Proyecciones (Antofagasta. On line) | vol. 39, n. 4 (2020) | pp. 1005-1017.

10.22199/issn.0717-6279-2020-04-0063

PROYECCIONES
Journal of Mathematics

ISSN 0717-6279 (On line)

The lower bound and exact value of the information rate of some developed graph access structures

Abbas Cheraghi[1] orcid.org/0000-0001-5650-5102

[1]University of Khansar, Dept. of Mathematics, Khansar, Isfahan, Iran.
a.cheraghi@khn.ui.ac.ir

Received: February 2020 | Accepted: June 2020

Abstract:

Various studies have focused on secret sharing schemes and in all of them, each shareholder is interested in a shorter share. The information rate of a secret sharing scheme shows the ratio between the size of the secret to the maximum number of shares given to each shareholder. In this regard, the researchers investigated the optimal information rate of the graph access structure. This paper aims to discover the exact values for the optimal information rates of the two graph access structures, which remained as open problems in Van Dijk's paper. Furthermore, we introduced the developed multipartite graph and the developed cycle graph and calculated the exact value of their optimal information rate. Moreover, we presented a lower bound on the information rate for other developed graph access structures.

Keywords: Graph access structure; Perfect secret sharing scheme; Information rate.

MSC (2020): 18A10, 94A62.

Cite this article as (IEEE citation style):

A. Cheraghi, "The lower bound and exact value of the information rate of some developed graph access structures", *Proyecciones (Antofagasta, On line)*, vol. 39, no. 4, pp. 1005-1017, Aug. 2020, doi: 10.22199/issn.0717-6279-2020-04-0063.

Article copyright: © 2020 Abbas Cheraghi. This is an open access article distributed under the terms of the Creative Commons License, which permits unrestricted use and distribution provided the original author and source are credited.

1. Introduction

The secret sharing scheme represents a method of distributing secrets between shareholders. Only the approved subset can rebuild the secret [9]. If the unapproved subsets can't resume the least knowledge of the secret, we consider the scheme a perfect secret sharing scheme [2]. The access structure Γ represents the set of all approved subsets of shareholders that can resume the secret. The set of the minimal approved subsets of shareholders represents the basic access structure, which is called Γ_0. The information rate is an important indicator to measure the performance of the secret sharing scheme. It is expressed as the ratio of the width of the secret to the maximum share width provided to shareholders. The graph access structure is a collection of qualified subsets of two members. In other words, the two shareholders corresponding to the two ends of each different edge can recover the secret, while a single shareholder cannot obtain any valuable information from the secret. Also, if any superset of the qualified subset is qualified, the access structure is called monotone. Every shareholder is interested in a few shares. In this way, the information rate of the secret sharing scheme is the ratio between the size of the secret and the maximum share allocated to each shareholder. Therefore, the optimal information rate for the access structure Γ is the supremum of this ratio.

Blundo et al. [1] calculated the exact value of the optimal information rate of the path graph. The value of information rate on the graph access structures with six vertices studied yet [3, 4, 8, 12]. Also, Song considered the case of a graph access structure with nine vertices [10]. The polyhedral combinatorics tool [5] used to determine the information ratio of a graph with a maximum of 10 vertices and

a girth of at least 5. Van Dijk considered all 112 graph access structures with six vertices, but only proved the exact value of the information rate in 94 cases [12]. Gharahi and Hadian, considered the remaining 8 cases of the other graphs [3, 4]. Similarly, in [8], the information rate of another case is calculated. So far, there is insufficient exactness for nine of these access structures.

1.1. Our Contribution

This article introduces two solutions with six vertices in the nine graph access structures, which remained as open problems in Van Dijk's paper[12]. The optimal information rate for these access structures has not been calculated. We have established the exact value of the information rate of these

two structures. Furthermore, a more reasonable bound of the information rate of some developed graph access structures will be displayed. Finally, we introduced the developed multipartite graph and the developed cycle graph and calculated the exact value of their optimal information rate.

