An infinitude of counterexamples to Herzog’s conjecture on involutions in simple groups

Chimere Stanley Anabantia, Stefan Hammera, and Nneka Chigozie Okolib

Technische Universität Graz (TU Graz), Graz, Austria; Federal College of Education (Technical) Umunze, Anambra, Nigeria

ABSTRACT
In 1979, Herzog conjectured that two finite simple groups containing the same number of involutions have the same order. Zarrin, in a 2018 published paper, disproved Herzog’s conjecture with a counterexample. The goal of this article is to prove that there are infinitely many counterexamples to Herzog’s conjecture. In doing so, we obtain an explicit formula for the number of involutions in the groups involved.

ARTICLE HISTORY
Received 26 June 2020
Revised 26 September 2020
Communicated by Sarah Witherspoon

KEYWORDS
Elements of odd prime order; finite simple groups; involutions

MATHEMATICS SUBJECT CLASSIFICATION (2010)
Primary 20D60; Secondary 20D06; 05E15; 20H30

1. Introduction
We write \(I_n(G)\) for the number of elements of order \(n\) in a finite group \(G\). Herzog [4] conjectured that two finite simple groups containing the same number of involutions have the same order. Zarrin [6] disproved Herzog’s conjecture with the following counterexample:

\[I_2(PSp(4, 3)) = 315 = I_2(PSL(3, 4)), \text{ but } |PSp(4, 3)| = 25920 > 20160 = |PSL(3, 4)|.\]

Then, in view of Herzog’s conjecture and Conjecture 2.10 of [5], he conjectured that “if \(S\) is a non-abelian simple group and \(G\) a group such that \(I_2(G) = I_2(S)\) and \(I_p(G) = I_p(S)\) for some odd prime divisor \(p\), then \(|G| = |S|\)” Zarrin’s conjecture was disproved by the first author in [1], with the following counterexample:

\[I_2(PSL(4, 3)) = 7371 = I_2(PSL(3, 9))\]

and

\[I_{13}(PSL(4, 3)) = 1866240 = I_{13}(PSL(3, 9));\]

but

\[|PSL(4, 3)| = 6065280 < 42456960 = |PSL(3, 9)|.\]

The goal of this short note is to show that there are infinitely many counterexamples to Herzog’s conjecture. Moreover, we give fourteen (14) new counterexamples to Zarrin’s conjecture, and conclude with a conjecture that there are infinitely many counterexamples to Zarrin’s conjecture.
2. Main results

We begin by outlining the main results of this study. Theorem 2.1 is that there are infinitely many counterexamples to Herzog’s conjecture. In proving the result, we obtain explicit formulae (see Equations 18 and 19) for the number of involutions in the groups involved. We give fourteen new counterexamples to Zarrin’s conjecture in Table 1, and conclude with a conjecture (see Conjecture 2.5) on the infinitude of counterexamples to Zarrin’s conjecture.

**Theorem 2.1.** There are infinitely many counterexamples to Herzog’s conjecture.

**Proof.** Our goal is to show that given a natural number \(m \geq 3\),

\[ I_2(\Omega(+1, 2m, 2)) = I_2(\Omega(-1, 2m, 2)) \quad \text{and} \quad |\Omega(-1, 2m, 2)| \neq |\Omega(+1, 2m, 2)|. \]

Recall, from [2, p.6], that for \(m \in \mathbb{N}\), with \(m \geq 3\), and \(q\) a power of a prime,

\[ |\Omega(\pm 1, 2m, q)| = \frac{q^{m^2-m}(q^{m+1}+1)}{\gcd(4, q^{m+1})} \prod_{i=1}^{m-1} (q^{2^i} - 1). \]  

(1)

Therefore

\[ |\Omega(\pm 1, 2m, 2)| = \frac{2^{m^2-m}}{2m+1} \prod_{i=1}^{m} (2^{2^i} - 1). \]  

(2)

