Discrete Applied Mathematics 304 (2021) 55–62

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

On the information ratio of graphs without high-degree neighbors

Máté Gyarmati, Péter Ligeti [*]

Department of Computeralgebra, Eötvös Loránd University, Budapest, Hungary

ARTICLE INFO

Article history:
Received 6 January 2021
Received in revised form 11 May 2021
Accepted 6 July 2021
Available online 28 July 2021

Keywords:
Secret sharing
Information ratio
Entropy method
Decomposition construction
Graph covering

ABSTRACT

We consider the information ratio of graph based secret sharing schemes in a special case of graphs in which vertices of degree at least 3 are not connected by an edge. We prove that – after some trivial reduction of the original graph – the information ratio depends on the maximal value of the difference of the degree and the number of triangles containing a given vertex of the reduced graph. This result can be considered as a common generalization of previous results on the information ratio of special trees and graphs of girth at least 6.

1. Introduction

Secret sharing schemes were first introduced in the breakthrough papers of Shamir [14] and Blakley [2] as a method to distribute some sensitive information among participants such that only fixed coalitions, called qualified subsets of participants are able to recover the secret. If the non-qualified subsets have no information about the secret, then the resulting scheme is a perfect secret sharing. The collection of the qualified subsets is called access structure. It is easy to see that any access structure is monotone increasing, hence the minimal elements are sufficient to describe the structure. We are interested in graph based schemes, where every minimal element of the access structure has exactly two elements. In this special case, for any given graph the vertices can be considered as the participants and some coalition of participants is qualified if the respective vertices span any edge.

The efficiency of a particular system can be measured by the amount of information the participants must remember per secret bit. The maximum of these values is called the worst-case information ratio of the scheme.

Determining the value of the information ratio is a very hard problem even for small graphs or for small access structures in general. The standard techniques as using the Shannon-inequalities for lower bound and linear secret sharing for upper bound are not sufficient in many cases. Csirmaz presented a graph family [5] with a gap between the best lower bound arises from using the LP technique for Shannon-inequalities (Shannon-complexity) and the linear complexity. Padro et al. [9] proved that there exist access structures and graphs where adding so-called non-Shannon inequalities yields strictly better lower bound for the linear complexity and the information ratio, respectively.

The exact value of information ratio is only known for small graphs and some infinite graph families. It is now determined for almost all graphs with six vertices [3,10,13,16,17]. For the remaining 4 graphs both the Shannon- and the linear complexities are known but there is a gap between these values, see [9,11]. There are some results on general families of graphs, like for trees [8], for d-dimensional cubes [6], d-dimensional cubes with leaves [12], for graphs with

[*] Corresponding author.
E-mail addresses: hairl1@inf.elte.hu (M. Gyarmati), ligetipeter@inf.elte.hu (P. Ligeti).

https://doi.org/10.1016/j.dam.2021.07.011

large girth and no high-degree neighbors [7]. Other significant results provide only upper bounds but for a wider range of graphs i.e. asymptotic upper bounds for very dense graphs [1] or upper bound based on highest degree [15].

Within this paper we determine the exact information ratio of an additional general graph-class, namely of graphs in which vertices of degree at least three are not connected by an edge. The known results on some trees [8] and large girth graphs [7] are special cases of this new result. We use Shannon-inequalities and linear secret sharing to provide lower and upper bounds respectively.

1.1. Notation and notion

Let V be a finite set of participants. The qualified coalitions are described by a monotone increasing set of subsets of V called the access structure $\mathcal{A}$.

Definition 1. A perfect secret sharing scheme S realizing $\mathcal{A}$ is a collection of random variables ξ_v for every $v \in V$ and ξ_s with a joint distribution such that

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

As a consequence of monotonicity, the minimal elements of $\mathcal{A}$ characterize the access structure. In a graph-based scheme every minimal qualified subset has two elements, i.e. the scheme can be represented by the graph $G = (V, \min \mathcal{A})$.

Definition 2. Let $G = (V, E)$ be a graph. Then the worst-case information ratio of G is

$$\sigma(G) = \inf_{S} \max_{v \in V} \frac{H(\xi_v)}{H(\xi_s)}$$

where $H(.)$ is the Shannon-entropy and the infimum is taken over all perfect secret sharing schemes $\mathcal{S}$ realizing G.

