Some Theoretical and Practical Results for Edge Dominating Set

Dr. Nuha A. Rajab
Applied Sciences Department .University of Technology/ Baghdad
Email:Nuha.abd10@gmail.com

Received on: 5/1/2014 & Accepted on: 6/4/2014

ABSTRACT

One of the most brilliant branches of modern mathematics and computer applications is graph theory. Graph domination problem has become an extremely important research branch of graph theory in recent times. For instance, determining whether a graph has an induced matching that dominates its edges is a known problem of edges dominating set. Such problems are considered as NP-hard problems. There is, therefore, a growing interest towards finding new algorithms to produce better and more efficient results. In this paper, a new polynomial time algorithm is proposed to determine the set of edge domination. The generalized relations between graph properties (vertices, edges, regularity, and dominating edges) are deduced and abstracted in some important theoretical results, lemmas, propositions, and theorems. One field of applications for this type of domination is a secret sharing scheme. It is implemented to demonstrate its applicability and efficiency.

Keywords: Dominating vertices, minimum edges dominating set, regular graph, independent edges, and incidence matrices.

بعض النتائج النظرية والعملية لمجموعة الحافات المهيمنة

الخلاصة:

تعتبر نظرية البيانات فرع من الفروع المتميزة في الرياضيات الحديثة وتطبيقات الكمبيوتر. ظهر الاهتمام المتزايد في الاونة الاخيرة بمشاكل الهيمنة في نظرية البيانات, حيث تعتبر مشكلة تحديد التطابق في اي بيان, من مشاكل الهيمنة المعروفة, وذلك بايجاد مجموعة من حافات البيان التي تهيمن على بقية الحافات. تعتبر هيمنة الحافات من المشاكل المصنفة ضمن مشاكل (NP- hard)، وبالتالي فان هنالك اهتمام متزايد لايجاد خوارزميات جديدة لتطوير النتائج الحالية. في هذا البحث تم اقتراح خوارزمية جديدة لتحديد مجموعة الحافات المهيمنة في وقت محدد. كما تم استنتاج بعض القضايا والقضايا المساعدة والمبرهنات من العلاقات بين الرووس والحافات ودرجة انتظام البيان وعدد الحافات المهيمنة فيه. تعتبر برامج المشاركة السرية من التطبيقات المهمة لموضوع الهيمنة في نظرية البيانات، وتم تنفيذ الخوارزمية لإثبات امكانية تطبيقها وكفاءتها على هكذا نوع من البرامج.

https://doi.org/10.30684/etj.32.5B.8
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Introduction

Omination in graph theory is a natural model for many location problems in operations research [1]. Historically, the first domination-type problems came from chess in 1850s [2].

The study of domination in graphs was further developed in the late 1950s and 1960s Berge [3] wrote a book on graph theory, in which he introduced the "coefficient of external stability," that is now known as the domination number of a graph [4]. Ore [5] introduced the terms "dominating set" and "domination number" in his book on graph theory. The problems of domination in graphs were studied in more detail around 1964 by brothers, Yaglom et al [6]. An excellent treatment of the fundamentals of domination is given in the1972 in the book by Haynes [7].

Later, Cockayne and Hedetniemi [8] published a survey paper in which the notation $\gamma(G)$ was first used for the domination number of a graph G. In the same year, the concept of edge domination was introduced by Mitchell and Hedetniemi [9]. In 1980, Yannakakis and Gavril [10] proved that the edge dominating set problem for graph is NP-complete, even when restricted to planar or bipartite of maximum degree 3. They introduced an algorithm for finding minimum independent edge dominating sets in trees based on the relationship between edge dominating sets and independent sets in a total graph. Problem of determining the total domination number for a graph to be NP-complete was solved in 1984[see,11].

