11-1995

Rectangular Groups

Nick Fiala
Rose-Hulman Institute of Technology

Crystal Hanscom
Rose-Hulman Institute of Technology

Patrick Keenan
Rose-Hulman Institute of Technology

Tung Tran
Rose-Hulman Institute of Technology

MSTR 95-06

RECTANGULAR GROUPS

N. Fiala, C. Hanscom, P. Keenan, T. Tran

MS TR 95-06

November 1995

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198 Phone: (812) 877-8391

Rectangular Groups

Nick Fiala, Crystal Hanscom, Patrick Keenan, and Tung Tran

1. Introduction

A finite group G is said to be a (m, n)-**rectangle** if it contains subsets A and B such that $|A| > 1$, $A \subset B$, $AB = G$, and $|A| \cdot |B| = |G|$. For example, the dihedral group

$$D_n = \left\langle x, y : x^n = y^2 = e, xy = yx^{n-1} \right\rangle$$

is seen to be a $(2, n)$-rectangle for $n \geq 3$ by taking

i) $A = \{x, y\}$ and $B = \{x^i, y, x^j y : i = 1, 3, \ldots, n-2 \text{ and } j = 2, 4, \ldots, n-1\}$ if n is odd,

All authors supported by NSF grant DMS-9322338

ii) $A = \{x, y\}$ and $B = \{x^i, y, x^j y : i = 1, 3, \dots, n-3 \text{ and } j = 1, 3, \dots, n-1\}$ if n is even.

Our definition of a rectangular group is motivated by the fact that a non-trivial group can not be a **perfect square**; i.e., there does not exist a finite group which is a (m, m)-rectangle for any $m > 1$ (see [1] and [2]). The purpose of this paper is to show that there exist rectangular groups that are nearly perfect squares and to make some observations and conjectures concerning rectangular groups.

2. Rectangular groups that are nearly perfect squares

Let $\mathbb{Z}_n$ denote the cyclic group of order n, let $\mathrm{Aut}(\mathbb{Z}_n)$ denote the automorphism group of $\mathbb{Z}_n$, and let $\mathbb{Z}_n \times_\theta \mathrm{Aut}(\mathbb{Z}_n)$ denote the semi-direct product of $\mathbb{Z}_n$ with $\mathrm{Aut}(\mathbb{Z}_n)$ where θ represents the natural action of $\mathrm{Aut}(\mathbb{Z}_n)$ on $\mathbb{Z}_n$. Observe that $|\mathbb{Z}_n \times_\theta \mathrm{Aut}(\mathbb{Z}_n)| = |\mathrm{Aut}(\mathbb{Z}_n) \times \mathbb{Z}_n| = \phi(n) \cdot n$ where ϕ is the Euler ϕ-function.

Theorem 2.1. *$G = \mathbb{Z}_n \times_\theta Aut(\mathbb{Z}_n)$ is a $(\phi(n), n)$-rectangle for $n \geq 3$.*

Proof. Let $A = \{(\alpha, 1^\alpha) : \alpha \in \mathrm{Aut}(\mathbb{Z}_n)\}$, let $C = \{(id, k) : k \in \mathbb{Z}_n - \mathrm{orbit}(1)\}$, and set $B = A \cup C$. It follows that $|A| = \phi(n)$ and $|B| = |A| + |C| = \phi(n) + n - \phi(n) = n$. Thus, $|A| > 1$, $A \subset B$, and $|A| \cdot |B| = |G|$ as required.

To show that $AB = G$ it suffices to show that $|AB| = |G|$; i.e., $|AB| = \phi(n) \cdot n$. Since $AB = A(A \cup C) = A^2 \cup AC$, we have $|AB| = |A^2| + |AC| - |A^2 \cap AC|$.

Claim: $|A^2| = |A|^2$. If $(\alpha, 1^\alpha)(\beta, 1^\beta) = (\gamma, 1^\gamma)(\delta, 1^\delta)$, then $(\alpha\beta, 1^{\alpha\beta} + 1^\beta) = (\gamma\delta, 1^{\gamma\delta} + 1^\delta)$. It follows that $\alpha\beta = \gamma\delta$ and, in turn, that $1^\beta = 1^\delta$ (i.e., $\beta = \delta$) and $\alpha = \gamma$.

Claim: $|AC| = |A| \cdot |C|$. If $(\alpha, 1^\alpha)(id, k) = (\gamma, 1^\gamma)(id, l)$, then $(\alpha, 1^\alpha + k) = (\gamma, 1^\gamma + l)$. It follows that $\alpha = \gamma$ and, in turn, that $k = l$.

Claim: $|A^2 \cap AC| = 0$. If $(\alpha, 1^\alpha)(\beta, 1^\beta) = (\gamma, 1^\gamma)(id, k)$, then $(\alpha\beta, 1^{\alpha\beta} + 1^\beta) = (\gamma, 1^\gamma + k)$. It follows that $\alpha\beta = \gamma$ and, in turn, that $1^\beta = k$; i.e., $k \in \text{orbit}(1)$, a contradiction.

Thus

$$|AB| = (\phi(n))^2 + \phi(n) \cdot (n - \phi(n)) = |G|$$

and the result follows.

Corollary 2.2. *There exists a sequence of groups, $\{G_i\}$, such that G_i is a (m_i, n_i)-rectangle and $m_i/n_i \to 1$.*

Proof: Taking $G_i = \mathbb{Z}_{p_i} \times_\theta \text{Aut}(\mathbb{Z}_{p_i})$, where p_i is the i-th prime, and using the previous construction gives $m_i = p_i - 1$ and $n_i = p_i$.

3. Observations and conjectures

Let G be a (m,n)-rectangle with appropriate subsets A and B.

1. $|A^2| = |A|^2$. This follows because $G = AB = A(A \cup (B-A)) = A^2 \cup A(B-A)$ and $|A| \cdot |B| = |G|$.

2. No two elements of A may commute. Otherwise $|A^2| < |A|^2$.

3. No abelian group is a rectangle. (Our definition excludes trivial rectangles).

4. The quaternion group of order eight is a non-abelian group which is not a rectangle. The quaternion group has no subset A of cardinality two satisfying $|A^2| = |A|^2$.

5. No dihedral group is a (m,n)-rectangle for $m > 2$. Any subset of a dihedral group satisfying $|A^2| = |A|^2$ has cardinality at most two because any two rotations commute and any two reflections have the same square.

Conjecture 3.1. *If G is nilpotent and a (m,n)-rectangle, then $m/n \leq 1/2$. (Note that the ratio for D_4 is 1/2.)*

Conjecture 3.2. *If G is a (m,n)-rectangle, then m is bounded above by the order of the derived subgroup of G.*

References

[1] M. Cushman, *An elementary proof that finite groups lack unique product structures.* Journal of Algebra (to appear).

[2] D. Dimovsky, *Groups with unique product structures.* Journal of Algebra **146** (1992) 205-209.

Addresses of authors

Nick Fiala, Rose-Hulman Institute of Technology, Terre Haute IN 47803

Crystal Hanscom, Mills College, Oakland CA 94613

Patrick Keenan, University of Illinois, Urbana IL 61801

Tung Tran, Duke University, Durham NC 27708