Can. J. Math., Vol. XXX, No. 5, 1978, pp. 946–960

REGULAR REPRESENTATION OF FINITE GROUPS BY HYPERGRAPHS

STEPHANE FOLDES AND NAVIN M. SINGHI

0. Introduction and terminology.

0.1. All structures considered in this paper will be finite.

The product $\sigma\tau$ of two permutations σ and τ of a set V is defined by $\sigma\tau(x) = \sigma(\tau(x))$ for every $x \in V$. The set S_V of all permutations of V is a group under this operation. A *permutation group* on V is a subgroup of S_V.

Let P be a permutation group on a set V. If U is a subset of V such that $\sigma(U) \subseteq U$ for every $\sigma \in P$, then U is a *constituent* of P. The restriction of a $\sigma \in P$ to U is then denoted by $\sigma|U$. We write

$$P|U = \{\sigma|U \quad | \quad \sigma \in P\}.$$

U is called a *faithful constituent* if every $\sigma \in P$ is determined by its restriction to U. In this case the groups P and $P|U$ are isomorphic. The permutation group P is called *transitive* if its only constituents are V and the empty set $\emptyset$. For arbitrary P, a non-empty constituent U of P such that $P|U$ is transitive is called an *orbit* of P. For $x \in V$, the *stabilizer* P_x of x in P is the subgroup of P consisting of all $\sigma \in P$ for which $\sigma(x) = x$. If P is transitive and the stabilizer of some element x of V is trivial, then P is said to be *regular*. In this case all the stabilizers P_x, $x \in V$, are trivial.

Let B be an abstract group. For every $y \in B$, the permutation τ_y of B given by $\tau_y(x) = yx$ for every $x \in V$, is called a *left translation*. Left translations form a regular permutation group L_B on B. The mapping $y \to \tau_y$ is an isomorphism from B to L_B, a fact well known as Cayley's theorem [**2**]. Every regular permutation group P can be viewed as the group of left translations L_B in some abstract group B, isomorphic to P.

0.2. If V is a set and k is any positive integer, then let $P_k(V)$ denote the set of subsets of V having cardinality k. If E is any subset of $P_k(V)$, then the ordered pair $H = (V, E)$ is a *k-uniform hypergraph* on V. The elements of $V = V(H)$ are called *vertices*, those of $E = E(H)$ are called *lines*. A line A containing a vertex v is also said to be *incident* with v. A *graph* is a 2-uniform hypergraph.

A *sub-hypergraph* of $H = (V, E)$ is a k-uniform hypergraph $H_1 = (V_1, E_1)$ such that $V_1 \subseteq V$ and $E_1 \subseteq E$. H_1 is called an *induced sub-hypergraph* of H if every line A of H contained in V_1 is also a line of H_1. For every subset S of V,

Received April 12, 1977. This research was done during a visit of the second author to the Department of Combinatorics and Optimization, University of Waterloo.

H has a unique induced sub-hypergraph $H[S]$ with vertex set S. It is called the sub-hypergraph induced by S. If $H[S]$ has no lines, then S is said to be *independent*. H is *bipartite* if its vertex set is the union of two independent sets.

A *partition* of a set V is a set π of pairwise disjoint non-empty subsets of V such that $\bigcup_{A \in \pi} A = V$. A *component* of a hypergraph H is a non-empty subset C of $V(H)$ such that every line of H is either contained in C or is disjoint from it. C is a *connected component* if the only component of $H[C]$ is C itself. The set π of connected components is a partition of $V(H)$ and the hypergraph H is said to be *connected* if π has at most one block, $|\pi| \leqq 1$. A vertex v of a connected hypergraph H is a *cut vertex* if $H[V(H)\backslash\{v\}]$ is not connected.

The number of lines of H containing a given vertex v is called its *degree* and it is denoted by $d_H(v) = d(v)$. If two distinct vertices v and x lie together on some line then x is said to be a *neighbour* of v. The set $N_H(v) = N(v)$ of neighbours of v is called its *neighbourhood*. If H is a graph, then $d(v) = |N(v)|$ for every vertex v.

An *automorphism* of a hypergraph H is a permutation σ of $V(H)$ such that for every line A of H, $\sigma(A)$ is also a line of H. The set of all automorphisms is a permutation group on $V(H)$, denoted by Aut H.

0.3. We shall say that an abstract group B has a *regular representation* by a k-uniform hypergraph, if $L_B = \text{Aut } H$ for some k-uniform hypergraph H. Although for every $k \geqq 2$, every group is isomorphic to the automorphism group of some k-uniform hypergraph (R. Frucht [**8**], P. Hell and J. Nesetril [**9**]), not every group has a regular representation by a k-uniform hypergraph. The first counter examples were given by Frucht [**8**] and I. N. Kagno [**15**]. The simplest is the group Z_3 of order 3, which does not have a regular representation by a k-uniform hypergraph for any k.

