Iranian Journal of Mathematical Sciences and Informatics
Vol. 8, No. 2 (2013), pp 31-38
DOI: 10.7508/ijmsi.2013.02.003

Secret Sharing Based On Cartesian product Of Graphs

Hamidreza Maimani[a,*] and Zynolabedin Norozi[b]

[a] Department of Mathematics, Shahid Rajaee Teacher Training University,
Tehran, Iran
[b]Department of Security and Cryptography, Emam Hossen University,
Tehran, Iran

E-mail: maimani@ipm.ir
E-mail: znorozi@ihu.ac.ir

Abstract. The purpose of this paper is to study the information ratio of perfect secret sharing of product of some special families of graphs. We seek to prove that the information ratio of prism graphs Y_n are equal to $\frac{7}{4}$ for any $n \geq 5$, and we will gave a partial answer to a question of Csirmaz [10]. We will also study the information ratio of two other families $C_m \times C_n$ and $P_m \times C_n$ and obtain the exact value of information ratio of these graphs.

Keywords: Secret sharing, Cartesian graph product, Prism graph.

2000 Mathematics subject classification: 05C75, 13H10.

1. Introduction

The concept of secret sharing was introduced by Shamir (cf.[13]) and Blakley (cf.[1]) independently of each other in 1979

Secret sharing scheme is a way for sharing a secret data among a group of participants so that only specific subsets(which is called qualified subsets) are able to recover the secret by combining their shares. If, in addition, any unqualified subsets of participants are unable to get any information about the secret with their shares, the scheme is called *perfect*. The set of all qualified

[*] Corresponding Author

Received 12 May 2011; Accepted 16 January 2012

subsets is called the *access structure*. In this paper when we speak about a secret sharing scheme, it is assumed to be perfect. The efficiency of the system is the main question in this area. The efficiency of the system means: how many bits of information must be remembered for each bit of secret by the members of group in average or worst case.
The paper is organized as follows. In Section 1 we will state the definitions and theorems necessary to state and prove our theorems. In section 2 we will compute the information rate of two families of graphs and will give a partial answer to the question which state by Csirmaz in [10].

2. Definitions and Preliminaries

In this section we will give a rough definition of the notions we shall use later.Let G be a simple graph, we denote the set of its vertices by V , and the number of the vertices by n. A *complete graph* is a graph in which each pair of distinct vertices is joined by an edge. We denote the complete graph with n vertices by K_n. For r a nonnegative integer, an *r-partite graph* is one whose vertex-set is partitioned into r disjoint parts in such a way that the two end vertices for each edge lie in distinct partitions. A *complete r-partite graph* is one in which each *vertex* is joined to every vertex that is not in the same partition. The *complete* 2*-partite graph* (also called the *complete bipartite graph*) with exactly two partitions of size m and n, is denoted by $K_{m,n}$. $K_{1,n}$ is called *star.* A subset X of vertex set is called *independent set*, if there is no edge between vertices in X. For a graph G and a nonempty subset $S \subseteq V(G)$, the *vertex-induced subgraph*, denoted $\langle S \rangle$, is the subgraph of G with vertex-set S and edges incident to members of S. A collection of subgraphs of G is called a *covering* of the graph G if every edge of G is contained in one of the (not necessarily spanned) subgraphs in the collection. . For subsets of vertices we usually omit the $\bigcup$ sign, and denote $A \bigcup B$ by AB. Also, if v is a vertex, then Av denotes $A \bigcup \{v\}$. Finally, all logarithms in this paper are in base 2.

The *cartesian product* of graphs $G = G_1 \times G_2$, are sometimes simply called the graph product of graphs G_1 and G_2 with point sets V_1 and V_2 and edge sets E_1 and E_2 is the graph with the point set $V_1 \times V_2$ and $u = (u_1, u_2)$ is adjacent with $v = (v_1, v_2)$ whenever ($u_1 = v_1$ and u_2 adjacent v_2) or (u_1 adjacent v_1 and $u_2 = v_2$).

