JOURNAL OF COMBINATORIAL THEORY, Series B 30, 364–371 (1981)

Note

On the Number of Complete Subgraphs Contained in Certain Graphs

R. J. EVANS

University of San Diego, San Diego, California

AND

J. R. PULHAM AND J. SHEEHAN

University of Aberdeen, Aberdeen, Scotland

Communicated by the Managing Editors

Received October 5, 1979

We count the number of complete graphs of order 4 contained in certain graphs.

1. INTRODUCTION

Let $G^{(p)}$ be a graph of p vertices and let $\bar{G}^{(p)}$ be its complement. Let $k_m(G^{(p)})$ be the number of complete subgraphs of order m contained in $G^{(p)}$. Let

$$T_m(p) = \min(k_m(G^{(p)}) + k_m(\bar{G}^{(p)})),$$

where the minimum is taken over all graphs of p vertices. All of our terminology is now fairly standard and is to be found in either [2] or [8]. Erdös [4], using a simple counting argument, proved that

$$T_m(p) \leqslant \binom{p}{m} \Big/ 2^{\binom{m}{2}-1} \tag{1}$$

and conjectured that

$$\lim_{p\to\infty} T_m(p) \Big/ \binom{p}{m} = 2^{1-\binom{m}{2}}. \tag{2}$$

0095-8956/81/030364-08$02.00/0

In particular this would imply that

$$T_4(p) \sim \frac{1}{32}\binom{p}{4}. \tag{3}$$

Erdös comments on the difficulty of finding graphs G which give values of $k_4(G) + k_4(\bar{G})$ as small as $\binom{p}{4}/32$.

Goodman [6] calculated $T_3(p)$ exactly and showed that

$$T_3(p) \geqslant p(p-1)(p-5)/24. \tag{4}$$

The degree sequence of $G^{(p)}$ determines $k_3(G^{(p)}) + k_3(\bar{G}^{(p)})$ which is why the exact calculation of $T_3(p)$ proved to be a tractable and simple problem. The fact that this no longer holds true is the intrinsic reason why any such exact calculation of $T_m(p)$ $(m > 3)$ is likely to be very difficult. Write $w(p) = (p(p-1)(p-5)(p-17)/24)/32$. We prove that if p is prime and $p = 4u^2 + 1$ for some integer u, then

$$T_4(p) \leqslant w(p). \tag{5}$$

In view of (4), one might have suspected that

$$T_4(p) \geqslant w(p) \tag{6}$$

for general p. However, Thomason [10] has shown that this is false. The reader familiar with Ramsey theory will notice another pretty way of expressing $w(p)$. Write $r_s = r(K_s) - 1$, where $r(K_s)$ is the Ramsey number of K_s. Then

$$w(p) = (((p - r_1)(p - r_2)(p - r_3)(p - r_4))/24)/32.$$

To prove (5) we need to calculate $k_4(G(p))$ (see Theorem 1) for a certain well-known self-complementary graph $G(p)$. The calculations depend on some well-known techniques in number theory involving quadratic residues. In this context Proposition 3 may well be of independent interest.

2. Main Theorem

Let $p = 4k + 1$ be a prime number. Let $G(p)$ be the graph with vertices $\{0, 1, 2, \ldots, p-1\}_{\bmod p}$ and edges defined by

$$ij \in E \Leftrightarrow i - j \in R,$$

where R is the set of quadratic residues modulo p. This is the so-called Paley graph. This graph was used by Greenwood and Gleason [7] to show that

$r(K_4) = 18$. Let $H = \langle R \rangle$ be the subgraph of $G(p)$ induced by R. Let R_1 be the set of vertices in H which are neighbours of 1, i.e., $x \in R_1$ if and only if $x \in R$ and $x - 1 \in R$. Write $H_1 = \langle R_1 \rangle$. It is well known [3] that $|R_1| = k - 1$. Write

$$f(p) = |E(H_1)|.$$

PROPOSITION 1. $k_4(G(p)) = (p(p-1)\, f(p))/24$.

Proof. Since $G(p)$ is vertex transitive

$$k_4(G(p)) = (p \cdot k_3(H))/4 \tag{7}$$

and since H is also vertex transitive

$$\begin{aligned} k_3(H) &= (|V(H)| \cdot k_2(H_1))/3 \\ &= ((p-1)\, f(p))/6. \end{aligned} \tag{8}$$

The result follows from (7) and (8). Notice that $G(p)$ and H are both vertex transitive since for any vertex a of $G(p)$ and any $b \in R$ the map $x \mapsto a + bx$ is an automorphism of $G(p)$. ∎

COROLLARY. $T_4(p) \leqslant (p(p-1)\, f(p))/12$.

Proof. This follows immediately from Proposition 1 since $G(p)$ is self-complementary. ∎

Remark and Notation. The real difficulty now is to evaluate $f(p)$. We first of all (Proposition 2) express $f(p)$ in terms of a formula involving quadratic residues. For the relevant information about quadratic residues we recommend any elementary book on number theory, for example [3], together with [1].