1.2. Organization of the paper

The rest of the article is composed as follows: In section 2, the preliminaries required in the rest of the paper are reviewed. The exact value of the information rate of two remaining access structures of Van Dijks articles is presented in Section 3. Finally, Section 4 analyzes the information rate of the developed graph access structure.

2. Preliminaries

The Shamir's perfect secret sharing scheme is a method of distributing secrets between shareholders, such that the approved subset can rebuild the secret and the unapproved subsets can't resume the least knowledge of the secret [9]. In this section, quickly implement the symbols, definitions, and assumptions of Shamir's scheme used in this article.

2.1. Access structure

Let $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$ be a set of shareholders and $P(\mathbf{P})$ denote the power set of $\mathbf{P}$. Two distinct family Γ_Q and Γ_F of subsets of $\mathbf{P}$ referred to family of approved sets and unapproved sets, respectively. On the other hands $\Gamma_Q, \Gamma_F \subseteq P(\mathbf{P})$ and $\Gamma_Q \cap \Gamma_F = \emptyset$. We call the pair of (Γ_Q, Γ_F) as an access structure on $\mathbf{P}$ and denote by Γ. Define Γ_0 to consist of all the minimal approved sets:

$$\Gamma_0 = \{X \in \Gamma_Q \mid X' \notin \Gamma_Q \quad for\, all \quad X' \subsetneq X\}.$$

If $\Gamma_Q = \{X \mid Q \subseteq X \quad for\, all \quad Q \in \Gamma_0\}$ we say this access structure $\Gamma = (\Gamma_Q, \Gamma_F)$ on $\mathbf{P}$ has monotone increasing property. Let G be a graph with vertex set $V(G)$ and edge set $E(G)$. The stable set in the graph is a set of vertices, two of which are not adjacent. Suppose the set of shareholders $\mathbf{P}$ is the set of vertices of graph G i.e. $V(G) = \mathbf{P}$. If $\Gamma_0 = E(G)$ and Γ_F is the family of all stable sets of G then the monotone access structure $\Gamma = (\Gamma_Q, \Gamma_F)$ is a graph access structure .

2.2. Secret sharing scheme

We first explain the entropy tool, which is used to describe the formal definition of the secret sharing scheme. Using this tool, you can check the unconditional security of each scenario.

Definition 1. *Let the probability distribution* $\{p(x)\}_{x\in X}$ *on a set* X*. Entropy of* X *is represented by the symbol* $H(X)$ *and is defined as follows:*

$$H(X) = -\sum_{x\in X} p(x)\log_2 p(x).$$

The entropy $H(X)$ is a measure of the average uncertainty about which component of the set X is used, and the method of selecting components from X according to the probability distribution $\{p(x)\}_{x\in X}$. In the same way, apply $H(X|Y) = -\sum_{y\in Y}\sum_{x\in X} p(y)p(x|y)\log_2 p(x|y)$ to describe the conditional entropy of X given Y. Conditional entropy is the average measure of our uncertainty of the amount of X when we know the amount of Y.

Definition 2. *Let the access structure* Γ, $\mathbf{P}$ *shows the set of shareholders and* $\mathbf{K}$ *represents the set of all possible secrets. We call* Σ *a perfect secret sharing scheme for* Γ *if it has the following properties:*

1. *If* A *is an approved set of shareholders in* Γ_Q *then* $H(\mathbf{K}|A) = 0$*, that is, the shareholders in* A *can superimpose their shares to effectively reconstruct the content of the secret. In other words, with the presence of shareholder's shares, no ambiguity remains about the secret.*
2. *If* B *is an unapproved set of shareholders in* Γ_F *then* $H(\mathbf{K}|A) = H(\mathbf{K})$*, that is, even if the overlying shares in* B *are done, the size of the ambiguity secret will not be reduced. In other words, with the presence of shareholders in* B*, not even a single bit of information about the secret can be obtained.*

Throughout this article, we consider all secret sharing schemes to be perfect and prove that our proposed scheme is also perfect.

