Elements with Square Roots in Finite Groups

M. S. Lucido, **M. R. Pournaki***

Abstract

In this paper, we study the probability that a randomly chosen element in a finite group has a square root, in particular the simple groups of Lie type of rank 1, the sporadic finite simple groups and the alternating groups.

Keywords: Simple group of Lie type of rank 1, Sporadic finite simple group, Symmetric group, Alternating group, Generating function.

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

1 Introduction

Let S_n be the symmetric group on n letters and let $\sigma \in S_n$ be a permutation of length n. We say that σ has a *square root* if there exists a permutation $\tau \in S_n$ such that $\sigma = \tau^2$. Clearly, σ may have one or more square roots, or it may have none. Let ${S_n}^2$ be the set of all permutations of length n which have at least one square root. Then the probability that a randomly chosen permutation of length n has a square root is given by

$$\mathrm{p}(S_n) = \frac{|{S_n}^2|}{n!}.$$

The properties of $\mathrm{p}(S_n)$ have been studied by some authors. Asymptotic properties of $\mathrm{p}(S_n)$ were studied in [1], [3], [7] and in [4], which is devoted to the proof of a conjecture of Wilf [12] that $\mathrm{p}(S_n)$ is monotonically non-increasing in n. Therefore, it is natural to replace S_n by an arbitrary finite group G and study

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

where G^2 denotes the set of all elements of G which have at least one square root.

In this paper, we study the basic properties of $\mathrm{p}(G)$, the probability that a randomly chosen element in a finite group G has a square root. It is always true that

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

*The research of the second author was in part supported by a grant from IPM and ICTP.

in particular we characterize the groups G which assume the minimum and the maximum values. We calculate $\mathrm{p}(G)$ in the case in which G is a simple group of Lie type of rank 1 or when G is an alternating group. A table of $\mathrm{p}(G)$ for the sporadic finite simple groups is also given. Of course, this will give us some examples of the possible values of $\mathrm{p}(G)$ and is the beginning of a possible more complete study about finite simple groups. We also prove that 0 and 1 are accumulation points for the subset $\{\mathrm{p}(G) \mid \ G \text{ is a finite group}\}$ of the interval $[0, 1]$.

2 Basic Properties

Let G be a finite group and let g be an element of 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

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

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

We observe that the identity of a group G has trivially a square root. Therefore, we have

$$\frac{1}{|G|} \leq \mathrm{p}(G) \leq 1.$$

We want to characterize the groups G for which $\mathrm{p}(G)$ assumes the minimum and the maximum values.

Proposition 2.1 *Let G be a finite group. Then we have*
(i) $\mathrm{p}(G) = 1/|G|$ *if and only if G is an elementary abelian 2-group,*
(ii) $\mathrm{p}(G) = 1$ *if and only if $|G|$ is odd.*

For the proof of the above result, we need the following remark.

Remark 2.2 Let G be a finite group and suppose $g, x \in G$ such that $g = x^2$. Then either $|x| = |g|$ is odd, or $|x| = 2|g|$.

Proof of Proposition 2.1.

(i) If $\mathrm{p}(G) = 1/|G|$, then only the identity has a square root. Since every element of odd order has a square root, G cannot have non-trivial elements of odd order.

Therefore, G is a 2-group. If $\exp(G) > 2$, then there exists an element x of order 4 and therefore $x^2 (\neq 1)$ has a square root, contradicting the hypothesis. Therefore, $\exp(G) = 2$ and so G is an elementary abelian 2-group.

Conversely, if G is an elementary abelian 2-group, then only the identity has a square root, so $\mathrm{p}(G) = 1/|G|$.

(ii) Suppose that $\mathrm{p}(G) = 1$. This means that every element in G has a square root. Suppose, by contradiction, that $|G|$ is even. If P is a Sylow 2-subgroup of G, let 2^n be the exponent of P and y an element of P of order 2^n. Let $y = x^2$ for some $x \in G$, then by Remark 2.2, we have $|x| = 2|y| = 2^{n+1}$, contradicting the fact that $\exp(P) = 2^n$. So $|G|$ is odd.

Conversely, if $|G|$ is odd, then for any $g \in G$, $|g|$ is odd and therefore there exists an element x such that $g = x^2$. So every element in G has a square root and therefore $\mathrm{p}(G) = 1$. $\square$

By Proposition 2.1, to avoid trivialities we can suppose that $|G|$ is even. In this case, we denote by P a Sylow 2-subgroup of G. The following proposition presents a better lower bound for $\mathrm{p}(G)$ when G is a solvable group.

Proposition 2.3 *Let G be a finite group of even order, and P be a Sylow 2-subgroup of G. If G is solvable, then $\mathrm{p}(G) \geq 1/|P|$. Moreover, if G is nilpotent, then $\mathrm{p}(G) = \mathrm{p}(P)$.*

Proof. Let H be a $2'$-Hall subgroup of G. Then $|H|$ is odd, $|G| = |H||P|$ and we have $H = H^2 \subseteq G^2$. Therefore,

$$\mathrm{p}(G) \;=\; \frac{|G^2|}{|G|} \;\geq\; \frac{|H|}{|G|} \;=\; \frac{|H|}{|H||P|} \;=\; \frac{1}{|P|}.$$

Moreover, if G is nilpotent, then there is a subgroup Q for which $G = P \times Q$ and $|Q|$ is odd. Therefore, $\mathrm{p}(G) = \mathrm{p}(P \times Q) = \mathrm{p}(P)\mathrm{p}(Q) = \mathrm{p}(P)$. $\square$

It is easy to calculate $\mathrm{p}(G)$ if G is abelian.

