Research Article

Károly Harsányi and Péter Ligeti*

Exact information ratios for secret sharing on small graphs with girth at least 5

https://doi.org/10.1515/jmc-2018-0024
Received March 8, 2017; revised January 28, 2019; accepted January 29, 2019

Abstract: In a secret-sharing scheme, a piece of information – the secret – is distributed among a finite set of participants in such a way that only some predefined coalitions can recover it. The efficiency of the scheme is measured by the amount of information the most heavily loaded participant must remember. This amount is called information ratio, and one of the most interesting problems of this topic is to calculate the exact information ratio of given structures. In this paper, the information ratios of all but one graph-based schemes on 8 or 9 vertices with a girth at least 5 and all graph-based schemes on 10 vertices and 10 edges with a girth at least 5 are determined using two polyhedral combinatoric tools: the entropy method and covering with stars. Beyond the investigation of new graphs, the paper contains a few improvements and corrections of recent results on graphs with 9 vertices. Furthermore, we determine the exact information ratio of a large class of generalized sunlet graphs consisting of some pendant paths attached to a cycle of length at least 5.

Keywords: Information ratio, graph covering, secret sharing

MSC 2010: 94A60, 05C6

Communicated by: María González Vasco

1 Introduction

1.1 Motivation and notion

A secret-sharing scheme is a method of distributing secret data among a set of *participants* $\mathcal{P}$ so that only specified *qualified subsets* of participants are able to recover the secret. In addition, if the unqualified subsets collectively yield no extra information, i.e., the joint shares are statistically independent of the secret, then the scheme is called *perfect*. The description of qualified subsets among all possible subsets of participants is the *access structure*, denoted by $\mathcal{A}$. This family of subsets is supposed to be *monotone* in the sense that every superset of a qualified subset is qualified as well; hence every access structure can be determined by its *minimal* qualified subsets, denoted by $\min \mathcal{A}$. A well-studied special case is the so-called *graph-based secret sharing*, where the size of the minimal qualified subsets is two. In this case, every participant corresponds to a vertex of a graph, and a subset of participants is qualified if there is some edge between the respective vertices.

The most frequently investigated property is the efficiency of the system: how many bits of information the participants must remember for each bit of the secret in the worst case. This amount is the worst-case *information ratio* of the system. Note that the information ratio is the reciprocal of the information rate,

Károly Harsányi, Machine Perception Research Laboratory, Institute for Computer Science and Control, Hungarian Academy of Sciences, Budapest, Hungary, e-mail: harsanyika@gmail.com
***Corresponding author: Péter Ligeti,** Department of Computeralgebra, Faculty of Informatics, Eötvös Loránd University, Budapest, Hungary, e-mail: turul@cs.elte.hu. http://orcid.org/0000-0002-3998-0515

another widely used parameter of a system. One of the most challenging problems in the topic of secret sharing is to determine or at least estimate the information ratio of given structures. In this paper, the exact information ratio for a new family of graphs is determined based on the test results computed for small graphs.

1.2 Related work

Secret sharing was first introduced in two independent papers: a simple construction from Shamir [17] using Lagrangian interpolation and another composition from Blakley [2] based on the intersection properties of the hyperplanes of a finite-dimensional vector space. Both constructions are so-called *k-threshold schemes*, where the qualified subsets are exactly the subsets of participants of cardinality at least k.

Many papers on the subject of information ratio examine in some sense "small" systems. Jackson and Martin [13] and van Dijk [22] considered the case of $\mathcal{P} = 5$ and $\mathcal{P} = 6$, respectively (i.e., the vertex set of the hypergraph is small). Martí-Farré, Padró and Vázquez [15, 16] examined the cases when there are 3 or 4 minimal qualified subsets. The exact information ratio for several graph-classes is determined, like hypercubes [6], trees [9], recursive constructions [3] or graphs with large girth and no adjacent vertices of high degree [7]. Furthermore, the case of small graphs (i.e., small number of vertices) is examined in several papers: the information ratio has been computed for most graphs with at most 6 vertices [4, 5, 13, 21, 22], for some graphs with 7 vertices [12, 19, 23], as well as for all graphs with 9 vertices and 8 or 9 edges [18]. However, some of the results in [18] contradict [7, 9] and the results of this paper. The case of graphs with 10 vertices is an open problem currently. On the other hand, there is a rich literature of asymptotic results on secret sharing; see [1, 8, 10].

In this paper, we use two main tools for studying bounds for the information ratio: the *entropy method* for lower bounds and *covering with stars* for upper bounds. In practice, both of these methods have limitations. The entropy method has an extremely high computational requirement for graphs with a large number of vertices, and the star covering is known to produce secret-sharing schemes with high ratios compared to the exact information ratio, especially for dense graphs (i.e., graphs with a large number of edges); see Beimel, Farràs and Mintz [1]. In order to bypass these limitations, we examine graphs with small vertex set and without small circles: graphs on 8 or 9 vertices and graphs on 10 vertices and 10 edges, with a girth of at least 5. We present the exact information ratio for all but one graph in these graph families; see Section 2.5. Note that the information ratio of several graphs from these families was examined earlier since they intersect with the group of graphs examined in [7]. Here we present the graphs with previously unknown information ratios only.

