JOURNAL OF ALGEBRA 73, 573–585 (1981)

On Sharply Edge-Transitive Permutation Groups

LÁSZLÓ BABAI

Eötvös University, Budapest, Hungary
and
Université de Montréal, Québec, Canada

PETER J. CAMERON

Merton College, Oxford, England

MICHEL DEZA

C.N.R.S., Paris, France

AND

NAVIN M. SINGHI

Tata Institute of Fundamental Research, Bombay, India

Communicated by G. Higman

Received November 20, 1980

We consider the problem of determining the maximum possible out-degree $d(n)$ of a digraph on n vertices which admits a sharply edge-transitive group. We show that $d(n) \geqslant cn/\log\log n$ for every n, while $d(n) = \frac{1}{2}n$ infinitely often. Also, $d(n) = n - 1$ if and only if n is a prime power, whereas for non-prime-power values of n, we show that $n - d(n)$ tends to infinitely with n. The question has interesting group-theoretic aspects. This and related problems generalise the existence question for projective planes.

1. PROBLEMS AND STATEMENT OF RESULTS

By a digraph we mean a pair $X = (V, R)$, where $V = V(X)$ is the vertex set and $R \subseteq V \times V$ is an irreflexive relation on V such that

$$(\forall x \in V)(\exists y \in V)((x, y) \in R).$$

A subset G of its automorphism group will be called *sharply edge-transitive* if its action on R is sharply transitive, that is, for any $r_1, r_2 \in R$ there exists precisely one $\sigma \in G$ such that $\sigma r_1 = r_2$. (In particular, $|R| = |G|$.) The

0021-8693/81/120573-13$02.00/0

problem we propose is to determine *which digraphs admit a sharply edge-transitive set* (SETS) *or a sharply edge-transitive group* (SETG) of automorphisms.

We note that *the complete graph* K_n (regarded as a digraph with $n(n-1)$ edges) *admits a SETS if and only if there is a projective plane of order* n [6, Theorem 5.2], and *it admits a SETG if and only if there is a projective plane of order* n *over a near-field* (that is, n is a prime power) [6, Theorems 5.6, 5.7]. Hence our problems are generalisation of the existence problems for projective planes and are somewhat analogous to other generalisations such as the existence of large families of orthogonal Latin squares.

Let $d(X)$ denote the out-degree of the vertices of the digraph X. (This is the same for every vertex because we are dealing only with digraphs with transitive automorphism groups.) Clearly $|R| = |V|\, d(X)$. For an integer $n \geqslant 2$, let $d(n) = \max\{d(X) \mid X \text{ is a digraph on } n \text{ vertices admitting a SETG}\}$, and $d^*(n) = \max\{d(X) \mid X \text{ is a digraph on } n \text{ vertices admitting a SETS}\}$. (These are the numbers analogous to the maximum number of orthogonal Latin squares of order n.)

Clearly $2 \leqslant d(n) \leqslant d^*(n) \leqslant n-1$, and the results from [6] quoted above read as follows:

THEOREM 1 (Hall). *$d^*(n) = n-1$ if and only if there exists a projective plane of order n; and $d(n) = n-1$ if and only if n is a prime power.*

The aim of this paper is to present our first thoughts about the order of magnitude of $d(n)$, in the hope of raising some interest in this problem.

We first note that the question of graphs admitting a SETG can be formulated in abstract group-theory.

Suppose G is a group and H is a proper subgroup of G. Suppose that there exists $g \in G$ such that $H \cap gHg^{-1} = (1)$, the trivial group. Let V be the set of all left cosets of H in G, and define $R_g = \{(xH, xhgH) \mid h \in H, xH \in V\} \subseteq V \times V$. Using the fact that $H \cap gHg^{-1} = (1)$, it can easily be seen that the digraph $X_g = (V, R_g)$ admits G as a SETG (with G acting on V by left multiplication). Further, the subgroup H is the stabiliser of the vertex $H \in V$. The following theorem shows that the converse is also true.

THEOREM 2. *The following are equivalent:*

(i) *X is a digraph admitting a group G as SETG;*

(ii) *there is a subgroup H of G and an element $g \in G$ such that $H \cap gHg^{-1} = (1)$, and X is isomorphic to the digraph X_g defined above.*

COROLLARY 3. *$d(n) = \max\{|H| \mid H$ is a subgroup of index n of a group G and intersects some G-conjugate of itself trivially$\}$.*

We next establish lower bounds for $d(n)$.

PROPOSITION 4. *For any* $n_1, n_2 > 1$, $d(n_1 n_2) \geqslant d(n_1)\, d(n_2)$.

COROLLARY 5. *If* $n = q_1 \cdots q_k$, *where the* q_i *are prime powers, then* $d(n) \geqslant (q_1 - 1) \cdots (q_k - 1)$.