Let $\phi(n)$ denote the Legendre symbol (n/p). Let

$$S = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \phi(1 - x^2)\, \phi(1 - y^2)\, \phi(x^2 - y^2).$$

Write $p = a^2 + b^2$ where b is odd. Let $a = 2n$ and $b = 2m - 1$. Then

$$k = n^2 + m(m-1). \tag{9}$$

PROPOSITION 2. $f(p) = (S + (p-1)(p-19) + 60)/64$.

Proof. Let Z_p^* denote the non-zero elements of the Galois field $GF(p)$. Let

$$X = \{(x, y) \in Z_p^* \times Z_p^* : x, y \neq \pm 1; x \neq \pm y\}.$$

$$S_0 = \sum_{(x,y) \in X} \phi(1 - x^2)\, \phi(1 - y^2)\, \phi(x^2 - y^2).$$

Write $\psi(x) = \phi(1 - x^2)$. We define subsets A_i of X by the following table:

Subset	$\psi(x)$	$\psi(y)$	$\psi(xy^{-1})$
A_1	1	1	1
A_2	1	1	−1
A_3	1	−1	1
A_4	1	−1	−1
A_5	−1	1	1
A_6	−1	1	−1
A_7	−1	−1	1
A_8	−1	−1	−1

Thus, for example, $(x, y) \in A_7$ if and only if $(x, y) \in X$ and $\psi(x) = \psi(y) = -1$, $\psi(xy^{-1}) = 1$. Let $\alpha_i = |A_i|$. We have, by definition,

$$8f(p) = \alpha_1. \tag{10}$$

It is well known that (see, for example, [3])

$$|\{x : x \in Z_p^*, \psi(x) = 1\}| = 2(k - 1). \tag{11}$$

Using (11) we easily obtain

$$\alpha_1 + \alpha_2 = \alpha_1 + \alpha_3 = 4(k - 1)(k - 2), \tag{12}$$

$$\begin{aligned} \alpha_3 + \alpha_4 &= \alpha_5 + \alpha_6 = \alpha_7 + \alpha_8 = \alpha_2 + \alpha_4 \\ &= \alpha_5 + \alpha_7 = \alpha_6 + \alpha_8 = 4k(k - 1). \end{aligned} \tag{13}$$

Since $\psi(x) = \psi(x^{-1})$,

$$\alpha_3 = \alpha_5; \qquad \alpha_4 = \alpha_6. \tag{14}$$

Moreover

$$\begin{aligned} S_0 &= \sum_{(x,y) \in X} \psi(x)\, \psi(y)\, \psi(xy^{-1}) \\ &= \alpha_1 - \alpha_2 - \alpha_3 + \alpha_4 - \alpha_5 + \alpha_6 + \alpha_7 - \alpha_8. \end{aligned} \tag{15}$$

Hence, from (10) and (12)–(15)

$$S_0 = 64f(p) + 8(k-1)(7-2k). \tag{16}$$

Now

$$\begin{aligned} S &= S_0 + 2\left(\sum_{y=1}^{p-1} \psi(y)\right) \\ &= S_0 + 2\left[\left(\sum_{y=0}^{p-1} \psi(y)\right) - 1\right] \\ &= S_0 - 4. \end{aligned} \tag{17}$$

The result follows from (16) and (17). ∎

PROPOSITION 3. $S = 2(p+1) - 4a^2$.

Proof. We have

$$S = \sum_{x}\sum_{y} \phi((x-1)(y-1)(x-y))\{1+\phi(x)\}\{1+\phi(y)\} = A + 2B + C, \tag{18}$$

where

$$A = \sum_{x}\sum_{y} \phi((x-1)(y-1)(x-y)),$$

$$B = \sum_{x}\sum_{y} \phi((x-1)(y-1)(x-y)x),$$

$$C = \sum_{x}\sum_{y} \phi((x-1)(y-1)(x-y)xy).$$

It is easy to see that $A = 0$, $B = 1$. Now

$$C = \sum_{x,\, y \neq 0}\sum \phi\left(\frac{x+1}{y}\right)\phi\left(\frac{y+1}{x}\right)\phi(y-x)$$

so

$$C + 2 = \sum_{\substack{x,\, y \neq 0 \\ x+y \neq -1}}\sum \phi\left(\frac{x+1}{y} \cdot \frac{y+1}{x} \cdot (y-x)\right).$$

Set

$$t = \frac{x+1}{y}, \qquad u = \frac{y+1}{x},$$

so

$$x = \frac{t+1}{ut-1}, \qquad y = \frac{u+1}{ut-1}.$$

Then

$$C + 2 = \sum_{\substack{u,t \neq -1 \\ ut \neq 1}} \sum \phi\left(t \cdot u \cdot \frac{u-t}{ut-1}\right)$$
$$= \sum_{u,t \neq -1} \sum \phi(tu(u-t)(ut-1)).$$