Additionally, we determine the exact information ratio for a new family of graphs suggested by the above results for small graphs. Since the information ratio of trees was determined in [9], the next step is to examine unicyclic graphs, which are not covered in other papers, like [7]. This problem is very hard to handle in general; however, some regularity can be observed for a particular graph class of the examined small graphs. Based on these observations, the exact information ratio of generalized sunlet graphs is determined. These graphs are special unicyclic graphs containing only one cycle and pendant paths attached to some but not all vertices of the cycle.

2 Information ratio of graph based schemes

2.1 Definitions

In this section, we describe the precise definitions used in the paper.

Definition 1. A finite set $\mathcal{P}$ on n elements is called the set of *participants*. Let $\mathcal{A} \subseteq 2^{\mathcal{P}}$ be a monotone increasing set of subsets. $\mathcal{A}$ is called an *access structure*, and the elements of $\mathcal{A}$ are the *qualified subsets*.

Every access structure is monotone increasing; hence its minimal elements describe the whole structure. $\mathcal{A}$ is called *graph-based access structure* if every minimal qualified subset has two elements; then $\mathcal{A}$ can be described by the graph $G = (\mathcal{P}, \min \mathcal{A})$.

Note that a secret-sharing scheme is a method for distributing some secret information amongst the participants such that it can be reconstructed by the qualified subsets only.

Definition 2. A *perfect secret sharing* $\mathcal{S}$ realizing the access structure $\mathcal{A}$ is an $(n+1)$-tuple $(\xi_1, \dots, \xi_n, \xi_s)$, where ξ_i for every $i \in \mathcal{P}$ and ξ_s are random discrete variables 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.

(To avoid trivial cases, we always assume the secret ξ_s is not constant with probability 1.)

Suppose that the discrete random variable ξ has m different values $x_1, \dots, x_m$ with probabilities $p_i = \Pr(\xi = x_i)$ for $i = 1, \dots, m$. The size of ξ is measured by its *Shannon entropy*, or information content, and is traditionally denoted by $\mathbf{H}(\xi) = -\sum_i p_i \log_2 p_i$.

As we noted above, the information ratio measures the ratio between the largest size of the information of participants and the size of the secret.

Definition 3. The *information ratio* of an access structure $\mathcal{A}$ is

$$c(\mathcal{A}) = \inf_{\mathcal{S}} \max_{i \in \mathcal{P}} \frac{\mathbf{H}(\xi_i)}{\mathbf{H}(\xi_s)},$$

where the infimum is taken over all perfect schemes $\mathcal{S}$ realizing $\mathcal{A}$. For graph-based access structures, the notation $c(G)$ is used.

2.2 Lower bound

For each subset A of the participants, one can define the real-valued function f as

$$f(A) = \frac{\mathbf{H}(\{\xi_i : i \in A\})}{\mathbf{H}(\xi_s)},$$

where $\mathbf{H}$ is the Shannon entropy. Clearly, the information ratio is the maximal value in $\{f(i) : i \in \mathcal{P}\}$, while the average information ratio is the average of these values. Using the standard properties of the entropy function, the following so-called *Shannon inequalities* hold for all subsets A, B of the participants:
(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 a qualified set and B is not, then $f(A) + 1 \leq f(B)$ (strong monotonicity);
(e) if neither A nor B is qualified but $A \cap B$ is so, then $f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$ (strong submodularity).

The *entropy method* (see, e.g., Blundo et al. [4]) can be rephrased as follows: 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 (worst-case) information ratio is also at least r. This means that the solution of the LP problem arising from all the Shannon inequalities yields a lower bound for the information ratio of a system. Unfortunately, the size of this LP problem can be too large to solve it, even in the case of few participants. Hence one needs to reduce the number of the inequalities by identifying some adequate structural properties of the graph. Let us mention that, in the case of up to 10 vertices, like in Figures 1, 2 and 3, these kinds of tricks are not necessary because of the small vertex set.

However, we prove bounds for a large graph class in Section 2.4; hence some sophisticated methods are required. Here we present two necessary known results without proofs only. For the rest of the paper, let f be a real-valued function satisfying the properties (a)–(e) above. The first lemma on a connected vertex set can be found in [9].

Lemma 2.1. *Let A be a connected subset of vertices of G. Then*

$$\sum_{v\in A} f(v) \geq f(A) + |A| - 2.$$

The second useful result is the so-called *independent sequence method* of [3, 6].