Notice that the average information ratio is considered in several works as well, however we focus on the worst-case scenario only.

1.2. Related work

One interesting problem in secret sharing is to determine the exact information ratio for some given family of graphs. Here we recall two related results on trees [8] and on large girth graphs [7].

For a subset X of vertices let $\mathcal{N}(X)$ denote the vertices adjacent to any vertex from X, i.e. the set of neighbors of X. Prior to present the result on trees, we recall the definition of the following useful notion from [8]:

Definition 3. Let X be a connected subset of vertices in G. X is a core if for each $v \in X$ there is a neighbor $w \in \mathcal{N}(v) \setminus X$ such that from X it is connected to v only, and these neighbors form an independent set.

Theorem 1. *[Csirmaz, Tardos [8]] Let G be tree and let c be the size of the maximal core in G. Then*

$$\sigma(G) = 2 - \frac{1}{c}.$$

The main contribution of this work is to extend the following result by removing the restriction for the girth:

Theorem 2 (*Csirmaz, Ligeti [7]*)**.** *Let G be a graph of maximum degree d satisfying the following properties:*

- *every vertex has at most one neighbor of degree one;*
- *vertices of degree at least 3 are not connected by an edge;*
- *the girth of the graph is at least 6.*

Then

$$\sigma(G) = 2 - \frac{1}{d}.$$

The above results yield interesting open problems. One straightforward generalization of the last result could be to lessen or remove any assumptions. Furthermore, in both of the above results, the values of the information ratio have the same structure, but they depend on (seemingly) different quantities. An interesting problem is to find any relation between these results apart from the formula. Within this paper we propose a solution for these problems. On one hand, we will show that it is possible to eliminate both the first and the last assumption by reducing the graph in some meaningful way and by extending the formula with the number of triangles containing a given vertex. On the other hand, we will mention that it is possible to generalize them in a common framework by constructing a maximal core in special trees using vertices of maximal degree.

The exact information ratio can be determined by proving lower and upper bounds that coincide. The used methods are significantly different, we collect the main tools for both directions in the following sections.

1.3. Lower bounds

The only known method for proving lower bounds is the so-called entropy method. As a first step, let S be a perfect secret sharing scheme based on graph $G = (V, E)$ with shares ξ_v for $v \in V$ and secret ξ_s, and define the set function

$$f(A) = \frac{H(\xi_v : v \in A)}{H(\xi_s)}$$

for each $A \subseteq V$. $f(A)$ is the normalized entropy of the shares belonging to the participants in A. Notice that $\max_{v\in V} f(v) = \sigma(G)$. Using standard properties of the entropy function (1–3) and perfect secret sharing (4–5) [4] the following so called Shannon-inequalities hold for all $A, B \subseteq V$:

(1) $f(\emptyset) = 0$, and in general $f(A) \geq 0$ (positivity);
(2) if $A \subseteq B \subseteq V$ then $f(A) \leq f(B)$ (monotonicity);
(3) $f(A) + f(B) \geq f(A \cap B) + f(A \cup B)$ (submodularity).
(4) if $A \subseteq B$, A is an independent set of vertices and B is not, then $f(A) + 1 \leq f(B)$ (strong monotonicity);
(5) if neither A nor B is an independent set of vertices but $A \cap B$ is so, then $f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$ (strong submodularity).

Let f be any real-valued function satisfying the Shannon-inequalities. Then any lower bound given to $\max_{v\in V} f(v)$ is also a lower bound for the information ratio. The value $\kappa(G) = \max_{v\in V} f(v)$ is called Shannon-complexity.

We remark that (1)–(5) do not fully characterize the information ratio. There are so-called non-Shannon inequalities and AK-information constraints that are also satisfied by the normalized entropy function and cannot be derived from the Shannon-inequalities, see [9]. The addition of these constraints improves the lower bound that can be obtained even for some access structures on five participants. There are other types of constraints i.e. non-Shannon rank inequalities or common information constraints providing lower bounds only for linear schemes. Adding these types of inequalities to the Shannon-inequalities yields better lower bounds on linear secret sharing for some graphs on six vertices [9] and on general graph families [5]. However, in our case the Shannon-complexity provides a tight lower bound.

