On the adjacency properties of generalized Paley graphs

W. Ananchuen*

School of Liberal Arts
Sukhothai Thammathirat Open University
Pakkred, Nonthaburi 11120, THAILAND

Abstract

Let m and n be non-negative integers and k be a positive integer. A graph G is said to have property $P(m,n,k)$ if for any $m+n$ distinct vertices of G there are at least k other vertices, each of which is adjacent to the first m vertices but not adjacent to any of the latter n vertices. We know that almost all graphs have property $P(m,n,k)$. However, for the case $m,n \geq 2$, almost no such graphs have been constructed, with the only known examples being Paley graphs which are defined as follows. For $q \equiv 1 \pmod 4$ a prime power, the Payley graph G_q of order q is the graph whose vertices are elements of the finite field $\mathbf{F}_q$; two vertices a and b are adjacent if and only if their difference is a quadratic residue. By using higher order residues on finite fields we can generate other classes of graphs which we refer to as generalized Paley graphs. For any m,n and k, we show that all sufficiently large (order) graphs obtained by taking cubic and quadruple residues have property $P(m,n,k)$.

1. Introduction

All graphs considered in this paper are finite, loopless and have no multiple edges. For the most part, our notation and terminology follows that of Bondy and Murty [10]. Thus G is a graph with vertex set V(G), edge set E(G), $\nu(G)$ vertices and $\varepsilon(G)$ edges.

Let m and n be non–negative integers and k a positive integer. A graph G is said to have property P(m,n,k) if for any disjoint sets A and B of vertices of G with $|A| = m$ and $|B| = n$ there exist at least k other vertices, each of which is adjacent to every vertex of A but not adjacent to any vertex of B. The class of graphs having property P(m,n,k) is denoted by $\mathcal{G}$(m,n,k). The cycle C_ν of length ν is a member of $\mathcal{G}(1,1,1)$ for every $\nu \geq 5$. The well–known Petersen graph is a member of $\mathcal{G}(1,2,1)$ and also of $\mathcal{G}(1,1,2)$. The class

* Research supported by The Thailand Research Fund grant BRG/07/2541.

$\mathcal{G}$(m,n,k) has been studied by Ananchuen and Caccetta [2, 3, 5, 6], Blass et. al. [7], Blass and Harary [8], Exoo [13], Exoo and Harary [14, 15]. In addition, some variations of the above adjacency property have been studied by Alspach et. al. [1], Ananchuen and Caccetta [4], Bollobás [9], Caccetta et. al. [11, 12] and Heinrich [16].

In 1979, Blass and Harary [8] established, using probabilistic methods, that almost all graphs have property P(n,n,1). From this it is not too difficult to show that almost all graphs have property P(m,n,k). Despite this result, few graphs have been constructed which exhibit the property P(m,n,k); some constructions for the class $\mathcal{G}$(1,n,k) were given in [5].

An important graph in the study of the class $\mathcal{G}$(m,n,k) is the so–called **Paley graph** G_q defined as follows. Let $q \equiv 1 \pmod 4$ be a prime power. The vertices of G_q are the elements of the finite field $\mathbf{F}_q$. Two vertices a and b are adjacent if and only if their difference is a quadratic residue, that is $a - b = y^2$ for some $y \in \mathbf{F}_q$.

In [3, 4] we proved that for a prime power $q \equiv 1 \pmod 4$:

$G_q \in \mathcal{G}(1,n,k)$ for every $q > \{(n-2)2^n + 2\}\sqrt{q} + (n + 2k - 1)2^n - 2n - 1$;

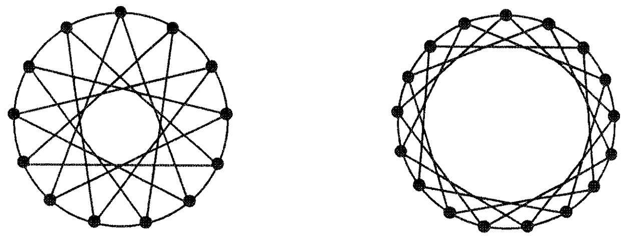
$G_q \in \mathcal{G}(n,n,k)$ for every $q > \{(2n-3)2^{2n-1} + 2\}\sqrt{q} + (n + 2k - 1)2^{2n-1} - 2n^2 - 1$;

and $G_q \in \mathcal{G}(m,n,k)$ for every $q > \{(t-3)2^{t-1} + 2\}\sqrt{q} + (t + 2k - 1)2^{t-1} - 1$,

where $t \geq m + n$.

By using higher order residues on finite fields we can generate other classes of graphs. More specifically, for $q \equiv 1 \pmod 3$ a prime power we define the **cubic Paley graph,** $G_q^{(3)}$ as follows. The vertices of $G_q^{(3)}$ are the elements of the finite field $\mathbf{F}_q$. Two vertices a and b are adjacent if and only if $a - b = y^3$ for some $y \in \mathbf{F}_q$. Since $q \equiv 1 \pmod 3$ is a prime power, -1 is a cubic in $\mathbf{F}_q$. The condition -1 is a cubic in $\mathbf{F}_q$ is needed to ensure that ab is defined to be an edge when ba is defined to be an edge. Consequently, $G_q^{(3)}$ is well–defined. Figure 1(a) gives an example.

For $q \equiv 1 \pmod 8$ a prime power, define the **quadruple Paley graph** $G_q^{(4)}$ as follows. The vertices of $G_q^{(4)}$ are the elements of the finite field $\mathbf{F}_q$. Two vertices a and b are adjacent if and only if $a - b = y^4$ for some $y \in \mathbf{F}_q$. Since $q \equiv 1 \pmod 8$ is a prime power, −1 is a quadruple in $\mathbf{F}_q$. The condition −1 is a quadruple in $\mathbf{F}_q$ is needed to ensure that ab is defined to be an edge when ba is defined to be an edge. Figure 1(b) gives an example.