In the case of graphs a theory has been developed and a standard terminology has been adopted. Groups having a regular representation by a 2-uniform hypergraph, i.e. by a graph, are said to have a *GRR* (graphical regular representation). Among abelian groups, only groups of the form Z_2^n, $n = 2, 3, 4$, have a *GRR* (C. Y. Chao [**4**], W. Imrich [**11**; **12**], M. H. McAndrew [**16**], G. Sabidussi [**19**]). The problem is more complicated for non-abelian groups. Using the theorem of W. Feit and J. G. Thompson [**5**] on the solvability of groups of odd order, L. A. Nowitz and M. E. Watkins have shown that if B is non-abelian and of order coprime to 6, then it has a *GRR* [**18**]. Imrich extended this result to the case of $|B|$ odd and sufficiently large [**13**; **14**]. Other classes of groups have also been examined by Nowitz [**17**] and Watkins [**22**; **23**; **24**].

In this paper we show that given any integer $k \geqq 3$, every group B of sufficiently large order has a regular representation by a k-uniform hypergraph H. The argument consists of two steps. We first define the hypergraph H with vertex set $V(H) = B$ in such a way that the relation $L_B \subseteq \text{Aut } H$ becomes obvious. Then, since L_B is transitive on B, in order to prove the equality

$L_B = \text{Aut}\, H$ it suffices to show that the stabilizer in Aut H of the identity element e of B, $(\text{Aut}\, H)_e$, is trivial. The construction makes use of special generating sum-free sets in a sufficiently large group B. Also we have to deal separately with groups of exponent >2 and elementary abelian 2-groups.

1. Groups of exponent > 2.

1.1. Let B be any group. A set D of elements of B is called *sum free* if

$$\{x\, y \mid x, y \in D\} \cap D = \emptyset.$$

This is equivalent to the condition $x^{-1}y \notin D$, for any $x, y \in D$. Clearly D cannot contain the identity element e of B. A sum free set D is called a *δ-set* if the following additional conditions are fulfilled:

(i) for every $x \in D$, $x^{-1} \in D$ only if $x^{-1} = x$;
(ii) D has two distinct elements a and b such that $a^2 \neq e$ and $b^2 \neq e$.

It is clear that the elements a and b of condition (ii) must also satisfy

$$a^2 \neq b, \quad b^2 \neq a, \quad ab \neq e.$$

For every $x \in B$, let (x) denote the subgroup of B generated by x.

1.2. An elementary abelian 2-group B (a group of exponent 2, i.e. such that $x^2 = e$ for every $x \in B$) cannot have a δ-set.

1.3. Proposition. *Let a finite group B of exponent >2 have order at least* 18. *Then B has two distinct elements a and b such that*

$$a^2 \neq e, \quad a^2 \neq b, \quad b^2 \neq e, \quad b^2 \neq a, \quad ab \neq e.$$

Proof. Assume that the proposition is false for some group B of exponent >2, $|B| \geqq 18$. Let a be an element of B having largest possible order. Then $x^2 \neq a$ for every $x \notin (a)$, because otherwise we would have $(x) \supset (a)$, contradicting the choice of a. Indeed we must have $x^2 = e$ for every $x \notin (a)$, because otherwise letting $b = x$, the pair a, b would satisfy the requirements of the proposition. This shows also that $(x\, a)^2 = e$ for every $x \notin (a)$, i.e.

$$x\, a\, x = a^{-1}, \quad x\, a = a^{-1}\, x.$$

Further, if we had $|(a)| \geqq 7$, then setting $b = a^3$ the pair a, b would satisfy the requirements of the proposition. Therefore $|(a)| \leqq 6$ and, in view of $|B| \geqq 18$, we can choose $x, y \in B\backslash(a)$ such that the product $x\, y \notin (a)$. Then $x\, a\, x = a^{-1}\, x\, x = a^{-1}$ and $y\, a\, y = a^{-1}\, yy = a^{-1}$, so that

$$x\, a\, x = y\, a\, y, \quad x\, y\, a = a\, x\, y.$$

But also, since $x\, y \notin (a)$, we have $x\, y\, a = a^{-1}\, x\, y$, and hence

$$a\, x\, y = a^{-1}\, x\, y, \quad a = a^{-1},$$

contradicting the choice of a.

1.4. PROPOSITION. *Let d be an integer $\geqq 2$ and B a finite group. If*

$$|B| \geqq 3(d^3 + d^2),$$

then B has a generating δ-set of size at least d.

Proof. According to proposition 1.3, B has a δ-set $\{a, b\}$ containing two elements.

Let D be a maximum size δ-set of B, $|D| = n$, $D = \{x_1, \ldots, x_n\}$ and assume that the sum $\sum_{i=1}^n |(x_i)|$ is largest possible. In order to prove that D generates B, we shall show that the set

$$\bar{D} = \bigcup_{i=1}^n (x_i) \cup \{x^{-1}y, xy^{-1}, xy \mid x, y \in D\}$$

is the entire group B. For otherwise let z be any element of $B\backslash\bar{D}$. If $z^2 \notin D$, then $D \cup \{z\}$ is a δ-set, a contradiction to the maximality of D. On the other hand, if $z^2 = x_i \in D$, then

$$D' = (D\backslash\{x_i\}) \cup \{z\}$$

is a δ-set of maximum size $n = |D|$. But $(z) \supset (x_i)$, so that

$$\sum_{x \in D'} |(x)| > \sum_{x \in D} |(x)|,$$

contradicting the maximality of the latter sum.