For simplicity we usually write AB instead of $A \cup B$ for subsets of vertices, and a instead of $\{a\}$ for vertices.

Let us recall the following two results as non-trivial consequences of the Shannon inequalities introduced by Csirmaz and Tardos [8]:

Lemma 1. *Let A be a connected subset of vertices of G. Then*

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

Lemma 2. *Let A be a connected subset of vertices and B be an independent subset of vertices of G such that there exists a 1-factor from B to A. Then*

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

Although these general estimations are useful in our case as well, we need a more specific result on a generalization of the core:

Lemma 3. *Let $A = \{a_1, a_2, \dots\} \subset V$ be a set of vertices in G, and $B \subset V \setminus A$ be an independent subset of vertices of G such that there exists $A' \subset A$ with the following properties:*

1. *There is a perfect matching between A' and B. We index the elements of B such that the pair of $a_i \in A'$ is b_i and the remaining ones are indexed arbitrarily by $|A'| + 1, \dots, |A|$.*
2. *a_i and b_j are not connected if $i \neq j$.*

Furthermore there exists an independent set of vertices $C \subset V \setminus (A \cup B)$ such that there is no edge between C and $A' \cup B$.

Then $f(AC) - f(C) \geq |B|$ and $f(AC) - f(C) \geq |B| + 1$ if A is connected.

Proof. The proof is similar to the proof of Lemma 2, but for the sake completeness we present it. Let $B_i = \{b_1, \dots, b_i\}$. Define $d_i = f(AB_iC) - f(B_iC)$. We claim that $d_i \geq d_{i+1} + 1$ if $1 \leq i \leq |B| - 1$.

The set $a_{i+1}B_iC$ is independent but AB_iC and $a_{i+1}B_{i+1}C$ are not, consequently the strong submodularity gives

$$f(AB_iC) - f(a_{i+1}B_iC) \geq f(AB_{i+1}C) - f(a_{i+1}B_{i+1}C) + 1 \tag{1}$$

Furthermore submodularity for $a_{i+1}B_iC$ and $B_{i+1}C$ yields

$$f(a_{i+1}B_iC) - f(B_iC) \geq f(a_{i+1}B_{i+1}C) - f(B_{i+1}C)$$

By summing up these two inequalities we have

$$f(AB_iC)-f(B_iC)\geq f(AB_{i+1}C)-f(B_{i+1}C)+1$$

and this proves the claim.

The inequalities together give $d_1 \geq d_2+1 \geq \cdots \geq d_i+i-1 \geq \cdots \geq d_{|B|}+|B|-1$, and $d_{|B|}=f(ABC)-f(BC)\geq 1$ because BC is independent but ABC is not.

If A is connected then also $d_0 \geq d_1+1$. Otherwise, we can only use the usual submodularity in (1) hence all we can say is just $d_0 \geq d_1$.

Thus $f(AC)-f(C)=d_0\geq |B|+1$, if A is connected and $f(AC)-f(C)=d_0\geq |B|$ otherwise. This completes the proof. □

1.4. Upper bounds

There are plenty of methods in contrast with the lower bounds, since every construction yields an upper bound for the information ratio. One notable example is the decomposition theorem of Stinson [15], here we present a special case of the results for graph based schemes:

Theorem 3 (*Stinson Decomposition [15]*). *Let G be a graph and let G be covered with complete multipartite graphs, such that every vertex is covered by at most p graphs and every edge is covered by at least e graphs. Then*

$$\sigma(G)\leq \frac{p}{e}.$$

Let us note, that the first assumption in Theorem 2 is a purely technical one from the information ratio point of view, since different leaf neighbors of a given vertex v are "equivalent" in any secret sharing schemes in the sense that they can always get the same share. The case is similar for every two opposite 2-degree vertices of a given cycle of length 4, hence it is possible to remove one of them without any effect on the information ratio. Though our result will hold for arbitrary graphs, in fact we will working on graphs without such configurations. More precisely:

Definition 4. Let $G=(V,E)$ be a graph and consider the following reduction steps:

1. let $v,u_1,u_2\in V: d(u_1)=d(u_2)=1, \{u_1,v\},\{u_2,v\}\in E \Rightarrow V=V\setminus\{u_1\}$
2. let $u_1,u_2\in V: u_1,u_2\in C_4, d(u_1)=d(u_2)=2, \{u_1,u_2\}\notin E\Rightarrow V=V\setminus\{u_1\}$

Let G^* be the graph arising from G by every possible execution of the above two iterative reduction steps. G^* is the reduced graph of G.