(a) $G_{13}^{(3)}$ (b) $G_{17}^{(4)}$

Figure 1. Graphs $G_{13}^{(3)}$ and $G_{17}^{(4)}$.

In this paper the adjacency properties of the classes $G_q^{(3)}$ and $G_q^{(4)}$ are studied. More specifically, we prove that:

- $G_q^{(3)} \in \mathcal{G}(2,2,k)$ for every $q > [\frac{1}{4}(79 + 3\sqrt{36k+701})]^2$;
- $G_q^{(3)} \in \mathcal{G}(m,n,k)$ for every $q > (t2^{t-1} - 2^t + 1)2^m\sqrt{q} + (m + 2n + 3k - 3)2^{-n}3^{t-1}$, where $t \geq m + n$; and
- $G_q^{(4)} \in \mathcal{G}(m,n,k)$ for every $q > (t2^{t-1} - 2^t + 1)3^m\sqrt{q} + (m + 3n + 4k - 4)3^{-n}4^{t-1}$, where $t \geq m + n$.

2. Finite Fields

In this section, we present some results on finite fields that we make use of in establishing our main theorems. We begin with some basic notation and terminology.

Let $\mathbf{F}_q$ be a finite field of order q where q is a prime power and let $\mathbf{F}_q[x]$ be a polynomial ring over $\mathbf{F}_q$.

A **character** χ of $\mathbf{F}_q^*$, the multiplicative group of the non-zero elements of $\mathbf{F}_q$, is a map from $\mathbf{F}_q^*$ to the multiplicative group of complex numbers with $|\chi(x)| = 1$ for all

$x \in \mathbf{F}_q^*$ and with $\chi(xy) = \chi(x)\chi(y)$ for any $x, y \in \mathbf{F}_q^*$.

Among the character of $\mathbf{F}_q^*$, we have the **trivial** character χ_o defined by $\chi_o(x) = 1$ for all $x \in \mathbf{F}_q^*$; all other character of $\mathbf{F}_q^*$ are called **nontrivial**. With each character χ of $\mathbf{F}_q^*$, there is associated the **conjugate** character $\bar{\chi}$ defined by $\bar{\chi}(x) = \overline{\chi(x)}$ for all $x \in \mathbf{F}_q^*$. A character χ is of **order** d if $\chi^d = \chi_o$ and d is the smallest positive integer with this property.

It will be convenient to extent the definition of nontrivial character χ to the whole of $\mathbf{F}_q$ by defining $\chi(0) = 0$. For χ_o we define $\chi_o(0) = 1$.

Observe that

$$\chi^t(a) = \chi(a^t) \tag{2.1}$$

for any $a \in \mathbf{F}_q$ and t a positive integer.

If χ is a nontrivial character of $\mathbf{F}_q$, we know that (see [17]), for $a, b \in \mathbf{F}_q$ with $a \neq b$

$$\sum_{x \in F_q} \chi(x-a)\bar{\chi}(x-b) = -1. \tag{2.2}$$

The following lemma, due to Schmidt [18], is very useful to our work.

Lemma 2.1. Let χ be a nontrivial character of order d of $\mathbf{F}_q$. Suppose $f(x) \in \mathbf{F}_q[x]$ has precisely s distinct zeros and is not a d^{th} power; that is f(x) is not of the form $c\{g(x)\}^d$, where $c \in \mathbf{F}_q$ and $g(x) \in \mathbf{F}_q[x]$. Then

$$\left| \sum_{x \in F_q} \chi(f(x)) \right| \leq (s-1)\sqrt{q}. \qquad \square$$

The next lemma is a generalization of Lemma 3.2 proved in [3].

Lemma 2.2. Let χ be a nontrivial character of order d of $\mathbf{F}_q$. If $a_1, a_2, \ldots, a_s$ are distinct elements of $\mathbf{F}_q$ and $s \equiv 0 \pmod{d}$, then there exists $c \in \mathbf{F}_q^*$ such that

$$\sum_{x\in F_q} \chi\{(x-a_1)(x-a_2)\ldots(x-a_s)\} = -1 + \sum_{x\in F_q} \chi\{c(x-b_1)(x-b_2)\ldots(x-b_{s-1})\}$$

for some distinct elements $b_1, b_2, \ldots, b_{s-1}$ of $\mathbf{F}_q$.

Proof: We write

$$\sum_{x\in F_q} \chi\{(x-a_1)(x-a_2)\ldots(x-a_s)\}$$

$$= \sum_{x\in F_q} \chi\{x(x+a_1-a_2)(x+a_1-a_3)\ldots(x+a_1-a_s)\}. \qquad (2.3)$$

Note the latter equality is valid, since x and $x + a_1$ assume all values in $\mathbf{F}_q$. Now, since a_1, $a_2, \ldots, a_s$ are distinct, then $c_i = a_1 - a_{i+1} \neq 0$ for $1 \leq i \leq s-1$.

If $x \neq 0$, then there exists an x^{-1} such that $xx^{-1} = 1$. Furthermore, $\chi(x^{-1})^s = 1$, since $s \equiv 0 \pmod d$ and χ is a character of order d. If $x = 0$, then $\chi(x) = 0$. Thus , we can write (2.3) as

$$\sum_{x\in F_q^*} \chi\{x(x+c_1)(x+c_2)\ldots(x+c_{s-1})\}$$

$$= \sum_{x\in F_q^*} \chi(x^{-1})^s\chi\{x(x+c_1)(x+c_2)\ldots(x+c_{s-1})\}$$

$$= \sum_{x\in F_q^*} \chi\{xx^{-1}(xx^{-1}+c_1x^{-1})(xx^{-1}+c_2x^{-1})\ldots(xx^{-1}+c_{s-1}x^{-1})\}$$

$$= \sum_{x\in F_q^*} \chi\{(1+c_1x^{-1})(1+c_2x^{-1})\ldots(1+c_{s-1}x^{-1})\}.$$