A *prism* graph of order n, Y_n, is the graph Cartesian product $Y_n = K_2 \times C_n$, where K_2 is the complete graph on two vertices and C_n is the cycle graph on n vertices. This graph is corresponding to the skeleton of an n-prism. Prism graphs are therefore both planar and polyhedral. A prism graph of order n has $2n$ vertices and $3n$ edges. Generally, a prism graph is the graph Cartesian product $Y_{m,n} = P_m \times C_n$. It can therefore be viewed formed by connecting concentric cycle graphs C_n along spokes. Therefor this graph has mn vertices and $m(2n-1)$ edges.

Now we will define a perfect secret sharing scheme based on a finite graph G. We will use the notation and terminology of [10].

A *perfect secret sharing scheme* $\mathcal{S}$ for a finite graph G is a collection of random variables ξ_v for each $v \in V$ and a ξ_s (the secret) with a joint distribution so that
(i) Two random variables ξ_v and ξ_w together recover the value of ξ_s if vw is an edge in G;
(ii) For any independent set, A, the ξ_s and the collection $\{\xi_v : v \in A\}$ are statistically independent.
We denote the Shannon entropy or information content of variable ξ as $\mathbf{H}(\xi)$. Shannon entropy measured the size of random variable of ξ and it is well defined and finite, see [11].
For a vertex v of G, the *information ratio* of v is defined as the fraction $\frac{\mathbf{H}(\xi_v)}{\mathbf{H}(\xi_s)}$ and tells us how many bits of information v must be remembered for each bit in the secret. The worst case *information ratio* of $\mathcal{S}$ is the highest information ratio among all participants. The information ratio of the graph G, denoted by $R(G)$, is defined as

$$R(G) = \inf_{\mathcal{S}} \max_{v} \frac{\mathbf{H}(\xi_v)}{\mathbf{H}(\xi_s)}.$$

In order to determine the information ratio of a given one has to prove by different techniques that upper and lower bounds for $R(G)$ coincide.
For the lower bound we apply the entropy method which describe it as follows. For any subset A of the vertices we define the real-valued function f as

$$f(A) = \frac{\mathbf{H}(\{\xi_v : v \in A\})}{\mathbf{H}(\xi_S)}.$$

It is obvious that, the maximum value in the set $\{f(v) : v \in V\}$ is equal to the information ratio of $\mathcal{S}$. Using standard properties of the entropy function, (see in [11]), the following inequalities hold for all subsets A, B of the participants:
(a) $f(A) \geq 0$ and $f(\varnothing) = 0$;
(b) if A is a subset of B, then $f(A) \leq f(B)$;
(c) $f(A) + f(B) \geq f(A \bigcap B) + f(A \bigcup B)$;
(d)if A is an independent subset of non-independent set,B, then $f(A) + 1 \leq f(B)$;
(e) If A and B are not independent sets, but $A \bigcap B$ is an independent set, then $f(A) + f(B) \geq 1 + f(A \bigcap B) + f(A \bigcup B)$

Properties (a), (b), and (c) are called *positivity, monotonicity*, and *submodularity*, respectively. Properties (d) and (e) which are obtained from the other properties of f, are called *strict monotonicity* and *strict submodularity*, respectively.

Now we can restate the entropy method as follows (see [2],[3],[5]): Suppose that we prove that for any real-valued function f which satisfies properties (a)-(e), there exists a vertex $v \in G$, such that $f(v) \geq r$. Then, the functions coming from secret sharing secret sharing schemes also satisfy these properties. Hence we conclude that the worst case information ratio of G is at least r.

The following theorem is due to Csirmaz [9], and play an important role in this paper.