In 1995, Hwang and Chang [12] constructed the minimum edge dominating set MED by interchange edges. Let (u, v) and (v, w) be two adjacent edges in MED and let S be the set of edges different from (v, w) adjacent to w. It cannot be that $S \cap MED = \emptyset$, or the elements of $MED - \{(v, w)\}$ dominate all the elements of S, since in either case drop (v, w) from MED, thereby contradicting its minimality. Therefore, there is an edge $(w, z) \in S, z \neq v$, such that (w, z) is dominated only by the edge (v, w) of MED. Hence, by replacing (v, w) by (w, z) in E, an edge dominating set of the same size can be obtained having fewer pairs of adjacent edges. Continuing in this way one obtains a minimum independent edge dominating set having $|MED|$ elements.

Another algorithm for finding minimum independent edges dominating set dependent on tree $T(G)$ was introduced by Chang [12]. Fujito [13] investigated an approximate polynomial time of the edge dominating for unit-weighted graph. The edge dominating set problem is polynomially equivalent to the minimum maximal matching problem in either exact or approximate computation. Duckworth and Mans [14] used a covered vertex to construct an algorithm to find the minimum independent edge set. Duckworth and Wormald [15] used a search-tree technique based on enumeration minimal vertex cover. They introduced an efficient algorithm to determine an edge dominating set. Alon and Gutner[16] introduced an algorithm for finding a dominating set of fixed size in degenerated graphs. For a dense graph, Cardinal and et al. [17] improved approximation bounds for edge dominating set. Rooij and Bodlaender [18] introduced exact algorithms for edge domination, which combines enumeration approaches of minimal vertex covers in the input graph with the branches and reduces paradigm. Xiao and Nagamochi[19] improved parameterized algorithm for the edge dominating set problem.

Throughout this paper, we consider simple graphs that are connected, regular, unweighted, and undirected. In addition to this section that introduces the related work on the domination sets, the paper consists of 5 other sections. Section 2, presents the theoretical concepts, the proposed algorithm with an illustrative example is discussed in Section 3. In Section 4, the theatrical results are introduced. The application of the proposed algorithm in secret sharing scheme is presented in Section 5. Section 6, then concludes the papers.

1. Theoretical Concepts

A graph or an undirected graph G is an ordered pair $G = (V;\ E)$ where V is a set of elements, which are called vertices or nodes, and E; is a set of unordered pairs of distinct vertices called edges or lines. The cardinality of $V(G)$ and $E(G)$ is the order of G (i.e.$|V(G)| = n$) and the size of G, respectively. A graph G is said to be r-regular if every vertex in $V(G)$ has a degree r (i.e. each vertex is adjacent to precisely r other vertices in G); the degree of the edges being the sum of the degrees of its endpoints. A simple connected graph without cycle denoted a tree, and a vertex u in a connected graph G is said to be cut vertex if the removal of u leads G to be disconnected. For other basic graph-theoretical definitions, we refer the reader to [3,7, 20].

A subset D of V is called a dominating set of G if every vertex not in D is adjacent to some vertex in D. The domination number $\gamma(G)$ of G is the minimum cardinality taken over all dominating sets of G. A dominating set ID is called an independent dominating set if no two vertices of D are adjacent. The independent domination number $ID(G)$ of G is the minimum cardinality takes over all independent dominating sets of G [21]. A set of minimum independent dominating vertices of an r-regular graph of order n is $\left\lceil \frac{n}{r+1} \right\rceil$ [22].

A subset ED of E is called an edge dominating set of G if every edge not in ED is adjacent to some edge in ED. The edge domination number $ED(G)$ of G is the minimum cardinality taken over all edge dominating sets of G. The maximum order of a partition of E into edge dominating sets of G is called the edge dominatic number of G and is denoted by $EDM(G)$. An edge dominating set ED is called an independent edge dominating set IED if no two edges are adjacent. The independent edge domination number $IED(G)$ of G is the minimum cardinality taken over all independent edge dominating sets of G. The edge independent number $IED'(G)$ is defined to be the number of edges in a maximum independent set of edges of G [10].

