ON GROUP ELEMENTS HAVING SQUARE ROOTS

ASHISH KUMAR DAS

Communicated by Cheryl Praeger

Abstract. Given a finite group $G$, let $p(G)$ denote the probability that a randomly chosen element in $G$ has a square root. The object of this paper is to show that the set $\{p(G) \mid G \text{ is a finite group}\}$ is a dense subset of the closed interval $[0, 1]$.

1. Introduction

Let $G$ be a finite group. An element $g$ of $G$ is said to have a square root $h$ in $G$ if $g = h^2$. The probability that a randomly chosen element in $G$ has a square root in $G$ is given by

$$p(G) = \frac{|G^2|}{|G|},$$

where $G^2 = \{g \in G \mid g = h^2 \text{ for some } h \in G\} = \{g^2 \mid g \in G\}$.

Note that $p(G)$ as a function of finite groups is totally multiplicative i.e if $G$ and $H$ are any two finite groups then $p(G \times H) = p(G)p(H)$.

It is easy to see that

$$0 < \frac{1}{|G|} \leq p(G) \leq 1,$$

and so, the set $X = \{p(G) \mid G \text{ is a finite group}\}$ is a subset of the closed interval $[0, 1]$. In [1], Lucido and Pournaki have shown that both 0 and 1 are limit points of $X$. In this paper we show that every point in the

MSC(2000): Primary 20A05, 20D60, 20P05; Secondary 05A15
Keywords: Finite group, Projective special linear group
Received: 4 May 2006
© 2005 Iranian Mathematical Society.
interval $[0,1]$ is a limit point of $X$. More precisely, we prove here the following theorem:

**Theorem 1.1.** The set $\{ p(G) \mid G \text{ is a finite group} \}$ is dense in $[0,1]$.

For proving the theorem, we shall make use of the following facts (see [1], Propositions 2.1 and 3.1):

**Fact 1.2.** If, for $k \geq 1$, $G = (\mathbb{Z}/2\mathbb{Z})^k$, an elementary abelian 2-group, then $p(G) = 1/2^k$.

**Fact 1.3.** If, for $k \geq 2$, $G = PSL(2,2^k)$, a projective special linear group, then $p(G) = (2^k - 1)/2^k$.

2 Proof of the Theorem

To prove the theorem, it is enough to show that if $0 < x < 1$ then $x$ is a limit point of $X = \{ p(G) \mid G \text{ is a finite group} \}$. So, let $x \in (0,1)$. Then, there exists an integer $m \geq 0$ such that $1/2 \leq 2^m x < 1$; noting that $(0,1) = \bigcup_{m \geq 0} [1/2^{m+1}, 1/2^m)$. Let us put $y = 2^m x$. Then, we can choose a positive integer $n_1$ such that

$$
\frac{2^{n_1} - 1}{2^{n_1}} \leq y < \frac{2^{n_1+1} - 1}{2^{n_1+1}};
$$

noting that $[1/2,1) = \bigcup_{n \geq 1} [(2^n - 1)/2^n, (2^{n+1} - 1)/2^{n+1})$. Let us put

$$
s_1 = \frac{2^{n_1} - 1}{2^{n_1}}, \quad r_1 = \frac{2^{n_1+1} - 1}{2^{n_1+1}}.
$$

Once again, we can choose a positive integer $n_2$ such that

$$
\frac{2^{n_2} - 1}{2^{n_2}} \leq y/r_1 < \frac{2^{n_2+1} - 1}{2^{n_2+1}};
$$

noting that $1/2 \leq y/r_1 < 1$. As before, we put

$$
s_2 = \frac{2^{n_2} - 1}{2^{n_2}}, \quad r_2 = \frac{2^{n_2+1} - 1}{2^{n_2+1}}.
$$

Proceeding in this way, we can choose positive integers $n_1, n_2, n_3, \ldots$ successively and obtain sequences $\{s_i\}$ and $\{r_i\}$ such that, for $i \geq 1$,

$$
s_i = \frac{2^{n_i} - 1}{2^{n_i}}, \quad r_i = \frac{2^{n_i+1} - 1}{2^{n_i+1}},
$$

and

$$
s_i \leq \frac{y}{r_1 r_2 \ldots r_{i-1}} < r_i.$$
Clearly, $0 < s_i < r_i < 1$ for all $i \geq 1$. Also, we have $n_i \leq n_{i+1}$ for all $i \geq 1$; because

\[
\frac{y}{r_1 r_2 \ldots r_{i-1}} < \frac{y}{r_1 r_2 \ldots r_{i-1} r_i} < r_{i+1}.
\]

Thus, \{$s_i$\} is a monotonically increasing sequence which is also bounded above by 1, and hence it is convergent. Moreover, \{$s_i$\} has infinitely many distinct terms; otherwise \{$s_i$\} and hence \{$r_i$\} will be an eventually constant sequence and so, for some integer $j \geq 1$, we shall have

\[
\frac{y}{r_1 r_2 \ldots r_{j-1} r_j^{k-1}} < r_j \quad \text{or,}
\]

\[
y < r_1 r_2 \ldots r_{j-1} r_j^k \quad (k \geq 1).
\]

This is impossible, since $y > 0$ and $\lim_{k \to \infty} r_j^k = 0$. Therefore, it follows that the sequence \{$s_i$\} converges to 1 because (after omitting repeated terms) \{$s_i$\} can be viewed as a subsequence of \{$(2^n-1)/2^n$\}. This in turn implies that the sequence \{$a_i$\}, where $a_i = y/(r_1 r_2 \ldots r_{i-1})$, converges to 1, and hence the sequence \{$b_k$\}, where $b_k = r_1 r_2 \ldots r_{i-1}$, converges to $y$. Thus we have

\[
\lim_{k \to \infty} \frac{r_1 r_2 \ldots r_{i-1}}{2^m} = \frac{y}{2^m} = x.
\]

Now, for each $i \geq 1$, we consider the group

\[
G^{(i)} = G_0 \times G_1 \times \ldots G_{i-1},
\]

where

\[
G_0 = (\mathbb{Z}/2\mathbb{Z})^m, \quad G_k = PSL(2, 2^{n_k+1}) \quad (k \geq 1).
\]

Then, invoking Facts 1.2 and 1.3, we have

\[
p(G^{(i)}) = p(G_0)p(G_1)\ldots p(G_{i-1})
\]

\[
= \frac{1}{2^m r_1 r_2 \ldots r_{i-1}},
\]

and so we have $\lim_{i \to \infty} p(G^{(i)}) = x$. Thus, $x$ is a limit point of the set $X = \{p(G) \mid G \text{ is a finite group}\}$. This completes the proof of the theorem.

In spite of the above theorem, the following question is still open.

**Question.** Which rational values in the interval $[0, 1]$ does the function $p(G)$ take as $G$ runs through the set of all finite groups?
REFERENCES


Ashish Kumar Das
Department of Mathematics
North Eastern Hill University
Permanent Campus
Shillong-793022
Meghalaya
India

e-mail: akdas@nehu.ac.in