 together finish the proof of the theorem. □

3. Conclusion

We examined the information ratio of two graph classes with many leaves, the sunlet graphs and complete graphs with leaves. In the case of the sunlet graphs, the upper bound was trivial, and the lower bound was tricky, however in the case of the complete graphs with leaves, the lower bound was just calculated with the LP, and the secret sharing constructions were harder to find. In the former we used the usual entropy method. In the latter we defined a new weighted graph and used the weighted graph decomposition from S u n and C h e n [19].

Appendix A. Decomposition of K_5^4



REFERENCES

[1] BLAKLEY, G. R.: *Safeguarding cryptographic keys.* In: Proc. of the Nat. Comp. Conf. Vol. 48, 1979, pp. 313–317.

[2] BLUNDO, C.—DE SANTIS, A.—DE SIMONE, R.—VACCARO, U.: *Tight bounds on the information rate of secret sharing schemes*, Des. Codes Cryptogr. **11** (1997), 107–122.

[3] BLUNDO, C.—DE SANTIS, A.— STINSON, D. R.—VACCARO, U.: *Graph decomposition and secret sharing schemes*, J. Cryptology **8** (1995), no. 1, 39–64.
[4] BRICKELL, E. F.—STINSON, D. R.: *Some improved bounds on the information rate of perfect secret sharing schemes*, J. Cryptology **5** (1992), 153–166.
[5] CSIRMAZ, L.: *Secret sharing schemes on graphs*, Studia Sci. Math. Hungar. **44** (2007), 297–306.
[6] ——— *An impossibility result on graph secret sharing*, Des. Codes Cryptogr. **53** (2009), no. 3, 195–209.
[7] CSIRMAZ, L.—LIGETI, P.: *On an infinite family of graphs with information ratio* $2–1/k$, Computing **85** (2009), 127–136.
[8] ——— *Secret sharing on large girth graphs*, Cryptogr. Commun. (2018); https://doi.org/10.1007/s12095-018-0338-x
[9] CSIRMAZ, L.—TARDOS, G.: *Optimal information rate of secret sharing schemes on trees*, IEEE Trans. Inform. Theory **59** (2013), no. 4, 2527–2630.
[10] DEHKORDI, M. H.—SAFI, A.: *The complexity of the connected graph access structure on seven participants*, J. Math. Cryptol. **11** (2017), no. 1, 25–35.
[11] FARRÀS, O.—KACED, T.— MARTIN, S.—PADRÓ, C.: *Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing*, Report 2017/919,2017, Cryptology ePrint Archive, https://eprint.iacr.org/2017/919
[12] HARSÁNYI, K.—LIGETI, P.: *Exact information ratios for secret sharing on small graphs with girth at least 5*, J. Math. Cryptol. (2019) https://doi.org/10.1515/jmc-2018-0024
[13] JACKSON, W.—MARTIN, K. M.: *Perfect secret sharing schemes on five participants*, Des. Codes Cryptogr. **9** (1996), 233–250.
[14] SHAMIR, A.: *How to share a secret*, Commun. ACM **22** (1979), 612–613.
[15] SONG, Y.—LI, Z.—LI, Y.—XIN, R.: *The optimal information rate for graph access structures of nine participants*, Front. Comput. Sci. **9**, (2015) no. 5, 778–787.
[16] SONG, Y.—LI, Z.— WANG, W.: *The information rate of secret sharing schemes on seven participants by connected graphs*. In: *Recent Adv. in CSIE Vol. 4* (Z. Quian et al, eds.), *Lecture Notes in Electrical Engnr.* Vol. 127 (2012), pp. 637–645.
[17] STINSON, D. R.: *New general lower bounds on the information rate of secret sharing schemes*. In: *Advances in Cryptology—CRYPTO '92*, *Lecture Notes in Comput. Sci.* Vol. 740, 1993, pp. 168–182.
[18] ——— *Decomposition construction for secret sharing schemes*, IEEE, Trans. Inform. Theory **40** (1994), no. 1, 118–125.
[19] SUN, H. L.—CHEN, B. L.: *Weighted decomposition construction for perfect secret sharing schemes*. Comput. Math. Appl. **43** (2002), no. 6–7, 877–887.
[20] VAN DIJK, M.: *On the information rate of perfect secret sharing schemes*, Des. Codes Cryptogr. **6** (1995) no. 2, 143–169.
[21] WANG, W.—LI, Z.—SONG, Y.: *The optimal information rate of perfect secret sharing schemes*. In: *International Conference on Business Management and Electronic Information* Vol. 2, IEEE, 2011, pp. 207–212.

Received August 31, 2018

3in Research Group
Faculty of Informatics
Eötvös Loránd University
Budapest, Martonvásár
HUNGARY
E-mail: gyarmati93mate@gmail.com
turul@cs.elte.hu