2.3. Information rate

Now, we need to introduce a tool that can be used to test the superiority of a scheme over other schemes on the access structure.

Definition 3. *Let* $\mathbf{S}_p$ *be the set of all possible shares allocated to each shareholder* p*. In this case, the information rate of the specific scheme* Σ *on the access structure* Γ *is defined by*

$$\rho(\Sigma) = \frac{\log_2 |\mathcal{K}|}{\max\limits_{p \in \mathbf{P}} \log_2 |S_p|}.$$

Besides, the optimal information rate of the access structure Γ *is defined by*

$$\rho^*(\Gamma) = \sup_{\sum} \rho\left(\sum\right), \tag{2.1}$$

where the supremum is on all schemes that are expressed for the access structure Γ*.*

The information rate of each graph access structure is less than or equal to one because the length of each share is greater than or equal to the length of the secret[7]. When $\rho^*(\Gamma) = 1$, we say that this is the best case for the information rate, because each shareholder holds only one share per secret, not more. Therefore, we call such a scheme an ideal scheme. The value of the optimal information rate represents the superiority of a scheme to other schemes on the access structure Γ. Therefore, estimate bound for this value has always been considered.

3. The exact value of the information rate

Van Dijk considered the information rate of the secret sharing scheme of the graph access structure on the six shareholders [12]. Of the 112 graph access structures of six shareholders, only 94 found the best information rate. Thus, in the case of unresolved secret sharing schemes on the six shareholders' association graphs, some of the types of information sharing were obtained from time to time [3, 4, 8]. Initially, we present the well-known theorems that are needed to prove our claims.

Theorem 4. *([6]) Let* Γ *be the graph access structure that corresponds to the connected graph* G*. Then* $\rho^*(\Gamma) = 1$ *if and only if* G *is a complete multipartite graph.*

Theorem 5. *([6]) Let* Γ *be the graph access structure that corresponds to the connected graph* G*. If* G *is an incomplete multipartite graph, then* $\rho^*(\Gamma) \leq \frac{2}{3}$*.*

It is straightforward that if H is an induced subgraph of G, then any secret sharing scheme on the access structure G can be transformed into a secret sharing scheme on the access structure H by limiting its shareholders to shareholders H. Consequently, the next theorem is clear.

Theorem 6. *Let G be a graph and H the induced subgraph of G. Then $\rho^*(\Gamma(G)) \leq \rho^*(\Gamma(H))$.*

Using the above theorem, it is possible to find suitable upper bound for the optimal information rate of the graphs that have induced subgraphs with known information rates.

3.1. The exact value of the graph access structure with six vertices

In this section, the two remaining access structures of Van Dijk's articles Γ_{55} (Fig. 3.1) and Γ_{70} (Fig. 3.2), the exact value's information rate of which has not yet been calculated, are questioned. Van Dijk in [12] shows that $\frac{3}{5} \leq \rho^*(\Gamma_i) \leq \frac{2}{3}$ for $i = 55, 70$ that so far this bound has remained unchanged. In this article, we will calculate the exact value of the best information rate for these two structures as follows.

Theorem 7. *The exact value of the optimal information rate of Γ_{55} is $\frac{2}{3}$.*

Proof. To prove, we perform a secret sharing scheme for access structure Γ_{55} as follows. Let S_{v_j} for $j = 1, \ldots, 6$, are the set of all shares given to shareholder v_j and the secret is the pair $K = (k_1, k_2)$. Also, the values r_i for $i = 1, \ldots, 5$, and the secret parts k_1, k_2 randomly selected from $GF(q)$.