Theorem 2.1. *(a)Let f be a modular function which has the properties (a)-(e). If abc is an induced path in G, and $X \subseteq G$ is a subset of vertices such that acX is an independent set, then $f(a) + f(b) + f(cX) \geq f(acX) + 2$.*
(b) Let a, b, c and d be the vertices of graph G, such that ab, bc, cd are edges and ad, bd are not edges. If X is an independent set of vertices of G and no vertex in X is connected to any of a, b, c or d, then

$$f(bcX) - f(X) \geq 3.$$

In the following theorem we will state information ratio of some families of graphs. For the proofs of this theorem the reader can see [6], [7], and [8].

Theorem 2.2. *(a) Let G be a graph. Then $R(G') \leq R(G)$ for any induced subgraph G' of G.*
(b)$R(G) = 1$ if and only if G is a complete multi partite graph, and $R(G) \geq \frac{3}{2}$ otherwise
(c) Let C_n be a cycle of order $n \geq 5$. $R(C_n) = \frac{3}{2}$.
(d)Let Q_n be the n-cube. If $n \geq 2$, then $R(Q_n) = \frac{n}{2}$.

For the upper bound we use the Stinsons decomposition technique. In [14], Stinson states a method for general secret sharing schemes, which is called λ-decomposition construction. This method is a recursive construction for construction a scheme by using smaller schemes as building blocks. This method in graph access structure based on the finding a covering for the graph G such that every edges of G must appear in at least λ subgraphs of this covering. We will state this method in the following theorem.

Theorem 2.3. *Let G_i be a family of subgraphs of graph G, such that every edge of G belongs to at least k of G_i. For a vertex $v \in G$ define $r_i(v) = 0$ if $v \notin V(G_i)$, and $r_i(v) = R(G_i)$ otherwise. Then $R(G) \leq \sup\limits_{v \in G} \sum \frac{r_i(v)}{k}$*

Corollary 2.4. *Suppose that* Π *is a covering of graph* G *and every subgraphs in* Π *is a complete multi partite graph. If every edges of* G *is covered by at least* e *subgraphs of* Π *and every vertices of* G *is covered by at most* p *subgraphs of* Π*, then* $R(G) \leq \frac{p}{e}$.

3. MAIN THEOREMS

In [10] Csirmaz asked the following question:

Question 3.1. *Let* G *be a graph with* $1 \leq R(G) \leq 2$*. Does there exist a* $k \in \mathbb{N}$ *such that* $R(G) = 2 - \frac{1}{k}$.

In this section we construct an infinite family of graphs G with $R(G) = \frac{7}{4}$ and gave a partial answer to the above question. In the rest of this section we gave two infinite families of graphs with information ratio 2.

Theorem 3.2. *Let* G *be a graph with* $\delta(G) \geq 2$*. Then* $R(G \times K_2) \leq \frac{R(G)+d}{2}$ *where* $d = \Delta(G)$.

Proof. We Consider the vertex set of $G \times K_2$ as follows:

$$V(G \times K_2) = \{(v,0) : v \in V(G)\} \bigcup \{(v,1) : v \in V(G)\}.$$

For any edge $uv \in E(G)$ consider the square G_{uv} as follows

$$(u,0) \longrightarrow (u,1) \longrightarrow (v,1) \longrightarrow (v,0) \longrightarrow (u,0).$$

Now consider the covering $\{G_0, G_1, G_{uv} : uv \in E(G)\}$ where G_i is induced graph by vertices $\{(v,i) : v \in V(G)\}$ for $i = 0,1$. In this covering every edge of G appears at least two times and every vertex of G appears at most $d+1$ times. Since $R(G_{uv}) = 1$ and every vertex appears in at most d times in the family of $\{G_{uv}\}_{uv \in E}$, we have $R(G \times K_2) \leq \frac{R(G)+d}{2}$ by Corollary 2.4. □

Theorem 3.3. *If* $n \geq 5$, *then* $R(Y_n) \leq \frac{7}{4}$.

Proof. This follows from the Theorem 3.2 and the fact that $R(C_n) = \frac{3}{2}$ for $n \geq 5$. □

Theorem 3.4. *If* $n \geq 5$*, then* $R(Y_n) \geq \frac{7}{4}$.