This is best possible for prime powers, and for some other values: for example, $d(28) = 18$.

COROLLARY 6. *There is a constant* $c > 0$ *such that* $d(n) \geqslant cn/\log\log n$ *for all* n.

Problem 7. Does there exist a constant $c > 0$ such that $d(n) \geqslant cn$ for all n?

If this problem has an affirmative answers, then necessarily $c \leqslant \frac{1}{2}$, since $d(n) = \frac{1}{2}n$ for infinitely many n, as the next result shows.

THEOREM 8. *If* p *is a prime greater than* 7, *then* $d(2p) = p$.

Let us consider this problem further. Let X be a digraph on n vertices with $d(X) \geqslant \frac{1}{2}n$, admitting the sharply edge-transitive group G. Instances in which G is primitive are comparatively rare.

Problem 9. Show that if G is a primitive SETG on a digraph X with $d(X) \geqslant \frac{1}{2}n$, then either G is sharply 2-transitive ($d(X) = n - 1$, n a prime power) or G is A_5 acting on unordered pairs ($n = 10$, $d(X) = 6$).

If G is imprimitive, let v be a vertex of X, and Δ a block of imprimitivity containing v. Then either all edges leaving v end at points of Δ, or none do. The condition $d(X) \geqslant \frac{1}{2}n$ forces the second alternative to hold; so v is joined to some of the points in some of the blocks of imprimitivity other Δ. A special case (which is natural to consider if we are trying to maximise $d(X)$) is that when v is joined to all the points in all the blocks other than Δ. In this case, X is the *complete multipartite graph* k_m^l, the complement of l disjoint copies of K_m. Indeed, if $d(X)$ is sufficiently large, then X must be complete multipartite:

PROPOSITION 10. *Let* X *be a digraph on* n *vertices admitting an edge-transitive group.*

(i) *If* $d(X) \geqslant \frac{1}{2}n$, *then* X *is undirected (equal to its converse).*

(ii) *If* $d(X) > n - 1 - (n-1)^{1/2}$, *then* X *is complete multipartite.*

This result is close to best possible:

EXAMPLE 11. If n is an even power of a prime, there is a digraph X on n vertices admitting a SETG, having $d(X) = n - 2n^{1/2} + 1$, and not complete multipartite.

The following proposition shows that the property of being complete multipartite can be recognised algebraically.

PROPOSITION 12. *Let X be a digraph admitting the group G as SETG. Suppose that g and H are as in Theorem 2, with $X \cong X_g$. Then X is complete multipartite if and only if, for any $x \in G$, there exist h, $h_1 \in H$ such that $x = g^{-1}hgh_1$ or $x = hgh_1$.*

We now give some examples.

PROPOSITION 13. *The digraph k_m^l admits a SETG in the following cases:*

(i) $l = 2$, *m arbitrary*;

(ii) *l an odd prime, $m = s^{(l-1)/2}$ for some $s > 1$ (and, in particular, $l = 3$, m arbitrary)*;

(iii) *$l = 4$, $m = s^2$, where s is a product of prime powers congruent to 1 (mod 3)*;

(iv) *$l = m$ a prime power*;

(v) *$l = q + 1$, $m = q - 1$, where q is a prime power*;

(vi) *$l = q + 1$, $m = \frac{1}{2}(q - 1)$, where q is a prime power with $q \equiv 3$ (mod 4)*;

(vii) *$l = q^2 + q + 1$, $m = q(q - 1)$, where q is a prime power*;

(viii) *$l = 2^{2a} + 1$, $m = 2^a - 1$, for a odd.*

COROLLARY 14. *$d(n) \geqslant \frac{1}{2}n$ if n is even; and $d(n) \geqslant \frac{2}{3}n$ if n is divisible by 3.*

We remark that $d(n) \geqslant \frac{1}{2}n$ for all $n < 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29 = 82{,}944{,}785$.

Problem 15. Determine the pairs (l, m) for which k_m^l admits a SETG.

Particular cases of this problem concern finding such pairs when either l or m is given. Note that, for $l = 2$ or 3, k_m^l always admits a SETG; and in fact 2 and 3 are the only integers with this property. We mention the following question.

Problem 16. Show that, for any $l > 3$, the set $M_l = \{m \mid k_m^l$ admits a SETG$\}$ has density zero; and, moreover, the set $\{l \mid M_l \neq \varnothing\}$ has density zero.

More is known about the other case. Tsuzuku [9] showed that k_2^l admits a SETG if and only if $l = 2, 3, 4$ or 7. (Tsuzuku's results was stated in a different way but is easily seen to be equivalent to this assertion.) The next two theorems generalise Tsuzuku's result; after stating them, we list some consequences.