Theorem 2.4 *Let G be a finite abelian group. Then we have*
(i) $\mathrm{p}(G) = 1/\big(1 + t(G)\big)$, *where $t(G)$ is the number of involutions of G,*
(ii) $\mathrm{p}(G) \leq 1/2$ *if and only if $|G|$ is even.*

Proof. (i) Since G is an abelian group, G^2 is a subgroup of G. It is now easy to see that $f : G \to G^2$ where $f(x) = x^2$ is an epimorphism. Therefore, $G/\mathrm{Ker}(f) \cong G^2$.

Thus,

$$\mathrm{p}(G) = \frac{|G^2|}{|G|} = \frac{1}{|\mathrm{Ker}(f)|} = \frac{1}{|\{x \in G |\ x^2 = 1\}|} = \frac{1}{1 + t(G)},$$

where $t(G)$ is the number of involutions of G.

(ii) We know that $t(G) \geq 1$ if and only if $|G|$ is even. Therefore, (ii) is a consequence of (i). $\square$

Corollary 2.5 *For any $\epsilon \in \mathbb{R}$ with $\epsilon > 0$, there exists a finite (abelian) group G such that $0 < \mathrm{p}(G) < \epsilon$.*

Proof. Let n be a positive integer such that $1/2^n < \epsilon$ and consider a finite elementary abelian 2-group G of order 2^n. Then we have $\mathrm{p}(G) = 1/2^n < \epsilon$. $\square$

The general case is not so easy to deal with. We can observe that neither (i) nor (ii) of Theorem 2.4 hold in the general case, as the following examples illustrate.

Example 2.6 Let $G = D_{2n}$ be a dihedral group of order $2n$. If C is the normal cyclic subgroup of G of order n, then every element of $G \setminus C$ has order 2. Therefore, $G^2 = C^2$ and

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

On the other hand, if C is of even order, then $\mathrm{p}(C) = 1/2$; and if C is of odd order, then $\mathrm{p}(C) = 1$. Therefore,

$$\mathrm{p}(G) = \begin{cases} 1/4 & \text{if } n \text{ is even,} \\ 1/2 & \text{if } n \text{ is odd.} \end{cases}$$

This example shows that $\mathrm{p}(G)$ can have no relation at all with the number of involutions in G. In fact, if $G = D_{2^n}$, then $t(G) = 2^{n-1} + 1$, while $\mathrm{p}(G) = 1/4$.

Example 2.7 Let $G = A_4$ be the alternating group on 4 letters, then

$$\mathrm{p}(G) = \frac{3}{4} > \frac{1}{2}.$$

3 Simple Groups of Lie Type of Rank 1

In this section, we calculate $\mathrm{p}(G)$ in the case in which G is a simple group of Lie type of rank 1. This will give us some examples of the possible values of $\mathrm{p}(G)$ and is the beginning of a possible more complete study about finite simple groups. We recall that the simple groups of Lie type of rank 1 are the projective special linear groups $PSL(2,q)$ with $q \geq 4$ a prime power, the Suzuki groups $Sz(q) \cong {}^2B_2(q)$ with $q \neq 2$ an odd power of 2, the Ree groups $R(q) \cong {}^2G_2(q)$ with $q \neq 3$ an odd power of 3, and the projective unitary groups $PSU(3,q^2)$ with $q \neq 2$ a prime power.

We observe that if g is an element of odd order of a finite group G, then g has a square root. We also remark that if g has a square root, then every conjugate of g has also a square root; it is therefore enough to consider the representative of each conjugacy class. Finally, we sometimes consider the set $G \setminus G^2$ in order to obtain $\mathrm{p}(G)$ since it generally requires less calculations.

Proposition 3.1 *If $G = PSL(2,q)$ with $q \geq 4$ a prime power, then*

$$\mathrm{p}(G) = \begin{cases} 3/4 & \textit{if } q \textit{ is odd}, \\ (q-1)/q & \textit{if } q \textit{ is even}. \end{cases}$$

Proof. We recall that $|G| = q(q-1)(q+1)/d$, where $d = (2, q-1)$. Let ν be a generator of the multiplicative group of the field of q elements. Denote

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad c = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad d = \begin{pmatrix} 1 & 0 \\ \nu & 1 \end{pmatrix}, \qquad a = \begin{pmatrix} \nu & 0 \\ 0 & \nu^{-1} \end{pmatrix},$$

and b an element of order $q+1$ (Singer cycle) in $SL(2,q)$. By abuse of notation, we use the same symbols for the corresponding elements in G. From the character table of $SL(2,q)$ (see [6, Theorem 38.1] and [8]), one gets easily the character table of $PSL(2,q)$. We reproduce it below for the convenience of the reader.

We first suppose that q is odd and $q \equiv 1 \pmod 4$. Then in the above notation, the elements $1,\ c,\ d,\ a^l$ and b^m for $1 \leq l \leq (q-1)/4$ and $1 \leq m \leq (q-1)/4$ form a set of representatives for the conjugacy classes of G. The complex character table head of G is

x class representative	1	c	d	a^l	$a^{(q-1)/4}$	b^m
$\lvert C_G(x)\rvert$	$\lvert G\rvert$	p	p	$(q-1)/2$	$q-1$	$(q+1)/2$

for $1 \leq l < (q-1)/4$ and $1 \leq m \leq (q-1)/4$. We count the elements which do not have square roots.

