PROBABILITY THAT AN ELEMENT OF A FINITE GROUP
HAS A SQUARE ROOT

BY

M. S. LUCIDO (Udine) and M. R. POURNAKI (Tehran)

Abstract. Let $G$ be a finite group of even order. We give some bounds for the probability $p(G)$ that a randomly chosen element in $G$ has a square root. In particular, we prove that $p(G) \leq 1 - \lfloor \sqrt{|G|} \rfloor / |G|$. Moreover, we show that if the Sylow 2-subgroup of $G$ is not a proper normal elementary abelian subgroup of $G$, then $p(G) \leq 1 - 1 / \sqrt{|G|}$. Both of these bounds are best possible upper bounds for $p(G)$, depending only on the order of $G$.

1. Introduction. Let $G$ be a finite group and let $g \in G$. If there exists an element $h \in G$ for which $g = h^2$, then we say that $g$ has a square root. Clearly, $g$ may have one or more square roots, or it may have none. Let $G^2$ be the set of all elements of $G$ which have at least one square root, i.e.,

$$G^2 = \{g \in G \mid \text{there exists } h \in G \text{ such that } g = h^2\},$$

or simply $G^2 = \{g^2 \mid g \in G\}$. Then

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

is the probability that a randomly chosen element in $G$ has a square root.

The properties of $p(S_n)$, where $S_n$ denotes the symmetric group on $n$ letters, have been studied by some authors. Asymptotic properties of $p(S_n)$ were studied in [1], [2], [8] and in [3], which is devoted to the proof of a conjecture of Wilf [9] that $p(S_n)$ is non-increasing in $n$. Recently, the basic properties of $p(G)$ for an arbitrary finite group $G$ have been studied by the authors of this paper (see [7]). Moreover, they calculated $p(G)$ when $G$ is a simple group of Lie type of rank 1 or when $G$ is an alternating group. A table of $p(G)$ for the sporadic finite simple groups was also given.

In this paper we give some bounds for the probability that a randomly chosen element in a given finite group has a square root. In particular, we

2000 Mathematics Subject Classification: Primary 20A05, 20D60, 20P05; Secondary 05A15.

Key words and phrases: finite group, probability.

Research of the second author supported in part by grant no. 83200112 from IPM.
give the following best possible upper bounds for $p(G)$, depending only on $|G|$ (see Theorems 2.11 and 2.13).

**Main Theorem.** Let $G$ be a finite group of even order. Then

$$p(G) \leq 1 - \lfloor \sqrt{|G|} \rfloor / |G|.$$  

Moreover, if the Sylow 2-subgroup of $G$ is not a proper normal elementary abelian subgroup of $G$, then $p(G) \leq 1 - 1/\sqrt{|G|}$, and both bounds are the best possible.


2. The best possible bounds. By [7, Proposition 2.1(ii)], $p(G) = 1$ if and only if $|G|$ is odd. Therefore we deal with even order groups. The following theorem presents an upper bound for $p(G)$ when $G$ has even order, improving the bound $p(G) < 1$.

**Theorem 2.1.** Let $G$ be a finite group of even order, and $P$ be a Sylow 2-subgroup of $G$. Then $p(G) \leq 1 - 1/|P|$.

Let $P$ be the additive group of the field $GF(2^n)$ and let $H = GF(2^n)^\times$ be its multiplicative group. Let $G = PH$ be the semidirect product of these groups, with $H$ acting on $P$ by multiplication. Then $p(G) = 1 - 1/|P|$, which shows that the bound in Theorem 2.1 is sharp.

The following corollary is just a combination of Theorem 2.1 and Proposition 2.3 of [7].

**Corollary 2.2.** Let $G$ be a finite group of even order, and $P$ be a Sylow 2-subgroup of $G$. If $G$ is solvable, then $1/|P| \leq p(G) \leq 1 - 1/|P|$.