There remains to prove that D contains at least d elements. This again will be a consequence of the equality $\bar{D} = B$. Suppose that $|D| = n < d$. We shall obtain a contradiction, If we had $|(x_i)| < 3\,d^2$ for every $x_i \in D$, then

$$|B| = |\bar{D}| < n\ (3\,d^2) + 3n^2,$$
$$|B| < d\ (3\,d^2) + 3d^2 = 3(d^3 + d^2),$$

a contradiction to the initial assumption on the order of B. Therefore $|(x_i)| \geqq 3\,d^2$ for some $x_i \in D$. Keeping this subscript i fixed, observe that for each $x_j \in D$, the equation $z^2 = x_j$ has at most two solutions $z \in (x_i)$. Consequently there are at most $2n$ elements in (x_i), the square of which belongs to D. On the other hand, we have the inequality

$$|\{x^{-1}\,y, x\,y^{-1}, x\,y \mid x, y \in D\}| \leqq 3\,n^2,$$

so that it is possible to find an element

$$z \in (x_i)\backslash\{x^{-1}\,y,\ x\,y^{-1},\ x\,y|x,\ y \in D\}$$

such that $z \notin D$, $z^{-1} \notin D$, $z^2 \notin D$. Then $D \cup \{z\}$ is a δ-set strictly larger than D, which contradicts the choice of D.

1.5. If n and m are integers, then we denote by $[n, m]$ the set of integers i such that $n \leqq i$ and $i \leqq m$.

Let k and n be integers, $k \geqq 2$, $n \geqq 2k + 3$. Let $G_{k,n}$ be the k-uniform hypergraph defined by

$$\begin{aligned} V(G_{k,n}) &= [1, n] \\ E(G_{k,n}) &= \{[i, i + k - 1] | 1 \leqq i \leqq n - k - 1\} \\ &\qquad \cup \{[i, i + k - 2] \cup \{n - 1\} | i = 2, k + 1\} \\ &\qquad \cup \{S \cup \{n\} | S \subseteq [1, n - 1], |S| = k - 1\}. \end{aligned}$$

The graph $G_{2,10}$ is pictured in Figure 1.

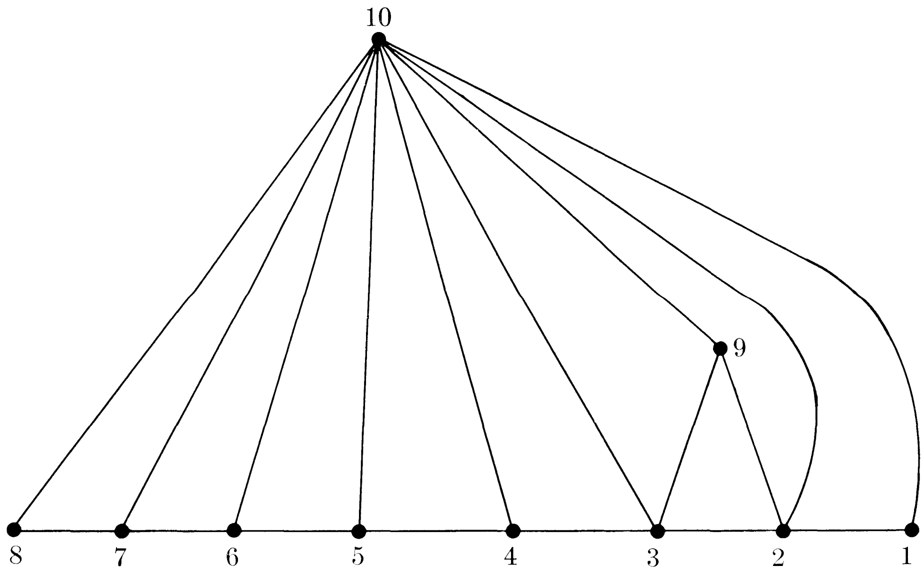

FIGURE 1.

A hypergraph G is called a $(k, n) - arc$ if it is isomorphic to $G_{k,n}$.

1.51. LEMMA. *For every* $x \in V(G_{k,n})$, $x \neq n$, *we have* $d(x) < d(n)$.

Proof. It is clear from the definition of $G_{k,n}$ that

$$d(n) = \binom{n-1}{k-1}.$$

Also every $x \in [1, n - 1]$ lies together with n in some line exactly $\binom{n-2}{k-2}$ times, and lies in at most $k + 1$ lines not containing n, so that

$$d(x) \leqq k + 1 + \binom{n-2}{k-2}.$$

Using the inequalities

$$k + 1 < \binom{2k+1}{k-1} \leqq \binom{n-2}{k-1},$$

we get

$$d(x) \leqq k + 1 + \binom{n-2}{k-2} < \binom{n-2}{k-1} + \binom{n-2}{k-2} = \binom{n-1}{k-1} = d(n).$$

1.52. The vertex of largest degree of any $(k, n) -$ arc G is called the *distinguished vertex* of G.

1.53. LEMMA. *The automorphism group of* $G_{k,n}$ *is trivial.*

Proof. Obviously

$$V(G_{k,n})\backslash\{n\} = [1, n-1]$$

is a constituent of Aut $G_{k,n}$. Also it is not difficult to see that

$$\text{Aut } G_{k,n} \mid [1, n-1]$$

is trivial, and consequently so is Aut $G_{k,n}$.