Based on the above arguments it is easy to see, that $\sigma(G)=\sigma(G^*)$, hence any proven results for reduced graphs can be extended to significantly larger family of (non-reduced) graphs.

A star is a special complete bipartite graph, hence we can apply the above decomposition result for covering with stars. From covering with stars we can prove the following upper bound on the information ratio:

Lemma 4. *Let $G=(V,E)$ be a graph and $G^*=(V^*,E^*)$ be its reduced graph of maximum degree d. If G^* is triangle-free and its vertices of degree at least 3 are not connected by an edge, then there exists a star covering of G^* satisfying the following properties:*

(a) Every vertex is covered at most $2d-1$ times.
(b) Every edge is covered at least d times.
(c) If $v\in V^*$ is a vertex with $d(v)\geq 3$ then there exist $d-1$ v-stars (i.e. stars with center v).
(d) If $v\in V^*$ is a vertex with degree 2, then there exists a v-star on 3 vertices.
(e) If $v\in V^*$ is a leaf then v is covered exactly d times.

Proof. We present a star covering satisfying the 5 properties. We call a star *complete v-star*, if the center of the star is v, and the star contains all neighbors of v.

1. If v is a vertex with $d(v)\geq 3$ then add $d-1$ samples of complete v-stars to the covering.
2. If v is a vertex with $d(v)=2$, add one complete v-star to the covering. Furthermore if $uv\in E^*$ and $d(u)\leq 2$ then add $d-2$ uv edge to the covering.
3. Finally if v is a leaf then add 1 complete v-star to the covering (this is only an edge).

It is easy to check that the construction above satisfies all of the properties. By the first and second parts of the construction (c) and (d) obviously hold.

Let v be any vertex. If $d(v)\geq 3$ then v is covered $d-1$ times by the v-stars, and v is included in d additional stars, whose center is the neighbor of v. Now let us suppose that $d(v)=2$, and the neighbors of v are u and w with $d(u)\geq d(w)$. If $d(u)\geq d(w)\geq 3$, then v is contained in 1 v-star, $d-1$ u-stars and $d-1$ w-stars. If $d(u)\geq 3$ but $d(w)\leq 2$ then v is contained in 1 v-star, $d-1$ u-star, 1 complete w-star, and $d-2$ vw edges. Finally if $2 \geq d(u) \geq d(w)$, then v is contained in 1–1 complete v-, u-, and w-star, and $d-2$ uv and $d-2$ vw edges. The number of stars covering v is altogether $2d-1$ in all of the three cases. At last let v be a vertex of degree 1 with neighbor u. If $d(u) \geq 3$ then v is contained in the complete v-star and $d-1$ u-stars. Otherwise v contained in the 1 complete v-star, 1 complete u-stars and $d-2$ additional uv edges, that is altogether d stars in both cases.

Let uv be any edge with $d(u) \geq d(v)$. If $d(u) \geq 3$, then uv is contained in $d-1$ u-stars and 1 v-stars. Otherwise uv is contained in one u-star, one v-star (which may be only an edge if v is leaf), and $d-2$ additional uv edge. In both cases the number of stars covering uv is d. □

As a trivial consequence of Theorem 3 and Lemma 4 we get:

Lemma 5. *Let G be a graph and G^* be its reduced graph of maximum degree d. If G^* is triangle-free and its vertices of degree at least 3 are not connected by an edge, then*

$$\sigma(G^*) \leq 2 - \frac{1}{d}.$$

Let us note, that this lemma can also be proven directly using Theorem 1 and claiming that in reduced trees any vertex of maximal degree together with all but one of its neighbors (i.e. a possible leaf) is a core.

2. Results

Prior to a general presentation of the new results we discuss three cases depending on the girth of the respective reduced graphs, since the proofs are slightly different.