THEOREM 17. *For any $m > 1$, there are only finitely many values of l for which k_m^l admits a SETG.*

THEOREM 18. *If m is prime and k_m^l admits a SETG, then $l = 2$, 3, $m + 2$ (with $m + 1$ a power of 2), $2m + 2$ (with m odd and $2m + 1$ a prime power), $m^2 + 2m + 2$ (with $m + 1$ an odd power of 2), m^t (with $t \leqslant m$), or $l = 7$, $m = 2$.*

Remarks. (1) Examples are known in all cases except $l = m^t$ for $t > 1$ and m odd.

(2) Results similar to Theorems 17 and 18 have been obtained by T. Ito (personal communication).

COROLLARY 19. *$d(n) = n - 2$ if and only if $n = 6$ or 14, while $d(n) = n - 3$ if and only if $n = 15$ or 24.*

COROLLARY 20. *If n is not a prime power, then $d(n) \leqslant n - n^{1/7}$.*

In this result, $\frac{1}{7}$ cannot be replaced by any number greater than $\frac{1}{3}$. (Proposition 13(viii) shows that $d(n) \geqslant n - [n^{1/3}]$ for infinitely many non-prime powers.)

Other values of $d(n)$ which follow from Theorem 18 include $d(63) = 56$, $d(255) = 240$, $d(455) = 448$, and so on.

The proofs of Theorems 17 and 18 use the determination of doubly transitive groups in which the two-point stabilisers have odd order, by Bender [1, 2]. It seems possible that a complete determination of doubly transitive groups (which would follow in essence from the determination of finite simple groups) could contribute to the solution of Problem 15.

A permutation group G acting on a set V is said to be *geometric* of type $(\{0, m\}, n)$ if

(i) G is transitive on V, and $|V| = n$; and

(ii) the stabiliser of a point of V fixes exactly m points and is sharply transitive on the remaining $n - m$ points.

Geometric groups have been studied in [5] (see Proposition 5.10 and the remarks before it in [5] for details about type $(\{0, m\}, n)$). Such groups with $m = 2$ and 3 have been determined by Tsuzuku [9] and Ito and Kiyota [8], respectively.

Let G be a geometric group of type $(\{0, m\}, n)$ acting on a set V. Let

$$R = \{(u, v) \mid u, v \in V, G_{uv} = (1)\}.$$

It can easily be seen that the digraph $X = (V, R)$ is a complete multipartite graph k_m^l, where $n = lm$, and G acts on it as a SETG. Many, but not all,

groups G which act on k_m^l as SETG are geometric groups. We give the following sufficient condition.

PROPOSITION 21. *Let G be a group acting as SETG on a digraph X. Then G is a geometric group if the smallest prime divisor of $d(X)$ is greater than $n - d(X) - 1$. In particular, this holds for $X = k_m^l$ if the smallest prime divisor of $l - 1$ is greater than $m - 1$ and m is prime.*

The following table gives the values of $d(n)$ for $n \leqslant 27$. We have excluded prime power n, for which $d(n) = n - 1$.

n	6	10	12	14	15	18	20	21	22	24	26
$d(n)$	4	6	8	12	12	12	16	14	11	21	13

In all cases in the table except $n = 10$, the digraph X realising the bound is complete multipartite and is given in Proposition 13. (For $n = 10$, X is the line graph of K_5.) Upper bounds are obtained from Proposition 10, Theorems 17 and 18, and *ad hoc* arguments.

Other lower bounds include $d(110) \geqslant 72$ (from the Mathieu group M_{11}, acting on ordered pairs) and $d(q(q+1)(q^2+q+1)) \geqslant q^2(q-1)^2$ for prime powers q (from $PGL(3, q)$, acting on ordered pairs of points of the projective plane).

We remark that 6 and 14 are the only values on n, other than prime powers, for which we know the value of $d^*(n)$. For, in these cases, $n - 2 = d(n) \leqslant d^*(n) < n - 1$, the strict inequality coming from Theorem 1 and the Bruck–Ryser theorem; so $d^*(6) = 4$, $d^*(14) = 12$.

We conclude this section with the remark that the concept of SETG can be generalised in many ways. Among the general problems, perhaps one of the most interesting is Tutte's problem of studying s-transitive (or sharply s-transitive) graphs. Note that each sharply 1-transitive graph gives a digraph admitting a SETG in our sense. See [3, 10] for interesting results on s-transitive graphs. Another generalisation is: what is the order of the largest transitive permutation group of degree n having a *base* of size s (a set of s points fixed pointwise only by the identity)? Our problem is the case $s = 2$.

2. SHARPLY EDGE-TRANSITIVE GROUPS

In this section we prove Theorems 2 and 8, Propositions 4 and 10, and Corollaries 3, 5, and 6.