It is already clear, from Equation (2), that \( |\Omega(-1, 2m, 2)| > |\Omega(+1, 2m, 2)| \). For the equality on the number of involutions, we first make use of [3, Theorem 5.6] which gives a formula for the number of involutions in \(O(\pm 1, 2m, 2)\) as follows:

| Nr. | Groups G | |\( |G| \) | \(I_2(G)\) | \(p\) | \(I_p(G)\) |
|-----|----------|---|------|--------|-----|----------|
| 1   | PSL(4, 4) | 987,033,600 | 69,615 | 7     | 31,334,400 |
|     | PSL(3, 16)| 1,425,715,200 |
| 2   | PSU(4, 4) | 1,018,368,000 | 69,615 | 13    | 62,668,800 |
|     | PSL(3, 16)| 1,425,715,200 |
| 3   | PSU(4, 5) | 14,742,000,000 | 406,875 | 5     | 244,140,624 |
|     | PSL(3, 25)| 50,778,000,000 |
| 4   | PSL(4, 7) | 2,317,591,180,800 | 5,884,851 | 7     | 13,841,287,200 |
|     | PSL(3, 49)| 11,072,935,641,600 |
| 5   | PSL(4, 8) | 34,558,531,338,240 | 17,039,295 | 73    | 1,623,710,176,160 |
|     | PSL(3, 64)| 93,801,727,918,080 |
| 6   | PSU(4, 8) | 34,693,789,777,920 | 17,039,295 | 19    | 405,775,319,040 |
|     | PSL(3, 64)| 93,801,727,918,080 |
| 7   | PSU(4, 9) | 101,798,586,432,000 | 43,584,723 | 73    | 6,693,605,683,200 |
|     | PSL(3, 81)| 1,852,734,273,062,400 |
| 8   | PSL(4, 11) | 2,069,665,112,592,000 | 216,145,083 | 7     | 6,224,555,729,600 |
|     | PSL(3, 121)| 15,315,521,833,180,800 |
| 9   | PSL(5, 4) | 258,492,255,436,800 | 21,999,615 | 31    | 4,548,250,828,800 |
|     | PSL(3, 16)| 23,499,295,948,800 |
| 10  | PSL(7, 4) | 72,736,898,347,485,916,060,188,672,000 | 374,910,580,965,375 | 127   | 239,748,062,672,541,016,129,536,000 |
|     | \(\Omega(+1, 14, 2)\) | 1,691,555,775,522,928,280,469,504,004 |
| 11  | PSL(4, 10) | 987,033,600 | 69,615 | 17    | 46,448,640 |
|     | \(\Omega(-1, 8, 2)\) | 197,406,720 |
| 12  | PSL(5, 4) | 258,492,255,436,800 | 21,999,615 | 11    | 1,516,083,609,600 |
|     | \(\Omega(-1, 10, 2)\) | 25,015,379,558,400 |
| 13  | PSL(6, 4) | 361,310,134,959,341,568,000 | 74,351,051,775 | 13    | 1,588,176,417,403,699,200 |
|     | \(\Omega(-1, 12, 2)\) | 51,615,733,565,620,224,000 |
| 14  | PSL(7, 4) | 72,736,898,347,485,916,060,188,672,000 | 374,910,580,965,375 | 43    | 79,916,020,890,847,005,376,512,000 |
|     | \(\Omega(-1, 14, 2)\) | 1,718,194,449,153,210,615,595,008,000 |
\[ I_2(O(-1,2m,2)) = \sum_{r \text{ even}}^{m-1} \frac{|O(-1,2m,2)|}{A_r} + \sum_{r \text{ even}}^{m} \frac{|O(-1,2m,2)|}{B_r} + \sum_{r \text{ odd}}^{m} \frac{|O(-1,2m,2)|}{C_r}, \]  

(3)

where

\[ A_r = 2^{\left(\frac{r(r-1)}{2} + r(2m-2r)\right)} |Sp(r,2)||O(-1,2m-2r,2)|, \]

\[ B_r = 2^{1 + \left(\frac{r(r-1)}{2} + (r-1)(2m-2r)\right) - 1} |Sp(r-2,2)||Sp(2m-2r,2)| \]

and

\[ C_r = 2^{1 + \left(\frac{r(r-1)}{2} + (r-1)(2m-2r)\right) - 1} |Sp(r-1,2)||Sp(2m-2r,2)|. \]

On the other hand,

\[ I_2(O(+1,2m,2)) = \sum_{r \text{ even}}^{m} \frac{|O(+1,2m,2)|}{A_r} + \sum_{r \text{ even}}^{m} \frac{|O(+1,2m,2)|}{B_r} + \sum_{r \text{ odd}}^{m} \frac{|O(+1,2m,2)|}{C_r}, \]  

(4)

where

\[ A_r = 2^{\left(\frac{r(r-1)}{2} + r(2m-2r)\right)} |Sp(r,2)||O(+1,2m-2r,2)|, \]

\[ B_r \] and \( C_r \) are as given above. We note here that

\[ |O(\pm 1,2m,2)| = 2|\Omega(\pm 1,2m,2)| = \frac{2m^2 - m + 1}{2^{m+1}} \prod_{i=1}^{m} (2^{2i} - 1) \]  