2.1. Girth 5

Theorem 4. *Let G be a graph such that its vertices of degree at least 3 are not connected by an edge. Furthermore, in G^* let the girth be 5 and let d be the maximum degree. Then*

$$\sigma(G) = 2 - \frac{1}{d}$$

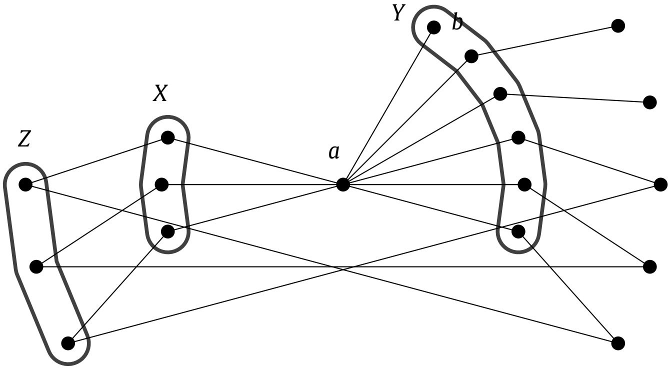
Proof.

We can assume that $d \geq 3$, otherwise the graph is either a path or a cycle. The upper bound is coming from Lemma 5. For the lower bound let a be vertex of maximum degree in G^*. First, suppose that there is a leaf neighbor of a, call it b.

Denote the set of cycles of length 5 containing a by $\mathcal{C}$. Consider the union of the elements of $\mathcal{C}$ and denote the intersection with $\mathcal{N}(a)$ by D. For $v \in D$ define the value $\gamma(v)$ as the number of cycles of $\mathcal{C}$ containing v. Consider $u \in D$, the neighbors of u are a and s. We claim that if $d(s) = 2$, then $\gamma(u) = 1$. Suppose that $d(s) = 2$ and $\gamma(u) > 1$. The other neighbor of s is t. u is contained in multiple cycles of $\mathcal{C}$ and each cycle must contain a, u, s and t in that order. If v_1 and v_2 ($v_1 \neq v_2$) are the fifth vertices of two such cycles, then av_1tv_2 must be a quadrangle which is a contradiction.

Let $u \in \mathcal{N}(a)$ be a vertex with $\gamma(u) > 1$, and $austv$ be a cycle from $\mathcal{C}$. Then by the previous claim $d(s) > 2$, which implies that $d(t) = 2$ and $\gamma(v) = 1$. Therefore if u is contained in multiple elements of $\mathcal{C}$, then each vertex of $\mathcal{N}(a)$ which is contained in the same cycle of $\mathcal{C}$ as u is only contained in that element of $\mathcal{C}$. Hence the elements of D can be partitioned into two sets X and Y, such that for each $C \in \mathcal{C}$, one of the two vertices of $C \cap D$ is in X and the other is in Y. Put all the remaining vertices of $\mathcal{N}(a)$ in Y. Note that X and Y form a partition of $\mathcal{N}(a)$.

Consider the set $\mathcal{N}(X)$ and let $Z = \mathcal{N}(X) \setminus \{a\}$. All vertices in X have degree two and one of their neighbors is a. Denote $z_1, z_2 \in Z$ as the other neighbor of $x_1, x_2 \in X$y. If $x_1 \neq x_2$ then $z_1 \neq z_2$ because otherwise $ax_1z_1x_2$ is a quadrangle which is a contradiction. Thus there exists a perfect matching between X and Z and there are no other edges between this set of vertices.



We claim that X, Y and Z satisfy the conditions of Lemma 3 with $A = \{a\} \cup X$, $A' = X$, $B = Z$, and $C = Y$. Clearly X and Y are independent sets and there is no edge between X and Y because the graph is triangle free. Furthermore there is no edge between Y and Z because if there is an edge between $y \in Y$ and $z \in Z$, and the pair of z in the perfect matching is $x \in X$ then $axyz$ is a quadrangle. Substituting these values in Lemma 3 gives

$$f(aXY) - f(Y) \geq |X| + 1. \tag{2}$$

Consider now Y and $\mathcal{N}(Y)$. By the same argument the set of edges between $\mathcal{N}(Y) \setminus \{a\}$ and $Y \setminus \{b\}$ is a perfect matching. Applying Lemma 3 with $A = A' = Y \setminus \{b\}$, $B = \mathcal{N}(Y) \setminus \{a\}$, and $C = \{b\}$ yields:

$$f(Y) - f(b) \geq |Y| - 1. \tag{3}$$

Let us denote $S = \{a\} \cup \mathcal{N}(a) \setminus \{b\} = \{a\} \cup X \cup Y \setminus \{b\}$. S and $\{a\} \cup \{b\}$ are both connected, but they intersection $\{a\}$ is not thus we can apply the strong submodularity

$$f(S) + f(ab) - f(aXY) - f(a) \geq 1 \tag{4}$$

By submodularity we know that

$$f(a) + f(b) - f(ab) \geq 0 \tag{5}$$

Adding up the four inequalities (2), (3), (4) and (5) gives

$$f(S) \geq |X| + |Y| + 1. \tag{6}$$

S is connected and $|S| = |\{a\}| + |\mathcal{N}(a)| - |\{b\}| = |\mathcal{N}(a)| = d$ thus (6) and Lemma 1 together yield

$$\sum_{v \in S} f(v) \geq f(S) + |S| - 2 \geq |X| + |Y| + 1 + |S| - 2 = 2d - 1$$

Hence for some vertex $v \in S$ we get

$$f(v) \geq \frac{2d-1}{|S|} = \frac{2d-1}{d} = 2 - \frac{1}{d}.$$

Now, suppose that every neighbor of a has degree 2, then choose any $b \in \mathcal{N}(a)$. Let G' be the graph arising from G^* by the deletion of the other neighbor of b. This completes the proof by $\sigma(G^*) \geq \sigma(G')$ and applying the above argument for G' □

2.2. Girth 4

Note that this case is trivial, since the girth cannot be 4 in the reduced graph G^*, i.e. the second reduction step replaces every C_4 by a path of length 2. It is easy to see that if G has girth 4 and vertices of degree at least 3 are not connected by an edge, then G^* is either a tree or has girth 5, which cases are covered in Theorems 1 and 4 respectively.

2.3. Girth 3

In this case we will see that the information ratio depends on the number of triangles incident to the vertices in addition to the maximal degree.

Theorem 5. *Let G be a graph such that vertices of degree at least 3 are not connected by an edge and let the girth of G^* be 3. Let $t(v)$ denote the number of triangles containing v in the reduced graph G^*, and let $\delta(v) = d(v) - t(v)$. Then*

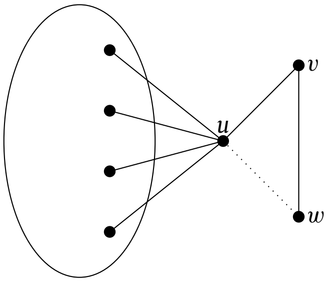
$$\sigma(G) = 2 - \frac{1}{\max_{v \in V^*} \delta(v)}$$

Proof.

We prove the theorem in two steps: first by giving a construction yielding an upper bound, next by proving the same lower bound using the entropy method.

For the upper bound, we construct a covering of G^* with stars and triangles such that each edge is covered $\delta = \max_{v \in V} d(v) - t(v)$ and each vertex is covered at most $2\delta - 1$ times. Hence, the upper bound is a consequence of the decomposition theorem of Stinson [15].

Note that in G^* any triangle has two vertices of degree two. Let u, v, w be the vertices of a triangle with $d(u) \geq 3$ and $d(v) = d(w) = 2$. Delete the edge $\{u, w\}$. Do this for all triangles in the graph, call the resulted graph G'. By this operation the degree of the vertex u is decreased by $t(u)$, hence the new degree of u in G' is $d(u) - t(u) = \delta(u)$. We deleted one edge from each triangle in the reduced graph, hence G' is either a tree or the girth of G' is at least 5.



Apply the star covering of Lemma 4. If u is a vertex of $d(u) \geq 3$ then the covering contains $\delta(u) - 1$ u-stars, and if v is a vertex of $d(v) = 2$ then the covering contains at least one complete v-star (i.e. a v-star containing both of v-s neighbors).