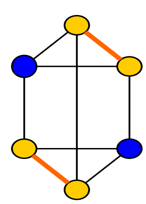


Figure (1) IED sets

A domination polynomial of vertices and edges, such that, the vertex domination polynomial of a given graph G is $D_0(G,x) = \sum_{i=\gamma_{0(G)}}^{n} d_0(G,i)x^i$, where $d_0(G,i)$ is the number of vertex dominating set of G with size I, and $\gamma_{0(G)}$ is the vertex domination number of G. However, the edge domination polynomial of G is the polynomial

$D_1(G,x) = \sum_{i=\gamma_{1(G)}}^{|E(G)|} d_1(G,i)x^i$, where $d_1(G,i)$ is the number of edge dominating set of G with size I, and $\gamma_{1(G)}$ is the edge domination number of G. The edge domination polynomial of G is equal to the vertex domination polynomial of a line graph, see [23, 24].

A set of edges M of a graph $G = (V, E)$ is called a matching if no two of its elements are adjacent. A matching is maximal if no other edges can be added to it. An independent edge dominating set *IED* is in fact a maximal matching [12]. The size of the minimum edge dominating set of a graph G is equal to the size of its maximal matching.

2. The Proposed Algorithm

This algorithm is designed to find the edge dominating sets with their numbers in the r-regular graph $G = (V, E)$, where $|V| = n, and\ |E| = m$. The process depends on the adjacent matrix of edges, such that for each edge in the graph, the set of its adjacent edges is computed, as well as, the adjacent set A_k of k- independent edges $I_k = \{e_1, e_2, \dots, e_k\}, k = 2,3, \dots, m$. The cardinality of A_k is also computed. Hence, if $|A_k| = m - |I_k|$, then the minimum independent edge dominating set is determined. All the above concepts are presented in the following algorithm:

The Algorithm

Input the number of vertices n, the number of edges m, the regular degree r, the adjacent matrix of edges

$AE = a_{ij} = \begin{cases} 1 & if\ e_i\ adjacent\ e_j \\ 0 & otherwise \end{cases}$.

Output the minimum independent dominating edges IDE_l, and $|IDE_l|$ with the number l.

Compute $l = \left\lceil \frac{m}{(2r-1)} \right\rceil$

For $i = 1$ to m

Compute $A(i)$ the adjacent set of edge e_i, such that $A(i) = \{\, e_j\ if\ a_{ij} = 1\}$,

For $i_1 = 1$ to m

For $i_2 = 1$ to m

.

.

.

For $i_l = 1$ to m

Construct a matrix

$A_l = a_l(i_1, i_2, \dots, i_l) =$

$$\begin{cases} 1 & if \quad e_{i_1}, e_{i_2}, \dots, e_{i_2}\ are\ adjacent \\ 0 & if \quad i_1 = i_2 = \cdots = i_l \\ A(i_1) \cup A(i_2) \cup \dots \cup A(i_l) & otherwise \end{cases},$$

If $a_l(i_1, i_2, \dots, i_l) = m - l$, then $N = N + 1$, and IED_l is $a_l(i_1, i_2, \dots, i_l)$,

End For i_l

.

.

.

End For i_2

End For i_1
$N_1 = \frac{N}{2}$, the number of edge dominating sets.
End.

Example:

Let G be a 3- regular simple graph, given in Figure 2 below. The above algorithm is applied to find the minimum edge dominating sets, the cardinality of each set, in addition to the number of all of them as follows:

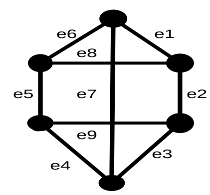


Figure (2) 3-regular graph

The incident matrix $AE = a_{ij}$ for the graph in Figure 2 is:

$$AE = \begin{array}{c} \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \\ e_6 \\ e_7 \\ e_8 \\ e_9 \end{array} \begin{array}{c} \begin{array}{ccccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 & e_8 & e_9 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

Compute $l = 2$,

In Table 1, the adjacent edges $A(i)$ for all edges $e_i, i = 1,2, \dots ,9$ are found in such a way that when $a_{ij} = 1$ in the row r_i, the edge e_j is adjacent, or is an element in $A(i)$.