Proof of Theorem 2. Suppose $X = (V, R)$ is a digraph admitting a group G as SETG. Now G acts transitively on V. Fix a vertex $v \in V$; let $H = G_v$, the stabiliser of v. Suppose $(v, w) \in R$, and choose $g \in G$ such that $gv = w$.

Then $gHg^{-1} = G_w$, and sharp edge-transitivity forces $H \cap gHg^{-1} = (1)$. Further, V can be identified with the set of left cosets of H ($w \leftrightarrow gH$ if $gv = w$), and this identification gives an isomorphism from X to X_g. ∎

Corollary 3 follows immediately.

Proof of Proposition 4. The *direct product* of $X_i = (V_i, R_i)$, $i = 1, 2$, is defined as $X = (V, R)$, where $V = V_1 \times V_2$, and $((x_1, x_2), (y_1, y_2)) \in R$ if and only if $(x_i, y_i) \in R_i$ for $i = 1, 2$. If G_i acts on V_i, then $G_1 \times G_2$ acts componentwise on $V_1 \times V_2$. It is easily seen that if G_1 abd G_2 are SETGs on X_1 and X_2, respectively, then $G_1 \times G_2$ is a SETG on X; clearly $d(X) = d(X_1)\, d(X_2)$. The result follows. ∎

The same construction, applied to two copies of the complete graph, produces Example 11.

Proof of Corollary 5. All we have to do is to apply Proposition 4 and use $d(q) = q - 1$ for prime powers q (Theorem 1). ∎

Proof of Corollary 6. Corollary 5 implies that $d(n) \geqslant \varphi(n)$, where φ is Euler's function. Now $\varphi(n) \geqslant (e^{-\gamma} + o(1))n/\log\log n$, where γ is Euler's constant (see [7, Theorem 328, p. 267]).

Proof of Proposition 10. Part (i) is clear. For (ii), if the complement of the graph X has two non-adjacent vertices at distance 2 then, by edge-transitivity of X, the complement has diameter 2 and consequently degree at least $(n-1)^{1/2}$. Otherwise the complement of X is the disjoint union of complete graphs.

Proof of Theorem 8. Let G act as a SETG on a digraph X with $2p$ vertices, where p is a prime greater than 7. Suppose first that G is primitive. By a theorem of Wielandt [11, p. 94], either G is 2-transitive or G has rank 3 with subdegrees 1, $s(2s+1)$, $(s+1)(2s+1)$, with $p = 2s^2 + 2s + 1$. The first case cannot occur, by Theorem 1. Since a vertex stabiliser acts sharply transitively on one of its orbits, one of the non-trivial subdegrees must divide the other. This forces $s = 1$, $p = 5$, contrary to assumption.

Next, suppose G has p blocks of imprimitivity, each of size 2. By theorems of Galois and Burnside (see [11, p. 29]), the permutation group $\bar{G}$ induced on the set of blocks is soluble or 2-transitive. If it is soluble, then for any block Δ, $|\bar{G}_\Delta|$ divides $p - 1$; so $|G_v|$ divides $2(p-1)$. The same conclusion obviously holds if $\bar{G}$ is 2-transitive. By Tsuzuku's theorem [9] (see Theorem 17), $d(X) = 2(p-1)$ implies $p \leqslant 7$; so $d(X) \leqslant p - 1$.

Finally, suppose G has two blocks of imprimitivity, each of size p. If v is a vertex in a block Δ, then either all edges leaving v end in Δ, or all such edges end outside Δ; in either case, $d(X) \leqslant p$.

We conclude that $d(2p) \leqslant p$. However, $d(2p) \geqslant p$, by Corollary 14. ∎

3. Complete Multipartite Graphs

In this section we prove the remaining Propositions 12, 13, and 21, Theorems 17 and 18, and Corollaries 14, 19, and 20.

Proof of Proposition 12. Let H be a subgroup of a group G, and let $g \in G$ satisfy $H \cap gHg^{-1} = (1)$. Let X denote the digraph X_g. Suppose X is a complete multipartite graph. Now by definition $(H, hgH) \in R$ for all $h \in H$. Since X is symmetric this implies (hgH, H) and hence $(H, hg^{-1}H)$ are also edges of X for all $h \in H$. Now if $x \in G$ and $(H, xH) \in R$, then clearly $xH = hgH$ for some $h \in H$, that is, $x = hgh'$ for some h, $h' \in H$. If $(H, xH) \notin R$, then since X is complete multipartite and $(H, g^{-1}H) \in R$, we have $(g^{-1}H, xH) \in R$, whence $g^{-1}hgH = xH$ for some $h \in H$ and so $x = g^{-1}hgh'$ for some h, $h' \in H$.