1.54. LEMMA. $G_{k,n}$ *is not bipartite if* $n \geqq k^2 - k + 2$.

Proof. Suppose that

$$V(G_{k,n}) = [1, n] = V_1 \cup V_2,$$

where V_1 and V_2 are independent sets. Assuming that $n \in V_1$, we must have

$$|V_1 \cap [1, n-2]| \leqq k - 2.$$

But also for every $i \in V_1 \cap [1, (n-2) - k]$ we must have

$$V_1 \cap [i+1, i+k] \neq \emptyset,$$

because otherwise $[i+1, i+k]$ would be a line of $G_{k,n}$ contained in V_2. For similar reasons,

$$V_1 \cap [1, k] \neq \emptyset.$$

It follows that

$$\begin{aligned} n - 2 = |[1, n-2]| &\leqq (k-1) + |V_1 \cap [1, n-2]| \cdot k \\ &\leqq (k-1) + (k-2)k = k^2 - k - 1, \end{aligned}$$

a contradiction.

1.55. LEMMA. *If* $n \geqq 2k + 6$, *then*

$$2d(x) < d(n)$$

for every $x \in V(G_{k,n})$, $x \neq n$.

https://doi.org/10.4153/CJM-1978-082-9 Published online by Cambridge University Press

Proof. We have already seen in the proof of Lemma 1.51 that

$$d(x) \leqq k + 1 + \binom{n-2}{k-2}.$$

Consequently

$$2d(x) \leqq 2k + 2 + 2\binom{n-2}{k-2} \leqq n - 4 + 2\binom{n-2}{k-2}.$$

But the assumption $n \geqq 2k + 6$ implies also that

$$n - 3 + \binom{n-2}{k-2} \leqq \binom{n-2}{k-1}$$

and

$$2d(x) < \binom{n-2}{k-1} + \binom{n-2}{k-2} = \binom{n-1}{k-1} = d(n).$$

1.6. PROPOSITION. *Let k be any integer $\geqq 3$. Let a finite group B have a generating δ-set D containing at least $k^2 + 1$ elements. Then B has a regular representation by a k-uniform hypergraph H.*

Proof. I. Let n be the cardinality of D. Let G be a $(k - 1, n) -$ arc with vertex set $V(G) = D$, and assume that the distinguished vertex of G is an element a of D having order larger than 2.

Let H be defined by

$$V(H) = B,$$
$$E(H) = \{\{t, t\,x_1, \ldots, t\,x_{k-1}\} | \{x_1, \ldots, x_{k-1}\} \in E(G), t \in B\}.$$

Obviously every left translation of B is an automorphism of H. We have to prove that the stabilizer $(\text{Aut } H)_e$ is trivial.

Clearly $N_H(e)$ is a constituent of $(\text{Aut } H)_e$. Define a $(k - 1) -$ uniform hypergraph G_1 by

$$V(G_1) = N_H(e),$$
$$E(G_1) = \{\{x_1, \ldots, x_{k-1}\} | \{e, x_1, \ldots, x_{k-1}\} \in E(H)\}.$$

Then $(\text{Aut } H)_e \,|\, N_H(e) \subseteq \text{Aut } G_1$.

II. Let

$$E_0 = E(G),$$
$$E_1 = \{\{x, xy_1, \ldots, xy_{k-2}\} | \{x, y_1, \ldots, y_{k-2}\} \in E(G), x^2 = e\},$$
$$E_2 = \{\{x^{-1}, x^{-1}\,y_1, \ldots, x^{-1}y_{k-2} | \{x, y_1, \ldots, y_{k-2}\} \in E(G), x^2 \neq e\}.$$

It follows from the axioms of a δ-set that E_0, E_1 and E_2 are pairwise disjoint. Moreover, for every $A_0 \in E_0$ and $A_2 \in E_2$, we have $A_0 \cap A_2 = \emptyset$.