Since, for each i, $c_i \neq 0$, then c_i^{-1} exists. Further, $\chi(c_1c_1^{-1}c_2c_2^{-1}\ldots c_{s-1}c_{s-1}^{-1}) = 1$. Now using the same idea as above we can write

$$\sum_{x\in F_q^*} \chi\{(1+c_1x^{-1})(1+c_2x^{-1})\ldots(1+c_{s-1}x^{-1})\}$$

$$= \sum_{x\in F_q^*} \chi(c_1c_2\ldots c_{s-1})\chi\{(c_1^{-1}+x^{-1})(c_2^{-1}+x^{-1})\ldots(c_{s-1}^{-1}+x^{-1})\}. \qquad (2.4)$$

Let $c = c_1c_2\ldots c_{s-1}$. Since $c_i \neq 0$, for each i, we have $c \neq 0$. As x assumes all values in $\mathbf{F}_q^*$, so does x^{-1}. Hence, we can write (2.4) as

$$\sum_{x\in F_q^*} \chi(c)\chi\{(x+c_1^{-1})(x+c_2^{-1})\ldots(x+c_{s-1}^{-1})\}$$

$$= \sum_{x\in F_q} \chi(c)\chi\{(x+c_1^{-1})(x+c_2^{-1})\ldots(x+c_{s-1}^{-1})\} - \chi(c)\chi(c^{-1})$$

$$= \sum_{x \in F_q} \chi\{c(x + c_1^{-1})(x + c_2^{-1}) \dots (x + c_{s-1}^{-1})\} - 1.$$

This completes the proof of the lemma. ❑

Using Lemma 2.1, we have the following corollary to Lemma 2.2.

Corollary. Let χ be a nontrivial character of order d of $\mathbf{F}_q$. If $a_1, a_2, \dots, a_s$ are distinct elements of $\mathbf{F}_q$ and $s \equiv 0 (\text{mod } d)$ then

$$\left| \sum_{x \in F_q} \chi\{(x - a_1)(x - a_2)\dots(x - a_s)\} \right| \leq 1 + (s-2)\sqrt{q}.$$ ❑

Let g be a fixed primitive element of the finite field $\mathbf{F}_q$; that is g is a generator of the cyclic group $\mathbf{F}_q^*$. Define a function α by

$$\alpha(g^t) = e^{\frac{2\pi i t}{3}},$$

where $i^2 = -1$. Therefore, α is a cubic character, character of order 3, of $\mathbf{F}_q$. The values of α are the elements of the set $\{1, \omega, \omega^2\}$ where $\omega = e^{\frac{2\pi i}{3}}$. Note that α^2 is also a cubic character and $\overline{\alpha} = \alpha^2$. Moreover, if a is not a cubic of an element of $\mathbf{F}_q^*$, then $\alpha(a) + \alpha^2(a) = -1$.

Further, define a function β by

$$\beta(g^t) = i^t.$$

Therefore, β is the quadruple character, character of order 4, of $\mathbf{F}_q$. The values of β are in the set $\{1, -1, i, -i\}$. Observe that β^3 is also a quadruple character and $\overline{\beta} = \beta^3$ while β^2 is a quadratic character. Moreover, if a is not a quadruple of an element of $\mathbf{F}_q^*$, then $\beta(a) + \beta^2(a) + \beta^3(a) = -1$.

Lemma 2.3. Let α be a cubic character of $\mathbf{F}_q$ and let A and B be disjoint subsets of $\mathbf{F}_q$. Put

$$g = \sum_{x\in F_q} \prod_{a\in A}\{1 + \alpha(x-a) + \alpha^2(x-a)\}\prod_{b\in B}\{2 - \alpha(x-b) - \alpha^2(x-b)\}.$$

As usual, an empty product is defined to be 1. Then

$$g \geq 2^n q - (t2^{t-1} - 2^t + 1)2^t\sqrt{q},$$

where $|A| = m$, $|B| = n$ and $t = m + n$.

Proof: Let $A \cup B = \{c_1, c_2, \dots, c_t\}$. Expanding g and noting that $\sum_{x\in F_q} 2^n = 2^n q$, we can write

$$\begin{aligned}|g - 2^n q| \leq & \left|\sum_{x\in F_q}\sum_{\chi\in\{\alpha,\alpha^2\}}\sum_{i=1}^{t} 2^{t-1}\chi(x-c_i)\right| + \\ & \left|\sum_{x\in F_q}\sum_{\chi_j\in\{\alpha,\alpha^2\}}\sum_{i_1<i_2} \{2^{t-2}\chi_1(x-c_{i_1})\chi_2(x-c_{i_2})\}\right| + \dots + \\ & \left|\sum_{x\in F_q}\sum_{\chi_j\in\{\alpha,\alpha^2\}}\sum_{i_1<i_2<\dots<i_s} \{2^{t-s}\chi_1(x-c_{i_1})\chi_2(x-c_{i_2})\dots\chi_s(x-c_{i_s})\}\right| + \dots + \\ & \left|\sum_{x\in F_q}\sum_{\chi_j\in\{\alpha,\alpha^2\}} \{\chi_1(x-c_1)\chi_2(x-c_2)\dots\chi_t(x-c_t)\}\right|.\end{aligned}$$

Now, by (2.1) and Lemma 2.1 we obtain

$$\begin{aligned}|g - 2^n q| &\leq \sum_{s=1}^{t} 2^s 2^{t-s}\binom{t}{s}(s-1)\sqrt{q} \\ &= (t2^{t-1} - 2^t + 1)2^t\sqrt{q}.\end{aligned}$$