We recall that if a Sylow 2-subgroup of a finite group is cyclic, then the group has a normal 2-complement (see for example [6, 7.2.2]), and it is therefore solvable. We thus get the following corollary.

**Corollary 2.3.** Let $G$ be a finite group such that $|G| = 2m$, where $m$ is odd. Then $p(G) = 1/2$.

In order to prove Theorem 2.1, we must first explain a few things about decomposition of an element in a finite group. So let $G$ be a finite group. We can uniquely decompose each element $x \in G$ into $x = x_2x_2' = x_2'x_2$, where $x_2$ is a 2-element of $G$ and $x_2'$ is an element of $G$ of odd order. Moreover, if $x$ has a square root then so also does $x_2$. In the following, when we speak about $x_2$ and $x_2'$, we always mean this unique decomposition of $x$. We also need the following result originally proved by Frobenius (see [5] and also Corollary 41.11 of [4] as a more accessible reference).

**Remark 2.4.** Let $G$ be a finite group, $a \in G$, and $n$ be a positive integer. Then the number of solutions of the equation $x^n = a$ in $G$ is a multiple of $\gcd(n, |C_G(a)|)$. In particular, the number of solutions of the equation $x^n = 1$ in $G$ is a multiple of $\gcd(n, |G|)$.
**Proof of Theorem 2.1.** Choose \( a \in G \) such that \( a \) is a 2-element of maximal order in \( G \). We claim that if \( x \in G \) and \( x = x_2 x_2' \) with \( x_2 \) a conjugate of \( a \), then \( x \) does not have a square root. To prove the claim, suppose that \( a = h^2 \) for some \( h \in G \). Then by [7, Remark 2.2] we have \( |h| = 2|a| \), which contradicts the definition of \( a \). Therefore \( a \) does not have a square root and the same is true for its conjugates. Hence, \( x_2 \) does not have a square root, which in turn implies that \( x \) does not have a square root. Therefore the claim holds and we have

\[
\{ x \in G \mid x_2 \text{ is conjugate to } a \} \subseteq G \setminus G^2.
\]

Observe also that the number of \( x \in G \) for which \( x_2 \) is conjugate to \( a \) is equal to \( |G : C_G(a)| t \), where \( t \) is the number of elements of odd order of \( C_G(a) \). Therefore

\[
|G : C_G(a)| t \leq |G| - |G^2|.
\]

We now write \( |G| = 2^k m \) where \( k \geq 1 \) and \( m \) is odd. Then it is clear that \( |C_G(a)| = 2^{k'} m' \) for some positive integers \( k' \) and \( m' \) such that \( k' \leq k \) and \( m' \mid m \). On the other hand, it is easy to see that an element \( x \) in \( C_G(a) \) has odd order if and only if \( x^{m'} = 1 \). Therefore, \( t \) is equal to the number of solutions of the equation \( x^{m'} = 1 \) in \( C_G(a) \). By Remark 2.4, this is a multiple of \( \gcd(m', 2^{k'} m') = m' \). Hence, \( m' \leq t \) and thus \( |G : C_G(a)| m' \leq |G : C_G(a)| t \leq |G| - |G^2| \). By dividing both sides by \( |G| \) we obtain

\[
\frac{m'}{|C_G(a)|} \leq 1 - p(G),
\]

which in turn implies that

\[
p(G) \leq 1 - \frac{m'}{2^{k'} m'} = 1 - \frac{1}{2^{k'}} \leq 1 - \frac{1}{2^k} = 1 - \frac{1}{|P|},
\]

as required. ■

The following theorem gives another upper bound for \( p(G) \) when \( G \) has even order, depending only on the order of \( G \) and the number of 2-elements of \( G \).

**Theorem 2.5.** Let \( G \) be a finite group of even order, and denote by \( Q \) the set of 2-elements of \( G \). Then \( p(G) \leq 1 - \frac{|Q|}{2|G|} \).