Lemma 2.2. *Let A be a connected subset of vertices with $|A| \geq 2$, and let B be an independent subset of vertices of G such that there exist a 1-factor from B to A. Then*

$$f(A) \geq |B| + 1.$$

2.3 Upper bound

As a consequence of the pioneering work of Stinson [20], every covering of the graph G with complete multipartite graphs yields an upper bound for the information ratio, i.e., if there is a covering such that every vertex is covered by at most p graphs and every edge is covered by at least e graphs, then the information ratio is at most p/e. Stinson proved the general upper bound $\frac{\max d(v)+1}{2}$ by covering with stars. As a consequence of the result of Erdős and Pyber [10], the information ratio of any graph is at most $O(n/\log n)$ based on a covering with complete bipartite graphs. Csirmaz, Ligeti and Tardos [8] generalized the theorem to uniform hypergraphs using covering with complete multipartite graphs. Note that this technique is not universal; see [1, 8] for the limitations of the covering method.

In order to provide upper bounds, we present a construction in the special case of the covering with stars (i.e., with graphs having all but one vertex of degree one, which is a special complete bipartite graph). Recent studies suggest that upper bounds generated by graph coverings are often far from the optimal information ratio [1]. However, star covering was successfully utilized to determine the optimal information ratio for relatively sparse families of graphs (i.e., graphs with a small number of edges) like trees [9] and graphs with large girth [7]. Note that the different degree-one neighbors of a given vertex are equivalent from the secret-sharing point of view. Hence, if there are at least two leaves adjacent to a given vertex, then we can reduce the graph by deleting all but one of these leaves.

Star covering can be rephrased as an LP problem. Let us recall the formal description from [7]. Note that introducing fractional covering, instead of $p, e \in \mathbb{N}$, we can suppose that $e = 1$ and $p \in \mathbb{Q}$. The rephrased linear program is the following:

- *Variables*:
  - p (a global variable): the maximal number of covering of the vertices,
  - x_{uv}, x_{vu} for every edge $uv \in E$: the number of u-stars or v-stars containing uv,
  - l_v for every vertex $v \in V$: the number of v-stars;
- *LP problem*:

$$\min p \quad \text{subject to} \quad \begin{cases} x_{uv} + x_{vu} \geq 1 & \text{for every } uv \in E, \\ l_u + \sum_{uv\in E} x_{vu} \leq p & \text{for every } u \in V, \\ x_{uv} \leq l_u & \text{for every } u \in V,\ uv \in E. \end{cases}$$

The LP problem has two main advantages: The size of the 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 reconstructed from the optimal solution of the LP easily.

In the following figures, we present the collection of the new graphs with exact information ratio: 12 graphs on 8 vertices with 8 edges, 19 graphs on 9 vertices with 9 edges, 22 graphs on 9 vertices with 10 edges, 8 graphs on 9 vertices with 11 edges and 50 graphs on 10 vertices with 10 edges. In [18], graphs with 9 vertices and 9 edges were previously examined, but, for 20 of these graphs, the information ratios were not correctly determined. These graphs can be reduced to 12 graphs by deletion of multiple leaves. We marked our results on these graphs with *.

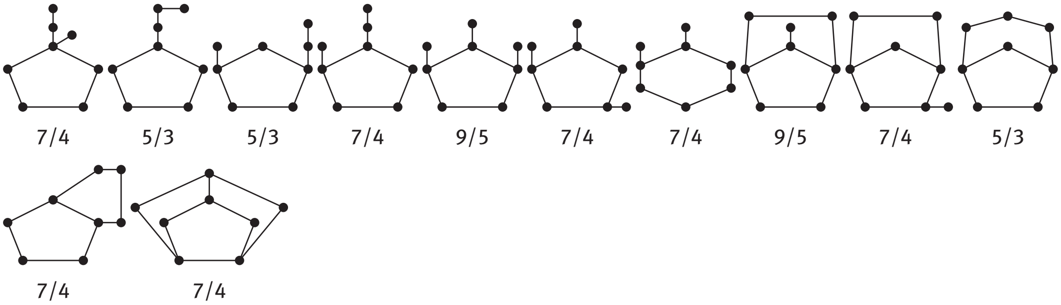


Figure 1: Graphs on 8 vertices.