Table (1) Adjacent edges to e_i.

$i = 1$	$A(1) = \{e_2, e_6, e_7, e_8\}$
$i = 2$	$A(2) = \{e_1, e_3, e_8, e_9\}$
$i = 3$	$A(3) = \{e_2, e_4, e_7, e_9\}$
$i = 4$	$A(4) = \{e_3, e_5, e_7, e_9\}$
$i = 5$	$A(5) = \{e_4, e_6, e_8, e_9\}$
$i = 6$	$A(6) = \{e_1, e_5, e_7, e_8\}$
$i = 7$	$A(7) = \{e_1, e_3, e_4, e_6\}$
$i = 8$	$A(8) = \{e_1, e_2, e_5, e_6\}$
$i = 9$	$A(9) = \{e_2, e_3, e_4, e_5\}$

The adjacent matrix $A_2(i_1, i_2)$, is constructed, in Table 2, in such a way that the entry $a_2(i_1, i_2)$ is the union of the sets $A(i_1)$, and $A(i_2)$. Compute the number of edges in each entry $a_2(i_1, i_2)$ of Table 2, such that, the entry with the cardinality 7 (the bold entry) represents the set of adjacent edges to e_{i_1}, and e_{i_2}. Therefore, the edges e_{i_1} and e_{i_2} are the dominating set in this graph. In fact, they are independent due to the zero entry a_{ij} in the adjacent matrix.

Table (2)The adjacent edges to e_{i_1} and $e_{i_2}, i_1, i_2 = 1, 2, \dots, 9$.

	$A(1)$	$A(2)$	$A(3)$	$A(4)$	$A(5)$	$A(6)$	$A(7)$	$A(8)$	$A(9)$
$A(1)$	0	1	$\{e_2, e_4, e_6, e_8, e_9\}$	$\boldsymbol{\{e_2, e_3, e_5, e_6, e_7, e_8, e_9\}}$	$\{e_2, e_4, e_6, e_7, e_8, e_9\}$	1	1	1	$\boldsymbol{\{e_2, e_3, e_4, e_5, e_6, e_7, e_8\}}$
$A(2)$	1	0	1	$\{e_3, e_4, e_5, e_7, e_9\}$	$\{e_4, e_6, e_7, e_8, e_9\}$	$\{e_1 , e_4, e_5, e_7, e_8, e_9\}$	$\{ e_1, e_3, e_4, e_6, e_7, e_9\}$	1	1
$A(3)$	$\{e_2, e_4, e_6, e_7, e_8, e_9\}$	1	0	1	$\{e_2, e_4, e_6, e_7, e_8, e_9\}$	$\boldsymbol{\{e_1, e_2, e_4, e_5, e_7, , e_8, e_9\}}$	1	$\boldsymbol{\{e_1, e_2, e_4, e_5, e_6, e_7, e_9\}}$	1
$A(4)$	$\boldsymbol{\{e_2, e_3, e_5, e_6, e_7, e_8, e_9\}}$	$\{e_2, e_3 , e_5, e_7, e_9\}$	1	0	1	$\{e_1, e_3, e_5, e_7 , e_8, e_9\}$	1	$\boldsymbol{\{e_1, e_2, e_3, e_5, e_6, e_7, e_9\}}$	1
$A(5)$	$\{e_2, e_4, e_6, e_7, e_8, e_9\}$	$\{e_2, e_4, e_6, e_7, e_8, e_9\}$	$\{e_2, e_4, e_6, e_7, e_8, e_9\}$	1	0	1	$\{e_1, e_3, e_4, e_6, e_8, e_9\}$	1	1
$A(6)$	1	$\{e_1 , e_4, e_5, e_7, e_8, e_9\}$	$\boldsymbol{\{e_1, e_2, e_4, e_5, e_7, , e_8, e_9\}}$	$\{e_1, e_2, e_5, e_7, , e_8, e_9\}$	1	0	1	1	$\boldsymbol{\{e_1, e_2, e_3, e_4, e_5, e_7, e_8\}}$
$A(7)$	1	$\{e_1, e_3, e_4, e_6, e_7, e_9\}$	1	1	$\{e_1, e_3, e_4, e_6, e_8, e_9\}$	1	0	$\{e_1, e_2, e_3, e_4, e_5, e_6\}$	$\{e_1, e_2, e_3, e_4, e_5, e_6\}$
$A(8)$	1	1	$\boldsymbol{\{e_1, e_2, e_4, e_5, e_6, e_7, e_9\}}$	$\boldsymbol{\{e_1, e_2, e_3, e_5, e_6, e_7, e_9\}}$	1	1	$\{e_1, e_2, e_3, e_4, e_5, e_6\}$	0	$\{e_1, e_2, e_3, e_4, e_5, e_6\}$
$A(9)$	$\boldsymbol{\{e_2, e_3, e_4, e_5, e_6, e_7, e_8\}}$	1	1	1	1	$\boldsymbol{\{e_1, e_2, e_3, e_4, e_5, e_7, e_8\}}$	$\{e_1, e_2, e_3, e_4, e_5, e_6\}$	$\{e_1, e_2, e_3, e_4, e_5, e_6\}$	0