**Proof.** Suppose \( a \in Q \). By Remark 2.4, the number of solutions of the equation \( x^2 = a \) in \( G \) is a multiple of \( \gcd(2, |C_G(a)|) \). Hence, this number is either 0 or \( \geq 2 \). But by [7, Remark 2.2] all solutions of this equation lie in \( Q \). Therefore, \( |G| - |G^2| \geq |Q|/2 \), or \( p(G) \leq 1 - \frac{|Q|}{2|G|} \) as required. ■

We now prove an easy but useful lemma.

**Lemma 2.6.** Let \( G \) be a finite group, and \( N \) be a normal subgroup of \( G \). Then \( p(G) \leq p(G/N) \).
Proof. Note that $gN \in G/N$ has a square root if and only if there is $xN \in G/N$ for which $gN = (xN)^2$ if and only if $x^2 \in gN$. Therefore, $gN \in G/N$ does not have a square root if and only if there is no element $x \in G$ with $x^2 \in gN$. Hence, if a coset in $G/N$ does not have a square root, then no element of this coset has a square root in $G$, and therefore $|G| - |G^2| \geq |N|(|G/N| - |(G/N)^2|)$. By dividing both sides by $|G|$ we obtain $1 - p(G) \geq 1 - p(G/N)$, or $p(G) \leq p(G/N)$ as required. 

As corollaries of Lemma 2.6, we give an upper bound for $p(G)$ when $G$ is a finite 2-group, depending only on the order of $G$, and then an upper bound for $p(G)$ when $G$ is a finite nilpotent group.

**Corollary 2.7.** Let $G$ be a finite 2-group such that $|G| \geq 4$. Then $p(G) \leq 1 - 1/\sqrt{|G|}$.

**Proof.** Suppose that $\Phi(G)$ is the Frattini subgroup of $G$. By Lemma 2.6 and Theorem 2.4(i) of [7], we have

$$p(G) \leq p\left(\frac{G}{\Phi(G)}\right) = \frac{1}{|G/\Phi(G)|} \leq \frac{1}{2}.$$ 

Since $|G| \geq 4$, we obtain $1/2 \leq 1 - 1/\sqrt{|G|}$, and so the above inequality implies that $p(G) \leq 1 - 1/\sqrt{|G|}$ as required. 

**Corollary 2.8.** Let $G$ be a finite nilpotent group of even order, and $P$ be a Sylow 2-subgroup of $G$. If $|P| = 2$, then $p(G) = 1/2$. If $|P| > 2$, then $1/|P| \leq p(G) \leq 1 - 1/\sqrt{|P|} \leq 1 - 1/\sqrt{|G|}$.

**Proof.** The first statement is Corollary 2.3. The second statement comes from Corollary 2.7 and Proposition 2.3 of [7], which states that if $G$ is nilpotent, then $p(G) = p(P)$. 

The following two propositions give upper bounds for $p(G)$, depending on the order of $G$, but only for special classes of even order groups.

**Proposition 2.9.** Let $G$ be a finite group of even order. If $G$ contains more than one Sylow 2-subgroup, then $p(G) \leq 1 - 1/\sqrt{|G|}$.

**Proof.** Let $P$ be a Sylow 2-subgroup of $G$. Since $G$ has at least two distinct Sylow 2-subgroups, $P$ is not normal in $G$. By Remark 2.4, the number of solutions of the equation $x^{[P]} = 1$ in $G$ is a multiple of $\gcd(|P|, |G|) = |P|$. Therefore, $|P|$ divides the number of solutions of $x^{[P]} = 1$ in $G$. But if we let $Q$ be the set of 2-elements of $G$, then the set of solutions of the equation $x^{[P]} = 1$ in $G$ is just $Q$, and this means $|P|$ divides $|Q|$. Hence, either $|P| = |Q|$ or $|P| \leq |Q|/2$. In the first case $P = Q$ is normal in $G$, contrary to hypothesis. Hence, $|P| \leq |Q|/2$. On the other hand, by Theorem 2.5, we have $p(G) \leq 1 - |Q|/2|G|$, and so $p(G) \leq 1 - |P|/|G|$. This inequality together
with Theorem 2.1 now implies that \((1 - p(G))^2 \geq (|P|/|G|)(1/|P|) = 1/|G|\), and so \(p(G) \leq 1 - 1/\sqrt{|G|}\) as required. ■

**Proposition 2.10.** Let \(G\) be a finite group of even order with elementary abelian Sylow 2-subgroups. Then \(p(G) \leq 1 - \lfloor \sqrt{|G|}\rfloor/|G|\).