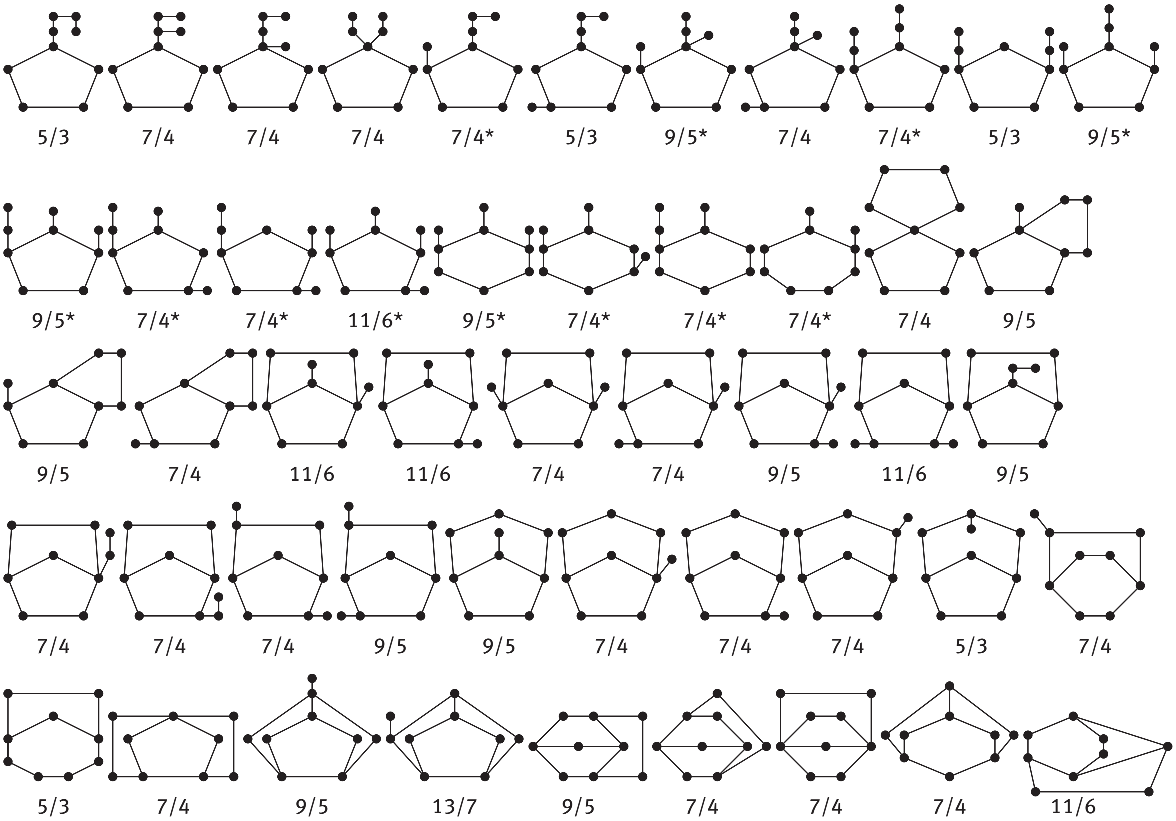
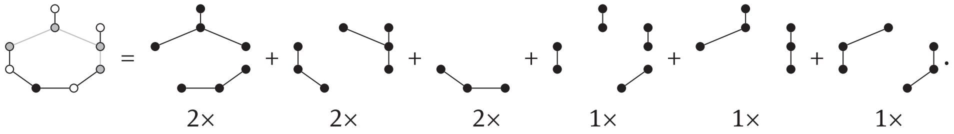


Figure 2: Graphs on 9 vertices.

Here we present the analysis of an example in detail. Let the gray vertices be a connected set A, and let the empty ones be an independent set B. Then there is a 1-factor from A to B; hence, from Lemma 2.1 and Lemma 2.2, we get a 7/4 lower bound. On the other hand, the following star covering yields the same upper bound, claiming that the information ratio of this graph is 7/4 in contrast with the 5/3 value reported in [18]:



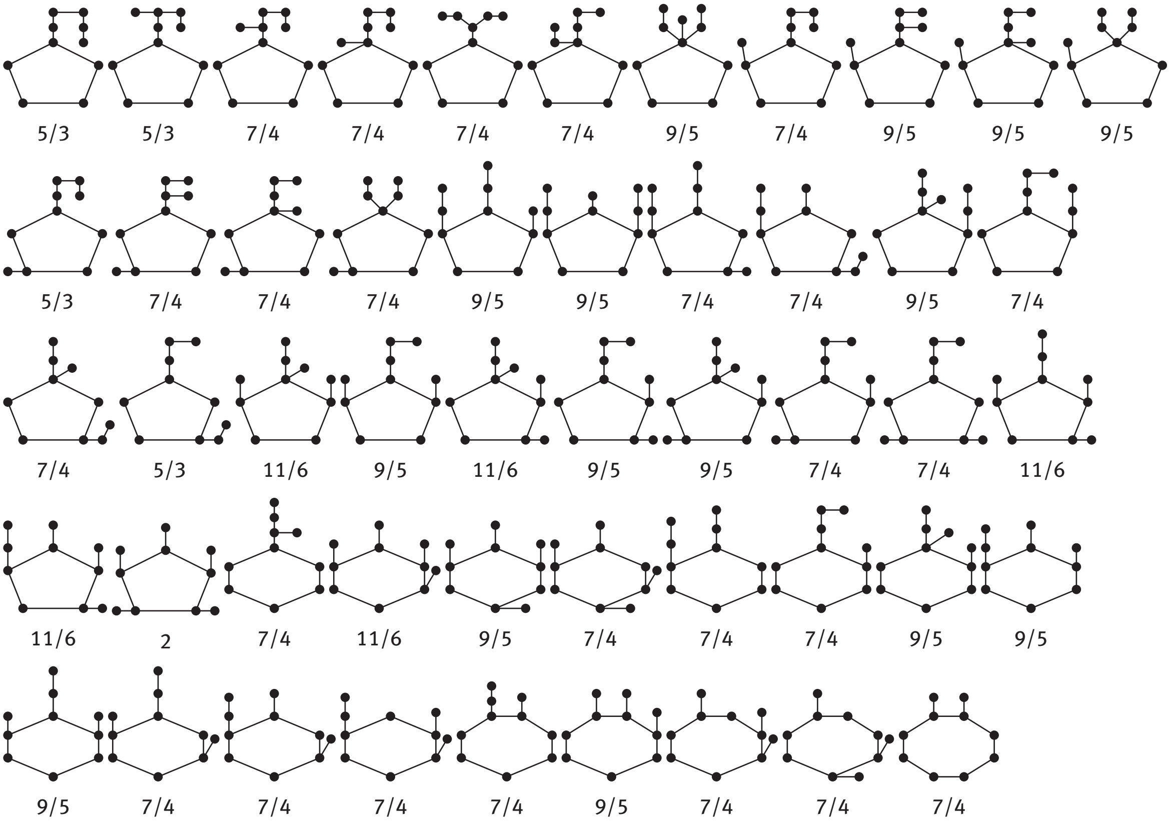


Figure 3: Graphs on 10 vertices.

2.4 Information ratio of generalized sunlet graphs

The next step is to find any connection between the structure of some reasonable family of the above graphs and its information ratio and conclude a general statement for this family of graphs. An obvious extension is the common generalization of some known result, namely, by allowing one cycle (in contrast with the case of trees [9]) and high-degree neighbors (in contrast with the graph-family examined in [7]). It is possible to identify a particular family of graphs fulfilling these assumptions. The *n-sunlet graph* is the graph on $2n$ vertices obtained by attaching one pendant edge to every vertex of a cycle of length n. Let us consider the following generalization of this notion: *generalized n-sunlet* is a graph obtained by attaching at most one pendant path to every vertex of a cycle of length n. Let a connected vertex set A of the cycle be called an *arc* of G if one path is attached to every vertex of A. The length of an arc A equals the number of edges of A. It is important to note that this definition includes arcs with length 0 (i.e., arcs containing only one vertex). See Figure 4 for an example of a generalized 12-sunlet graph with arcs of length 4, 1 and 0 highlighted in gray.

Lemma 2.3. *Let G be a generalized n-sunlet graph with a maximal arc of length $k \le n-2$. Then*

$$c(G) \le 2 - \frac{1}{k+3}.$$

Proof. The main idea of the proof is to use the decomposition technique of Stinson [20] by constructing a covering of G with directed stars such that the in-degrees of the leaves for every directed star are 1. Then the star covering number of a vertex is equal to the maximum number of outgoing edges and the sum of all incoming edges. Therefore, we replace every edge $e = \{u, v\}$ of G by $k+3$ directed edges, and the direction of the edges will be defined later depending on the degrees of the vertices incident. There are two general cases:

(i) If $\deg(v) = 1$, then take $k+3$ copies of (u, v).

(ii) If $\deg(u) = 2$, $\deg(v) = 3$, then take 1 copy of (u, v) and $k+2$ copies of (v, u).

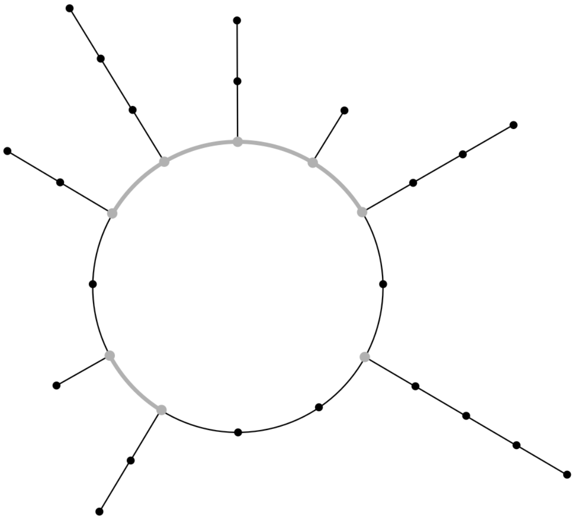


Figure 4: A generalized 12-sunlet graph.

The remaining two cases have two subcases based on the parity of the size of the maximal arc. Here we present the odd case in detail only; the even case is similar. Suppose that k is odd, and let $k + 3 = 2m$.

(iii) If $\deg(u) = \deg(v) = 2$, then take m copies of (u, v) and m copies of (v, u).

(iv) If $\deg(u) = \deg(v) = 3$, then this is an edge of an arbitrary arc A.