In each steps, N will be computed. If $N = 12$, such that, N_1 is the independent edge dominating sets in the given graph.

3. Theoretical Analysis

Table(3) is constructed from the proposed algorithm for edge dominating set. It tabulates the relations between the number of vertices, edges, regularity, and number of edge dominating set. Based on these values, important generalized relations are abstracted in some important lemmas, propositions, and theorems, as follows:

Table(3) The cardinality of the edge dominating set

Ver.	$r = 2$		$r = 3$		$r = 4$		$r = 5$		$r = 6$		$r = 7$		$r = 8$	
	no. E	MID	no. E	MID	no. E	MID	no. E	MID	no. E	MID	no. E	MID	no. E	MID
4	4	2	6	2										
5	5	2	-	-	10	2								
6	6	2	9	2	12	2	15	2						
7	7	3	-	-	14	2	-	-	21	2				
8	8	3	12	3	16	3	20	3	24	3	28	3		
9	9	3	-	-	18	3	-	-	27	3	-	-	36	3
10	10	4	15	3	20	3	25	3	30	3	35	3	40	3
11	11	4	---	--	22	4	--	--	33	3	-	-	44	3
12	12	4	18	4	24	4	30	4	36	4	41	4	48	4
13	13	5	--	--	26	4	-	-	39	4	-	-	52	4
14	14	5	21	5	28	4	35	4	42	4	48	4	56	4
15	15	5	-	-	30	5	-	-	45	5	-		60	4
16	16	6	24	5	32	5	40	5	48	5	56	5	64	5
17	17	6	-	-	34	5	-	-	51	5	-	-	68	5
18	18	6	27	6	36	6	45	5	54	5	63	5	72	5
19	19	7	-	-	38	6	-	-	57	6	-	-	76	6
20	20	7	30	6	40	6	50	6	60	6	70	6	80	6

Lemma 4.1: Let $G = (V; E)$ be a simple graph of order $|V| = n$, if the minimum independent edge domination set *IED*, with $|IED| = 2$, then $\sum_{i=1}^{4} deg(v_i) = m - 2$, where each edge in *IED* incident on v_i. Moreover, if G is regular, then $deg(v_i) \geq \frac{n}{2} - 1$.

Proof: Let G be a simple graph of order n, with $V = \{v_1, v_2, \ldots, v_n\}$, and size m, with $E = \{e_1, e_2, \ldots, e_m\}$. Since $|IED| = 2$, (say e_1, and e_2), then e_1, and e_2 are non-adjacent edges in G, but they are adjacent to $e_3, e_4, \ldots, e_m$. Therefore, e_1, e_2 are adjacent to $(m-2)$ edges in G. Let v_1, v_2, v_3, v_4 be the vertices incident on e_1, and e_2, then these two vertices are adjacent to $(n-4)$ vertices. Hence, $\sum_{i=1}^{4} deg(v_i) = 2(n-4) + 4 = 2n - 4$. It is obvious that, for a regular graph, $deg(v_i) = \frac{n}{2} - 1$.