Proof. To prove this theorem, we use the entropy method.Let f be a modular function which having properties (a)-(e). Suppose that

$$C_n : b_1 \longrightarrow b_2 \longrightarrow \cdots \longrightarrow b_n \longrightarrow b_1.$$

Label the vertices of Y_n as $a_i = (0, b_i)$ and $A_i = (1, b_i)$ for $1 \leq i \leq n$. Let $X = A_{n-1}, Y = a_3$. Since $a_1a_3A_{n-1}$ is an independent set and $a_1a_2a_3$ is a path, then by Theorem 2.1(a) we have,

$$f(a_1) + f(a_2) + f(a_3A_{n-1}) \geq f(a_1a_3A_{n-1}) + 2.$$

Similarly, $f(A_1) + f(A_n) + f(A_{n-1}a_3) \geq f(A_1A_{n-1}a_3) + 2$. Therefore

$$f(a_1)+f(a_2)+f(A_1)+f(A_n)+2f(a_3A_{n-1}) \geq f(A_1A_{n-1}a_3)+f(a_1a_3A_{n-1})+4.$$

By applying the sub-modularity property of f, we have

$$f(A_1A_{n-1}a_3) + f(a_1a_3A_{n-1}) + 4 \geq f(A_1A_{n-1}a_1a_3) + f(a_3A_{n-1}) + 4.$$

By adding the above inequalities we conclude that,

$$f(a_1) + f(a_2) + f(A_1) + f(A_n) \geq 4 + f(a_1a_3A_1A_{n-1} - f(A_{n-1}a_3).$$

Since $a_1a_3A_1A_{n-1}$ is a qualified set and $A_{n-1}a_3$ is an independent set, then by Theorem 2.1(b)

$$f(a_1a_3A_1A_{n-1}) - f(a_3A_{n-1}) \geq 3$$

and therefore

$$f(a_1) + f(a_3) + f(A_1) + f(A_n) \geq 7.$$

Hence at least one of $f(a_1), f(a_2), f(A_1), f(A_n)$ is at least $\frac{7}{4}$ and the lower bound is obtained. □

Corollary 3.5. *For any $n \geq 5$, we have $R(Y_n) = \frac{7}{4}$.*

Proof. The result follows from Theorems 3.3 and 3.4. □

Remark 3.6. *For $n = 3$, the graph Y_3 is a graph with 6 vertices. In [12], M. van Dijk showed that $R(Y_3) = \frac{3}{2}$. For $n = 4$, the graph Y_4 is 3-cube, and then $R(Y_4) = \frac{3}{2}$ by Theorem 2.2(d).*

Now we study the information ratio of $Y_{m,n}$. First of all we state the following Lemma

Lemma 3.7. [8] *Let G be the graph of Fig. 1. Then $R(G) = 2$.*

Theorem 3.8. *For any $m, n \geq 4$, $R(Y_{m,n}) = 2$.*

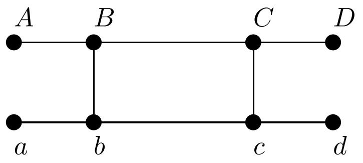

Fig. 1

Proof. Suppose that

$$P_m : a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_m,$$

and

$$C_n : b_1 \longrightarrow b_2 \longrightarrow \cdots \longrightarrow b_n \longrightarrow b_1$$