**Proof.** Suppose \(P\) is an elementary abelian Sylow 2-subgroup of \(G\). Consider \(x \neq 1\) as an element of \(P\). If there is \(y \in G\) such that \(x = y^2\), then by [7, Remark 2.2] we have \(|y| = 4\), which is a contradiction. Therefore, \(x \in G \setminus G^2\), and so \(P \setminus \{1\} \subseteq G \setminus G^2\). Hence, \(|P| - 1 \leq |G| - |G^2|\). On the other hand, by Theorem 2.1, \(p(G) \leq 1 - 1/|P|\) and so \(|G^2| \leq |G| - |G^2|/|P|\), which implies \(|G|/|P| \leq |G| - |G^2|\). Therefore, \(|G| - |G|/|P| \leq (|G| - |G^2|)^2\), or

\[|G| \leq (|G| - |G^2|)^2 + |G|/|P| \leq (|G| - |G^2|)(|G| - |G^2| + 1) < (|G| - |G^2| + 1)^2.\]

This implies that \(\sqrt{|G|} < |G| - |G^2| + 1\), so \(\sqrt{|G|} \leq |G| - |G^2|\), and hence \(p(G) \leq 1 - \lfloor \sqrt{|G|}\rfloor/|G|\) as required. ■

The bound of Proposition 2.10 is the best possible. In fact, if \(G\) is the group described just after the statement of Theorem 2.1, then \(p(G) = 1 - \lfloor \sqrt{|G|}\rfloor/|G|\).

We can now state the following theorem which gives lower and upper bounds for \(p(G)\), depending only on the order of \(G\).

**Theorem 2.11.** Let \(G\) be a finite group of even order. Then

\[1/|G| \leq p(G) \leq 1 - \lfloor \sqrt{|G|}\rfloor/|G|.\]

**Proof.** It is clear that \(1/|G| \leq p(G)\) (see also Proposition 2.1 of [7]). Therefore we prove the second inequality. We first consider groups \(G\) with \(|G| < 26\). Among these, by Corollary 2.3, we only need to deal with groups whose order is divisible by 4. Moreover, if \(G\) is nilpotent, then by Proposition 2.3 of [7] and by Corollary 2.7, we have

\[p(G) = p(P) \leq 1 - \frac{1}{\sqrt{|P|}} \leq 1 - \frac{1}{\sqrt{|G|}} \leq 1 - \frac{\lfloor \sqrt{|G|}\rfloor}{|G|},\]

and we are done. Therefore we should prove the second inequality only for groups of order 12, 20 and 24. In these cases, if the Sylow 2-subgroup is normal, we are done, and otherwise we can use Proposition 2.9. Hence, the second inequality holds for groups \(G\) with \(|G| < 26\).

We now suppose that \(|G| \geq 26\). Let \(N \neq 1\) be a minimal normal subgroup of \(G\).

Suppose that \(G/N\) has odd order. In this case \(|N|\) is even. Since \(N\) is minimal normal, it is isomorphic to a direct product of isomorphic simple groups. There are two possibilities. If \(N \cong \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2\) is an elementary abelian 2-group, then \(N\) is the unique Sylow 2-subgroup of \(G\). Hence,
Proposition 2.10 implies that $p(G) \leq 1 - \lfloor \sqrt{|G|} \rfloor / |G|$, which gives the second inequality. If $N \cong S \times \cdots \times S$, where $S$ is a non-abelian simple group, then $G$ has at least two distinct Sylow 2-subgroups and so, by Proposition 2.9, we obtain $p(G) \leq 1 - 1/\sqrt{|G|} \leq 1 - \lfloor \sqrt{|G|} \rfloor / |G|$, which gives the second inequality.

