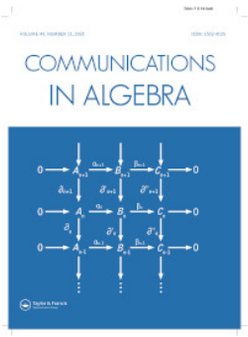


Taylor & Francis
Taylor & Francis Group

Communications in Algebra

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/lagb20

On the replacement property for PSL(2,*p*)

David Cueto Noval, Aidan A. Lorenz & Baran Zadeoğlu

To cite this article: David Cueto Noval, Aidan A. Lorenz & Baran Zadeoğlu (2021) On the replacement property for PSL(2,*p*), Communications in Algebra, 49:11, 4970-4979, DOI: 10.1080/00927872.2021.1933999

To link to this article: https://doi.org/10.1080/00927872.2021.1933999

Published online: 12 Jun 2021.

Submit your article to this journal

Article views: 44

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=lagb20

COMMUNICATIONS IN ALGEBRA®
2021, VOL. 49, NO. 11, 4970–4979
https://doi.org/10.1080/00927872.2021.1933999

Taylor & Francis
Taylor & Francis Group

Check for updates

On the replacement property for PSL(2,*p*)

David Cueto Noval[a,b], Aidan A. Lorenz[b,c], and Baran Zadeoğlu[b,d]

[a]Department of Mathematics, University of Oviedo, Oviedo, Spain; [b]Department of Mathematics, Cornell University, Ithaca, New York, USA (2018 SPUR/REU); [c]Department of Mathematics, Temple University, Philadelphia, Pennsylvania, USA; [d]Department of Mathematics, Bilkent University, Ankara, Turkey

ABSTRACT
The replacement property (or Steinitz Exchange Lemma) for vector spaces has a natural analog for finite groups and their generating sets. For the special case of the groups $\mathrm{PSL}(2,p)$, where p is a prime larger than 5, first partial results concerning the replacement property were published by Benjamin Nachman (2014). Second partial results were published by Hy P.G. Lam (2017). The main goal of this paper is to provide a complete answer for $\mathrm{PSL}(2,p)$.

ARTICLE HISTORY
Received 25 March 2021
Revised 4 May 2021
Communicated by Mark Lewis

KEYWORDS
Exchange lemma; finite groups; minimal generating sets; minimax sets; PSL(2, *p*); replacement property

2020 MATHEMATICS SUBJECT CLASSIFICATION
20F05; 20G40

1. Introduction

There is an ongoing effort to create a theory for groups and their generating sequences, analogous to the theory of vector spaces and their respective bases; see [2, 8–10]. In detail, for a given group G, a sequence $s = (g_1, \ldots, g_n) \in G^n$ such that G is generated by the $\{g_i\}_{i=1}^n$ is called a *generating sequence of length n*; if no proper subsequence of s generates G, then s is called *irredundant*. The largest possible length of an irredundant generating sequence of G will be denoted by $m(G)$. The group G is said to satisfy the *replacement property* (abbr. *RP*) if any $1 \neq g \in G$ can replace an element in all irredundant generating sequences of length $m(G)$ to yield a new generating sequence of G. This property, an obvious analog of the Steinitz Exchange Lemma, does not generally hold for groups. Note that in the case of groups, the new generating sequence need not be irredundant. This definition is motivated further below.

This paper focuses on the groups $\mathrm{PSL}(2,p)$, where p is a prime number > 5. Our main tool is an analysis of the maximal subgroups $\mathrm{PSL}(2,p)$ and their intersections. The following theorem summarizes our findings.

Theorem 1.1. *The groups* $\mathrm{PSL}(2,p)$ *with* $p \in \{7, 11, 19, 31\}$ *satisfy RP. For all other primes* $p > 5$, $\mathrm{PSL}(2,p)$ *satisfies RP if and only if* $p \equiv 3$ *or* -3 *mod 8 and* $p \equiv 3$ *or* -3 *mod 10. In other words, we have the following:*

Even though *RP* fails for the majority of primes, examples of failure are rare in these cases, in the sense that most elements of $\mathrm{PSL}(2,p)$ can still replace an element in every irredundant generating sequence of length $m(G)$. An element that fails to do so will be called a *witness to failure*.