If a is the element of order $(q-1)/2$ defined above, then the elements of even order of G are conjugate to some power of a. If we consider the subgroup $\langle a \rangle$, then the number of elements which do not have square roots in $\langle a \rangle$ is exactly $|\langle a \rangle|/2 = (q-$

1)/4 by Theorem 2.4. Since the (distinct) conjugates of $\langle a\rangle$ have trivial intersection with $\langle a\rangle$, the total number of elements of G which do not have square roots is obtained by multiplying $(q-1)/4$ by the number of conjugates of $\langle a\rangle$, which is $|G:N_G(\langle a\rangle)|$. Hence,

$$|G\setminus G^2| = \frac{|\langle a\rangle|}{2}|G:N_G(\langle a\rangle)| = \frac{q-1}{4}\frac{|G|}{q-1} = \frac{|G|}{4}.$$

We now suppose that q is odd and $q\equiv 3 \pmod 4$. Then in the above notation, the elements 1, c, d, a^l and b^m for $1\le l\le (q-3)/4$ and $1\le m\le (q+1)/4$ form a set of representatives for the conjugacy classes of G. The complex character table head of G is

x class representative	1	c	d	a^l	b^m	$b^{(q+1)/4}$
$\lvert C_G(x)\rvert$	$\lvert G\rvert$	p	p	$(q-1)/2$	$(q+1)/2$	$q+1$

for $1\le l\le (q-3)/4$ and $1\le m<(q+1)/4$. We count the elements which do not have square roots.

If b is the element of order $(q+1)/2$ defined above, then the only elements of even order of G are conjugate to some power of b. If we consider the subgroup $\langle b\rangle$, then the number of elements which do not have square roots in $\langle b\rangle$ is exactly $|\langle b\rangle|/2 = (q+1)/4$ by Theorem 2.4. Since the conjugates of $\langle b\rangle$ have trivial intersection with $\langle b\rangle$, the total number of elements of G which do not have square roots is obtained by multiplying $(q+1)/4$ by the number of conjugates of $\langle b\rangle$, which is $|G:N_G(\langle b\rangle)|$. Hence,

$$|G\setminus G^2| = \frac{|\langle b\rangle|}{2}|G:N_G(\langle b\rangle)| = \frac{q+1}{4}\frac{|G|}{q+1} = \frac{|G|}{4}.$$

We conclude $\mathrm{p}(G)=3/4$ in both cases.

If $q=2^n$, then the only elements which do not have square roots are the elements of order 2. There is only one class containing q^2-1 elements, therefore

$$\mathrm{p}(G) = 1-\frac{q^2-1}{q(q^2-1)} = 1-\frac{1}{q} = \frac{q-1}{q}. \quad \square$$

Corollary 3.2 *For any $\epsilon\in\mathbb{R}$ with $\epsilon>0$, there exists a finite (non-abelian simple) group G such that $1-\epsilon<\mathrm{p}(G)<1$.*

Proof. Let n be a positive integer such that $1/2^n<\epsilon$ and consider $G = PSL(2,q)$, where $q=2^n$. Then we have $\mathrm{p}(G)=(q-1)/q$. On the other hand,

$1 - \epsilon < (q-1)/q < 1$, therefore $1 - \epsilon < \mathrm{p}(G) < 1$. $\square$

Proposition 3.3 *If $G = Sz(q)$ with $q = 2^f$, $f \geq 3$ an odd positive integer, then $\mathrm{p}(G) = (q-1)/q$.*

Proof. We recall that the order of G is $q^2(q^2+1)(q-1)$, where $q = 2^f$, $f \geq 3$ an odd positive integer. The conjugacy classes of the Suzuki groups are well known (see, for example, [10] or [2, Theorem 5.10]). The group G only has semi-simple classes and four unipotent classes. By [2], the Sylow 2-subgroups of G have exponent 4. Therefore, the only elements which do not have square roots are the elements of order 4, which are non-real. There are two classes of elements of order 4, each class containing $(q^2+1)q(q-1)/2$ elements. We can conclude that

$$\mathrm{p}(G) = 1 - \frac{(q^2+1)q(q-1)}{q^2(q^2+1)(q-1)} = 1 - \frac{1}{q} = \frac{q-1}{q}. \quad \square$$

Proposition 3.4 *If $G = R(q)$ with $q = 3^f$, $f \geq 3$ an odd positive integer, then $\mathrm{p}(G) = 5/8$.*

Proof. We recall that the order of G is $q^3(q^3+1)(q-1)$, where $q = 3^f$, $f \geq 3$ an odd positive integer. The conjugacy classes of the Ree groups are well known (see, for example, [11]). Since all the elements of odd order have square roots, we recall here the conjugacy classes of the elements of even order of G:

x class representative	$\lvert C_G(x)\rvert$
JT	$2q$
JT^{-1}	$2q$
JR^a	$q-1$
JS^b	$q+1$
J	$q(q-1)(q+1)$

with $1 \leq a \leq (q-3)/4$ and $1 \leq b \leq (q-3)/8$. Here J is an element of order 2, whose centralizer is $\langle J \rangle \times L$ with $L \cong PSL(2,q)$ and therefore has order $q(q-1)(q+1)$. Moreover, R, S, and T are elements of L such that $|R| = (q-1)/2$ (odd), $|S| = (q+1)/4$ (odd), and $|T| = 3$.

Also, JR^a has order $2|R^a|$, and $a = 1, \ldots, (q-3)/4$. The centralizer of JR^a has order $q-1$. Moreover, $(JR^a)^2 = R^{2a}$ and therefore no element of the type JR^a has a square root in G.