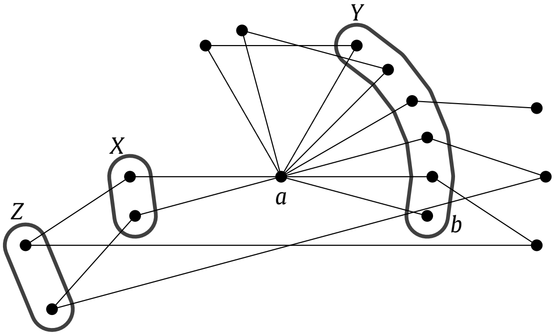
Apply the same construction for G^* but with two modifications for each triangle in G^*. Let u, v, w be the vertices of a triangle in G^* with $d(u) \geq 3$ and $\{u, w\}$ is the deleted edge. First, add 1–1 copy of this edge to all $\delta(u) - 1$ u-stars. Second, replace the complete v-star with a triangle on vertices u, v, w. Leave all the other stars from the covering unchanged.

It is clear that the covering numbers outside the triangles remain the same. Check the covering of the vertices and edges for a fixed triangle on vertices u, v, w, with $d(u) \geq 3$, and uw is the deleted edge in G'.

The modification of the construction leaves the covering number of u and v unchanged. w is covered δ times in G', and it is only increased by $\delta - 1$ (with the $\delta - 1$ u-stars) hence w and all the other vertices of the graph are covered at most $2\delta - 1$ times. The new construction only adds uw edges therefore both uv and vw are covered δ times as in the covering of G'. $\{u, w\}$ is contained in $\delta - 1$ u-stars and in one triangle on vertices u, v, w thus the edge $\{u, w\}$ is also covered at least δ times. The same argument can be applied for all triangles in the graph independently, therefore the proof for the upper bound is complete.

The proof of the lower bound is very similar to the girth 5 case in Theorem 4, only some minor changes are needed. Let a be any vertex with $\delta = \delta(a)$, and let $\mathcal{N}(a)$ is the neighbor set of A as before. Similarly to the proof of Theorem 4, we can assume that there exists a leaf neighbor b of a.

Let X and Y be two subsets of vertices of $\mathcal{N}(a)$ defined in the following way. Divide the vertices of $\mathcal{N}(a)$ contained in a cycle of girth 5 into two disjoint sets, X and Y as in the 5 girth case. Now consider the triangles containing a. Both of the other two vertices is adjacent to a. Put one of them into Y and leave out the other one form X and Y. Finally, put all the remaining vertices of $\mathcal{N}(a)$ into Y. Clearly $X \cap Y = \emptyset$ but now $X \cup Y \subsetneq N(a)$ because one vertex of each triangle belongs to neither X nor Y.



X and Y are independent set of vertices and there is no edge between X and Y because $X \cup Y \subset \mathcal{N}(a)$ and every triangle containing a has at most one common vertex with $X \cup Y$. Let define $Z = \mathcal{N}(X) \setminus \{a\}$. Every vertex of X is contained in only one cycle (e.g. a C_5), thus $|Z| = |X|$ and there is a perfect matching between X and Z similarly to the 5 girth case. X, Y and Z satisfy the conditions of Lemma 3 with $A = \{a\} \cup X$, $A' = X$, $B = Z$ and $C = Y$ (note that Z is independent, because the high degree vertices are not connected). As we mentioned before X and Y are independent and there is no edge between them, hence the only condition we have to check is that there is no edge between Y and Z. This is clearly true by the same argument as in the 5 girth case extended with the fact that all quadrangles have been removed from the graph in the reduction step. Lemma 3 implies that

$$f(aXY) - f(Y) \geq |X| + 1. \tag{7}$$

Consider now Y and $\mathcal{N}(Y)$. Similarly as in the girth 5 case, there is a perfect matching between $Y \setminus \{b\}$ and $\mathcal{N}(Y) \setminus \{a\}$ and no other edge. The application of Lemma 3 with $A = A' = Y \setminus \{b\}$, $B = \mathcal{N}(Y) \setminus \{b\}$ and $C = \{b\}$ arises:

$$f(Y) - f(b) \geq |Y| - 1. \tag{8}$$

Define $S = \{a\} \cup X \cup Y \setminus \{b\}$. S and $\{a\} \cup \{b\}$ are connected, but they intersection $\{a\}$ is not hence we can apply the strong submodularity:

$$f(S) + f(ab) - f(aXY) - f(a) \geq 1 \tag{9}$$

By submodularity we know that

$$f(a) + f(b) - f(ab) \geq 0 \tag{10}$$

Adding up the four inequalities (7), (8), (9) and (10) we have

$$f(S) \geq |X| + |Y| + 1. \tag{11}$$

S is connected and $|S| = |X| + |Y| = d(a) - t(a) = \delta$ therefore (11) and Lemma 1 together yield

$$\sum_{v \in S} f(v) \geq f(S) + |S| - 2 \geq |X| + |Y| + 1 + \delta - 2 = 2\delta - 1$$