CONTACT Baran Zadeoğlu baranzadeoglu@gmail.com Department of Mathematics, Bilkent University, Ankara, Turkey.
© 2021 Taylor & Francis Group, LLC

mod8 \ mod10	$p \equiv \pm 1$	$p \equiv \pm 3$
$p \equiv \pm 1$	*RP* fails	*RP* fails
$p \equiv \pm 3$	*RP* fails	*RP* holds

Theorem 1.2. *Witnesses to failure for* $\mathrm{PSL}(2,p)$ *must have order 2 or 3; if* $p \not\equiv \pm 1 \bmod 10$, *they must have order 2.*

The rare occurrences of witnesses to failure can be observed empirically via computer algebra systems such as GAP [4]. In fact, checking whether a finite group satisfies *RP* can be done computationally. All the code used for this paper can be found on the second author's GitHub page. For the majority of this paper, proof methodology is elementary and applicable for other classes of groups provided that $m(G)$ and the isomorphism classes of maximal subgroups are known. However, the latter half of the proof of the Theorem 1.1 uses extensive knowledge about the subgroup lattice of the group. This can be reduced to character theoretic level using Mackey's theorem and other considerations of [7].

2. Notational conventions and definitions

Definition 2.1. *For a finite group G, r(G) (resp. m(G)) denotes the length of the shortest (resp. longest) irredundant generating sequence of G.*

Notation 2.2. $\Gamma_n(G)$ *will denote the set of all irredundant generating sequences of G of length n.*

Applying a more general theorem of Tarski [11] to groups, D. Collins was able to show that for all n with $r(G) \leq n \leq m(G), \Gamma_n(G) \neq \emptyset$.

Definition 2.3. *A sequence of subgroups* $(H_1, \ldots, H_n)$ *of a group is said to be in* ***general position*** *if, for all* $j \in I = \{1, \ldots, n\}$, *we have*

$$\bigcap_{i \neq j} H_i \not\subseteq H_j.$$

We think of maximal subgroups in general position as group theoretic analogs of hyperplanes in general position: maximal subobjects which become strictly smaller upon intersection.

Definition 2.4. *For* $S = (M_1, \ldots, M_n)$ *a sequence of maximal subgroups of a group, we say a sequence* $s = (g_1, \ldots, g_n)$ ***corresponds*** *to S if* $g_i \in M_j$ *for all* $j \neq i$, *but* $g_i \notin M_i$.

Given an irredundant generating sequence $s = (g_1, \ldots, g_n)$ of a finite group G, we can construct a corresponding sequence of maximal subgroups in the following fashion: let

$$H_i := \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n \rangle$$

Since G is finite, each H_i is contained in some maximal subgroup M_i. We thus associate to the irredundant generating sequence $s = (g_1, \ldots, g_n)$, the sequence of maximal subgroups $S := (M_1, \ldots, M_n)$. It is straight forward to see that S is in general position.

Remark 2.5. Though we can associate any irredundant generating sequence with a corresponding sequence of maximal subgroups in general position, we typically cannot do the converse. One can observe that given a sequence of maximal subgroups in general position S, any sequence corresponding to S will be irredundant. However these irredundant sequences are not necessarily generating sequences. The question remains open as to when we can make the converse association.

Definition 2.6. *Given a sequence of maximal subgroups $S = (M_1, \ldots, M_n)$, we call the* ***radical of S*** *(denoted $rad(S)$) the intersection of all M_i:*

$$\mathrm{rad}(S) := \bigcap_{1 \le i \le n} M_i.$$

In each of the following two definitions, G is a finite group, and $s = (g_1, \ldots, g_n)$ is an irredundant generating sequence of G.

Definition 2.7. *G satisfies the* ***replacement property relative to s*** *if for all $1 \neq g \in G$, there exists $i \in \{1, \ldots, n\}$ such that $s' := (g_1, \ldots, g_{i-1}, g, g_{i+1}, \ldots, g_n)$ generates* G.

Remark 2.8. An alternative definition to 2.7 replaces "$g \neq 1$" with "$g \notin \Phi(G)$" where $\Phi(G)$ denotes the Frattini subgroup of G, which is well known to consist of all non-generators of G. For our purposes in studying $\mathrm{PSL}(2, p)$, we have that $\Phi(\mathrm{PSL}(2, p)) = \{1\}$ for all p, so the definitions are equivalent.