Finally, JS^b has order $2|S^b|$. Here $S = S_0^2$ with S_0 an element of L of order $(q+1)/2$. Using the character table of $PSL(2,q)$ (see [6]), we easily obtain that there are $(q-3)/8$ such classes. The centralizer of JS^b has order $q+1$. Moreover, $(JS^b)^2 = S^{2b}$ and therefore no element of the type JS^b has a square root in G.

Since there is no element in G of order 4 or 12, the elements J, JT, and JT^{-1} do not have square roots. Then

$$|G \setminus G^2| = \frac{|G|}{q(q^2-1)} + \frac{|G|}{2q} + \frac{|G|}{2q} + \frac{q-3}{4}\frac{|G|}{q-1} + \frac{q-3}{8}\frac{|G|}{q+1} = \frac{3}{8}|G|.$$

Therefore, $\mathrm{p}(G) = 5/8$. $\square$

Proposition 3.5 *If $G = PSU(3,q^2)$ with q a prime power and $d = (3, q+1)$, then*

$$\mathrm{p}(G) = \begin{cases} (5q^2+3q-4)/8q(q+1) & \text{if } q \text{ is odd,} \\ (q^3-q-d)/q^2(q+1) & \text{if } q \text{ is even.} \end{cases}$$

Proof. The character table of G can be found in [9]. We reproduce the character table head below for the convenience of the reader. Let θ, σ, ρ, and ω be elements of the field $\mathbb{F}_{q^2}$ with q^2 elements such that $\theta^3 \neq 1$, $\omega^3 = 1$, $\sigma^{q-1} = \rho$, and $\rho^{q+1} = 1$. Denote

$$1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad b_l = \begin{pmatrix} 1 & 0 & 0 \\ \theta^l & 1 & 0 \\ 0 & \theta^l & 1 \end{pmatrix}, \quad c_k = \begin{pmatrix} \rho^k & 0 & 0 \\ 0 & \rho^k & 0 \\ 0 & 0 & \rho^{-2k} \end{pmatrix},$$

$$d_k = \begin{pmatrix} \rho^k & 0 & 0 \\ 1 & \rho^k & 0 \\ 0 & 0 & \rho^{-2k} \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad f_{k,l,m} = \begin{pmatrix} \rho^k & 0 & 0 \\ 0 & \rho^l & 0 \\ 0 & 0 & \rho^m \end{pmatrix},$$

$$g_k = \begin{pmatrix} \rho^k & 0 & 0 \\ 0 & \sigma^k & 0 \\ 0 & 0 & \sigma^{-qk} \end{pmatrix},$$

and τ an element of order $(q^2-q+1)/d$ in $PSU(3,q^2)$. By abuse of notation, we use the same symbols for the corresponding elements in G. The complex character table head of G is

conjugacy class	x class representative	parameters	number of classes	$\lvert C_G(x)\rvert$
$\mathcal{C}_1$	1		1	$\lvert G\rvert$
$\mathcal{C}_2$	a		1	$q^3(q+1)/d$
$\mathcal{C}_3^l$	b_l	$0 \le l \le d-1$	d	q^2
$\mathcal{C}_4^k$	c_k	$1 \le k \le \big((q+1)/d\big)-1$	$\big((q+1)/d\big)-1$	$q(q+1)^2(q-1)/d$
$\mathcal{C}_5^k$	d_k	$1 \le k \le \big((q+1)/d\big)-1$	$\big((q+1)/d\big)-1$	$q(q+1)/d$
$\mathcal{C}_6'$	e		$(d-1)/2$	$(q+1)^2$
$\mathcal{C}_6^{k,l,m}$	$f_{k,l,m}$	$1 \le k < l \le (q+1)/d$ $l < m \le q+1$ $k+l+m \equiv 0 \pmod{q+1}$	$(q^2-q+1-d)/6d$	$(q+1)^2/d$
$\mathcal{C}_7^k$	g_k	$1 \le k \le (q^2-1)/d$ $k \not\equiv 0 \pmod{q-1}$ $\mathcal{C}_7^k = \mathcal{C}_7^{-qk}$ $(\mathrm{mod}\ (q^2-1)/d)$	$(q^2-q-2)/2d$	$(q^2-1)/d$
$\mathcal{C}_8^k$	τ^k	$1 \le k \le \big((q^2-q+1)/d\big)-1$ $\mathcal{C}_8^k = \mathcal{C}_8^{-qk} = \mathcal{C}_8^{q^2k}$ $(\mathrm{mod}\ (q^2-q+1)/d)$	$(q^2-q+1-d)/3d$	$(q^2-q+1)/d$

We count the elements which do not have square roots. We first suppose that $q = 2^n$ is even, then all the semi-simple elements have square roots. Therefore, the only classes we have to consider are $\mathcal{C}_2$, $\mathcal{C}_3^l$, and $\mathcal{C}_5^k$ with l and k as described above. We observe that there is only a conjugacy class $\mathcal{C}_2$ of elements of order 2. Since $\exp_2\big(PSU(3,2^{2n})\big) = 4$, the elements of order 2 have square roots. The elements of the classes $\mathcal{C}_3^l$ have all order 4, and therefore they do not have square roots for any $0 \le l \le d-1$.

We observe that if there exists an element g such that $g^2 \in \mathcal{C}_5^k$ for some k, then also $g \in \mathcal{C}_5^i$ for some i. But if $g \in \mathcal{C}_5^i$, then $g^2 \in \mathcal{C}_4^{2i}$. Therefore, the elements of the classes $\mathcal{C}_5^k$ do not have square roots.