Conversely, suppose every $x \in G$ is expressible in one of these forms. Now clearly $g^{-1} \neq g^{-1}hgh_1$, since this would imply $g \in H$. Hence $g^{-1} = hgh_1$ for some h, $h_1 \in H$. This implies that $(H, g^{-1}H)$ and hence (gH, H) are edges, whence X is undirected. The fact that X is complete multipartite now follows by reversing the above argument. ∎

Proof of Proposition 13. (i) Set $V = Z_m \times Z_2$, and $R = \{((a, b), (c, d)) \in (Z_m \times Z_2)^2 \mid b \neq d\}$. The wreath product $G = Z_m \text{ wr } Z_2$, generated by

$$\lambda: \quad (a, 0) \mapsto (a + 1, 0), \quad (a, 1) \mapsto (a, 1)$$

and

$$\tau: \quad (a, b) \mapsto (a, b + 1),$$

is a SETG on $X = (V, R)$.

(ii) Let K denote the sharply 2-transitive group $\{x \mapsto ax + b \mid a \neq 0\}$ of permutations of Z_l, where l is an odd prime. Let

$$M = \{(a_0, a_1, \ldots, a_{l-1}) \mid a_i \in Z_s, a_0 + \cdots + a_{l-1} = 0\}.$$

Then M is a K-module, and we may form the split extension $G = MK$. Let L be the subgroup $\{x \mapsto ax \mid a \neq 0\}$ of K, and N the subgroup

$$\{(a_0, a_1, \ldots, a_{l-1}) \mid a_0 = 0, a_i + a_{l-i} = 0\}$$

of M. Then N is L-invariant, and so $H = NL$ is a subgroup of G. Let g be the element $x \mapsto x + 1$ of K. Since $L \cap gLg^{-1} = (1)$, we have $H \cap gHg^{-1} \subseteq M$. Suppose $(a_0, \ldots, a_{l-1}) \in H \cap gHg^{-1}$. Then, for all $i \in Z_l$, $a_i = -a_{l-i} = a_{i+2}$, so $0 = a_0 = a_2 = \cdots$. Thus $H \cap gHg^{-1} = (1)$. The conclusion now follows from Theorem 2.

(iii) With the given hypothesis on s, there is a ring R of order s (a direct sum of Galois fields) containing an element ω with $\omega^3 = 1$ and $\omega - 1$ invertible. Now the construction is similar to the previous one. Let K denote the alternating froup A_4, M the additive group of R^4, and G the split extension MK. Let L be the stabiliser of the first letter (in A_4), N the L-submodule $\{(a, b, \omega b, \omega^2 b) \mid a, \quad b \in R\}$, and $H = NL$. As before, $H \cap gHg^{-1} = |1|$ if g is the permutation (1 2)(3 4) in A_4.

(iv), (vi) and (viii) follows from examples of geometric groups given by Cameron and Deza [5, Examples 5.3, 5.11]; see the remarks in Section 1.

(v) Let X be the set of non-zero vectors in $V(2, q)$, R the set of ordered bases, and $G = GL(2, q)$.

(vii) Let $G = PGL(3, q)$. Let H denote the subgroup of G fixing a line L of the projective plane and inducing a sharply transitive group on L. (Then H is sharply 2-transitive on the complement of L and contains all elations and homologies with axis L.) As in [5, Example 5.12], $H \cap gHg^{-1} = (1)$ if g does not fix L. Note that, if $q > 3$, then G is not a geometric group, since no sharply transitive group is normal in $PGL(2, q)$. The other examples in this proposition are all geometric; but Cameron and Deza [6, Example 5.3] give a further of a non-geometric SETG (with $l = m = q$). ∎

Corollary 14 follows from parts (i) and (ii) of this proposition (with $l = 3$ in (ii)).

Before proving Theorems 17 and 18, we make some preliminary remarks. Let G act as a SETG on k_m^l. Then $|G| = l(l-1)m^2$. Let B denote the set of multipartite blocks, and $\bar{G}$ the permutation group induced on B by G. Then $\bar{G}$ is a doubly transitive group, in which the stabiliser of two letters has order dividing m^2. (The quotient $m^2/|\bar{G}_{bb'}|$ is the order of the subgroup of G fixing every block.)

Proof of Theorem 17. We divide the proof into two cases, depending on the parity of m.

Case 1. m even. For this case we generalise Tsuzuku's method [9]. First we introduce some notation. Let $B = \{b_1, \ldots, b_l\}$, and $b_i = \{x_{i1}, \ldots, x_{im}\}$; let G_{ij} be the stabiliser of x_{ij}. Then clearly $G_{ij} \cap G_{i_1 j_1} = (1)$ for $i \neq i_1$. Let U_{ij} be the set of elements of order 2 in G_{ij}, and $U = |U_{ij}|$. Note that U is independent of i and j. Further, $U \neq 0$, since by our assumption $|G_{ij}| = (l-1)m$ is even. Let $F = \bigcup U_{ij}$, where the union is taken over $1 \leqslant i \leqslant l$, $1 \leqslant j \leqslant m$.