Let the *center* of an arc A be its middle vertex v_c if $|A|$ is even or its middle edge $e_c = \{v_{c_1}, v_{c_2}\}$ if $|A|$ is odd. The number of copies of the directed edges is based on the hop distance of the edge from the center. If $|A|$ is odd, then, in place of the center edge e_c, take m copies of (v_{c_1}, v_{c_2}) and m copies of (v_{c_2}, v_{c_1}). For all other edges, regardless of the parity of $|A|$, direct $m - x$ edges towards the center and $m + x$ edges outwards if the distance of the edge from the closest center vertex is x. See Figure 5 for an illustration of the direction of the edges.

Now we have to summarize the covering numbers of the edges and the vertices only. Every edge and 1-degree vertex is covered by $2m = k + 3$ directed stars. Every 2-degree vertex without a 3-degree neighbor is covered by $3m = 3/2(k + 1) + 3$ directed stars. Every 2-degree vertex with a 3-degree neighbor is covered by $4m - 1 = 2(k + 3) - 1$ stars. At last, every 3-degree vertex is covered by at most $4m - 1 = 2(k + 3) - 1$ stars. Then we are done if k is odd.

Now suppose that k is even, and let $k + 3 = 2m + 1$. We replace every edge $e = \{u, v\}$ with $2m + 1$ directed edges such that, if $\deg(u) = \deg(v) = 2$, then take $m + 1$ copies of (u, v) and m copies of (v, u), in contrast with case (iii). The corresponding case of direction of the edges of arcs is illustrated in Figure 6.

To demonstrate the constructed star covering, we include an example in Figure 7 of a generalized sunlet graph with maximal arc of length 5 (i.e., $k = 5$, $m = 4$). For instance, the vertex depicted by the white dot is covered by $7 + 1 + 5 + 2 = 15$ stars.

Similarly as above, all edges are covered by $2m + 1 = k + 3$ directed stars, and all vertices are covered by at most $4m - 1 = 2(k + 3) - 1$ directed stars, which completes the proof. □

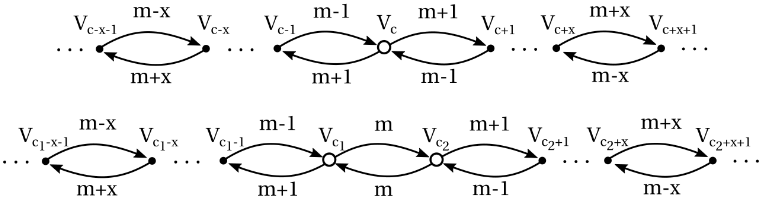


Figure 5: The direction of edges in even and odd arcs, respectively, when k is odd.

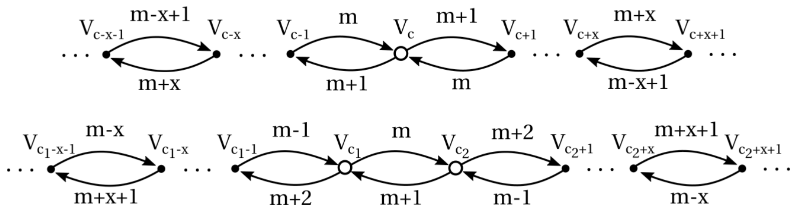


Figure 6: The direction of edges in even and odd arcs, respectively, when k is even.