Proposition 4.2: The cardinality of minimum independent edge dominating set of an r-regular simple graph is $|IED| = \left\lceil \frac{rn}{2(2r-1)} \right\rceil$.

Proof: Since minimum independent dominating set of vertices for an r-regular graph is $\left\lceil\frac{n}{r+1}\right\rceil$, and the degree of edge is $2(r-1)$, also the number of edges is $\frac{rn}{2}$, we obtained that $|IED| = \left\lceil\frac{rn}{2(2r-1)}\right\rceil$, which represents the number of independent edge dominating sets in G.

Lemma 4.3: The sequence of the edge dominating set for 2-regular and simple graph $G = (V, E)$ of order $n = 3i + 1$, $i = 1,2, \ldots$, in each three consecutive places are equal.

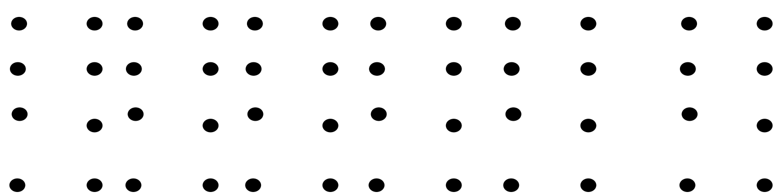
Proof: Since $|IED| = \left\lceil\frac{rn}{2(2r-1)}\right\rceil$ (by proposition 5.2), and $r=2$, then for 2-regular graph the number of dominating set is $\left\lceil\frac{n}{3}\right\rceil$, such that $|IED|$ for each three consecutive sequence are equals i.e. 2, 2, 2, 3, 3, 3, 4, 4, 4, 5, 5, 5, ….

Proposition 4.4: There is no edge dominating set of cardinality two for $n \geq 8$.

Proof: The lemma is proven for $n = 8$ and its true for a graph of order $n \geq 8$. For $n = 8$ the regular degree can be 2, 3, 4, 5, 6, 7; all of these cases are discussed as follows:

For $r=2$, then $m = 8$, if we assume that $|IED| = 2$, then each edge is adjacent to only two edges. Therefore, the graph possesses four other edges in addition to the two independent edges dominated. Hence, the total number of the edges is six, which is a contradiction with $m = 8$, as illustrated in Figure 3(a).

For $r = 3, m = 12$ and $|IED| = 2$, the two independent edges in this case are adjacent to eight other edges, but since the total number of edges in G is twelve, which leads a contradiction, also see Figure 3(b). A similar contradiction is obtained for the other remaining cases $r = 4, 5, 6, 7$ as illustration in Figure 3(c-f).



a b

Figure (3) Independent dominating edge set of graphs of order 8.

Theorem 4.5: Let $G = (V, E)$ be a simple regular graph of order $|V| = n$, and size $|E| = m$.

- If the size of G is a prime number, and $r = 2$, then there exists a minimum independent edge dominating set IED, with $|IED|=\left\lceil\frac{m}{3}\right\rceil$.
- If $r > 2$, and m is any integer, such that $gcd(r, m) > 1$, then there exist a minimum independent edge dominating set in G.

Proof: Let $G = (V, E)$ be a simple r-regular graph, of order n, and size m.

- Also, let m be a prime number, if $r = 2$, then $deg(v_i) = 2$, for $v_i \in G$. Each edge $e \in E$ is adjacent to two edges, then the number of independent set of cardinality three is $\frac{n}{3}$, but since m is prime then n is also prime, and $\frac{n}{3}$ cannot be an integer number. Therefore, it must be at least one edge is in common between two sets, and $|IED| = \left\lceil\frac{n}{3}\right\rceil$.

- If $gcd(r,m) = 1$, and since the summation of the degrees of vertices for a regular graph is rn, and this sum equals twice the number of edges, in this case the number of vertices is $\frac{2m}{r}$, which is a rational number. This is a contradiction since n is an integer number. Hence, there is no graph that satisfies these conditions.