Thus

$$C = \sum_{u,t \neq 0} \sum \phi(tu(u-t)(ut-1)).$$

Replace t by t/u to obtain

$$C = \sum_t \phi(t)\, \phi(t-1) \sum_u \phi(u)\, \phi(u^2 - t).$$

Let χ be a character (mod p) of order 4 and consider the Jacobi sum $K(\chi) = \sum_n \chi(n)\, \phi(1-n)$. For suitably chosen signs of a and b, $K(\chi) = b + ai$. The Jacobsthal sum $\sum_u \phi(u)\, \phi(u^2 - t)$ equals $\bar{\chi}(t)\, K(\chi) + \chi(t)\, K(\bar{\chi})$. Since $\bar{\chi}(t)\, \phi(t) = \chi(t)$,

$$\begin{aligned} C &= K(\chi) \sum_t \chi(t)\, \phi(t-1) + K(\bar{\chi}) \sum_t \bar{\chi}(t)\, \phi(t-1) \\ &= K(\chi)^2 + K(\bar{\chi})^2 \\ &= (b+ai)^2 + (b-ai)^2 \\ &= 2(b^2 - a^2). \end{aligned} \tag{19}$$

The result now follows from (18) and (19). ∎

Remark. The idea for the transformation $(x, y) \to (t, u)$ came from a paper of the Lehmers [9]. The well-known relation between Jacobsthal and Jacobi sums is proved, for example, by Berndt and Evans [1] in Theorem 2.7. The formula $K(\chi) = b + ai$ is proved, e.g., in Theorem 3.9 of this paper. A. Selberg has evaluated a sum more general than C, namely, $\sum \sum_{x, y \in GF(q)} \chi_1(xy)\, \chi_2((1-y)(1-x))\, \chi_3^2(x-y)$, where χ_1, χ_2, χ_3 are characters on the finite field $GF(q)$ with q odd. For details, see [5].

PROPOSITION 4. $f(p) = ((p-9)^2 - 4a^2)/64$.

Proof. This follows from Propositions 2 and 3. ∎

THEOREM 1. $k_4(G(p)) = (p(p-1)((p-9)^2 - 4a^2))/1536$.

Proof. This follows from Propositions 1 and 4. ∎

THEOREM 2. *Suppose p is prime and* $p = 4u^2 + 1$ *for some integer u. Then* $k_4(G(p)) = ((p(p-1)(p-5)(p-17))/24)/64$.

Proof. In Theorem 1 put $a^2 = p - 1$. ∎

THEOREM 3. *Suppose p is prime and* $p = 4u^2 + 1$ *for some integer u. Then* $T_4(p) \leqslant w(p)$.

Proof. This follows from Theorem 2, Proposition 1 and its Corollary. ∎

3. FINAL REMARKS

Character sums can be very delicate. We were lucky that C was tractable. Let $D = \sum_x \sum_y \phi((x+1)(y+1)(x+y)xy)$ be the sum obtained from C (defined below (18)) by simply changing the minusses to plusses. It appears to be surprisingly difficult to evaluate D. We have made the following conjecture, based on computer calculations.

Conjecture. Let p be any odd prime, and write $p = c^2 + 2d^2$ if $p \equiv 1$ or 3 (mod 8). Then

$$\begin{aligned} \left(\frac{2}{p}\right) D &= -p \qquad \text{if} \quad p \equiv 5 \text{ or } 7 \pmod 8, \\ &= -p + 4c^2 \qquad \text{if} \quad p \equiv 1 \text{ or } 3 \pmod 8. \end{aligned} \tag{20}$$

Using the transformation $(x, y) \to (t, u)$ in [9], Emma Lehmer has proved (20) in the case $p \equiv 5$ or 7 (mod 8). No elementary proof of the case $p \equiv 1$ or 3 (mod 8) appears to be known.

ACKNOWLEDGMENTS

We are deeply indebted to both referees.

REFERENCES

1. B. C. BERNDT AND R. J. EVANS, Sums of Gauss, Jacobi and Jacobsthal, *J. Number Theory* **11** (1979), 349–398.
2. J. A. BONDY AND U. S. R. MURTY, "Graph Theory with Applications," Macmillan & Co., London, 1976.

3. H. DAVENPORT, The Higher Arithmetic," Hutchinson, London, 1952.
4. P. ERDÖS, On the number of complete subgraphs contained in certain graphs, *Magyar Tud. Akad. Mat. Kut. Int. Közl* **7** (1962), 459–474.
5. R. EVANS, Identities for products of Gauss sums and finite fields, *Enseign. Math.*, to appear.
6. A. W. GOODMAN, On sets of acquaintances and strangers at any party, *Amer. Math. Monthly* **66** (1959), 778–783.
7. R. E. GREENWOOD AND A. M. GLEASON, Combinatorial relations and chromatic graphs, *Canad. J. Math.* **7** (1955), 1–7.
8. F. HARARY, "Graph Theory," Addison–Wesley, Reading, Mass., 1969.
9. D. H. AND E. LEHMER, On the cubes of Kloosterman sums, *Acta Arith.* **6** (1960), 15–22.
10. A. G. THOMASON, Ph.D. Thesis, Cambridge University, 1979.