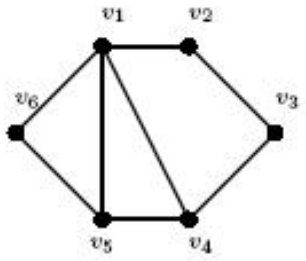

Figure 3.1: Γ_{55}

$$S_{v_1} = \{r_1 + r_2 + r_3 + 4k_1, r_3 + 2k_2, r_4 + r_5 + k_1 - 3k_2\},$$
$$S_{v_2} = \{r_1 + 3k_1, r_3, r_2\},$$
$$S_{v_3} = \{r_1 + 2k_1, r_3 + 2k_2, r_5 + k_1 - 2k_2\},$$
$$S_{v_4} = \{r_1 + r_5 + 4k_1 - 2k_2, r_3, r_4 + r_2\},$$
$$S_{v_5} = \{r_1 + 2r_3 + r_4 + r_5 + 3k_1 + 2k_2, r_3 + r_4 + 2k_2, r_2\},$$
$$S_{v_6} = \{r_1 + r_2 + r_3 + 3k_1, r_3 + r_4, r_5 + k_1 - 2k_2\}.$$

Based on the number of shares allocated to each of the six shareholders, we have: $\max_{1 \le i \le 6} |S_{v_i}| = 3$. This means that a maximum of 3 shares will be given to each shareholder to share two secrets, k_1 and k_2, between the six shareholders. Now, according to definition 3, we conclude that the lower bound of the optimal information rate of Γ_{55} is equal to $\frac{2}{3}$, i. e. $\frac{2}{3} \le \rho^*(\Gamma_{55})$.

On the other hand, the access structure Γ_{55} is an incomplete multipartite graph. Thus, according to theorem 5, the optimal information rate for this scheme is at most equal to $\frac{2}{3}$, i. e. $\rho^*(\Gamma_{55}) \le \frac{2}{3}$. So the exact value of the information rate is equal to $\frac{2}{3}$. □

With a simple review, we will find that both keys k_1 and k_2 do not depend on the shareholders' share of each stable set. Therefore, it can be immediately concluded that the scheme proposed for the access structure Γ_{55} in the previous theorem is perfect.

Theorem 8. *The exact value of the optimal information rate of* Γ_{70} *is* $\frac{2}{3}$.

Proof. To prove, we perform a secret sharing scheme for access structure Γ_{70} as follows. Let S_{v_j} for $j = 1, \ldots, 6$, are the set of all shares given to shareholder v_j and the secret is the pair $K = (k_1, k_2)$. Also, the values r_i for $i = 1, \ldots, 5$, and the secret parts k_1, k_2 randomly selected from $GF(q)$.

$$S_{v_1} = \{r_1 + r_2 + r_3 + 4k_1, r_3 + 2k_2 + k_1, 2r_4 + r_5 + k_1 - 3k_2\},$$
$$S_{v_2} = \{r_1 + 3k_1 + 2k_2, r_3, r_2\},$$
$$S_{v_3} = \{r_1 + \tfrac{5}{2}k_1 + 3k_2, r_3 - 2k_2 - k_1, r_5 + k_1 - 2k_2 + 2r_4\},$$
$$S_{v_4} = \{r_1 + r_2 + 3k_1 - 2k_2, r_3, 2r_4 + r_5 - 6k_2 + k_1\},$$
$$S_{v_5} = \{r_1 + r_2 + 2r_3 + r_4 + r_5 + 4k_1, r_5 + 2r_4 + k_1 - 2k_2, r_4 - r_3 - k_1\},$$
$$S_{v_6} = \{r_1 + r_4 + r_2 + 3k_1, r_4 + r_3 - 2k_2, r_5 + k_1 - 2k_2\}.$$

Based on the number of shares allocated to each of the six shareholders, we have: $\max_{1 \le i \le 6} |S_{v_i}| = 3$. This means that a maximum of 3 shares will be given to each shareholder to share two secrets, k_1 and k_2, between the six shareholders. Now, according to definition 3, we conclude that the lower bound of the optimal information rate of Γ_{70} is equal to $\frac{2}{3}$, i. e. $\frac{2}{3} \le \rho^*(\Gamma_{70})$.