We therefore count them:

$$|G \setminus G^2| = \frac{|G|}{q^2}d + \frac{|G|d}{q(q+1)}\frac{q+1-d}{d} = |G|\frac{q^2+q+d}{q^2(q+1)}.$$

Hence,

$$\mathrm{p}(G) = \frac{q^3-q-d}{q^2(q+1)}.$$

We now suppose that q is odd. The elements of the classes $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3^l$, $\mathcal{C}_6'$ and $\mathcal{C}_8^k$ with l and k as described above have all odd order and therefore they have square roots.

We observe that $g_k^{(q-1)/2}$ is a square root of (a conjugate of) the element c_k. Therefore, all the elements in the classes $\mathcal{C}_4^k$ have square roots.

We observe that the conjugacy classes $\mathcal{C}_5^k$ where $1 \leq k \leq \big((q+1)/d\big) - 1$ are in one to one correspondence with the non-trivial classes of a cyclic group of order $(q+1)/d$. Moreover, we observe that if there exists an element g such that $g^2 \in \mathcal{C}_5^k$ for some k, then also $g \in \mathcal{C}_5^i$ for some i. Therefore, there are exactly $(q+1)/2d$ classes such that their representatives do not have square roots.

We consider the conjugacy classes $\mathcal{C}_7^k$ with k as described in the character table. Then g_k is a square if and only if $k \equiv 2l \pmod{(q^2-1)/d}$. Therefore, there are exactly $(q^2-1)/4d$ classes such that their representatives do not have square roots since $\mathcal{C}_7^k = \mathcal{C}_7^{-qk}$.

We consider the classes $\mathcal{C}_6^{k,l,m}$ with k, l, and m as described in the character table. We first suppose that $d = 3$. We observe that $f_{k,l,m}$ is a square if and only if $k \equiv 2i \pmod{(q+1)/d}$ and $l \equiv 2j \pmod{(q+1)/d}$. Then it is enough to count the pairs (i,j) such that $1 \leq i < j \leq (q+1)/6$. There are $(q^2-4q-5)/72$ such pairs. Since we are considering the elements which do not have square roots, there are $\big((q^2-q-2)/18\big) - \big((q^2-4q-5)/72\big) = (q+1)(q-1)/8d$ such classes.

If $d = 1$, then $f_{k,l,m}$ is a square if and only if $k \equiv 2r \pmod{q+1}$, $l \equiv 2s \pmod{q+1}$, and $m \equiv 2t \pmod{q+1}$. We count the triples (r,s,t) such that $1 \leq r < s < t \leq (q+1)/2$ and $r+s+t \equiv 0 \pmod{(q+1)/2}$. The number is $\Big(\big((q+1)/2\big)^2 - 3(q+1)/2 + 2\Big)/6 = (q^2-4q+3)/24$. Since we are considering the elements which do not have square roots, there are $\big((q^2-q)/6\big) - \big((q^2-4q+3)/24\big) = (q+1)(q-1)/8d$ such classes.

Therefore, in both cases, we have $(q^2-1)/8d$ classes of the type $\mathcal{C}_6^{k,l,m}$.

We can now count the total number of elements which are not square roots:

$$|G \setminus G^2| = \frac{|G|d}{q(q+1)}\frac{q+1}{2d} + \frac{|G|d}{q^2-1}\frac{q^2-1}{4d} + \frac{|G|d}{(q+1)^2}\frac{q^2-1}{8d} = |G|\frac{3q^2+5q+4}{8q(q+1)}.$$

Therefore,

$$\mathrm{p}(G) = 1 - \frac{3q^2+5q+4}{8q(q+1)} = \frac{5q^2+3q-4}{8q(q+1)}. \quad \square$$

We observe that if G is a simple group of Lie type of rank 1, then $\mathrm{p}(G) > 1/2$.

Therefore, one may ask: *For which finite simple groups G, is* $\mathrm{p}(G) > 1/2$?

In Theorem 4.4 of the next section, we shall see that for almost all alternating groups G, $\mathrm{p}(G) < 1/2$. Moreover, if G is one of the sporadic groups M_{12}, J_2, Ru, Co_3, Co_2, Fi_{22}, HN, Fi_{23}, Co_1, B, and M, then $\mathrm{p}(G) < 1/2$.

Using the character tables in [5], it is easy to calculate $\mathrm{p}(G)$ for the sporadic finite simple groups. If G is a sporadic finite simple group, then the values of $\mathrm{p}(G)$ range from $\mathrm{p}(Ru) = 193/640$ to $\mathrm{p}(M_{22}) = 35/48$:

G	p(G)
M_{11}	7/12
M_{12}	19/48
J_1	5/8
M_{22}	35/48
J_2	97/240
M_{23}	109/168
HS	641/1280
J_3	71/120
M_{24}	2531/4480
McL	1313/2520
He	2251/4480
Ru	193/640
Suz	24959/45360
$O'N$	141/256
Co_3	602501/1451520
Co_2	215003/516096
Fi_{22}	777325/1769472
HN	42553/88000
Ly	191527/356400
Th	62873/120960
Fi_{23}	1410125881/3503554560
Co_1	2475448999/6227020800
J_4	11959273/21288960
Fi'_{24}	3975787073/7472424960
B	0,409880211038948
M	0,442588701109859

4 Symmetric and Alternating Groups

Let S_n be the symmetric group on n letters. As already mentioned, some properties of $\mathrm{p}(S_n)$ were studied by several authors:

Theorem 4.1 ([12]) *The probability that a randomly chosen permutation of S_n ($n \geq 1$) has a square root is given by*

$$\begin{aligned} 1+\sum_{n=1}^{\infty}\mathrm{p}(S_n)t^n &= \left(\frac{1+t}{1-t}\right)^{1/2}\prod_{m=1}^{\infty}\cosh\left(\frac{t^{2m}}{2m}\right) \\ &= 1+t+\frac{1}{2}t^2+\frac{1}{2}t^3+\frac{1}{2}t^4+\frac{1}{2}t^5+\frac{3}{8}t^6+\frac{3}{8}t^7+\frac{7}{20}t^8+\frac{7}{20}t^9+\dots\ . \end{aligned}$$

By the above theorem, the first terms of the sequence $\{\mathrm{p}(S_n)\}_{n\geq 1}$ are

$$1,\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{3}{8},\ \frac{3}{8},\ \frac{7}{20},\ \frac{7}{20},\ \dots\ .$$

We now consider the alternating group A_n ($n \geq 2$), and give the analogue of the above theorem.