We claim that $E(G_1) = E_0 \cup E_1 \cup E_2$. The inclusion $E_0 \cup E_1 \cup E_2 \subseteq E(G_1)$ is readily verified. On the other hand, let $A = \{z_1, \dots, z_{k-1}\} \in E(G_1)$. By definition,

$$\{e, z_1, \dots, z_{k-1}\} = \{t, tx_1, \dots, tx_{k-1}\}$$

for some $t \in B$ and

$$\{x_1, \dots, x_{k-1}\} \in E(G).$$

If $e = t$, then $A \in E_0$. Otherwise e is one of the tx_i, $i = 1, \dots, k - 1$, and there is no loss of generality in assuming that $e = tx_1$. In this case

$$\{e, z_1, \dots, z_{k-1}\} = \{x_1^{-1}, e, x_1^{-1}x_2, \dots, x_1^{-1}x_{k-1}\},$$
$$A = \{x_1^{-1}, x_1^{-1}x_2, \dots, x_1^{-1}x_{k-1}\} \in E_1 \cup E_2.$$

III. Let us denote

$$D^{-1} = \{x^{-1} | x \in D\},$$
$$F = \{x^{-1} y | x, y \in D\}.$$

From the axioms of a δ-set it is clear that $F \cap D = \emptyset$ and $F \cap D^{-1} = \emptyset$. It follows from part II that $V(G_1) \subseteq D \cup D^{-1} \cup F$, and also that $G_1 [D] = G$.

Ler K be the connected component of G_1 that contains the distinguished vertex a of G. Since, according to Lemma 1.54, $G = G_1 [D]$ is not bipartite, it follows that $G_1 [K]$ is not bipartite. For every other connected component $K' \neq K$ of G_1, if there is any, we have

$$K' \cap D = \emptyset$$
$$K' = (D^{-1} \cap K') \cup (F \cap K').$$

But $D^{-1} \cap K'$ being disjoint from D, is independent in G_1, and so is $F \cap K'$. Hence $G_1 [K']$ is bipartite and K is a constituent of Aut G_1 and also of $(\text{Aut } H)_e$. We have

$$\text{Aut } G_1 | K \subseteq \text{Aut } G_1 [K]$$

and consequent.y

$$(\text{Aut } H)_e | K \subseteq \text{Aut } G_1[K].$$

It will follow from the subsequent parts IV–VI, that the vertex a of K is fixed by every automorphism of $G_1 [K]$. For every $x \in K$, we shall write

$$d(x) = d_{G_1[K]}(x),$$
$$N(x) = N_{G_1[K]}(x).$$

IV. It follows from part II that every $x \in D \backslash D^{-1}$ is incident in G_1 only with lines of G. In view of Lemma 1.51, $d(x) < d(a)$ for every $x \in D \backslash \bar{D}$, $x \neq a$.

If $x \in D \cap D^{-1}$, then

$$\{x, y_1, \dots, y_{k-2}\} \rightarrow \{x, xy_1, \dots, xy_{k-2}\}$$

is a bijection from the set of lines of G incident with x to the set

$$\{A \in E(G_1)\backslash E(G) | x \in A\}.$$

Consequently, in view of Lemma 1.55, we have

$$d(x) = 2\, d_G(x) < d(a)$$

for every $x \in D \cap D^{-1}$.

For every $x \in K \cap (D^{-1}\backslash D)$ we have $N(x) \subseteq F$, so that $N(x)$ is independent in G_1, while $N(a) = D\backslash\{a\}$ is not independent in G_1.

If $x \in K \cap F$, then we have to examine separately the cases $k = 3$ and $k \geqq 4$.

V. Let $k = 3$. Since $G_1\,[K]$ is a graph, we have $d(x) = |N(x)|$ for every $x \in K$. Also, since $x \in F$, $N(x) \subseteq D \cup D^{-1}$.

If $N(x) \subseteq D^{-1}\backslash D$, then $N(x)$ is independent in G_1 while $N(a)$ is not.

If $N(x) \subseteq D$, then every element of $N(x)$ has order 2, so that

$$|N(x)| \leqq |D| - 2 < n - 1, d(x) < d(a).$$

If $N(x) \nsubseteq D$ and $N(x) \nsubseteq D^{-1}\backslash D$ then, since no vertex in D is adjacent in G_1 to a vertex in $D^{-1}\backslash D$, x is a cut vertex of $G_1[N(x) \cup \{x\}]$. On the contrary, a is not a cut vertex of $G_1\,[N(a) \cup \{a\}] = G_1\,[D] = G$.

VI. Let $k \geqq 4$. If $|N(x) \cap (D \cup D^{-1})| \geqq 2$, then let S be any subset of $N(x)$ such that

$$|S| = k - 2, \quad |S \cap (D \cup D^{-1})| \geqq 2.$$

Clearly $S \cup \{x\} \notin E\,(G_1)$. On the contrary, for every subset S of $N(a)$ containing $k - 2$ elements, $S \cup \{a\} \in E\,(G_1)$.

If $|N(x) \cap (D \cup D^{-1})| = 1$, then every line of G_1 incident with x is incident with the unique element y of $N(x) \cap (D \cup D^{-1})$. But it is easy to find two lines of G, and hence of G_1, the intersection of which contains only a and no other vertex.

VII. The different properties of a and of the other vertices $x \neq a$ of $G_1[K]$, discussed in the preceding parts IV–VI, show that every automorphism of $G_1\,[K]$ must fix a. Consequently

$$D = N\,(a) \cup \{a\} = N_{G_1}(a) \cup \{a\}$$

is a constituent of Aut $G_1\,[K]$, hence of Aut G_1, and finally of $(\text{Aut } H)_e$. Therefore

$$(\text{Aut } H)_e | D \subseteq \text{Aut } G_1\,[D] = \text{Aut } G.$$

But, according to Lemma 1.53, Aut G is trivial. Consequently $(\text{Aut } H)_e|D$ is trivial.