On the other hand, the access structure Γ_{70} is an incomplete multipartite graph. Thus, according to theorem 5, the optimal information rate for

this scheme is at most equal to $\frac{2}{3}$, i. e. $\rho^*(\Gamma_{70}) \leq \frac{2}{3}$. So the exact value of the information rate is equal to $\frac{2}{3}$.

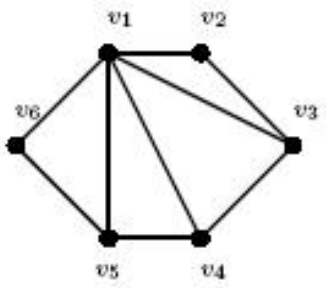

Figure 3.2: Γ_{70}

□

With a simple review, we will find that both keys k_1 and k_2 do not depend on the shareholders' share of each stable set. Therefore, it can be immediately concluded that the scheme proposed for the access structure Γ_{70} in the previous theorem is perfect.

4. Information rate of developed graph access structures

In this article, the term "*developing vertex*" refers to a vertex connected to a limited number of new vertices. Suppose, $|V(G)|$ indicates the number of vertices of the graph G. For every vertex $u \in V(G)$ the notation $N_G(u)$ indicates the set of neighbours of u in G and $d_G(u) = |N_G(u)|$. We are introducing a novel category of graphs.

Definition 9. *Let $K_{p_1,\cdots,p_k}$ as a complete multipartite graph. If $u \in V(K_{p_1,\cdots,p_k})$, then the complete multipartite graph that developed on u defined by $K^u_{p_1,\cdots,p_k}$.*

Example 10. *In the following, you can see $K^u_{2,3}$ that developed on the vertex u.*

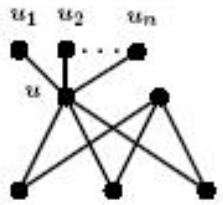

Figure 4.1: $K^u_{2,3}$

Presently we want to calculate the information rate of $K^u_{p_1,\cdots,p_k}$. We perform this by using the Stinson l-decomposition theorem, which you will see underneath.

Theorem 11. *[11] (l-decomposition construction) Suppose that Γ is an access structure having basis Γ_0 and suppose that $l \geq 1$ is an integer. Let $\mathbf{K}$ be a specified key set, and for $1 \leq h \leq l$, suppose that $D_h = \{\Gamma_{h,1}, \cdots, \Gamma_{h,n_h}\}$ is an ideal decomposition of Γ_0 for the key set $\mathbf{K}$. Let $\mathbf{P}_{h,j}$ denote the shareholder set for the access structure $\Gamma_{h,j}$. For every shareholder P_i, define*

$$R_i = \sum_{h=1}^{l} |\{j | P_i \in \mathbf{P}_{h,j}\}|.$$

Then there exists a perfect secret sharing scheme realizing Γ, having information rate $\rho = \frac{l}{R}$, where

$$R = \max\{R_i | 1 \leq i \leq w\}.$$

Definition 12. *A star graph with n vertices is a complete bipartite graph that one part has only one vertex and the rest is on the other part. In fact, the star graph with n vertices is the same as bipartite graph $K_{1,n-1}$.*

Theorem 13. *Let G is the complete multipartite $K_{p_1,\cdots,p_k}$ with $|V(K_{p_1,\cdots,p_k})| \geq 3$. Suppose H is the developed graph access structure $K^u_{p_1,\cdots,p_k}$ with n new leaves $u_1, \ldots, u_n$ connected to vertex u. Then $\rho^*(K^u_{p_1,\cdots,p_k}) = \frac{2}{3}$.*

Proof. We apply the idea of 2-decomposition construction on the graph H. For all $K^u_{p_1,\cdots,p_k}$ with $|V(K_{p_1,\cdots,p_k})| \geq 3$, we can give two ideal decompositions in the following way.