are path and cycle of length m, n respectively. Let

$$A = (a_2, b_1), B = (a_2, b_2), C = (a_3, b_2), D = (a_4, b_2),$$

$$a = (a_1, b_3), b = (a_2, b_3), c = (a_3, b_3), d = (a_3, b_4).$$

The subgraph induced by the set $\{a, b, c, d, A, B, C, D\}$ is isomorphic to graph of Fig. 1. Hence $R(Y_{m,n}) \geq 2$ by Theorem 2.2(a). Set $b_{m+1} = b_1$ and $v_{ij} = (a_i, b_j)$. For upper bound consider the coverings $\Pi_1 = \{v_{11}v_{1m}, v_{n1}v_{nm}\}$ and $\Pi_2 = \{G_{i,j} : 1 \leq i \leq n, 1 \leq j \leq m+1\}$, where $G_{i,j}$ is the square induced by the set $\{v_{i,j}, v_{i,j+1}, v_{i+1,j+1}, v_{i+1,j}\}$. In this covering every edge appears at least two times and every vertex to appears at most four times and since the information of every edge and every square is equal to 1, we have $R(Y_{m,n}) \leq 2$ by Corollary 2.4 . Hence we have $R(Y_{m,n}) = 2$ For any $m, n \geq 4$. □

Now we study the information ratio of cartesian product of two cycles.

Theorem 3.9. *For any $m, n \geq 5, R(C_m \times C_n) = 2$.*

Proof. Suppose that

$$C_m : a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_m \longrightarrow a_1,$$

and

$$C_n : b_1 \longrightarrow b_2 \longrightarrow \cdots \longrightarrow b_n \longrightarrow b_1.$$

are cycles of lengths m, n respectively. Clearly $P_{m-1} \times C_n$ is an induced subgraph of $C_m \times C_n$, hence $R(C_m \times C_n) \geq 2$ by Theorem 2.2(a). Set $b_{m+1} = b_1, a_{n+1} = a_1$ and $v_{ij} = (a_i, b_j)$. For upper bound consider the covering $\Pi_2 = \{G_{i,j} : 1 \leq i \leq n, 1 \leq j \leq m+1\}$, where $G_{i,j}$ is the square induced by the set $\{v_{i,j}, v_{i+1,j+1}, v_{i+,j+1}, v_{i+1,j}\}$. In this covering every edge appears at least two times and every vertex appears at most four times and since the information of every edge and every square is equal to 1, we have $R(C_m \times C_n) \leq 2$ by Corollary 2.4. Hence we have $R(C_m \times C_n) = 2$ For any $m, n \geq 4$. □

Acknowledgement. The authors would like to thank the referees for their useful suggestions which led to an improvement of the present note.

References

1. G. R. Blakley, *Safeguarding cryptographic keys*, American Federation of information Proceding Societies: National Computer Conference, 1979, pp. 313-317.
2. C. Blundo, A. De santis, RD. Simone, U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, *Des. Codes Crypt.*, **11**, (1979), 107-122.
3. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the size of shares of secret sharing scheme, *J. Crypt.*, **6**(3), (1993), 157-168.
4. A. Cheraghi, On the Pixel Expansion of Hypergraph Access Structures in Visual cryptography Schemes, *Iranian Journal of Mathematical Sciences and Informatics*, **5**(2), (2010), 45-54.
5. L. Csirmaz, The size of a share must be large, *J Crypt.*, **10**, (1997), 223-231.
6. L. Csirmaz, Secret sharing schemes on graphs, *Stud Math Hung.*, **44**, (2007), 297-306.
7. L. Csirmaz, *Secret sharing on the d-dimensional cube*, manuscript.
8. L. Csirmaz, Secret sharing on infinte graphs, *Tatra Mt. Math. Publ.*, **41**, (2008), 1-18.
9. L. Csirmaz, *Secret sharing on the infinite ladder*, manuscript.
10. L. Csirmaz, P. Ligeti, On an infinite family of graphs with information ratio $2 - \frac{1}{k}$, *Computing*, **85**, (2009), 127-136.
11. I. Csiszar, J. Korner, *Information theory. Coding theorems for discrete memoryless systems*, Academic Press, New York, 1981.
12. M. van Dijk, On the information rate of perfect secret sharing schemes, *Designs, Codes and Cryptography*, **6**, (1995), 143-169.
13. A. Shamir, How to share a secret, *Commun. ACM*, **22**, (1979), 612-613.
14. D. R. Stinson, Decomposition construction for secret sharing schemes, *IEEE Trans. Inform. Theory*, **40**, (1994), 118-125.