Therefore, $g \geq 2^n q - (t2^{t-1} - 2^t + 1)2^t\sqrt{q}$ as required. ❑

Lemma 2.4. Let α be a cubic character of $\mathbf{F}_q$ and A be a subset of m vertices of $\mathbf{F}_q$. Put

$$g = \sum_{x\in F_q} \prod_{a\in A}\{1 + \alpha(x-a) + \alpha^2(x-a)\}.$$

As usual, an empty product is defined to be 1. Then

$$g \geq q - [1 - m^2 + m + (2m-3)3^{m-1})]\sqrt{q} - (m^2 - m).$$

Proof: Let $A = \{a_1, a_2, \dots, a_m\}$. We can write

$$g = \sum_{x\in F_q} 1 + \sum_{x\in F_q}\sum_{\chi\in\{\alpha,\alpha^2\}}\sum_{i=1}^{m} \chi(x-a_i) +$$

$$\sum_{x\in F_q}\sum_{\chi_j\in\{\alpha,\alpha^2\}}\sum_{i_1<i_2}\{\chi_1(x-a_{i_1})\chi_2(x-a_{i_2})\}+\ldots+$$

$$\sum_{x\in F_q}\sum_{\chi_j\in\{\alpha,\alpha^2\}}\sum_{i_1<i_2<\ldots<i_s}\{\chi_1(x-a_{i_1})\chi_2(x-a_{i_2})\ldots\chi_s(x-a_{i_s})\}+\ldots+$$

$$\sum_{x\in F_q}\sum_{\chi_j\in\{\alpha,\alpha^2\}}\{\chi_1(x-a_1)\chi_2(x-a_2)\ldots\chi_m(x-a_m)\}. \tag{2.5}$$

Consider

$$h=\sum_{x\in F_q}\sum_{\chi_j\in\{\alpha,\alpha^2\}}\{\chi_1(x-a_{i_1})\chi_2(x-a_{i_2})\}$$

for some a_{i_1}, a_{i_2} with $i_1 < i_2$. Then by using (2.2) we have

$$h=\sum_{x\in F_q}\{\alpha(x-a_{i_1})\alpha(x-a_{i_2})+\alpha(x-a_{i_1})\alpha^2(x-a_{i_2})+\alpha^2(x-a_{i_1})\alpha(x-a_{i_2})+$$

$$\alpha^2(x-a_{i_1})\alpha^2(x-a_{i_2})\}$$

$$=-2+\sum_{x\in F_q}\{\alpha(x-a_{i_1})\alpha(x-a_{i_2})+\alpha^2(x-a_{i_1})\alpha^2(x-a_{i_2})\}.$$

Using the same idea as above together with (2.1), (2.2) and Lemma 2.1 we get from (2.5)

$$|g-[q-(m^2-m)]|\le\sum_{s=3}^{m}2^s\binom{m}{s}(s-1)\sqrt{q}+(m^2-m)\sqrt{q}$$

$$=[1+(2m-3)3^{m-1}-(m^2-m)]\sqrt{q}.$$

Therefore, $g \ge q-[1-m^2+m+(2m-3)3^{m-1})]\sqrt{q}-(m^2-m)$ as required. ❑

Lemma 2.5. Let β be a quadruple character of $\mathbf{F}_q$ and let A and B be disjoint subsets of $\mathbf{F}_q$. Put

$$g=\sum_{x\in F_q}\prod_{a\in A}\{1+\beta(x-a)+\beta^2(x-a)+\beta^3(x-a)\}\prod_{b\in B}\{3-\beta(x-b)-\beta^2(x-b)-\beta^3(x-b)\}.$$

As usual, an empty product is defined to be 1. Then

$$g\ge 3^n q-(t2^{t-1}-2^t+1)3^t\sqrt{q},$$

where $|A| = m$, $|B| = n$ and $t = m + n$.

Proof: Let $A \cup B = \{c_1, c_2, \ldots, c_t\}$. Expanding g and noting that $\sum_{x\in F_q} 3^n = 3^n q$, we can write

$$\left| g - 3^n q \right| \le \left| \sum_{x\in F_q} \sum_{\chi\in\{\beta,\beta^2,\beta^3\}} \sum_{i=1}^{t} 3^{t-1}\chi(x-c_i) \right| +$$

$$\left| \sum_{x\in F_q} \sum_{\chi_j\in\{\beta,\beta^2,\beta^3\}} \sum_{i_1<i_2} \{3^{t-2}\chi_1(x-c_{i_1})\chi_2(x-c_{i_2})\} \right| + \ldots +$$

$$\left| \sum_{x\in F_q} \sum_{\chi_j\in\{\beta,\beta^2,\beta^3\}} \sum_{i_1<i_2<\ldots<i_s} \{3^{t-s}\chi_1(x-c_{i_1})\chi_2(x-c_{i_2})\ldots\chi_s(x-c_{i_s})\} \right| + \ldots +$$

$$\left| \sum_{x\in F_q} \sum_{\chi_j\in\{\beta,\beta^2,\beta^3\}} \{\chi_1(x-c_1)\chi_2(x-c_2)\ldots\chi_t(x-c_t)\} \right| .$$

Now, by (2.1) and Lemma 2.1 we have

$$\left| g - 3^n q \right| \le \sum_{s=1}^{t} 3^s 3^{t-s}\binom{t}{s}(s-1)\sqrt{q}$$

$$= (t2^{t-1} - 2^t + 1)3^t\sqrt{q}\,.$$

Therefore, $g \ge 3^n q - (t2^{t-1} - 2^t + 1)3^t\sqrt{q}$ as required. ❑

Lemma 2.6. Let β be a quadruple character of $\mathbf{F}_q$ and A be a subset of m vertices of $\mathbf{F}_q$. Put

$$g = \sum_{x\in F_q} \prod_{a\in A} \{ 1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)\}.$$