$D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$,
$\Gamma_{1,1} = \{K_{p_1,\cdots,p_k}\} = \{G\}$,
$\Gamma_{1,2} = \{K_{1,n} \mid V(K_{1,n}) = \{u\} \cup \{u_1, \ldots, u_n\}\}$,
$D_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$,
$\Gamma_{2,1} = \{K_{p_1,\cdots,p_k} \setminus \{u\}\}$,
$\Gamma_{2,2} = \{K_{1,n+d_G(u)} \mid V(K_{1,n+d_G(u)}) = \{u\} \cup (\{u_1, \ldots, u_n\} \cup N_G(u)\}$.

Now, according to theorem 11 computes $\rho^*(K^u_{p_1,\cdots,p_k})$. The value of R is equivalent to the highest representation of each vertex under ideal decompositions. To calculate R, we first partition the vertices $K^u_{p_1,\cdots,p_k}$ into four categories.

$V_1 = \{u_1, u_2, \ldots, u_n\}$,
$V_2 = \{u\}$,
$V_3 = \{v | v \in N_G(u)\} = N_{K_{p_1,\cdots,p_k}}(u)$,
$V_4 = V(G) \setminus (V_3 \cup \{u\}) = V(G) \setminus (N_G(U) \cup \{u\})$.

It is easy to check that $\bigcup_{i=1}^{4} V_i = V(K^u_{p_1,\cdots,p_k})$.
We will review the number of vertices of each of these four categories.

- Vertices located on V_1 are present in two sub-decompositions $\Gamma_{1,2}$ and $\Gamma_{2,2}$.
- Vertex u located on V_2 is present in three sub-decompositions $\Gamma_{1,1}$, $\Gamma_{1,2}$ and $\Gamma_{2,1}$.
- Vertices located on V_3 are present in three sub-decompositions $\Gamma_{1,1}$, $\Gamma_{2,1}$ and $\Gamma_{2,2}$.
- Vertices located on V_4 are present in two sub-decompositions $\Gamma_{1,1}$ and $\Gamma_{2,1}$.

Therefore, for two ideal decompositions, $R = 3$. Thus according to theorem 11, there is a scheme for $K^u_{p_1,\cdots,p_k}$ with information rate equals to $\frac{2}{3}$. $K^u_{p_1,\cdots,p_k}$ is an incomplete multipartite graph, so according to theorem 5 we have $\rho^*(K^u_{p_1,\cdots,p_k}) \leq \frac{2}{3}$. Thus $\rho^*(K^u_{p_1,\cdots,p_k}) = \frac{2}{3}$ for $|V(K_{p_1,\cdots,p_k})| \geq 3$. □

In the following, we intend to develop more than one vertex of a complete bipartite graph and try to find a lower bound for its information rate. But the exact value of their information rate hasn't been calculated, which could be of interest to researchers. At the last moment, consider the cycle

of development from a vertex and find a new lower bound for them $\frac{2}{5}$. So far, the exact value of its information rate has been uncalculated.

Definition 14. *Let $K_{p_1,\cdots,p_k}$ as a complete multipartite graph. If $u_1, u_2, \ldots, u_m \in V(K_{p_1,\cdots,p_k})$, then the complete multipartite graph that developed on vertices $u_1, u_2, \ldots, u_m$ defined by $K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k}$.*

We develop m vertices of a complete multipartite graph and prove that a new lower bound for its information rate, that equals to $\frac{1}{2}$.