VIII. Since D generates B, every $x \in B$ can be written as a product of elements of D. Let $l(x)$ be the minimum number of factors in such an expression of x. We have, e.g., $l(x) = 0$ if and only if $x = e$, and $l(x) = 1$ if and only if $x \in D$.

We prove by induction on $l(x)$ that every $\sigma \in (\text{Aut } H)_e$ fixes x. This is true by definition if $l(e) = 0$. For $l(x) = 1$ this is exactly the triviality of $(\text{Aut } H)_e|D$, proved in VII.

If the claim is false, let $x \in B$ such that $\sigma(x) \neq x$ for some $\sigma \in (\text{Aut } H)_e$, and assume that $l(x) = g$ is smallest possible. Then $x = y_1 \dots y_g$ with $y_i \in D$ for $1 \leqq i \leqq g$. Now

$$l(x\, y_g^{-1}) = l(x) - 1$$

and hence, by the induction hypothesis,

$$\sigma(x\, y_g^{-1}) = x\, y_g^{-1}.$$

Consider the automorphism τ of H given by $\tau(z) = x\, y_g^{-1} z$ for every $z \in B$. We have $\tau^{-1} \sigma \tau \in (\text{Aut } H)_e$, and consequently

$$\tau^{-1} \sigma \tau(y_g) = y_g, \quad \sigma \tau(y_g) = \tau(y_g), \quad \sigma(x) = x.$$

2. Groups of exponent 2.

2.1. We recall that if every non-identity element of a group B has order 2, then B is necessarily isomorphic to some Z_2^n. Although the term elementary abelian 2-group is often used and might be more informative to designate such groups, in the sequel we shall consistently call them groups of exponent 2.

The notation will be kept multiplicative.

2.2. LEMMA. *For every integer $n \geqq 6$ there exists a graph G_n having n vertices, each of them of degree at least* 2, *and such that* Aut G_n *is trivial.*

Proof. Let

$$V(G_n) = [1, n],$$
$$E(G_n) = \{\{i, i+1\} | i \in [1, n-1]\} \cup \{\{1, n\}, \{1, n-1\}, \{1, n-2\}\}.$$

The graph G_6 is pictured in Figure 2.

Remark. Every graph having less than 6 and at least 2 vertices has a non-trivial automorphism group.

2.3. PROPOSITION. *Every finite group B of exponent* 2 *and having order at least* 2^6 *has a regular representation by a 3-uniform hypergraph H.*

Proof. Let D be a minimal set of generators for B. (D is a basis of B if this is viewed as a vector space over the two-element field.) Certainly

$$|D| = \log_2 |B| \geqq 6.$$

According to Lemma 2.2, there is a graph G such that

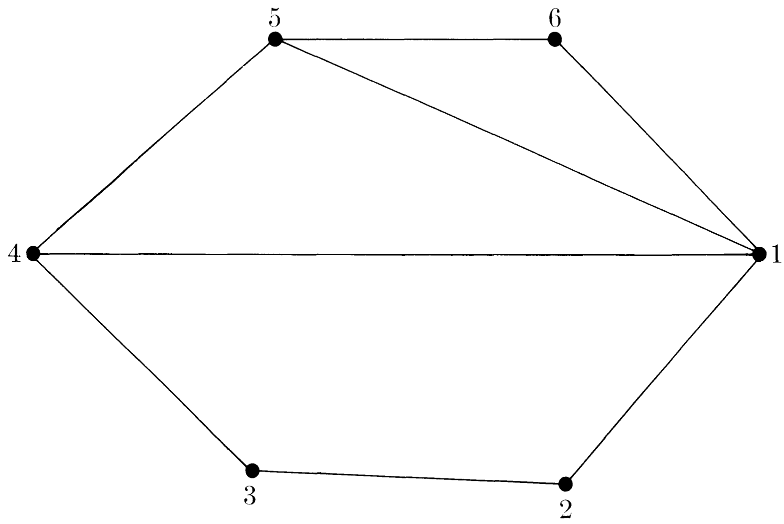

FIGURE 2.

(i) $V(G) = D$;
(ii) Aut G is trivial;
(iii) every vertex of G has degree at least 2.

Let H be defined by

$$V(H) = B,$$

$$E(H) = \{\{t, tx, ty\} \mid \{x, y\} \in E(G), t \in B\}.$$

Every left translation of B is an automorphism of H. We shall prove that $(\text{Aut } H)_e$ is trivial.