As usual, an empty product is defined to be 1. Then

$$g \ge q - [1 + (3n-4)4^{m-1}]\sqrt{q}\,.$$

Proof: Let $A = \{a_1, a_2, \ldots, a_m\}$. We can write

$$g = \sum_{x\in F_q} 1 + \sum_{x\in F_q} \sum_{\chi\in\{\beta,\beta^2,\beta^3\}} \sum_{i=1}^{m} \chi(x-a_i) +$$

$$\sum_{x\in F_q} \sum_{\chi_j\in\{\beta,\beta^2,\beta^3\}} \sum_{i_1<i_2} \{\chi_1(x-a_{i_1})\chi_2(x-a_{i_2})\} + \ldots +$$

$$\sum_{x\in F_q} \sum_{\chi_j\in\{\beta,\beta^2,\beta^3\}} \sum_{i_1<i_2<\ldots<i_s} \{\chi_1(x-a_{i_1})\chi_2(x-a_{i_2})\ldots\chi_s(x-a_{i_s})\} + \ldots +$$

$$\sum_{x\in F_q} \sum_{\chi_j\in\{\beta,\beta^2,\beta^3\}} \{\chi_1(x-a_1)\chi_2(x-a_2)\ldots\chi_m(x-a_m)\}.$$

Then, by (2.1) and Lemma 2.1 we have

$$| g - q | \le \sum_{s=1}^{m} 3^s \binom{m}{s} (s-1)\sqrt{q}$$

$$= [1 + (3m - 4)4^{m-1}]\sqrt{q}.$$

Therefore, $g \ge q - [1 + (3m - 4)4^{m-1}]\sqrt{q}$ as required. ❑

3. The Generalized Paley Graphs

For $q \equiv 1 \pmod 3$ a prime power, there exists a cubic character α of $\mathbf{F}_q$ and $\alpha(-a) = \alpha(a)$ for all $a \in \mathbf{F}_q$. Further, for $q \equiv 1 \pmod 8$ a prime power, there exists a quadruple character β of $\mathbf{F}_q$ and $\beta(-a) = \beta(a)$ for all $a \in \mathbf{F}_q$.

Observe that if a and b are any vertices of $G_q^{(3)}$, then for t = 1 and 2

$$\alpha^t(a-b) = \begin{cases} 1, & \text{if a is adjacent to b,} \\ 0, & \text{if } a = b, \\ \omega \text{ or } \omega^2, & \text{otherwise.} \end{cases}$$

Also, if a and b are any vertices of $G_q^{(4)}$, then for t = 1 and 3

$$\beta^t(a-b) = \begin{cases} 1, & \text{if a is adjacent to b,} \\ 0, & \text{if } a = b, \\ -1, i \text{ or } -i, & \text{otherwise.} \end{cases}$$

Note that β^2 is a quadratic character; that is

$$\beta^2(a-b) = \begin{cases} 1, & \text{if } a-b \text{ is a quadratic ressidue,} \\ 0, & \text{if } a = b, \\ -1, & \text{otherwise.} \end{cases}$$

Before stating our results, we need the following notation. For disjoint subsets A and B of V(G), we denote by n(A/B) the number of vertices of G not in $A \cup B$ that are adjacent to each vertex of A but not adjacent to any vertex of B. When $A = \{a_1, a_2, \dots, a_m\}$ and $B = \{b_1, b_2, \dots, b_n\}$, we sometimes write for convenience $n(A/B) = n(a_1, a_2, \dots, a_m / b_1, b_2, \dots, b_n)$.

Theorem 3.1. Let $q \equiv 1 (\mathrm{mod}\ 3)$ be a prime power and k a positive integer. If

$$q > [\frac{1}{4}(79 + 3\sqrt{36k + 701})]^2,$$

then $G_q^{(3)} \in \mathcal{G}(2,2,k)$.

Proof: Let $S = \{a, b, c, d\}$ be any set of distinct vertices of $G_q^{(3)}$. Then $n(a, b/c, d) \geq k$ if and only if

$$f = \sum_{\substack{x \in F_q \\ x \notin S}} \{[1 + \alpha(x-a) + \alpha^2(x-a)][1 + \alpha(x-b) + \alpha^2(x-b)]$$

$$[2 - \alpha(x-c) - \alpha^2(x-c)][2 - \alpha(x-d) - \alpha^2(x-d)]\}$$

$$\geq k3^4.$$

To show that $f \geq k3^4$, it is clearly sufficient to establish that $f > (k-1)3^4$.

We can write

$$g = \sum_{x \in F_q} \{[1 + \alpha(x-a) + \alpha^2(x-a)][1 + \alpha(x-b) + \alpha^2(x-b)]$$

$$[2 - \alpha(x-c) - \alpha^2(x-c)][2 - \alpha(x-d) - \alpha^2(x-d)]\}$$

$$= \sum_{x \in F_q} 4 + \sum_{x \in F_q} \sum_{\chi \in \{\alpha, \alpha^2\}} \{4\chi(x-a) + 4\chi(x-b) - 2\chi(x-c) - 2\chi(x-d)\} +$$

$$\sum_{x \in F_q} \sum_{\chi_i \in \{\alpha, \alpha^2\}} \{\chi_1(x-c)\chi_2(x-d) - 2\chi_1(x-a)\chi_2(x-c) -$$

$$2\chi_1(x-a)\chi_2(x-d) - 2\chi_1(x-b)\chi_2(x-c) -$$

$$2\chi_1(x-b)\chi_2(x-d) + 4\chi_1(x-a)\chi_2(x-b)\} +$$

$$\sum_{x \in F_q} \sum_{\chi_i \in \{\alpha, \alpha^2\}} \{\chi_1(x-a)\chi_2(x-c)\chi_3(x-d) + \chi_1(x-b)\chi_2(x-c)\chi_3(x-d) -$$

$$2\chi_1(x-a)\chi_2(x-b)\chi_3(x-c) - 2\chi_1(x-a)\chi_2(x-b)\chi_3(x-d)\} +$$

$$\sum_{x \in F_q} \sum_{\chi_i \in \{\alpha, \alpha^2\}} \{\chi_1(x-a)\chi_2(x-b)\chi_3(x-c)\chi_4(x-d)\}. \quad (3.1)$$

