12-1994

Square Roots of Finite Groups - II

Matthew Devos

David McAdams

Rebecca Rapoport

SQUARE ROOTS OF FINITE GROUPS – II

Matthew Devos, David McAdams,
and Rebecca Rapoport

MS TR 94-06

December 1994

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

FAX(812) 877-3198

Phone: (812) 877-8391

Square Roots of Finite Groups — II

Matthew Devos, David McAdams, and Rebecca Rapoport*

December 8, 1994

Abstract

A subset R of a finite group G is a square root of G if $R^2 = G$. If R is a square root of G for which $|R|^2 = G$, then R is referred to as a perfect square root of G. It can be shown using character theory that perfect square roots do not exist. The purpose of this paper is to work toward an elementary proof of this result.

1 Introduction

A subset R of a finite group G is a **square root** of G if $R^2 = G$. If R is a square root of G for which $|R|^2 = |G|$, then R is referred to as a **perfect square root** of G. Dimovski [2] has shown, using character theory, that no finite (non-trivial) group can have a perfect m-th root for $m \geq 2$. The purpose of this technical report is to continue the search, begun by Abhyankar and Grossman [1], for an elementary proof that perfect square roots do not exist.

2 Facts About Groups With Perfect Square Roots

Throughout this section R denotes a perfect square root of the finite group G.

*All three authors supported by NSF Grant NSF–DMS 9322338

Fact 1 *Let $a, b, c, d \in R$. If $a \neq c$ and $b \neq d$, then $ab \neq cd$.*

PROOF: If $ab = cd$, then $|R^2| < |R|^2$ and $R^2 \neq G$; i.e., there can be no 'repeated products' in R^2.

Fact 2 *Let $a, b \in R$. If $a \neq b$, then a is not in the centralizer of b.*

PROOF: If a is in the centralizer of b, then there is a repeated product in R^2: $ab = ba$.

The next three facts are immediate corollaries of Fact 2.

Fact 3 *The intersection of R with the center of G is trivial. In particular, the identity is not in R.*

Fact 4 *If $a, a^{-1} \in R$, then $a = a^{-1}$.*

Fact 5 *R contains a unique involution.*

PROOF: Since $1 \in R^2$, there exist $x, y \in R$ such that $xy = 1$; i.e., $x = y^{-1}$. It follows from Fact 4 that $x = y$, so x is an involution. If R contains two involutions a and b, then R^2 contains the repeated product $aa = bb$.

Fact 6 *The order G is divisible by 36.*

PROOF: It suffices to show that $2 \big| |G|$ and $3 \big| |G|$ because $|G|$ is a perfect square and 2 and 3 are distinct primes. That $2 \big| |G|$ follows from Fact 5.

To show that $3 \big| |G|$, first note that for all $x, y, z \in G$,

$$xyz = 1 \Leftrightarrow yzx = 1 \Leftrightarrow zxy = 1.$$

Now consider

$$P = \{\{a, b, c\} \subseteq R | abc = 1\}.$$

- $\emptyset \notin P$

- Let $a \in R$ be given. Since R is a square root, there exist $b, c \in R$ such that $bc = a^{-1}$. Then $abc = 1$, $\{a, b, c\} \in P$, and $a \in \bigcup_{X \in P} X$. Since $a \in R$ was arbitrary, $R \subseteq \bigcup_{X \in P} X$.

- Let $X = \{a, b, c\}$, $Y = \{a, d, f\} \in P$ be such that $X \bigcap Y \neq \emptyset$. We may assume without loss of generality that $abc = 1 = adf$. But then $bc = a^{-1} = df$. By Fact 1, we may conclude that $b = d$ and $c = f$. Thus $X = Y$.

These three points imply that P is a partition of R. Now, suppose that there exists $\{a, b\} \in P$ (so, $c = a$ or $c = b$). We may assume that $aba = 1$. Then $ab = a^{-1} = ba$, and by Fact 1, we conclude that $a = b$. Therefore, each element of P has cardinality one or three. If all elements of P have 3 elements, then $3 \Big| |R|$ and therefore $3 \Big| |G|$. If there exists $\{a\} \in P$, then $a^3 = 1$; i.e. $3 \Big| |G|$.