LEMMA 3.1. $U \leqslant m^2$.

Proof. We will show that $|U_{11}| \leqslant m^2$. Let $U(x_{ij})$ be the number of $\sigma \in F$ such that $\sigma x_{11} = x_{ij}$. Now since $U_{i1} \cap U_{i'1} = \varnothing$ for $i \neq i'$, we have $l|U_{11}| = |U_{11}| + |U_{21}| + \cdots + |U_{l1}| \leqslant |F| = \sum U(x_{ij})$, where the last summation is

over $1 \leqslant i \leqslant l$, $1 \leqslant j \leqslant m$. Now, for $i \neq 1$, any involution σ such that $\sigma x_{11} = x_{ij}$ takes the edge (x_{11}, x_{ij}) to the edge (x_{ij}, x_{11}). So there is at most one such σ, that is, $U(x_{ij}) \leqslant 1$ for $1 < i \leqslant l$. Also, for $j \neq 1$, $|U(x_{1j})| \leqslant |G_{11}| = (l-1)$. Hence $l|U_{11}| = |U_{11}| + (m-1)(l-1)m + (l-1)m$, whence $|U_{11}| \leqslant m^2$. ∎

LEMMA 3.2. *For each point x_{ij}, there is an involution in G_{ij} fixing at least $1 + (l-1)/m^2$ distinct blocks b_t.*

Proof. Let $i \neq 1$ be given. Consider the subgroup H_i of G_{11} consisting consisting of elements fixing the block b_i. Since $|b_i| = m$, we have $|H_i| = m$. Since m is even, there is an involution in H_i. Now $|U_{11}| \leqslant m^2$, so there is an element $\sigma \in U_{11}$ fixing at least $(l-1)/m^2$ blocks b_i for $i > 1$. Of course σ fixes b_1 as well. By transitivity of G on V, the same holds for any point. ∎

Now let σ_{ij} denote the element of U_{ij} guaranteed by Lemma 3.2, and B_{ij} the set of (at least $1 + (l-1)/m^2$) blocks fixed by σ_{ij}.

LEMMA 3.3. *There exist two distinct blocks b_s, b_t which are both contained in B_{i1} for at least $(1 + (l-1)/m^2)/m^2$ values of i.*

Proof. For any pair b_s, b_t of blocks, let $\alpha(b_s, b_t)$ denote the number of values of i such that both b_s and b_t are in B_{i1}. Let

$$\alpha = \max_{1 \leqslant s < t \leqslant l} \alpha(b_s, b_t).$$

Then clearly

$$l(l-1)\alpha \geqslant \sum_{i=1}^{l} |B_{i1}|\,(|B_{i1}| - 1) \geqslant \left(\frac{l-1}{m^2} + 1\right)\left(\frac{l-1}{m^2}\right) l.$$

Hence $\alpha \geqslant (1 + (l-1)/m^2)/m^2$. ∎

We can now complete the proof in case 1. As noted in the preliminary remarks, the stabiliser of any pair of blocks has order m^2; but Lemma 3.3 shows that some pair of blocks b_s, b_t is fixed by the identity and at least $(1 + (l-1)/m^2)/m^2$ involutions. Hence

$$1 + \frac{1}{m^2}\left(\frac{l-1}{m^2} + 1\right) \leqslant m^2,$$

that is, $l \leqslant m^6 - m^4 - m^2 + 1$.

Case 1. m odd. Here $\bar{G}$ is a doubly transitive group in which the stabiliser of two points has order dividing m^2, whence odd. Theorems of Bender [1, 2] show that either $\bar{G}$ has a regular normal subgroup or $\bar{G}$

contains $PSL(2, q)$, $PSU(3, q)$ or $Sz(q)$ for some prime power q. In the second alternative, the required bound is easily obtained. For example, in the case of $Sz(q)$, we have $l = q^2 + 1$ and $m^2 \geqslant q - 1$, so $l \leqslant m^4 + 2m^2 + 2$.

Thus suppose $\bar{G}$ has a regular normal subgroup $\bar{A}$, necessarily an elementary abelian r-group for some prime r. Then $\bar{G}_0$ acts as a group of linear transformations of $\bar{A} = V(d, r)$, a vector space over $GF(r)$; the fixed blocks of $\bar{G}_{01}$ can be identified with the vectors of its centraliser in $\bar{A}$, of dimension e, say. An involution in $\bar{G}_0$ fixes no non-zero vectors, and so acts as $x \mapsto -x$ on $\bar{A}$. (If $r = 2$, there is no such involution.)

Let $K = G_{01}$, N the normal subgroup of G fixing every block, and H_i the subgroup of K fixing a point in the ith block.