Now, by (2.1) (2.2) and Lemma 2.1 we get from (3.1)

$$g = 4q + 0 + [\sum_{x \in F_q} \alpha(x-c)\alpha(x-d) + \sum_{x \in F_q} \alpha^2(x-c)\alpha^2(x-d) - 2] -$$

$$2[\sum_{x \in F_q} \alpha(x-a)\alpha(x-c) + \sum_{x \in F_q} \alpha^2(x-a)\alpha^2(x-c) - 2] -$$

$$2[\sum_{x\in F_q} \alpha(x-a)\alpha(x-d) + \sum_{x\in F_q} \alpha^2(x-a)\alpha^2(x-d) - 2] -$$

$$2[\sum_{x\in F_q} \alpha(x-b)\alpha(x-c) + \sum_{x\in F_q} \alpha^2(x-b)\alpha^2(x-c) - 2] -$$

$$2[\sum_{x\in F_q} \alpha(x-b)\alpha(x-d) + \sum_{x\in F_q} \alpha^2(x-b)\alpha^2(x-d) - 2] +$$

$$4[\sum_{x\in F_q} \alpha(x-a)\alpha(x-b) + \sum_{x\in F_q} \alpha^2(x-a)\alpha^2(x-b) - 2] +$$

$$\sum_{x\in F_q} \sum_{\chi_i\in\{\alpha,\alpha^2\}} \{\chi_1(x-a)\chi_2(x-c)\chi_3(x-d) + \chi_1(x-b)\chi_2(x-c)\chi_3(x-d) -$$

$$2\chi_1(x-a)\chi_2(x-b)\chi_3(x-c) - 2\chi_1(x-a)\chi_2(x-b)\chi_3(x-d)\} +$$

$$\sum_{x\in F_q} \sum_{\chi_i\in\{\alpha,\alpha^2\}} \{\chi_1(x-a)\chi_2(x-b)\chi_3(x-c)\chi_4(x-d)\}.$$

By first applying (2.1) and Lemma 2.2 and then applying Lemma 2.1 we obtain

$$|g-4q-10| \le 2\sqrt{q} + 4\sqrt{q} + 4\sqrt{q} + 4\sqrt{q} + 4\sqrt{q} + 8\sqrt{q} +$$

$$[6((3-1)\sqrt{q}) + 2(3-2)\sqrt{q}] + [6((3-1)\sqrt{q}) + 2(3-2)\sqrt{q}] +$$

$$2[6((3-1)\sqrt{q}) + 2(3-2)\sqrt{q}] + 2[6((3-1)\sqrt{q}) + 2(3-2)\sqrt{q}] + 16(3\sqrt{q})$$

$$= 158\sqrt{q}.$$

Therefore,

$$g \ge 4q + 10 - 158\sqrt{q}.$$

Consider

$$g - f = \{1 + \alpha(a-b) + \alpha^2(a-b)\}\{2 - \alpha(a-c) - \alpha^2(a-c)\}\{2 - \alpha(a-d) - \alpha^2(a-d)\} +$$

$$\{1 + \alpha(b-a) + \alpha^2(b-a)\}\{2 - \alpha(b-c) - \alpha^2(b-c)\}\{2 - \alpha(b-d) - \alpha^2(b-d)\} +$$

$$2\{1 + \alpha(c-a) + \alpha^2(c-a)\}\{1 + \alpha(c-b) + \alpha^2(c-b)\}\{2 - \alpha(c-d) - \alpha^2(c-d)\} +$$

$$2\{1 + \alpha(d-a) + \alpha^2(d-a)\}\{1 + \alpha(d-b) + \alpha^2(d-b)\}\{2 - \alpha(d-c) - \alpha^2(d-c)\}$$

$$\le 108,$$

since $g - f$ achieves its maximum value when $ab, cd \notin E(G)$ and $ac, ad, bc, bd \in E(G)$.

Consequently,

$$f \ge g - 108$$

$$\ge 4q + 10 - 158\sqrt{q} - 108.$$

Hence, $f > (k-1)3^4$ for $q > [\frac{1}{4}(79 + 3\sqrt{36k+701})]^2$. As S is arbitrary, this completes the proof. ❑

Remark 1. When k = 1, Theorem 3.1 above asserts that $G_q^{(3)} \in \mathcal{G}(2,2,1)$ for all prime powers ≥ 1609. We have verified, using the computer, that $G_q^{(3)} \in \mathcal{G}(2,2,1)$ only if q is a prime power of order 151, 157 or at least 223. Table I gives the maximum k for which $G_q^{(3)} \in \mathcal{G}(2,2,k)$; we give only some of the computational results.

Table I. Maximum k for which $G_q^{(3)} \in \mathcal{G}(2,2,k)$.

Maximum k	Order q	Maximum k	Order q
0	≤ 139 and 163	14	601, 613, 619, 631, 634
1	151, 157, 223	15	661
2	169, 181, 193, 199, 229	16	673, 625
3	211, 241, 271, 361	17	691, 709, 769
4	256, 277, 289, 313	18	727, 733, 757
5	283, 307, 331	19	751
6	337, 343, 349, 373, 379	20	739, 787, 811, 829
7	367, 397, 409	22	823
8	433, 439, 463, 523	23	859, 883
9	421, 457, 487, 529	24	853, 877, 907
11	499	25	919, 937
12	547, 571, 577	27	967, 991
13	541, 607	28	997, 1009

For the class $\mathcal{G}(m,n,k)$, we have the following result.

Theorem 3.2. Let $q \equiv 1 \pmod 3$ be a prime power and k a positive integer. If

$$q > (t2^{t-1} - 2^t + 1)2^m\sqrt{q} + (m + 2n + 3k - 3)2^{-n}3^{t-1}, \quad (3.2)$$

then $G_q^{(3)} \in \mathcal{G}(m,n,k)$ for all m, n with $m + n \leq t$.