Next we assume that $G/N$ has even order. In this case, we apply induction on $|G|$. Since $|G/N| < |G|$, the inductive hypothesis implies that

(1) $p(G/N) \leq 1 - \lfloor \sqrt{|G/N|} \rfloor / |G/N|$,

and therefore, by Lemma 2.6, we have

(2) $p(G) \leq 1 - \lfloor \sqrt{|G/N|} \rfloor / |G/N|$.

We claim that if $|N| \geq 12$, then

(3) $1 - \lfloor \sqrt{|G/N|} \rfloor / |G/N| \leq 1 - \lfloor \sqrt{|G|} \rfloor / |G|$.

To prove the claim, observe that (3) is equivalent to $\lfloor \sqrt{|G|} \rfloor \leq \lfloor \sqrt{|G/N|} \rfloor |N|$. Therefore it is enough to prove that $\sqrt{|G|} \leq (\sqrt{|G/N|} - 1)|N|$, that is, $\sqrt{|G|} \geq |N| / (\sqrt{|N|} - 1)$. Since $|G| \geq 2|N|$, it is sufficient to show that $\sqrt{2} \geq \sqrt{|N|} / (\sqrt{|N|} - 1)$, which is true for $|N| \geq 12$. Therefore the claim holds and so for $|N| \geq 12$ we get, using (2), the inequality $p(G) \leq 1 - \lfloor \sqrt{|G|} \rfloor / |G|$, which is the second inequality.

We now suppose that $|N| \leq 11$. We observe that (1) is equivalent to

$|G/N| - |(G/N)^2| \geq \lfloor \sqrt{|G/N|} \rfloor$.

Therefore there are at least $\lfloor \sqrt{|G/N|} \rfloor$ cosets $g_1N, \ldots, g_lN$ such that there is no $x \in G$ with $x^2 \in g_iN$, $i = 1, \ldots, l$. Consequently,

(4) $|G| - |G^2| \geq |N|\lfloor \sqrt{|G/N|} \rfloor$.

For any $N$ such that $1 < |N| \leq 11$, it is easy to prove that

$\frac{|N|}{\sqrt{|N|} - 1} < 5$.

Since $|G| \geq 26$, we have $\sqrt{|G|} > 5$, therefore

$\frac{|N|}{\sqrt{|N|} - 1} < 5 < \sqrt{|G|}$.

This implies that $|N| < \sqrt{|G|}(\sqrt{|N|} - 1)$, which can be rewritten as

$0 < \sqrt{|G|}\sqrt{|N|} - \sqrt{|G|} - |N|$,
or

\[0 < \sqrt{|N|}(\sqrt{|G|} - \sqrt{|N|}) - \sqrt{|G|}.\]

So we have

\[\sqrt{|G|} < |N|((\sqrt{|G/N|} - 1) < |N|\sqrt{|G/N|}.\]

Since \(\sqrt{|G|} \leq \sqrt{|G|}\), using (4) we get \(\sqrt{|G|} \leq |G| - |G^2|\), which gives \(p(G) \leq 1 - \frac{\sqrt{|G|}}{|G|}\).

The cyclic group of order 4 shows that the bound in Theorem 2.11 is the best possible. In fact,

\[p(\mathbb{Z}_4) = 1/2 = 1 - 1/\sqrt{4}.\]

A natural question arises: Does the slightly stronger bound of Proposition 2.9 hold if \(P\) is normal but \(\Phi(P) > 1\), so that only elementary abelian normal Sylow 2-subgroups are responsible for the weaker bound of Theorem 2.11?

The answer is yes, as we prove in the following theorem.