First we observe that, if $l \geqslant 2m$ (which we may assume), then $|N| = m$ and N acts regularly on each block. For let $|N| = st$ and suppose the orbits of N have length s. Then N contains l pairwise disjoint subgroups of order t (the stabilisers of points in each block); so $st \geqslant 1 + l(t - 1)$, whence if $t > 1$, then

$$l \leqslant \frac{st - 1}{t - 1} = s + \frac{s - 1}{t - 1} \leqslant 2s - 1 \leqslant 2m - 1,$$

contrary to assumption. So N, and also A, is semiregular. Now A is normal in G, so its orbits are blocks of imprimitivity. But any such block containing points of two multipartite blocks is the whole of V. So $|A| = |V| = lm$, whence $|N| = m$.

Now $H_0 N = K$, and $H_0 \cap N = (1)$; so every element of K is uniquely expressible as hn, for $h \in H_0$, $n \in N$. In particular, this is true for elements of H_1. Now if hn, $h'n' \in H_1$ and $hn \neq h'n'$, then $h \neq h'$ and $n \neq n'$. (For example, if $n = n'$, then $h'n'n^{-1}h^{-1} = h'h^{-1} \in H_0 \cap H_1 = (1)$, so $h = h'$ also.) Thus, for each $n \in N$ there exists $h \in H_0$ such that $hn \in H_1$.

Let β be an element of G for which $\bar{\beta}$ is the map $x \mapsto 1 - x$. We may assume β is an involution, since $|N|$ is odd. Then β centralises K/N and interchanges H_0 and H_1; so, for $h \in H_0$, $h^\beta = hn \in H_1 (n \in N)$. Then $h = h^{\beta^2} = hnn^\beta$, so $n^\beta = n^{-1}$. By the previous paragraph, every element of N is inverted by β; so N is abelian. Moreover, the same argument works for any element β for which $\bar{\beta}$: $x \mapsto c - x$. So the product of two such elements, that is, an arbitrary element of A, centralises N. In particular, r is odd.

Take $\alpha \in A$ with $\bar{\alpha}$: $x \mapsto x + 1$; for $h \in H_0$, suppose $h^\alpha = hn \in H_1$. Then $h = h^{\alpha^r} = hn^r$; so every element of N has order r; that is, N is an elementary abelian r-group, and m is a power of r.

Now $\bar{K}$ fixes r^e blocks; the corresponding subgroups H_i are pairwise disjoint and so contain between them $r^e(m - 1)$ distinct elements of $K \backslash N$. Thus $r^e(m - 1) \leqslant m^2 - m$, or $r^e \leqslant m$.

LEMMA 3.4. *Let S be an r-group of linear transformations of a vector space V over $GF(r)$. Then* $\dim V \leqslant |S| \dim C_V(S)$.

Proof. This is well known if S is cyclic of order r. In general, let s be an element of order r in the centre $Z(S)$ of S: then $\dim C_V(s) \geqslant (1/r)\dim V$. Now $C_V(s)$ is S-invariant and hence admits the group $S/\langle s\rangle$ of order $|S|/r$; the centraliser of $S/\langle s\rangle$ in $C_V(s)$ is just $C_V(S)$. By induction,

$$\dim C_V(S) \geqslant \dim C_V(s)/(|S|/r) \geqslant \dim V/|S|. \quad \blacksquare$$

Applying this lemma with $V = \bar{A}$, $S = \bar{K}$, $\dim \bar{A} = d$, $\dim C_{\bar{A}}(\bar{K}) = e$, $|\bar{K}| = m$, gives $l = r^d \leqslant r^{em} \leqslant m^m$. $\blacksquare$

Proof of Theorem 18. By the theorem of Tsuzuku [9] mentioned in the Introduction, $m = 2$ implies $l = 2, 3, 4$ or 7; so we may assume m is odd. We may quote Bender's theorems [1, 2] again to deduce that $\bar{G}$ contains either a regular normal subgroup or $PSL(2, q)$, $PSU(3, q)$ or $Sz(q)$ for some prime power q.

If $\bar{G}$ has a regular normal subgroup, the proof of Theorem 17 shows that either $l = m^t$ $(t \leqslant m)$ or $l < 2m$. So we may suppose the latter alternative holds. Note that l is a prime power, and we may also assume $l \neq m$.

Suppose first that $\bar{G}$ is sharply 2-transitive. Then the subgroup N fixing all the blocks has order m^2. The derived group of $\bar{G}$ acts non-trivially on N; so $\bar{G} \leqslant \mathrm{Aut}(N) = GL(2, m)$. Assume $l \neq 2$. Since $Z(\bar{G}) = (1)$, we have $\bar{G} \cap Z(GL(2, m)) = (1)$, and so $\bar{G} \leqslant PGL(2, m)$.