Proof: It clearly suffices to establish the result for $m + n = t$. Let A and B be disjoint subsets of $V(G_q^{(3)})$ with $|A| = m$ and $|B| = n$. Then, $n(A/B) \geq k$ if and only if

$$f = \sum_{\substack{x \in F_q \\ x \notin A \cup B}} \prod_{a \in A} \{1 + \alpha(x-a) + \alpha^2(x-a)\} \prod_{b \in B} \{2 - \alpha(x-b) - \alpha^2(x-b)\}$$

$$> (k-1)3^t.$$

Let

$$g = \sum_{x \in F_q} \prod_{a \in A} \{1 + \alpha(x-a) + \alpha^2(x-a)\} \prod_{b \in B} \{2 - \alpha(x-b) - \alpha^2(x-b)\}.$$

Now, by Lemma 2.3 we have

$$g \geq 2^n q - (t2^{t-1} - 2^t + 1)2^t \sqrt{q}.$$

Consider

$$g - f = \sum_{x \in A \cup B} \prod_{a \in A} \{1 + \alpha(x-a) + \alpha^2(x-a)\} \prod_{b \in B} \{2 - \alpha(x-b) - \alpha^2(x-b)\}.$$

Since, in the product $\prod_{a \in A} \{1 + \alpha(x-a) + \alpha^2(x-a)\}$ each factor is at most 3 and one factor is 1 and in the product $\prod_{b \in B} \{2 - \alpha(x-b) - \alpha^2(x-b)\}$ each factor is at most 3 and one factor is 2 we have

$$g - f \leq 3^{t-1}m + 3^{t-1}2n$$
$$= (m + 2n)3^{t-1}.$$

Consequently,

$$f \geq 2^n q - (t2^{t-1} - 2^t + 1)2^t \sqrt{q} - (m + 2n)3^{t-1}.$$

Now, if inequality (3.2) holds, then $f > (k-1)3^t$ as required . Since A and B are arbitrary, this completes the proof of the theorem. ❑

For the case $n = 0$, we have the following sharper result.

Theorem 3.3. Let $q \equiv 1 \pmod 3$ be a prime power and k a positive integer. If

$$q > [1 - m^2 + m + (2m-3)3^{m-1}]\sqrt{q} + (m^2 - m) + (3k-2)3^{m-1}, \tag{3.3}$$

then $G_q^{(3)} \in \mathcal{G}(m,0,k)$.

Proof: Let A be any subset of m vertices of $G_q^{(3)}$. Then there are at least k other vertices, each of which is adjacent to every vertex of A if and only if

$$f = \sum_{\substack{x \in F_q \\ x \notin A}} \prod_{a \in A} \{ 1 + \alpha(x-a) + \alpha^2(x-a)\} > (k-1)3^m.$$

Let

$$g = \sum_{x \in F_q} \prod_{a \in A} \{ 1 + \alpha(x-a) + \alpha^2(x-a)\}.$$

Then, by Lemma 2.4 we have

$$g \geq q - [1 - m^2 + m + (2m-3)3^{m-1})]\sqrt{q} - (m^2 - m).$$

Consider

$$g - f = \sum_{x \in A} \prod_{a \in A} \{ 1 + \alpha(x-a) + \alpha^2(x-a)\}$$
$$\leq 3^{m-1},$$

since, each factor is at most 3 and one factor is 1.

Therefore,

$$f \geq q - [1 - m^2 + m + (2m-3)3^{m-1})]\sqrt{q} - (m^2 - m) - 3^{m-1}.$$

Now, if inequality (3.3) holds, then $f > (k-1)3^m$ as required. As A is arbitrary, this completes the proof of the theorem. ❑

We now turn our attention to the adjacent properties of the quadruple Paley graph $G_q^{(4)}$.

Theorem 3.4. Let $q \equiv 1 \pmod 8$ be a prime power and k a positive integer. If

$$q > [\frac{1}{6}(291 + \sqrt{1024k + 85193})]^2, \tag{3.4}$$

then $G_q^{(4)} \in \mathcal{G}(2,2,k)$.

Proof: Let $S = \{a, b, c, d\}$ be any set of distinct vertices of $G_q^{(4)}$. Then $n(a, b/c, d) \geq k$ if and only if

$$f = \sum_{\substack{x \in F_q \\ x \notin S}} \{[1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)][1 + \beta(x-b) + \beta^2(x-b) + \beta^3(x-b)]$$

$$[3 - \beta(x-c) - \beta^2(x-c) - \beta^3(x-c)][3 - \beta(x-d) - \beta^2(x-d) - \beta^3(x-d)]\}$$

$$> (k-1)4^4.$$

We can write

$$g = \sum_{x \in F_q} \{[1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)][1 + \beta(x-b) + \beta^2(x-b) + \beta^3(x-b)]$$

$$[3 - \beta(x-c) - \beta^2(x-c) - \beta^3(x-c)][3 - \beta(x-d) - \beta^2(x-d) - \beta^3(x-d)]\}.$$

Now using an argument similar to that used in the proof of Theorem 3.1 (except here we do not use (2.2)) we obtain:

$$|g - 9q| \le 9(9\sqrt{q}) + 12(9\sqrt{q}) + 9\sqrt{q} + 54(2\sqrt{q}) + 162(2\sqrt{q}) + 81(3\sqrt{q})$$

$$= 873\sqrt{q}. \quad .$$

Observe that

$$g - f \le 384,$$

since $g - f$ achieves its maximum value when ab, cd $\notin E(G)$ and ac, ad, bc, bd $\in E(G)$.

Consequently,

$$f \ge 9q - 873\sqrt{q} - 384.$$

Hence, $f > (k-1)4^4$ when (3.4) holds. As S is arbitrary, this completes the proof. ❑

For the class $\mathcal{G}(m,n,k)$, we have the following result.

Theorem 3.5. Let $q \equiv 1 \pmod 8$ be a prime power and k a positive integer. If

$$q > (t2^{t-1} - 2^t + 1)3^m\sqrt{q} + (m + 3n + 4k - 4)3^{-n}4^{t-1}, \qquad (3.5)$$

then $G_q^{(4)} \in \mathcal{G}(m,n,k)$ for all m, n with $m + n \le t$.