Theorem 4.2 *The probability that a randomly chosen permutation of A_n ($n \geq 2$) has a square root is given by*

$$\begin{aligned} 2+2t+\sum_{n=2}^{\infty}\mathrm{p}(A_n)t^n &= 2\left(\frac{1+t}{1-t}\right)^{1/2}\prod_{m=1}^{\infty}\cosh\left(\frac{t^{2m}}{2m}\right) \\ &- \left(\prod_{m=1}^{\infty}\left(1+\frac{t^{2m-1}}{2m-1}\right)\right)\left(\prod_{m=1}^{\infty}\cosh\left(\frac{t^{2m}}{2m}\right)-\prod_{m=1}^{\infty}\cos\left(\frac{t^{2m}}{2m}\right)\right) \\ &= 2+2t+t^2+t^3+\frac{3}{4}t^4+\frac{3}{4}t^5+\frac{3}{4}t^6+\frac{2}{3}t^7+\frac{9}{16}t^8+\frac{143}{240}t^9+\dots\ . \end{aligned}$$

For the proof of the above result, we need the following lemma.

Lemma 4.3 *Let σ be a permutation on n letters. Let c_i denote the number of cycles of length i in the disjoint cycle decomposition of σ. Then $\sigma \in {A_n}^2$ if and only if the following two conditions are satisfied:*
(i) *c_{2k} is even for all k,*
(ii) *$l = \sum_k c_{2k}$ is a multiple of 4 or $c_{2j-1} > 1$ for some j.*

Proof. First suppose $\sigma \in {A_n}^2$ so that there exists $\tau \in A_n$ with $\sigma = \tau^2$. Clearly, the square of a cycle of length k is a cycle of length k if k is odd, and is the product of two cycles of length $k/2$ if k is even. Therefore, a cycle of length $2k$ in σ can only be obtained by squaring a cycle of length $4k$ of τ. This gives the product of two cycles of length $2k$ in σ. Therefore, c_{2k} is even. To prove (ii), suppose for each j, we have $c_{2j-1} \leq 1$. Therefore, the disjoint cycle decomposition of σ consists of $l = \sum_k c_{2k}$ cycles of even order of lengths $2k_1, \ \ldots, \ 2k_l$ and possibly some cycles of odd length, each length $2j-1$ appearing only once. Therefore, τ consists of $l/2$ cycles of lengths $4k_1, \ \ldots, \ 4k_{l/2}$ and maybe some cycles of odd length. Since $\tau \in A_n$, $l/2$ is even, and therefore $l = \sum_k c_{2k}$ is a multiple of 4.

To prove the converse, first note the following two constructions. If a cycle $(a_1 \ a_2 \ a_3 \ \ldots \ a_k)$ has odd length, then it is the square of the cycle $(b_1 \ b_2 \ b_3 \ \ldots \ b_k)$, where $b_1 = a_1, \ b_3 = a_2, \ b_5 = a_3, \ \ldots,$ and the subscripts are taken modulo k. Thus, any cycle of odd length is the square of a cycle of the same length. Moreover, for any two cycles of the same arbitrary length, such as $(a_1 \ a_2 \ \ldots \ a_k)$ and $(b_1 \ b_2 \ \ldots \ b_k)$, consider $(a_1 \ b_1 \ a_2 \ b_2 \ \ldots \ a_k \ b_k)$. Then $(a_1 \ b_1 \ a_2 \ b_2 \ \ldots \ a_k \ b_k)^2 = (a_1 \ a_2 \ \ldots \ a_k)(b_1 \ b_2 \ \ldots \ b_k)$. Therefore, the product of two cycles of the same length is the square of a single cycle of doubled length. Now suppose σ has properties (i) and (ii) as in the assertion. We shall construct $\tau \in A_n$ such that $\sigma = \tau^2$. According to (i), we can write σ as the product of an even number of cycles of even length and some number of cycles of odd length. Divide these cycles of even length into groups of two cycles of equal length, using the scheme explained above. Now if $l = \sum_k c_{2k} = 4s$ for some s, this product of cycles can be represented as the square of $l/2$ cycles of even length. Similarly, each of the cycles of odd length is the square of a cycle of the same length. Therefore, we obtain a permutation τ such that $\sigma = \tau^2$ and τ has $l/2$ cycles of even length and some cycles of odd length, so $\tau \in A_n$. Otherwise, if $l = \sum_k c_{2k} = 4s + 2$ for some s, then by (ii), there are at least two cycles of the same odd length, say of length $2j-1$. Now divide the cycle decomposition of σ into the following groups: groups of two cycles of equal even lengths (there are $l/2$ such groups), a group of two cycles of length $2j-1$, and the rest, which are some cycles of odd length. Each of these groups is a square of a cycle, but note in particular that we write the two cycles of length $2j-1$ as the square of a single cycle of length $4j-2$, while we write the other cycles of odd length as the square of a cycle of the same length. Thus, we obtain τ such that $\sigma = \tau^2$ and τ consists of $l/2$ cycles of even length, another cycle of length $4j-2$ (even), and some cycles of odd length, so $\tau \in A_n$. $\square$

Proof of Theorem 4.2.