Suppose first that l is odd. Since the Sylow subgroups of $PGL(2, m)$ for odd primes other than m are cyclic, l is prime. Now an element of order l in $\bar{G}$ is conjugate to all its powers except the identity. Parabolic elements of $PGL(2, m)$ (those of order m) have this property, but other elements are conjugate only to their inverses. So we must have $l = 3$.

Now suppose l is a power of 2. Since $PGL(2, m)$ contains no elementary abelian subgroup of order 8, we have $l \leqslant 4$. But the case $l = 4$ cannot occur, since a subgroup of $PGL(2, m)$ isomorphic to A_4 is necessarily the projection of a subgroup of $GL(2, m)$ isomorphic to $SL(2, 3)$.

So we may suppose that $\bar{G}_{01}$ contains an element g of order m. Identifying $\bar{G}$ with a group of affine transformations of a vector space V (of order l), we see that $C_V(g)$ has dimension at least 1, and $V/C_V(g)$ contains at least $m + 1$ elements, forcing $l = |V| \geqslant 2(m + 1)$, contrary to assumption.

Now, suppose $\bar{G}$ contains $PSL(2, p^a)$. Then $|\bar{G}_{01}|$ is a divisor of $a(p^a - 1)$, itself divisible by $\frac{1}{2}(p^a + 1)$ (if p is odd) or $2^a - 1$ (if $p = 2$). Since $|\bar{G}_{01}| = m$ or m^2, this forces $\frac{1}{2}(p^a - 1)$ or $2^a - 1 = m$, giving $l = p^a + 1 = m + 2$ or $2m + 2$.

Suppose $\bar{G}$ contains $PSU(3, 2^a)$. Then m or m^2 is a divisor of $2a(2^{2a} - 1)$, itself divisible by $2^{2a} - 1$ or $\frac{1}{3}(2^{2a} - 1)$ according as a is even or odd. This is impossible unless $a = 1$, when $m = 3$, $l = 9$.

Finally, suppose $\bar{G}$ contains $Sz(q)$, $q = 2^{2a+1}$. As before we have $m = q - 1$, $l = q^2 + 1 = m^2 + 2m + 2$.

Proof of Corollary 19. If X is a digraph admitting a SETG, with $d(X) = n-2$ $(n > 2)$, then X is complete multipartite k_2^l (Proposition 10). By the case $m = 2$ of Theorem 18 (due to Tsuzuku [9]), we have $l = 2, 3, 4$ or 7, whence $n = 4, 6, 8$ or 14. But $d(4) = 3$, $d(8) = 7$ (Theorem 1).

The case $d(n) = n - 3$ is similar.

Proof of Corollary 20. If X admits a SETG and $d(X) > n - n^{1/7}$, then X is complete multipartite k_m^l (Proposition 10), with $l > m^6$. The proof of Theorem 17 shows that $\bar{G}$ has a regular normal subgroup, and that l and m are both powers of the same prime r. But then n is a power of r, contrary to assumption.

Proof of Proposition 21. Let G be a SETG on X, where the hypotheses of the proposition hold. The order of a vertex-stabiliser G_v is $d(X)$, and G_v has an orbit of length $d(X)$ consisting of vertices joined to v. By hypothesis, G_v cannot have an orbit of length x with $1 < x \leqslant n - d(X) - 1$ on the remaining points; so it fixes the $m - 1$ points not joined to v. Thus G is geometric.

REFERENCES

1. H. BENDER, Endliche zweifach transitive Permutationsgruppen, deren Involutionen keine Fixpunkt haben, *Math. Z.* **104** (1968), 175–204.
2. H. BENDER, Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festlasst, *J. Algebra* **17** (1971), 527–554.
3. N. L. BIGGS, "Algebraic Graph Theory," Cambridge Tracts in Math. 67, Cambridge Univ. Press, Cambridge, 1974.
4. I. F. BLAKE, G. COHEN, AND M. DEZA, Coding with permutations, *Information Contr.* **43** (1979), 1–19.
5. P. J. CAMERON AND M. DEZA, On permutation geometries, *J. London Math. Soc.* (2) **20** (1979), 373–386.
6. M. HALL, JR., Projective planes, *Trans. Amer. Math. Soc.* **54** (1943), 229–277.
7. G. H. HARDY AND E. M. WRIGHT, "An Introduction to the Theory of Numbers," 4th ed., Clarendon Press, Oxford, 1960.
8. T. ITO AND M. KIYOTA, Sharp permutation groups, *J. Math. Soc. Japan*, in press.
9. T. TSUZUKU, Transitive extensions of certain permutation groups of rank 3, *Nagoya Math. J.* **31** (1968), 31–36.
10. W. T. TUTTE, A family of cubical graphs, *Proc. Cambridge Philos. Soc.* **43** (1947), 459–474.
11. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York/London, 1964.