Clearly $N_H(e)$ is a constituent of $(\text{Aut } H)_e$. Define a graph G_1 by

$$V(G_1) = N_H(e)$$

$$E(G_1) = \{\{x, y\} \mid \{e, x, y\} \in E(H)\}.$$

Defining again $F = \{x\,y \mid x, y \in D\}$, we have

$$V(G_1) \subseteq D \cup F, \quad D \cap F = \emptyset.$$

Also $N_{G_1}(x\,y) = \{x, y\}$ for every $x\,y \in F \cap V(G_1)$, and $G_1[D] = G$. Clearly

$$d_{G_1}(x) = 2\,d_G(x) \geqq 4$$

for every $x \in D$, while

$$d_{G_1}(x) = 2$$

for every $x \in F \cap V(G_1)$. Therefore D is a constituent of Aut G_1 and hence of

$(\text{Aut } H)_e$, so that

$$(\text{Aut } H)_e \mid D \subseteq \text{Aut } G_1 [D] = \text{Aut } G.$$

But Aut G is trivial, so that every $\sigma \in (\text{Aut } H)_e$ fixes every element of D. To prove that every $\sigma \in (\text{Aut } H)_e$ fixes every $x \in B$, i.e. that $(\text{Aut } H)_e$ is trivial, we apply mutatis mutandis the argument of part VIII in the proof of Proposition 1.6.

2.4. PROPOSITION. *Let k be any integer $\geqq 4$ and B a finite group of exponent 2. If $|B| \geqq 4k + 2$, then B has a regular representation by a k-uniform hypergraph.*

Proof. I. Let $|B| = 2^n$ and let $\{x_1, \ldots, x_n\}$ be a minimal set of generators for B. Let

$$D = \left\{\prod_{i \in I} x_i | I \subseteq [1, n], |I| \text{ odd}\right\}.$$

D is a sum free set and

$$|D| = 2^{n-1} \geqq 2k + 1.$$

Let G be a $(k - 1, 2^{n-1})$ – arc (see 1.5) with $V(G) = D$. As before, let H be defined by

$$V(H) = B,$$

$$E(H) = \{\{t, tx_1, \ldots, tx_{k-1}\} | \{x_1, \ldots, x_{k-1}\} \in E(G), t \in B\}.$$

Let G_1 be the $(k - 1)$-uniform hypergraph defined by

$$V(G_1) = N_H(e),$$

$$E(G_1) = \{\{x_1, \ldots, x_{k-1}\} | \{e, x_1, \ldots, x_{k-1}\} \in E(H).$$

To prove that $(\text{Aut } H)_e$ is trivial, it will suffice to show, as in the proof of Propositions 1.6 and 2.3, that every $(\text{Aut } H)_e$ fixes every $x \in D$.

II. Let

$$E_1 = \{\{x, xy_1, \ldots, xy_{k-2}\} | \{x, y_1 \ldots, y_{k-2}\} \in E(G)\}.$$

Since D is a sum free set, $E(G) \cap E_1 = \emptyset$. An argument similar to that of part II in the proof of Proposition 1.6 can show that

$$E(G_1) = E(G) \cup E_1.$$

Also defining again $F = \{x\,y \mid x, y \in D\}$, we see that

$$V(G_1) = D \cup F, \quad D \cap F = \emptyset$$

and

$$G_1 [D] = G.$$

Let $a \in D$ be the distinguished vertex of the $(k - 1, 2^{n-1})$ – arc G.

https://doi.org/10.4153/CJM-1978-082-9 Published online by Cambridge University Press

III. For every $x \in D$, the correspondence

$$\{x, y_1, \ldots, y_{k-2}\} \rightarrow \{x, xy_1, \ldots, xy_{k-2}\}$$

is a bijection from $\{A \in E(G) \mid x \in A\}$ to $\{A \in E_1 \mid x \in A\}$. It follows from Lemma 1.51 that for every $x \in D$, $x \neq a$,

$$d_{G_1}(x) = 2\, d_G(x) < 2\, d_G(a) = d_{G_1}(a).$$

IV. Setting $N_1 = D\backslash\{a\}$, and $N_2 = \{ax \mid x \in D\}$, we have

$$N_{G_1}(a) = N_1 \cup N_2, \quad N_1 \cap N_2 = \emptyset.$$

Moreover, for every subset S of N_1 or of N_2 containing $k - 2$ elements,

$$S \cup \{a\} \in E\,(G_1).$$

On the contrary, assume that for a vertex $x \in F$, $N_{G_1}(x)$ is the union of two disjoint sets $N_{G_1}(x) = M_1 \cup M_2$ such that for every subset S of M_1 or of M_2 containing $k - 2$ elements,

$$S \cup \{x\} \in E\,(G_1).$$

Since we can see without difficulty that $D \subseteq N_{G_1}(x)$, it is clear that one of the sets M_1 or M_2, say M_1, has to contain at least $k - 2$ elements of D. Let

$$S \subseteq M_1 \cap D, \quad |S| = k - 2.$$

We should have

$$S \cup \{x\} \in E\,(G_1)$$

which, in view of $k - 2 \geqq 2$, is impossible.