We are looking for the generating function of the sequence $\{\mathrm{p}(A_n)\}_{n\geq 2}$. Consider the cycle type vector $(c_1,\ c_2,\ \ldots)$ of a permutation of n letters. By Theorem 4.7.2 of [12], the coefficient of $(\prod_{m=1}^{n} {x_m}^{c_m})t^n/n!$ in the product $\prod_{m=1}^{\infty}\exp(x_m t^m/m)$ is the number of permutations of n letters whose cycle type is $(c_1,\ c_2,\ \ldots)$. The infinite products and infinite sums occurring in the assertion and in the following proof are considered as elements of the ring $\mathbb{C}[x_1, x_2, \ldots][[t]]$ of formal power series in the variable t over the polynomial ring $\mathbb{C}[x_1, x_2, \ldots]$ in the infinitely many variables $x_1, x_2, \ldots$. The elements exp, cosh, and cos are certain formal power series, which coincide with those derived by the Taylor expansion of corresponding analytical functions. Using this, it is easily checked that all products and sums occurring indeed are well defined.

Firstly, we calculate $|{S_n}^2 \setminus {A_n}^2|$. By Lemma 4.3, $\sigma \in {S_n}^2 \setminus {A_n}^2$ if and only if c_{2k} is even for all k, c_{2j-1} is 0 or 1 for all j, and the number of cycles of even length is 2 (mod 4). Therefore, with an argument similar to that used in [12, p. 147], one can obtain the generating function of the sequence $\{{S_n}^2 \setminus {A_n}^2\}_{n\geq 2}$. As c_{2k} should be even for all k and $c_{2j-1} \leq 1$ for all j, the terms $\exp\big(x_m t^m/m\big)$ in the product $\prod_{m=1}^{\infty}\exp\big(x_m t^m/m\big)$ should be replaced by $1 + x_m t^m/m$ and $\cosh\big(x_m t^m/m\big)$ for odd and even m's, respectively. The obtained expression is of the form

$$\Big(\prod_{m=1}^{\infty}\big(1 + x_{2m-1}\frac{t^{2m-1}}{2m-1}\big)\Big)\Big(\prod_{m=1}^{\infty}\cosh\big(x_{2m}\frac{t^{2m}}{2m}\big)\Big).$$

To impose condition $\sum_m c_{2m} \equiv 2 \pmod 4$, we need some more tricks. Replacing each x_{2m} in $\prod_{m=1}^{\infty}\cosh\big(x_{2m}t^{2m}/2m\big)$ by sx_{2m}, it is trivial that we only need to compute powers of s of the form s^{4l-2} in

$$F(t,s) = \prod_{m=1}^{\infty}\cosh\big(x_{2m}\frac{st^{2m}}{2m}\big).$$

But since F contains only even powers of s, it is enough to compute powers of s in

$$\frac{1}{2}\big(F(t,s) - F(t,is)\big) = \frac{1}{2}\Big(\prod_{m=1}^{\infty}\cosh\big(x_{2m}\frac{st^{2m}}{2m}\big) - \prod_{m=1}^{\infty}\cos\big(x_{2m}\frac{st^{2m}}{2m}\big)\Big).$$

Finally, if we replace s by 1, we obtain the generating function of the sequence $\{{S_n}^2 \setminus {A_n}^2\}_{n\geq 2}$:

$$\Big(\prod_{m=1}^{\infty}\big(1 + x_{2m-1}\frac{t^{2m-1}}{2m-1}\big)\Big)\Big(\frac{1}{2}\big(F(t,1) - F(t,i)\big)\Big) =$$

$$\frac{1}{2}\Big(\prod_{m=1}^{\infty}(1+x_{2m-1}\frac{t^{2m-1}}{2m-1})\Big)\Big(\prod_{m=1}^{\infty}\cosh(x_{2m}\frac{t^{2m}}{2m})-\prod_{m=1}^{\infty}\cos(x_{2m}\frac{t^{2m}}{2m})\Big).$$

Therefore, $|{S_n}^2 \setminus {A_n}^2|$ for $n \geq 2$ is equal to the coefficient of $t^n/n!$ in

$$\frac{1}{2}\Big(\prod_{m=1}^{\infty}(1+\frac{t^{2m-1}}{2m-1})\Big)\Big(\prod_{m=1}^{\infty}\cosh(\frac{t^{2m}}{2m})-\prod_{m=1}^{\infty}\cos(\frac{t^{2m}}{2m})\Big).$$

On the other hand, by [12, p. 148], $|{S_n}^2|$ for $n \geq 2$ is equal to the coefficient of $t^n/n!$ in

$$\Big(\frac{1+t}{1-t}\Big)^{1/2}\prod_{m=1}^{\infty}\cosh(\frac{t^{2m}}{2m}).$$

Hence, $|{A_n}^2|$ for $n \geq 2$ is equal to the coefficient of $t^n/n!$ in

$$\Big(\frac{1+t}{1-t}\Big)^{1/2}\prod_{m=1}^{\infty}\cosh(\frac{t^{2m}}{2m})-\frac{1}{2}\Big(\prod_{m=1}^{\infty}(1+\frac{t^{2m-1}}{2m-1})\Big)\Big(\prod_{m=1}^{\infty}\cosh(\frac{t^{2m}}{2m})-\prod_{m=1}^{\infty}\cos(\frac{t^{2m}}{2m})\Big).$$