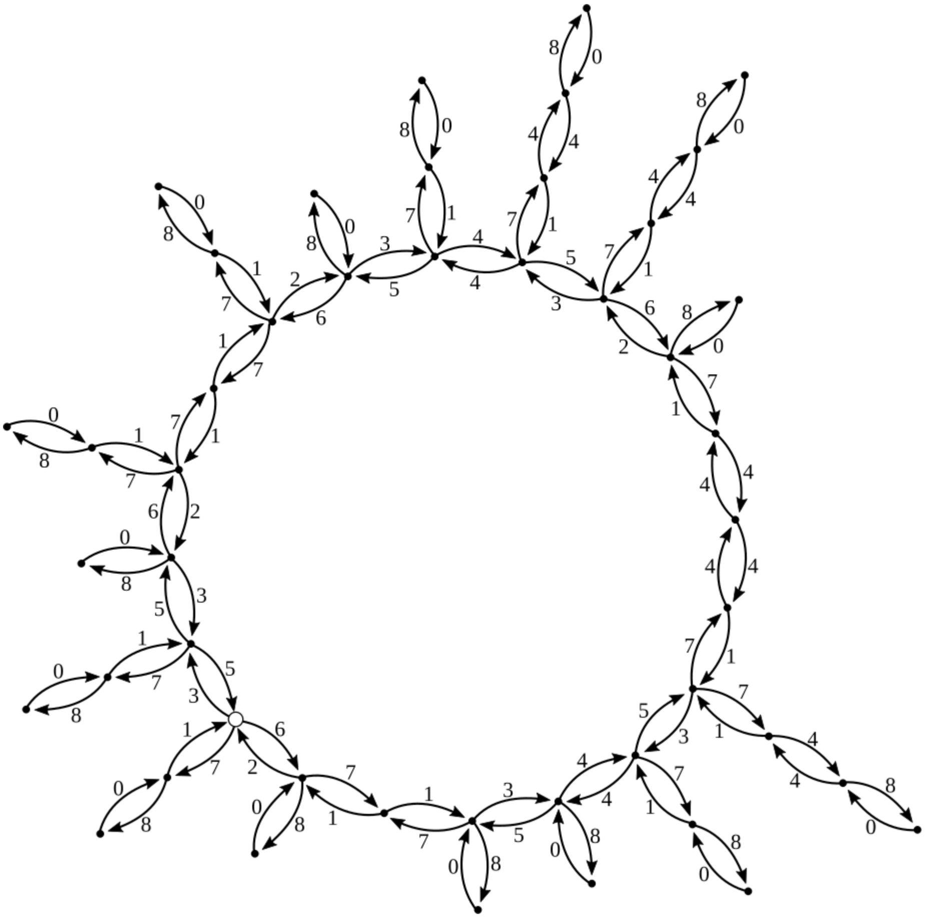


Figure 7: The star covering of a generalized sunlet graph with $k = 5$.

Lemma 2.4. *Let G be a generalized n-sunlet graph with a maximal arc of length $k \leq n - 6$. Then*

$$c(G) \geq 2 - \frac{1}{k+3}.$$

Proof. Let $C = (v_1, e_1, v_2, \ldots, v_n)$ be the cycle of the sunlet graph, and suppose that $A^* = (v_1, e_1, \ldots, v_{k+1})$ is a maximal arc. Then $A = \{v_n, v_1, v_2, \ldots, v_{k+2}\}$ is a connected subset of G on $k + 3$ vertices. By applying Lemma 2.1, we get

$$\sum_{v \in A} f(v) \geq f(A) + k + 1. \tag{2.1}$$

Let u_i denote the neighbor of v_i on the path attached to v_i for $i = 1, \ldots, k + 1$. Then

$$B = \{u_1, \ldots, u_{k+1}\} \cup \{v_{n-1}, v_{k+3}\}$$

is an independent vertex set on $k + 3$ vertices since the paths are disjoint and v_{n-1} and v_{k+3} are not incident when $k \leq n - 6$. Furthermore, there is a trivial 1-factor from B to A.

Then, from Lemma 2.2, we get

$$f(A) \geq k + 4. \tag{2.2}$$

Adding up (2.1) and (2.2), we get $f(a) \geq 2 - \frac{1}{k+3}$ for some $a \in A$, which completes the proof by the entropy method. □

Lemma 2.3 and Lemma 2.4 yield the following theorem.

Theorem 2.5. *Let G be a generalized n-sunlet graph with a maximal arc of length $k \leq n - 6$. Then*

$$c(G) = 2 - \frac{1}{k+3}.$$

Note that, if the first and the last attached paths have length at least 2, then we can weaken the assumption for the size of the arc to $k \leq n - 4$ in Lemma 2.4. In this case, A can be augmented on the paths instead of on the cycle such that the respective B will form an independent set. However, the results of Figures 1, 2 and 3 suggest that the same lower bound holds for $k \leq n - 2$ as well; the general case the size of the independent set B is smaller, and hence we can prove a slightly weaker result only.

Theorem 2.6. *Let G be a generalized n-sunlet graph with a maximal arc of length $n - 3 \leq k \leq n - 5$. Then*

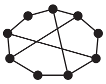
$$2 - \frac{1}{k+2} \leq c(G) \leq 2 - \frac{1}{k+3}.$$

If the length of a maximal arc is $k = n - 2$, then

$$2 - \frac{1}{k+1} \leq c(G) \leq 2 - \frac{1}{k+3}.$$

2.5 Discussion

As we noted above, we were unable to determine the exact information ratio for one graph with girth 5. In this case, there is a gap between the lower and upper bound. If one could calculate the information ratios of this graph, the description of the examined graph family would be complete:



$$11/6 \leq C \leq 2.$$

Our results suggest that the girth 5 is the limit of the star covering method. It is important to note that, for other families of graphs, new constructions and more powerful techniques are needed, like the use of non-Shannon information inequalities [11] for lower bounds, and other general techniques [14].

Note that there are 20 graphs with improved information ratios with regard to [18]. In fact, the authors determined smaller information ratios for these graphs, which is a consequence of some incorrect usage of the methods achieving upper bounds. In these cases, the authors used decomposition methods from [20, 21]; unfortunately, it is not possible to check how exactly. On the other hand, the lower bounds should have increased as well.