(5)

and from [2, p. 4], one sees immediately that

\[ |Sp(2m,2)| = 2m^{2m} \prod_{i=1}^{m} (2^{2i} - 1). \]  

(6)

Involutions in \( \Omega(\pm 1,2m,2) \) are characterized by fixed spaces of even dimensions. Whence

\[ I_2(\Omega(-1,2m,2)) = \sum_{r \text{ even}}^{m-1} \frac{|O(-1,2m,2)|}{A_r} + \sum_{r \text{ even}}^{m} \frac{|O(-1,2m,2)|}{B_r}, \]  

(7)

where

\[ A_r = 2^{\left(\frac{r(r-1)}{2} + r(2m-2r)\right)} |Sp(r,2)||O(-1,2m-2r,2)| \]  

(8)

and

\[ B_r = 2^{1 + \left(\frac{r(r-1)}{2} + (r-1)(2m-2r)\right) - 1} |Sp(r-2,2)||Sp(2m-2r,2)|. \]  

(9)

Similarly,

\[ I_2(\Omega(+1,2m,2)) = \sum_{r \text{ even}}^{m} \left[ \frac{|O(+1,2m,2)|}{A_r} + \frac{|O(+1,2m,2)|}{B_r} \right], \]  

(10)

where

\[ A_r = 2^{\left(\frac{r(r-1)}{2} + r(2m-2r)\right)} |Sp(r,2)||O(+1,2m-2r,2)| \]  

(11)

and \( B_r \) is as given in Equation (9). For the remainder of the proof, we show that Equations (7) and (10) are equal.
Using Equations (5), (6), (8), (9) and (11), we obtain

\[
A_r = \frac{2^{m^2-m+1-\frac{r^2}{2}} \prod_{i=1}^{r/2} (2^i - 1) \prod_{i=1}^{m-r+1} (2^i - 1)}{(2^{m-r+1}) \prod_{i=m-r+1}^{m} (2^i - 1)},
\]

(12)

\[
B_r = \frac{2^{m^2-2m+1-\frac{r^2}{2}} \prod_{i=1}^{r/2} (2^i - 1) \prod_{i=1}^{m-r+1} (2^i - 1)}{(2^r - 1) \prod_{i=m-r+1}^{m} (2^i - 1)},
\]

(13)

\[
\frac{|O(\pm 1, 2m, 2)|}{A_r} = \frac{2^{m-r+1} \times 2^{\frac{r^2}{2}-\frac{r}{2}} \times \prod_{i=m-r+1}^{m} (2^i - 1)}{\prod_{i=1}^{r/2} (2^i - 1)}
\]

(14)

and

\[
\frac{|O(\pm 1, 2m, 2)|}{B_r} = \frac{2^r - 1 \times 2^{\frac{r^2}{2}-\frac{r}{2}} \times \prod_{i=m-r+1}^{m} (2^i - 1)}{\prod_{i=1}^{r/2} (2^i - 1)}.
\]

(15)

Substituting Equations (14) and (15) in each of Equations (10) and (7), and simplifying the result, we obtain; respectively,

\[
I_2(\Omega(+1, 2m, 2)) = \sum_{r=2 \ (r \ even)}^{m} \frac{2^{(r/2)^2-r/2} \prod_{i=m-r+1}^{m} (2^i - 1)}{\prod_{i=1}^{r/2} (2^i - 1)}
\]

(16)

and

\[
I_2(\Omega(-1, 2m, 2)) = \sum_{r=2 \ (r \ even)}^{m-1} \frac{2^{(r/2)^2-r/2} \prod_{i=m-r+1}^{m} (2^i - 1)}{\prod_{i=1}^{r/2} (2^i - 1)} + M,
\]

(17)

where

\[
M = \begin{cases} 
0, & \text{if } m \text{ is odd} \\
2^{\frac{m^2}{2}-\frac{m}{2}} \times \prod_{i=m\over 2+1}^{m} (2^i - 1), & \text{if } m \text{ is even.}
\end{cases}
\]

Suppose \( m \) is odd. Then Equations (17) and (16) coincide; in particular,

\[
I_2(\Omega(-1, 2m, 2)) = \sum_{r=2 \ (r \ even)}^{m-1} \frac{2^{(r/2)^2-r/2} \prod_{i=m-r+1}^{m} (2^i - 1)}{\prod_{i=1}^{r/2} (2^i - 1)} = I_2(\Omega(+1, 2m, 2)).
\]

(18)