As a corollary to this fact we have

Fact 7 *No p-group has a perfect square root.*

Fact 8 *The number of elements of order four in R is odd.*

PROOF: Consider $I = \{a \in G \mid a^2 = 1\}$. The cardinality of I is even because $|G|$ is even and $|G - I|$ is even (each element may be paired with its distinct inverse). Now, for all $a, b \in R$, $ab \in I$ implies $ba \in I$, since ab and ba have the same order. There is exactly one element of order 2 in R and this element squared will yield an element in I. All products of distinct $a, b \in R$ will yield either 0 or 2 elements of I. Therefore, there must be an odd number of elements $c \in R$ such that $c^2 \in I$. Each of these elements has order 4.

Fact 9 *If $a \in G - 1$, then $Ra \cap R = \emptyset$ or $aR \cap R = \emptyset$.*

PROOF: Let $a \in G$ be given and assume that $Ra \cap R \neq \emptyset$ and $aR \cap R \neq \emptyset$. Then there exist $b, c \in R$ such that $ba \in R$ and $ac \in R$. Now put $x = ba$, $y = ac$ and observe that $bac = by = xc$. By Fact 1 we conclude that b = x and that y = c. Thus $b = x = ba$, and we find that $a = 1$. Since $a \in G$ was arbitrary, we have the desired result.

In a similar way it can be shown that;

i) if $a \in G - 1$, $Ra \cap R = \emptyset$ or $a^{-1}R \cap R = \emptyset$,

ii) if $a \in G - 1$, $aR \cap R = \emptyset$ or $Ra^{-1} \cap R = \emptyset$.

Fact 10 *For $g \in G$, gRg^{-1} is a perfect square root of G.*

PROOF: $(gRg^{-1})(gRg^{-1}) = gR^2g^{-1} = gGg^{-1} = G$.

Fact 11 *For $a \in R$, $aRa^{-1} \cap R = \{a\}$.*

PROOF: First, $a \in aRa^{-1} \cap R$ since $aaa^{-1} = a$. Second, if $b \in R$ and $b \in aRa^{-1}$ then $b = ara^{-1}$ for some $r \in R$. This would imply that $ba = ar$ for some $a, b, r \in R$ which would contradict the fact that R is a perfect square root (since $ba = ar$ would be a repeated product). Thus a is the only element in $aRa^{-1} \cap R$.

Fact 12 *If G has a perfect square root R, then it has at least $|R|$ perfect square roots.*

PROOF: For $a, b \in R$, $aRa^{-1} = bRb^{-1}$ implies that $R = a^{-1}bR(a^{-1}b)^{-1}$. But $R \cap a^{-1}bR(a^{-1}b)^{-1} = \{a^{-1}b\}$. Thus all conjugates of R by elements of R are different.

Fact 13 *The set $\{aR : a \in R\}$ partitions G.*

PROOF: For $g \in G$, there is a unique $\{a, r\} \subseteq R$ such that $g = ar$; i.e., $g \in aR$. If $g \in aR \cap bR$, then $g = ar_1 = br_2$ and R is not a perfect square root.

Fact 14 *$RR^{-1} = \{a \in G \mid aR \cap R \neq \emptyset\}$ and $R^{-1}R = \{a \in G \mid Ra \cap R \neq \emptyset\}$*

PROOF: Let $r \in RR^{-1}$ be given. Then there exist $x, y \in R$ such that $xy^{-1} = r$, and $ry = x$. Thus $rR \cap R \neq \emptyset$. Now, let $a \in \{a \in G \mid aR \cap R \neq \emptyset\}$ be given. Then there exist $x, y \in R$ such that $ay = x$ and $a = xy^{-1}$. Thus $a \in RR^{-1}$. The second result is analagous.