3 Summary

In this paper, the exact information ratio of all but two graph-based schemes up to 9 vertices or 10 vertices and 10 edges with girth at least 5 is determined using two polyhedral combinatoric methods: the entropy method and covering with stars. More precisely, the exact information ratio for 111 graphs are determined, 12 of them are improvements and corrections of recent results on graphs with 9 vertices [18]. Furthermore, the exact information ratios for a special graph-class of girth at least 5 is proved, namely, for a large family of generalized n-sunlet graphs with $n \geq 5$. This result can be considered as a common generalization of the known results for trees and graphs without high-degree neighbors.

Funding: This research has been partially supported by the ÚNKP-17-4 National Excellence Program of the Ministry of Human Capacities and the Lendület program of the Hungarian Academy of Sciences and by the Hungarian Government and co-financed by the European Social Fund, EFOP-3.6.3-VEKOP-16-2017-00001, Talent Management in Autonomous Vehicle Control Technologies.

References

[1] A. Beimel, O. Farràs and Y. Mintz, Secret sharing schemes for very dense graphs, in: *Advances in Cryptology—CRYPTO 2012*, Lecture Notes in Comput. Sci. 7417, Springer, Heidelberg (2012), 144–161.

[2] G. R. Blakley, Safeguarding cryptographic keys, in: *Proceedings of the 1979 AFIPS National Computer Conference*, IEEE Press, Piscataway (1979), 313–317.

[3] C. Blundo, A. De Santis, R. De Simone and U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, *Des. Codes Cryptogr.* **11** (1997), no. 2, 107–122.

[4] C. Blundo, A. De Santis, D. R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, *J. Cryptology* **8** (1995), no. 1, 39–64.

[5] E. F. Brickell and D. R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J. Cryptology* **5** (1992), no. 3, 153–166.

[6] L. Csirmaz, Secret sharing schemes on graphs, *Studia Sci. Math. Hungar.* **44** (2007), no. 3, 297–306.

[7] L. Csirmaz and P. Ligeti, On an infinite family of graphs with information ratio $2 - 1/k$, *Computing* **85** (2009), no. 1–2, 127–136.

[8] L. Csirmaz, P. Ligeti and G. Tardos, Erdős–Pyber theorem for hypergraphs and secret sharing, *Graphs Combin.* **31** (2015), no. 5, 1335–1346.

[9] L. Csirmaz and G. Tardos, Optimal information rate of secret sharing schemes on trees, *IEEE Trans. Inform. Theory* **59** (2013), no. 4, 2527–2530.

[10] P. Erdős and L. Pyber, Covering a graph by complete bipartite graphs, *Discrete Math.* **170** (1997), no. 1–3, 249–251.

[11] O. Farràs, T. Kaced, S. Martín and C. Padró, Improving the linear programming technique in the search for lower bounds in secret sharing, in: *Advances in Cryptology—EUROCRYPT 2018. Part I*, Lecture Notes in Comput. Sci. 10820, Springer, Cham (2018), 597–621.

[12] M. Hadian Dehkordi and A. Safi, The complexity of the connected graph access structure on seven participants, *J. Math. Cryptol.* **11** (2017), no. 1, 25–35.

[13] W.-A. Jackson and K. M. Martin, Perfect secret sharing schemes on five participants, *Des. Codes Cryptogr.* **9** (1996), no. 3, 267–286.

[14] T. Liu and V. Vaikuntanathan, Breaking the circuit-size barrier in secret sharing, in: *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing—STOC'18*, ACM, New York (2018), 699–708.

[15] J. Martí-Farré and C. Padró, Secret sharing schemes with three or four minimal qualified subsets, *Des. Codes Cryptogr.* **34** (2005), no. 1, 17–34.

[16] J. Martí-Farré, C. Padró and L. Vázquez, Optimal complexity of secret sharing schemes with four minimal qualified subsets, *Des. Codes Cryptogr.* **61** (2011), no. 2, 167–186.

[17] A. Shamir, How to share a secret, *Comm. ACM* **22** (1979), no. 11, 612–613.

[18] Y. Song, Z. Li, Y. Li and R. Xin, The optimal information rate for graph access structures of nine participants, *Front. Comput. Sci.* **9** (2015), no. 5, 778–787.

[19] Y. Song, Z. Li and W. Wang, The information rate of secret sharing schemes on seven participants by connected graphs, in: *Recent Advances in Computer Science and Information Engineering*, Springer, Berlin (2012), 637–645.

[20] D. R. Stinson, Decomposition constructions for secret-sharing schemes, *IEEE Trans. Inform. Theory* **40** (1994), no. 1, 118–125.

[21] H.-M. Sun and B.-L. Chen, Weighted decomposition construction for perfect secret sharing schemes, *Comput. Math. Appl.* **43** (2002), no. 6–7, 877–887.

[22] M. van Dijk, On the information rate of perfect secret sharing schemes, *Des. Codes Cryptogr.* **6** (1995), no. 2, 143–169.

[23] W. Wang, Z. Li and Y. Song, The optimal information rate of perfect secret sharing schemes, in: *International Conference on Business Management and Electronic Information. Vol. 2*, IEEE Press, Piscataway (2011), 207–212.