Hence for some vertex $v \in S$ we get

$$f(v) \geq \frac{2\delta - 1}{|S|} = 2 - \frac{1}{\delta}.$$

This completes the proof. □

Now we can summarize the results in the following form:

Corollary 1. *Let G be a graph such that its vertices of degree at least 3 are not connected by an edge. Let $t(v)$ denote the number of triangles containing v in the reduced graph G^*, and let $\delta(v) = d(v) - t(v)$. Then*

$$\sigma(G) = 2 - \frac{1}{\max_{v \in V^*} \delta(v)}$$

3. Conclusion

In this paper we determine the exact information ratio of a large family of graphs without neighbors of degree at least 3. We showed that the ratio depends on the maximal difference between the degree and the number of triangles incident to a given vertex in the reduced graph. This is a non-trivial generalization of separate known results on high-girth graphs and on special trees. On one hand, by removing the assumption on the girth, on the other hand, by claiming that the size of the maximal core is equal to the maximal degree in trees without high-degree neighbors.

Acknowledgments

This research has been partially supported by Application Domain Specific Highly Reliable IT Solutions project which has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Subprogramme) funding scheme, by the ÚNKP-20-3 New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund and by the Lendület programme of the HAS.

References

[1] A. Beimel, O. Farràs, Y. Mintz, Secret-sharing schemes for very dense graphs, J. Cryptol. 29 (2) (2014) 336–362.
[2] G.R. Blakley, Safeguarding cryptographic keys, in: Proc. of the Nat. Comp. Conf., Vol. 48, 1979, pp. 313–317.
[3] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro, Graph decomposition and secret sharing schemes, J. Cryptol. 8 (1995) 39–64.
[4] L. Csirmaz, The size of a share must be large, J. Cryptol. 10 (4) (1997) 223–231.
[5] L. Csirmaz, An impossibility result on graph secret sharing, Des. Codes Cryptogr. 53 (2009) 195–209.
[6] L. Csirmaz, Secret sharing on the d-dimensional cube, Des. Codes Cryptogr. 74 (2015) 719—729.
[7] L. Csirmaz, P. Ligeti, On an infinite family of graphs with information ratio $2 - 1/k$, Computing 85 (2009) 127–136.
[8] L. Csirmaz, G. Tardos, Optimal information rate of secret sharing schemes on trees, IEEE Trans. Inf. Theory 59 (2013) 2527–2630.
[9] O. Farràs, T. Kaced, S. Martin, C. Padró, Improving the Linear Programming Technique in the Search for Lower Bounds in Secret Sharing, Cryptology ePrint Archive, Report 2017/919, 2017, available at https://eprint.iacr.org/2017/919.
[10] M. Gharahi, M.H. Dehkordi, Perfect secret sharing schemes for graph access structures on six participants, J. Math. Cryptol. 7 (2013) 143–146.
[11] M. Gharahi, S. Khazaei, Optimal linear secret sharing schemes for graph access structures on six participants, Theoret. Comput. Sci. 771 (2019) 1–8.
[12] M. Gyarmati, P. Ligeti, Smallest graph achieving the stinston bound, IEEE Trans. Inform. Theory 66 (7) (2020) 4609–4612.
[13] W. Jackson, K.M. Martin, Perfect secret sharing schemes on five participants, Des. Codes Cryptogr. 9 (1996) 233–250.
[14] A. Shamir, How to share a secret, Commun. ACM 22 (1979) 612–613.
[15] D.R. Stinson, Decomposition construction for secret sharing schemes, IEEE Trans. Inf. Theory 40 (1994) 118–125.
[16] H.L. Sun, B.L. Chen, Weighted decomposition construction for perfect secret sharing schemes, Comput. Math. Appl. 43 (2002) 877–887.
[17] M. van Dijk, On the information rate of perfect secret sharing schemes, Des. Codes Cryptogr. 6 (1995) 143–160.