Fact 15 *If G and H have perfect square roots, then $G \times H$ has a perfect square root.*

PROOF: Say that R and S are perfect square roots of G and H respectively. Then $R \times S$ is a perfect square root of $G \times H$ because $(R \times S)^2 = R^2 \times S^2 = G \times H$ and $|G \times H| = |R \times S|^2$.

3 Small Square Roots

It is natural to ask for square roots which are as small as possible. For example, a square root of S_4 must have cardinality at least five. Does such a square root exist?

Fact 16 *There are 96 square roots of S_4 of cardinality 5.*

The fact which was established by computer (using Cayley, Magma, and C) raises the following question:

> Is it possible to find a sequence of square roots $\{T_n\}$ such that $T_n^2 = S_n$ and $|T_n|/\sqrt{n!} \to 1$ as $n \to \infty$?
>
> Related results for cyclic and dihedral groups follow.
>
> **Fact 17** *There exists a sequence of cyclic groups $\{C_{i^2}\}$ and a sequence of square roots $\{T_{i^2}\}$ of these cyclic groups such that $|T_{i^2}|/i \leq 2$ for each positive integer i.*
>
> PROOF: Consider $C_{i \cdot j}$. One square root of $C_{i \cdot j}$ is $\{1, x, x^2, \ldots, x^{i-1}, x^i, x^{2i}, x^{3i}, \ldots, x^{ji}\}$. There are $j + i$ elements in this root. To maximize the ratio, let $j = i$.

Fact 18 *There exists a sequence of dihedral groups* $\{D_{4i^2}\}$ *and a sequence of roots of those groups* $\{T_{4i^2}\}$ *such that* $|T_{4i^2}|/2\sqrt{2}i \leq \sqrt{2}$.

PROOF: Consider $D_{i \cdot j}$. One square root of $D_{i \cdot j}$ is

$$\{1, x, x^2, \ldots, x^{i-1}, y, yx, yx^2, yx^3, \ldots, yx^{i-1}, yx^i, yx^{2i}, yx^{3i}, \ldots, yx^{ji}\}$$

This root has $(2j + i)$ elements. To maximize the ratio, let $i = 2j$.

4 An upper bound on the cardinality of non-square roots

Fact 19 *Let* T *be a subset of a group* G. *If* $|T| > |G|/2$, *then* $T^2 = G$.

PROOF: Our strategy is to find subsets whose squares do not contain an element $x \in G$. We will see that such a subset's size must be less than half the size of the group. To do this, we associate to each $x \in G$ a graph of G. Notice that for $a \in G$, there is a unique $b \in G$ such that $ab = x$, there is a unique c such that $bc = x$, and so on:

$$\begin{aligned} ab &= x \\ bc &= x \\ &\vdots \\ fa &= x \end{aligned}$$

The list of elements a,b,c,...,f,... must cycle since G is finite: if $fb = x$, then $a = f$ since we already have $ab = x$. Each element of G belongs to exactly one of these 'cycles' and this set of cycles is the 'graph of G associated with x.' If a subset R contains a pair of adjacent elements in a cycle, then R^2 contains x ($ab = x$). If R contains any element in a one-cycle, then R^2 contains x as well ($g^2 = x$).

If $|R| > |G|/2$, then R contains more than half of the elements in some cycle of the graph of G associated with x. Thus, it contains some pair of adjacent elements in a cycle or some one-cycle element which implies $x \in R^2$. This is true for all x in G, so $R^2 = G$.

Fact 20 *G has a subset R of size $|G|/2$ such that $R^2 \neq G$ if, and only if, the graph of G associated with some x in G has only even length cycles.*

PROOF: Suppose the graph of G associated with x has only even-sized cycles. We can choose alternating elements in each cycle. This will give $R \subset G$: $|R| = |G|/2$ and $x \notin R^2$. Suppose the graph of G associated with every x in G has some odd length cycle. It is impossible to choose exactly half of the elements of G without getting adjacent elements in a cycle or an element in a one-cycle.

References

[1] Abhyankar, K. and Grossman, D. *Square roots of finite groups* Rose-Hulman Math. Tech. Report 94-03 (1994), 1-8.

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