V. It follows from III and IV that every $\sigma \in \operatorname{Aut} G_1$ fixes the distinguished vertex a. Therefore $N_{G_1}(a)$ is a constituent of Aut G_1. But it is easy to see that

$$\Pi = \{N_1, N_2\}$$

as defined in IV, is the only partition Π of $N_{G_1}(a)$ into two blocks such that for each block C of Π and every subset S of C containing $k - 2$ elements

$$S \cup \{a\} \in E\,(G_1).$$

Also N_2 is independent in G_1, while N_1 is not. Consequently $D = N_1 \cup \{a\}$ is a constituent of Aut G_1 and hence of $(\operatorname{Aut} H)_e$. But Aut $G_1\,[D] =$ Aut G is trivial, implying that every $\sigma \in (\operatorname{Aut} H)_e$ fixes every $x \in D$.

The proof is finished.

3. Main theorem. *There exists a polynomial $p(x)$ with the property that for every integer $k \geqq 3$, every finite group of order at least $p(k)$ has a regular representation by a k-uniform hypergraph.*

Proof. Let

$$p(x) = 3[(x^2 + 1)^3 + (x^2 + 1)^2],$$

a polynomial of degree 6. The result follows from Propositions 1.4, 1.6, 2.3, 2.4 and the inequalities

$$p(3) > 2^6$$

and

$$p(k) > 4k + 2$$

for every $k \geqq 4$.

4. Concluding remarks. Recently F. Hoffman has shown [**10**], that the theorem of Feit and Thompson on the solvability of groups of odd order, together with a result contained in [**7**], implies that every finite group of odd order $\geqq 5^7$ has a regular representation by a 3-uniform hypergraph.

For some classes of groups the bound $p(k)$ given in the main theorem is very crude. It was shown, for example, in [**6**] that a cyclic group Z_n has a regular representation by a 3-uniform hypergraph if and only if $n \neq 3, 4, 5$. We think that the polynomial $p(x)$ can be replaced by one of degree less that 6, perhaps even by a linear polynomial of the form $x + c$, c constant.

REFERENCES

1. C. Berge, *Graphes et hypergraphes* (Dunod, Paris, 1970).
2. A. Cayley, *On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$, Philos. Mag. *7* (1854), 40–47.
3. ——— *The theory of groups*, Proc. London Math. Soc. *9* (1878), 126–33.
4. C. Y. Chao, *On a theorem of Sabidussi*, Proc. Amer. Math. Soc. *15* (1964), 291–92.
5. W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. *13* (1963), 775–1029.
6. S. Foldes, *Symmetries*, Ph.D. Thesis, University of Waterloo, 1977.
7. S. Foldes and N. M. Singhi, *Regular representation of abelian groups by 3-uniform hypergraphs*, CORR 77–2, University of Waterloo, January, 1977.
8. R. Frucht, *Herstellung von Graphen mit vorgegebener abstrakter Gruppe*, Compositio Math. *6* (1939), 239–50.
9. P. Hell and J. Nesetril, *Graphs and k-societies*, Canad. Math. Bull. *13* (1970), 375–81.
10. F. Hoffman, *Note on δ-sets in finite groups*, written communication.
11. W. Imrich, *Graphen mit transitiver Automorphismengruppe*, Monatsh. Math. *73* (1969), 341–47.
12. ——— *Graphs with transitive abelian automorphism group*, Colloquia Math. Soc. Janos Bolyai *4*, Hungary (1969), 651–56.
13. ———*On graphical regular representations of groups*, Colloquia Math. Soc. Janos Bolyai *10*, Hungary (1973), 905–25.
14. ——— *On graphs with regular groups*, J. Comb. Theory *B19* (1975), 174–80.
15. I. N. Kagno, *Linear graphs of degree ≦6 and their groups*, Amer. J. Math. *68* (1946), 505–20.
16. M. H. McAndrew, *On graphs with transitive automorphism groups*, Notices Amer. Math. Soc. *12* (1965), 575.

17. L. A. Nowitz, *On the non-existence of graphs with transitive generalized dicyclic groups*, J. Comb. Theory *4* (1968), 49–51.

18. L. A. Nowitz and M. E. Watkins, *Graphical regular representations of non-abelian groups, I. and II.*, Can. J. Math. *24* (1972), 993–1008 and 1009–1018.

19. G. Sabidussi, *Vertex-transitive graphs*, Monatsh. Math. *68* (1964), 426–38.

20. A. P. Street, *Sum-free sets*, Lecture Notes in Math. *292* (Springer-Verlag, 1972), 123–271.

21. M. E. Watkins, *On the action of non-abelian groups on graphs*, J. Comb. Theory *B11* (1971), 95–104.

22. ——— *On graphical regular representations of $C_n \times Q$*, Lecture Notes in Math. *303* (Springer-Verlag, 1972), 305–11.

23. ——— *Graphical regular representations of alternating, symmetric, and miscellaneous small groups*, Aequationes Math. *11* (1975), 40–50.

24. ——— *Graphical regular representations of free products of groups*, J. Comb. Theory *B21* (1976), 47–56.

25. H. Wielandt, *Finite permutation groups* (Academic Press, 1964).

University of Waterloo,
Waterloo, Ontario;
Tata Institute of Fundamental Research,
Bombay, India