Proposition 4.6: Let $G = (V,E)$, be an r-regular graph, of order $|V| = n$, where $r > 2$, and $|E| = m$, that has a minimum independent edge dominating set. If r is an even number, then $\frac{r}{2}\,divide\ m$. Otherwise r divides m.

Proof: Let *G* be an r-regular graph with a minimum independent edge dominating set. For an even number r, $r = 2a$, since $m = \frac{rn}{2}$ (the size m equals to the summation of degrees of vertices divides by two), then $m = a \times n$. Therefore, $\frac{r}{2}$ divides m. For an odd number r, $2m = rn$, then n must be even. Hence, r divides m.

4. Applications

The variety of new parameters that can be developed from the basic definition of domination lead to their use in many applications, one of them is area of secret sharing scheme. Several approaches were developed to obtain an efficient implementation of a secret sharing scheme, where it is proven by Rajab et al. [22] that using domination property helps to improve the security and the efficiency of such systems. Secret sharing scheme refers to any method of distributing a secret among a group of participants, each of which allocates a share of the secret. The secret can only be reconstructed when the authorized shares are combined together; individual shares are of no use on their own. More formally, in a secret sharing scheme there is one *dealer* and n *players*. The dealer shares a secret S with the players, only when specific conditions are fulfilled. The dealer accomplishes this by giving each player a share in such a way that any group of t (*the threshold*) or more players can together reconstruct the secret K but no group of less than t players can. The collection of subsets of participants who can reconstruct the secret in this way is called *access structure* Γ. Γ is usually monotone, that is, if $X \in \Gamma$ and $X \subseteq X' \subseteq P$, then $X' \in \Gamma$. A minimal qualified subset $Y \in G$ is a subset of participants such that $Y' \notin \Gamma$ for all $Y' \subset Y, Y' \neq Y$. The basis of Γ, denoted by Γ_0, is the family of all minimal qualified subsets. Let 2^P denoted the collection of all subsets of P. For any $\Gamma_0 \subseteq \Gamma$, the closure of Γ_0 is defined as $cl(\Gamma_0) = \{X' : \exists X \in \Gamma_0, X \subseteq X' \subseteq P\}$. Therefore, an access structure Γ is the same as the closure of its basis $\Gamma_0 = (cl(\Gamma_0))$. The first step in the distribution of the key is to determine an appropriate field for the subsequent modular arithmetic. Because of this, an appropriate prime value q is needed, so that the needed arithmetic can be performed in Galois field.

The shares are assigned to participants. When a group of t elements coordinate their shares together, they can use their given x and y values. Each person will then create an equation with t unknown values of a_i. Through key reconstruction by all the participants, t different equations are generated. This system of equations can solved. Through the unique values of a_i, system will provide a unique solution.

The characteristics of the graph are used in the perfect secrete sharing scheme, such as adjacent to the vertices, the degree of regular, and domination properties. Using the same attributes given in [22], the domination of edges is used to construct Γ_0, such that each participant can be represented as an edge in the given graph, and a set of participants represent an element in Γ_0 if they correspond to a set of minimum independent edge that dominating other edges. After proving the applicability of this type of domination in the construction and reconstruction of secret sharing schemes, they have influenced the efficiency of these schemes. Since the desired purpose in secret sharing scheme is to get the length of the share as small as possible, the proposed scheme leads to an improved information rate. The comparison between vertices and edge domination is presented in Table (4)

Table (4) Comparison between vertices and edge domination

No. Ver.	No. edges	Regular	domination	
			Ver.	Edges
4	4	2	2	2
12	12	3	3	3
14	14	4	3	2
20	20	5	4	3
27	27	6	5	3
35	35	7	5	3
48	48	8	6	4

Conclusions

The algorithm for finding minimum independent edge domination set IED based on the adjacency matrix of edges is proposed in this paper. The determination of the number of different IED in a regular graph is presented. Important theoretical results for minimum independent edge dominating set in a regular graph are established as being dependent on the relation between the order, size, and regularity of the graph. These sets are applied in a perfect secrete sharing scheme to construct the basis of such systems. By some experiments, an improvement in the information rate of these schemes is demonstrated.