Theorem 15. *Let G is the complete multipartite $K_{p_1,\cdots,p_k}$ with $|V(K_{p_1,\cdots,p_k})| \geq 3$. Suppose H is the developed graph access structure $K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k}$. Then $\frac{1}{2} \leq \rho^*(K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k}) \leq \frac{2}{3}$.*

Proof. We apply the idea of 1-decomposition construction on the graph H. Suppose that $N^C(u_i) = N_H(u_i) \setminus N_G(u_i)$, for $1 \leq i \leq m$. For all $K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k}$ with $|V(K_{p_1,\cdots,p_k})| \geq 3$, we can give one ideal decomposition in the following way.

$$
\begin{aligned}
&D = \{\Gamma_{1,0}, \Gamma_{1,1}, \ldots, \Gamma_{1,m}\},\\
&\Gamma_{1,0} = \{K_{p_1,\cdots,p_k}\} = \{G\},\\
&\Gamma_{1,1} = \{K_{1,|N^C(u_1)|} \mid V(K_{1,|N^C(u_1)|}) = \{u_1\} \cup N^C(u_1)\},\\
&\vdots \qquad\quad \vdots \qquad\quad \vdots \qquad\quad \vdots\\
&\Gamma_{1,m} = \{K_{1,|N^C(u_m)|} \mid V(K_{1,|N^C(u_m)|}) = \{u_m\} \cup N^C(u_m)\}.
\end{aligned}
$$

Now, according to theorem 11 computes lower bound on the $\rho^*(K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k})$. With a simple review, we will see that in this decomposition, each vertex is covered a maximum of 2 times in total. Then for this ideal decomposition, $R = 2$. Thus according to theorem 11, there is a scheme for $(K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k})$ with information rate equals to $\frac{1}{2}$. It means that $\frac{1}{2} \leq \rho^*(K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k})$. According to theorem 5, we have $\frac{1}{2} \leq \rho^*(K^{u_1,u_2,\ldots,u_m}_{p_1,\cdots,p_k}) \leq \frac{2}{3}$. □

Finally, we introduce a developed cycle and prove the information rate of the developed cycle is exactly $\frac{2}{3}$.

Definition 16. *Let C_n is a cycle graph with length n. If $u \in V(C_n)$, then the developed cycle graph that developed on u defined by C^u_n.*

Theorem 17. *Let C^u_n is the developed cycle of the cycle graph C_n with $n \geq 3$. Then $\rho^*(C^u_n) = \frac{2}{3}$.*

Proof. If $n \geq 3$, $\rho^*(C_n^u) \leq \frac{2}{3}$ by theorem 5. Without loss of generality suppose that $C_n \setminus \{u\}$ represents the path $(v_1, v_2, \ldots, v_{n-1})$. We apply the idea of 2-decomposition construction on the graph C_n^u. Let $N^C(u) = N_{C_n^u}(u) \setminus N_{C_n}(u)$. Consider $K_{1,m}$ is a complete bipartite graph with two parts $\{u\}$ and $N_{C_n^u}(u)$ in which $|N_{C_n^u}(u)| = m$.

First suppose n is odd. For all C_n^u, we can give two ideal decompositions in the following way.

$D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$
$\Gamma_{1,1} = \{\{v_1, v_2\}, \{v_2v_3, v_3v_4\}, \ldots, \{v_{n-4}v_{n-3}, v_{n-3}v_{n-2}\}, \{v_{n-2}v_{n-1}\}\}$,
$\Gamma_{1,2} = \{K_{1,m} \mid V(K_{1,m}) = \{u\} \cup \{N_{C_n^u}(u)\}\}$,
$D_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$,
$\Gamma_{2,1} = \{\{v_1v_2, v_2v_3\}, \{v_3v_4, v_4v_5\}, \ldots, \{v_{n-3}v_{n-2}, v_{n-2}v_{n-1}\}\}$,
$\Gamma_{2,2} = \{K_{1,m} \mid V(K_{1,m}) = \{u\} \cup \{N_{C_n^u}(u)\}\}$.

If n is even, for all C_n^u, we can give two ideal decompositions in the following way.