Suppose \( m \) is even. Then using Equation (17), we obtain

\[
I_2(\Omega(-1, 2m, 2)) = \sum_{r=2 \ (r \ even)}^{m-1} \frac{2^{(r/2)^2-r/2} \prod_{i=m-r+1}^{m} (2^i - 1)}{\prod_{i=1}^{r/2} (2^i - 1)} + \left[2^{\frac{m^2}{2}-\frac{m}{2}} \times \prod_{i=m\over 2+1}^{m} (2^i - 1)\right]
\]

(19)

In both cases, \( I_2(\Omega(+1, 2m, 2)) = I_2(\Omega(-1, 2m, 2)) \). This completes the proof. □

Remark 2.2. Other than the infinitude of counterexamples to Herzog’s conjecture shown in the proof of Theorem 2.1, there are also infinitely many other counterexamples to the same conjecture. For instance, it can be shown, in a similar way as in the proof of Theorem 2.1, that:
i. given a natural number $m \geq 3$,
\begin{equation}
I_2(\Omega(-1, 2m, 2)) = I_2(\text{PSL}(m, 4)) \text{ and } |\Omega(-1, 2m, 2)| \neq |\text{PSL}(m, 4)|; 
\end{equation}

ii. given a natural number $m \geq 4$,
\begin{equation}
I_2(\Omega(+1, 2m, 2)) = I_2(\text{PSL}(m, 4)) \text{ and } |\Omega(+1, 2m, 2)| \neq |\text{PSL}(m, 4)|; 
\end{equation}

iii. for an odd prime power $q \geq 3$,
\begin{equation}
I_2(G(2, q)) = I_2(\text{PSL}(3, q^2)) \text{ and } |G(2, q)| \neq |\text{PSL}(3, q^2)|. 
\end{equation}

We note that
\begin{align*}
\Omega(+1, 6, 2) &\cong A_8 \cong \text{PSL}(4, 2), \\
\Omega(-1, 6, 2) &\cong \text{PSp}(4, 3)
\end{align*}

and
\[|\Omega(-1, 6, 2)| = 25920 > 20160 = |\Omega(+1, 6, 2)|.\]

Moreover, up to isomorphism, there is only one simple group of order 25920 and only two simple groups of order 20160; in the latter case, the two non-isomorphic simple groups are $\Omega(+1, 6, 2)$ and $\text{PSL}(3, 4)$. The base case (where $m = 3$) of the groups used as counterexample in the proof of Theorem 2.1 is synonymous to the counterexample given by Zarrin [6], who used an equivalent form of Equation (20); for $m = 3$.

Finally, Herzog’s conjecture was motivated by the fact that $A_8$ and $\text{PSL}(3, 4)$ have the same number of involutions. But $|A_8| = 20160 = |\text{PSL}(3, 4)|$; although $A_8 \not\cong \text{PSL}(3, 4)$. That was the reason why he conjectured that two finite nonabelian simple groups of different sizes cannot have the same number of involutions. It will be surprising for him and many others to see that $\text{PSL}(m, 4)$ and higher orders of a certain group “$\Omega(+1, 2m, 2)$” (which is isomorphic to $A_8$ for $m = 3$) can be used (see Equation (21)) to get infinitely many counterexamples to his conjecture.

Next, we refer to Table 1 for new counterexamples to Zarrin’s conjecture. We now give some observations on equalities that cannot hold in general on the number of involutions that coincide with groups that were used in giving more counterexamples to Zarrin’s conjecture above; so as to clear any dilemma of thought, on these, for the reader.

**Remark 2.3.** 1(i) For all odd prime powers $q > 3$, $I_2(\text{PSL}(4, q))$ and $I_2(\text{PSL}(3, q^2))$ do not always coincide. Two examples are given as
\[I_2(\text{PSL}(4, 5)) = 251875 < 406875 = I_2(\text{PSL}(3, 25))\]

and
\[I_2(\text{PSL}(4, 9)) = 25076871 < 43584723 = I_2(\text{PSL}(3, 81)).\]

(ii) For all odd prime powers $q > 3$, $I_2(\text{PSU}(4, q))$ is not always equal to $I_2(\text{PSL}(3, q^2))$. An example is
\[I_2(\text{PSU}(4, 7)) = 2683975 < 5884851 = I_2(\text{PSL}(3, 49)).\]

2. Although the equalities do not hold among the number of involutions in the mentioned groups, some of the numbers of their elements of odd prime order still coincide.