**Theorem 2.12.** Let \(G\) be a finite group of even order, and \(P\) be a Sylow 2-subgroup of \(G\). If \(p(G) > 1 - 1/\sqrt{|G|}\), then \(P\) is a proper normal elementary abelian subgroup of \(G\).

**Proof.** By Proposition 2.9, \(P\) is normal, and by Corollary 2.8, \(G\) is not nilpotent and therefore \(P \neq G\). Let \(\Phi = \Phi(P)\) be the Frattini subgroup of \(P\). We first suppose that \(\sqrt{|G|} \leq |P|/2\). Then \(1/\sqrt{|G|} \leq |P|/2|G|\), which implies, by Theorem 2.5,

\[p(G) \leq 1 - \frac{|P|}{2|G|} \leq 1 - \frac{1}{\sqrt{|G|}},\]

contrary to hypothesis.

Therefore we can suppose that \(|\Phi|^2 \leq |P|^2/4 \leq |G|\). Then, by Lemma 2.6 and Theorem 2.11, we have

\[p(G) \leq p(G/\Phi) \leq 1 - \frac{\sqrt{|G/\Phi|}}{|G/\Phi|} \leq 1 - \frac{|\Phi|/(\sqrt{|G/\Phi|} - 1)}{|G|}.\]

We want to prove that

\[
\frac{|\Phi|/(\sqrt{|G/\Phi|} - 1)}{|G|} \geq \frac{1}{\sqrt{|G|}}.
\]

This is equivalent to showing that

\[\sqrt{|G|} \geq \frac{|\Phi|}{\sqrt{|\Phi| - 1}}.\]

We first suppose that \(|\Phi| \geq 4\); then \(\sqrt{|\Phi| - 1} \geq 1\) and the inequality (5) is equivalent to \(|\Phi|^2 \leq |G|\), which we are assuming is true.
We then suppose $|\Phi| = 2$. If $P$ is cyclic, then by the remark preceding Corollary 2.3, $P$ has a normal 2-complement $Q$. Hence $G = P \times Q$ and by Corollary 2.7,

$$p(G) = p(P \times Q) = p(P)p(Q) = p(P)$$

$$\leq 1 - \frac{1}{\sqrt{|P|}} \leq 1 - \frac{1}{\sqrt{|G|}},$$

contrary to hypothesis. Thus $P$ is not cyclic, and this implies $|P| \geq 8$ and $|G| \geq 24$, so again

$$\sqrt{|G|} \geq \sqrt{24} > \frac{2}{\sqrt{2} - 1} = \frac{|\Phi|}{\sqrt{|\Phi|} - 1},$$

which is (5).

Thus (5) holds in both cases, and this implies $p(G) \leq 1 - 1/\sqrt{|G|}$, contrary to hypothesis. This last contradiction proves that $\Phi = \{1\}$.

We close this section by observing that Theorems 2.11 and 2.12 together prove the following theorem. Moreover, the group $G$ described just after the statement of Theorem 2.1 shows that the bound $p(G) \leq 1 - \lfloor \sqrt{|G|} \rfloor / |G|$ in Theorem 2.11 is the best possible and the cyclic group of order 4 shows that the better bound $p(G) \leq 1 - 1/\sqrt{|G|}$ is again the best possible.

**Theorem 2.13.** Let $G$ be a finite group of even order. If the Sylow 2-subgroup of $G$ is not a proper normal elementary abelian subgroup of $G$, then

$$p(G) \leq 1 - 1/\sqrt{|G|}.$$


Dipartimento di Matematica e Informatica
Università di Udine
Via delle Scienze 208
I-33100 Udine, Italy
E-mail: mslucido@dimi.uniud.it

Department of Mathematical Sciences
Sharif University of Technology
P.O. Box 11155-9415
Tehran, Iran

and

School of Mathematics
Institute for Studies in Theoretical Physics and Mathematics
P.O. Box 19395-5746
Tehran, Iran
E-mail: pournaki@ipm.ir

Received 22 February 2007;
revised 26 August 2007

(4876)