Therefore, $\mathrm{p}(A_n)$ for $n \geq 2$ is equal to the coefficient of t^n in

$$2\Big(\frac{1+t}{1-t}\Big)^{1/2}\prod_{m=1}^{\infty}\cosh(\frac{t^{2m}}{2m})-\Big(\prod_{m=1}^{\infty}(1+\frac{t^{2m-1}}{2m-1})\Big)\Big(\prod_{m=1}^{\infty}\cosh(\frac{t^{2m}}{2m})-\prod_{m=1}^{\infty}\cos(\frac{t^{2m}}{2m})\Big),$$

i.e.,

$$2+2t+t^2+t^3+\frac{3}{4}t^4+\frac{3}{4}t^5+\frac{3}{4}t^6+\frac{2}{3}t^7+\frac{9}{16}t^8+\frac{143}{240}t^9+\dots,$$

as required. $\square$

By the above theorem, the first terms of the sequence $\{\mathrm{p}(A_n)\}_{n\geq 2}$ are

$$1,\ 1,\ \frac{3}{4},\ \frac{3}{4},\ \frac{3}{4},\ \frac{2}{3},\ \frac{9}{16},\ \frac{143}{240},\ \dots .$$

We now come back to the alternating group to consider the asymptotics of $\mathrm{p}(A_n)$, as it is done for the symmetric groups in [3]: $\lim_{n\to+\infty}\mathrm{p}(S_n)=0$.

Theorem 4.4 $\lim_{n\to+\infty}\mathrm{p}(A_n)=0$.

Proof. Clearly, ${A_n}^2$ is a subset of ${S_n}^2$, so $|{A_n}^2| \leq |{S_n}^2|$ and hence $\mathrm{p}(A_n) \leq 2\mathrm{p}(S_n)$. Now $\lim_{n\to+\infty}\mathrm{p}(S_n)=0$ implies that $\lim_{n\to+\infty}\mathrm{p}(A_n)=0$. $\square$

We can then reformulate Corollary 2.5.

Corollary 4.5 *For any $\epsilon \in \mathbb{R}$ with $\epsilon > 0$, there exists a finite (non-abelian simple)* *group G such that* $0 < \mathrm{p}(G) < \epsilon$.

Finally, we recall another theorem which holds for the group S_n but has no analogue for the group A_n.

Theorem 4.6 ([12]) *For each $n \in \mathbb{N}$, we have* $\mathrm{p}(S_{2n}) = \mathrm{p}(S_{2n+1})$.

From the first terms of the sequence $\{\mathrm{p}(A_n)\}_{n\geq 2}$, we can observe that in this case, there is no analogue to Theorem 4.6. In fact, for example, $\mathrm{p}(A_6) \neq \mathrm{p}(A_7)$.

Acknowledgment: This work was done while the second author was a Postdoctoral Research Associate at the School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran, and a visiting scholar (Mathematics Research Fellowships 2002) at the Abdus Salam International Center for Theoretical Physics (ICTP), Trieste, Italy. He would like to express his thanks to both IPM and ICTP for the financial support. He also thanks C. Bessenrodt and M. Mohammad-Noori for useful comments which led to the improvement of the first draft, and A. Katanforoush for computing the Taylor expansions. Finally, the authors would like to thank the referee for his/her interest in the subject and making useful suggestions and comments which led to improvement and simplification of the first draft.

References

[1] E. A. Bender, *Asymptotic Methods in Enumeration*, SIAM Rev. **16** (1974), 485-515.

[2] N. Blackburn, B. Huppert, "*Finite Groups III*", Springer-Verlag, Berlin, Heidelberg, New York, 1982.

[3] J. Blum, *Enumeration of the Square Permutations in S_n*, J. Combinatorial Theory Ser. A **17** (1974), 156-161.

[4] M. Bona, A. McLennan, D. White, *Permutations with Roots*, Random Structures Algorithms **17** (2000), no. 2, 157–167.

[5] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson, "*Atlas of Finite Groups*", Clarendon Press, Oxford, 1985.

[6] L. Dornhoff, "*Group Representation Theory*", Part A, Marcel Dekker, New York,

1971.

[7] N. Pouyanne, *On the Number of Permutations Admitting an mth Root*, Electron. J. Combin. **9** (2002), no. 1, Research Paper 3, 12 pp. (electronic).

[8] I. Schur, *Untersuchung Uber Die Darstellung Der Endlichen Gruppen Durch Gebrochene Lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85-137.

[9] W. A. Simpson, J. S. Frame, *The Character Tables for $SL(3,q)$, $SU(3,q^2)$, $PSL(3,q)$, $PSU(3,q^2)$*, Canad. J. Math. **25** (1973), no. 3, 486-494.

[10] M. Suzuki, *On a Class of Doubly Transitive Groups*, Ann. of Math. (2) **75** (1962), 105-145.

[11] H. N. Ward, *On Ree's Series of Simple Groups*, Trans. Amer. Math. Soc. **121** (1966), 62-89.

[12] H. S. Wilf, "*Generatingfunctionology*", Second edition, Academic Press, Boston, MA, 1994.

The Authors' Addresses

M. S. Lucido, Dipartimento di Matematica e Informatica, Università di Udine, Via delle Scienze 208, I-33100 Udine, Italy.

E-mail address: mslucido@dimi.uniud.it

M. R. Pournaki, School of Mathematics, Institute for Studies in Theoretical Physics and Mathematics, P.O. Box 19395-5746, Tehran, Iran.

E-mail address: pournaki@ipm.ir