Writing $A_1 = \text{PSL}(4, 5)$ and $B_1 = \text{PSL}(3, 25)$ we have that
\[I_5(A_1) = 244140624 = I_5(B_1) \text{ and } I_{31}(A_1) = 234000000 = I_{31}(B_1),\]

and writing $A_2 = \text{PSL}(4, 9)$ and $B_2 = \text{PSL}(3, 81)$, we have that
\[I_7(A_2) = 557800473600 = I_7(B_2) \text{ and } I_{13}(A_2) = 1115600947200 = I_{13}(B_2).\]
Furthermore, writing $C = PSU(4,7)$ and $B = PSL(3,49)$, we have that

$$I_7(C) = 13841287200 = I_7(B)$$
$$I_{43}(C) = 189744307200 = I_{43}(B).$$

3. $I_2(PSL(4,8)) = 17039295 = I_2(PSU(4,8))$, but $I_p(PSL(4,8)) \neq I_p(PSU(4,8))$ for all odd prime divisors $p$ of both $|PSL(4,8)|$ and $|PSU(4,8)|$. This raises the question of whether another infinitude of counterexamples to Herzog’s conjecture can be obtained as follows: for a prime power $q \geq 3$, at least two of the following three involutions coincide: $I_2(PSL(4,q))$, $I_2(PSL(3,q^2))$ and $I_2(PSU(4,q))$? Thus, a natural question is whether all finite nonabelian simple groups not satisfying Herzog’s conjecture can be characterized?

A few of the groups listed above can be verified with the aid of the online MAGMA Calculator at http://magma.maths.usyd.edu.au/calc/; using Program 2.4 below.

**Program 2.4**. A program for obtaining the number of elements of order $p$ in a group $G$.

```plaintext
TestIpG := function(p,G)
a := 0; CC := ConjugacyClasses(G);
for Li in CC do if Li[1] eq p then a := a + Li[2]; end if; end for;
return a;
end function;
```

Motivated by these insights, we give the following conjecture:

**Conjecture 2.5.** There are infinitely many counterexamples to Zarrin’s conjecture. In particular, at least one of the following is true:

i. given an integer $m \geq 4$, there exists an odd prime $p_1$ such that

$$I_{p_1}(-1,2m,2)) = I_{p_1}(PSL(m,4)) \neq 0;$$

ii. given an odd integer $m > 4$, $p_2$ is the highest prime divisor of $|PSL(m,4)|$.

$$I_{p_2}(+1,2m,2)) = I_{p_2}(PSL(m,4)),$$

where $p_2$ is the highest prime divisor of $|PSL(m,4)|$.

The counterexamples 11, 12, 13 and 14 given for Zarrin’s conjecture in Table 1 above verify Conjecture 2.5(i) for $m = 4, 5, 6$ and 7 respectively. In the same vein, numbers 9 and 10 of the same Table 1 verify Conjecture 2.5(ii) for $m = 5$ and $m = 7$. Finally, Conjecture 2.5(i) together with Equation (20) are aimed at giving infinitely many counterexamples to Zarrin’s conjecture; the same is targeted by Conjecture 2.5(ii) and Equation (21).

**Funding**

The first author is supported by both TU Graz (R-1501000001) and partial funding from the Austrian Science Fund (FWF): P30934-N35, F05503, F05510. He is also at the Department of Mathematics, University of Nigeria, Nsukka. The second author acknowledges the support of the Austrian Science Fund (FWF): W1230.

**ORCID**

Chimere Stanley Anabanti [http://orcid.org/0000-0003-4564-4179]
References

[1] Anabanti, C. S. (2019). A counterexample to Zarrin’s Conjecture on sizes of finite nonabelian simple groups in relation to involution sizes. Arch. Math. 112(3):225–226. DOI: 10.1007/s00013-018-1265-y.

[2] Carter, R. W. (1972). Simple Groups of Lie Type. New York: Wiley Classics Library, John Wiley & Sons Ltd., 364 pp.

[3] Fulman, J., Guralnick, R., Stanton, D. (2017). Asymptotics of the number of involutions in finite classical groups. J. Group Theory 20(5):871–902. DOI: 10.1515/jgth-2017-0011.

[4] Herzog, M. (1979). On the classification of finite simple groups by the number of involutions. Proc. Am. Math. Soc. 77(3):313–314. DOI: 10.1090/S0002-9939-1979-0545587-2.

[5] Taghvasani, L. J., Zarrin, M. (2017). A characterization of $A_5$ by its same-order type. Monatsh. Math. 182(3):731–736. DOI: 10.1007/s00605-016-0950-9.

[6] Zarrin, M. (2018). A counterexample to Herzog’s Conjecture on the number of involutions. Arch. Math. 111(4):349–351. DOI: 10.1007/s00013-018-1195-8.