Proof: It clearly suffices to establish the result for $m + n = t$. Let A and B be disjoint subsets of $V(G_q^{(4)})$ with $|A| = m$ and $|B| = n$. Then, $n(A/B) \ge k$ if and only if

$$f = \sum_{\substack{x \in F_q \\ x \notin A \cup B}} \prod_{a \in A} \{1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)\} \prod_{b \in B} \{3 - \beta(x-b) - \beta^2(x-b) - \beta^3(x-b)\}$$

$$> (k-1)4^t.$$

Let

$$g = \sum_{x \in F_q} \prod_{a \in A} \{1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)\} \prod_{b \in B} \{3 - \beta(x-b) - \beta^2(x-b) - \beta^3(x-b)\}.$$

Now, by Lemma 2.5, we have

$$g \geq 3^n q - (t2^{t-1} - 2^t + 1)3^t \sqrt{q}.$$

Consider

$$g - f = \sum_{x \in A \cup B} \prod_{a \in A} \{1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)\} \prod_{b \in B} \{3 - \beta(x-b) - \beta^2(x-b) - \beta^3(x-b)\}.$$

Since, in the product $\prod_{a \in A} \{1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)\}$ each factor is at most 4 and one factor is 1 and in the product $\prod_{b \in B} \{3 - \beta(x-b) - \beta^2(x-b) - \beta^3(x-b)\}$ each factor is at most 4 and one factor is 3 we have

$$\begin{aligned} g - f &\leq 4^{t-1}m + 4^{t-1}3n \\ &= (m + 3n)4^{t-1}. \end{aligned}$$

Consequently,

$$f \geq 3^n q - (t2^{t-1} - 2^t + 1)3^t \sqrt{q} - (m + 3n)4^{t-1}.$$

Now, if inequality (3.5) holds, then $f > (k-1)4^t$ as required. Since A and B are arbitrary, this completes the proof of the theorem. ❑

For the case $n = 0$, we have the following result.

Theorem 3.6. Let $q \equiv 1 (\text{mod } 8)$ be a prime power and k a positive integer. If

$$q > [1 + (3m - 4)4^{m-1}]\sqrt{q} + (4k - 3)4^{m-1}, \qquad (3.6)$$

then $G_q^{(4)} \in \mathcal{G}(m,0,k)$.

Proof: Let A be any subset of m vertices of $G_q^{(4)}$. Then there are at least k other vertices, each of which is adjacent to every vertex of A if and only if

$$f = \sum_{\substack{x \in F_q \\ x \notin A}} \prod_{a \in A} \{1 + \beta(x-a) + \beta^2(x-a) + \beta^3(x-a)\} > (k-1)4^m.$$

Now using the method of proof of Theorem 3.3 together with Lemma 2.6, we get $f > (k-1)4^m$ when (3.6) holds. Hence, the result. ❑

ACKNOWLEDGEMENTS

Thanks due to Prof. L. Caccetta for several useful suggestion. Some of this work was done while the author was visiting Department of Electrical and Electronics Engineering, Ehime University, Matsuyama, Japan under financial support by The Matsumae International Foundation, Tokyo, Japan.

REFERENCES

[1] B. Alspach, C.C. Chen and K. Heinrich, **Characterization of a class of triangle–free graphs with a certain adjacency property,** J. Graph Theory 15 (1991), 375–388.

[2] W. Ananchuen and L. Caccetta, **Graphs with a prescribed adjacency property,** The Australasian Journal of Combinatorics 6 (1992), 155–175.

[3] W. Ananchuen and L. Caccetta, **On the adjacency properties of Paley graphs,** Networks, 23 (1993), 227–236.

[4] W. Ananchuen and L. Caccetta, **On graphs satisfying a strong adjacency property,** The Australasian Journal of Combinatorics 8 (1993), 153–168.

[5] W. Ananchuen and L. Caccetta, **On constructing graphs with a prescribed adjacency property,** The Australasian Journal of Combinatorics 10 (1994), 75–83.

[6] W. Ananchuen and L. Caccetta, A **note on graphs with a prescribed adjacency property,** The Bulletin of the Australian Mathematics Society, 50 (1994), 5–15.

[7] A. Blass, G. Exoo and F. Harary, **Paley graphs satisfy all first–order adjacency axioms,** J. Graph Theory 5 (1981), 435–439.

[8] A. Blass and F. Harary, **Properties of almost all graphs and complexes,** J. graph Theory 3 (1979), 225–240.

[9] B. Bollobás, **Random Graphs.** Academic Press, London (1985).

[10] J.A. Bondy and U.S.R. Murty, **Graph Theory with Applications.** The MacMillan Press, London (1976).

[11] L. Caccetta, P. Erdös and K. Vijayan, **A property of random graphs,** ARS Combinatoria 19A (1985), 287–294.

[12] L. Caccetta and K. Vijayan, **On minimal graphs with prescribed adjacency property,** ARS Combinatoria 21A (1986), 21–29.

[13] G. Exoo, **On an adjacency property of graphs,** J. Graph Theory 5 (1981), 371–378.

[14] G. Exoo and F. Harary, **The smallest graphs with certain adjacency properties,** Discrete math. 29 (1980), 25–32.

[15] G. Exoo and F. Harary, **The smallest graphs with certain adjacency properties,** Discrete Math. 29 (1980), 25–32.

[16] K. Heinrich, **Graphs determined by an adjacency property,** J. Combinatorial Mathematics and Combinatorial Computing 7 (1990), 3–9.

[17] R. Lidl and H. Niederreiter, **Finite Fields.** Addison–Wesley, London (1983).

[18] W.M. Schmidt, **Equations over Finite Fields, An Elementary Approach.** Lecture Notes in Mathematics, Vol. 536. Springer–Verlag, Berlin (1976).

(Received 16/6/2000)