References

[1] P. M. Pardalos, Handbook of Combinatorial Optimization, 1998.

[2] T.W. Haynes, S.T. Hedetniemi, and P.J. Slater. Fundamentals of Domination in Graphs. Marcel Dekker, New York, 1998.

[3] C. Berge, Theory of Graphs and its Applications, Methuen, London, 1962.

[4] J. M. Tarr, Domination in Graphs, MSc.thesis, University of South Florida,6-1-2010.

[5] O. Ore, Theory of Graphs. Amer. Math. Soc. Colloq. Publ., 38, 1962.

[6] A. M. Yaglom and I. M. Yaglom. Challenging Mathematical Problems with Elementary Solutions. Volume 1: Combinatorial Analysis and Probability Theory, 1964.

[7] F. Harary, Graph Theory, Massachusetts, Addison-Wesley, 1972.

[8] E. J. Cockayne and S.T. Hedetniemi, Towards a theory of domination in graphs, networks, 7(1977), 247-261.

[9] S. Mitchell and S. T. Hedetniemi, Edge domination in trees, *Congr. No*.19 (1977), 489-509.

[10] M. Yannakakis, and F. Gavril, Edge dominating sets in graphs, SIAM J. Appl. Math., Vol.38, No. 3, 1980.

[11] R. C. Laskar, J. Pfaff, S. M. Hedetniemi, S. R. Hedetniemi, On the algorithmic complexity of total domination. SIAM J. Algebraic Discrete Methods, 5 (1984), 420-425.

[12] G. J. Chang, Algorithmic Aspects of Domination in Graphs in: Handbook of Combinatorial Optimization, D.-Z. Du and P.M. Pardalos, eds., Vol.3,pp.339-405, 1998.

[13] T. Fujito, On approximability of the independent/connected edge dominating set problems, Elsever, Information Proccessing Letters, Vol. 79, (2001) 261-266.

[14] W. Duckworth, and B. Mans, "Randomized Greedy Algorithms for Finding Small k-Dominating Sets of Regular Graphs", Wiley Periodicals, Inc. Random Struct. Alg., 27, (2005) 401–412.

[15] W. Duckworth, and N.C. Wormald, On the independent domination number of random regular graph, ACMJ. Vol.15, No. 4, (2006) 513-522.

[16] N. Alon, and S. Gutner, Linear Time Algorithms for Finding a Dominating Set of Fixed Size in Degenerated Graphs, G. Lin (Ed.): COCOON, LNCS 4598, (2007) 394–405.c_Springer-Verlag Berlin Heidelberg.

[17] J. Cardinal, S. Langerman, and E. Levy, Improved approximation bounds for edges dominating set in dense graphs, Theor. Comput. Sci, Vol. 410, (2009) 949-957.

[18] J.M.M. van Rooij, and H. L. Bodlaender, Exact algorithms for edge domination, Sprenger, Algorithmic, Vol. 64, (2012) 535-563.

[19] M. Xiao, and H. Nagamochi, Parameterized dominating set in graph with degree bounded by 3, Theoretical Computer Science, 505 (2013) 2-15.

[20] R. Diestel, Graph Theory, Springer, New York, 2000.

[21] H. Fernau, Efficient enumeration-based exact algorithms, Springer-Vering Heidelberg, LNCS 4169,(2006) 142-153.

[22] N. Rajab, N. ASaidi, M. Said, and K. Kadhim, Secrete sharing scheme based graph domination, ICMA Conference, 2013.

[23] B. Askari, and M. Alaeiyan, The vertex domination polynomial and edge domination polynomial of a graph, AUA, No. 28, (2011) 157-162.

[24] S. Alikhania, and Y. Pengb, Introduction to domination polynomial of a graph, arXive:0905.2251v1 [math.CO] 14 May 2009.