$D_1 = \{\Gamma_{1,1}, \Gamma_{1,2}\}$
$\Gamma_{1,1} = \{\{v_1, v_2\}, \{v_2v_3, v_3v_4\}, \ldots, \{v_{n-3}v_{n-2}, v_{n-2}v_{n-1}\}\}$,
$\Gamma_{1,2} = \{K_{1,m} \mid V(K_{1,m}) = \{u\} \cup \{N_{C_n^u}(u)\}\}$,
$D_2 = \{\Gamma_{2,1}, \Gamma_{2,2}\}$,
$\Gamma_{2,1} = \{\{v_1v_2, v_2v_3\}, \{v_3v_4, v_4v_5\}, \ldots, \{v_{n-4}v_{n-3}, v_{n-3}v_{n-2}\}, n - 2\check{v}_{n-1}\}\}$,
$\Gamma_{2,2} = \{K_{1,m} \mid V(K_{1,m}) = \{u\} \cup \{N_{C_n^u}(u)\}\}$.

With a simple review, we will see that in these two decompositions, each vertex is covered a maximum of 3 times in total. Then for these ideal decompositions, $R = 3$. Thus according to theorem 11, there is a scheme for C_n^u with information rate equals to $\frac{2}{3}$. It means that $\frac{2}{3} \leq \rho^*(C_n^u)$. According to what explained at the beginning of the proof, we have $\rho^*(C_n^u) = \frac{2}{3}$. □

References

[1] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, "Graph decompositions and secret sharing schemes", *Journal of cryptology,* vol. 8, no. 1, pp. 39-64, Dec. 1995, doi: 10.1007/BF00204801

[2] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes", *Journal of cryptology*, vol. 5, no. 3, pp. 153-166, Oct. 1992, doi: 10.1007/BF02451112

[3] M. Gharahi and M. H. Dehkordi. "The complexity of the graph access structures on six participants", *Designs, codes and cryptography,* vol. 67, no. 2, pp. 169-173, Dec. 2013, doi: 10.1007/s10623-011-9592-z

[4] M. Gharahi and M. H. Dehkordi. "Perfect secret sharing schemes for graph access structures on six participants", *Journal of mathematical cryptology*, vol. 7, no. 2, pp. 143-146, Sep. 2013, doi: 10.1515/jmc-2012-0026

[5] K. Harsányi and P. Ligeti. "Exact information ratios for secret sharing on small graphs with girth at least 5", *Journal of mathematical cryptology*, vol. 13, no. 2, pp. 107-116, Jun. 2019, doi: 10.1515/jmc-2018-0024

[6] W.-A. Jackson and K. M. Martin. "Perfect secret sharing schemes on five participants", *Designs, codes and cryptography,* vol. 9, no. 3, pp. 267-286, Nov. 1996, doi: 10.1007/BF00129769

[7] H.-Ch. Lu and H.-L. Fu. "New bounds on the average information rate of secret-sharing schemes for graph-based weighted threshold access structures", *Information sciences*, vol. 240, pp. 83-94, Aug. 2013, doi: 10.1016/j.ins.2013.03.047

[8] P. Carles, L. Vázquez, and A. Yang. "Finding lower bounds on the complexity of secret sharing schemes by linear programming", *Discrete applied mathematics*, vol. 161, no. 7-8, pp. 1072-1084, May 2013, doi: 10.1016/j.dam.2012.10.020

[9] A. Shamir, "How to share a secret", *Communications of the ACM* vol. 22, no. 11, pp. 612-613, Nov. 1979, doi: 10.1145/359168.359176

[10] Y. Song, L. Zhihui, L. Yongming, and X. Ren. "The optimal information rate for graph access structures of nine participants", *Frontiers of computer science,* vol. 9, no. 5, pp. 778-787, Oct. 2015, doi: 10.1007/s11704-015-3255-6

[11] D. R. Stinson and M. B. Paterson, *Cryptography: theory and practice,* 4th ed. Boca Raton, FL: CRC Press Taylor & Francis Group, 2018.

[12] M. Van Dijk, "On the information rate of perfect secret sharing schemes", *Designs, codes and cryptography,* vol. 6, no. 2, pp. 143-169, Sep. 1995, doi: 10.1007/BF01398012