Thanks to an unpublished result from R.K. Dennis and D. Collins, we know that for a given finite group G and for all n with $r(G) \le n < m(G)$, there exists some $s \in \Gamma_n(G)$ such that G does not satisfy the replacement property relative to s. This allows us to define the replacement property in full generality:

Definition 2.9. *Let $m = m(G)$. We say G satisfies the* ***replacement property*** *(abbreviated RP) if* G *satisfies the replacement property for all $s \in \Gamma_m(G)$.*

Remark 2.10. In the case when $\Phi(G) \neq \{1\}$, one could also use the definition that G satisfies *RP* if and only if $G/\Phi(G)$ satisfies *RP* (in the sense of 2.9). This is in accordance with Remark 2.8.

Notice, in Definition 2.7, we do not require s' to be irredundant. If we did, this would quickly lead to the result that for any group G satisfying *RP* we would have that $r(G) = m(G)$, which too strictly limits the groups that might possibly enjoy this property. This can be demonstrated by the group S_4, an irredundant generating set containing transpositions and a cycle of length 4.

Some examples of groups that satisfy *RP* include M_{11} [10] and S_n (for $n > 6$ it follows from Theorem 2.1 in [1]).

Notation 2.11. *Given a finite group G, let $m = m(G)$. We call the subset*

$$W(G) := \{g \in G \mid \exists s \in \Gamma_m(G) \text{ such that } g \text{ cannot replace any element of } s\}$$

the set of ***witnesses to failure****.*

3. An equivalent condition and applications to PSL(2,p)

Proposition 3.1 (R.K. Dennis & D. Collins (Unpublished)). *For a finite group G, let $m = m(G)$. Then G satisfies RP if and only if for every sequence of maximal subgroups in general position of length m corresponding to some irredundant generating sequence, S, we have that $rad(S) = \{1\}$.*

Proof. We prove the "if" direction by contrapositive: assume G does not satisfy *RP*. Then there exists an irredundant generating sequence $s = (g_1, \ldots, g_m)$ and an element $1 \neq g \in G$ such that for no $i \in \{1, .., n\}$ can g_i be replaced by g to yield a generating sequence. Now for each i, let

$$\langle g_1, \ldots, g_{i-1}, g, g_{i+1}, \ldots, g_m \rangle =: H_i \lneq G$$

with proper containment because s was irredundant and g fails the replacement property relative

to s. For each H_i, pick a maximal subgroup M_i such that $H_i \leq M_i$. Clearly, the sequence $(M_1, ..., M_m)$ corresponds to s (thus, is in general position), and by construction, $g \in M_i$ for all i.

For the "only if" direction, assume there exists a sequence of maximal subgroups in general position of length m, $S = (M_1, ..., M_m)$ corresponding to some irredundant generating sequence of G, $s = (g_1, ..., g_m)$, where $\mathrm{rad}(S) \neq \{1\}$ so there exists a nontrivial element, $x \in \mathrm{rad}(S)$. Then,

$$\langle g_1, ..., g_{i-1}, x, g_{i+1}, ..., g_m \rangle \leq M_i \lneq G$$

because $x \in M_i$ by assumption. Since i was arbitrary, we know that x fails the replacement property relative to s, and hence G does not satisfy RP. □

For a sequence S of maximal subgroups in general position corresponding to an irredundant generating sequence we have that $\mathrm{rad}(S) \subseteq W(G)$. It is known that for any finite non-abelian simple group G, $r(G) = 2$. A further result by Jambor [5] follows:

Theorem 3.2 (Jambor [5]). *$m(\mathrm{PSL}(2,p)) = 3$ for all primes except 7, 11, 19, and 31 in which cases we have $m(\mathrm{PSL}(2,p)) = 4$.*

Another important result that will be useful in our discussion is the classification of isomorphism types of maximal subgroups of $\mathrm{PSL}(2,p)$ from [3]:

Theorem 3.3. *All maximal subgroups of $\mathrm{PSL}(2,p)$ are isomorphic to one of the following:*

1. $\mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}$
2. D_{p-1}
3. D_{p+1}
4. A_5 *if and only if* $p \equiv \pm 1 \bmod 10$
5. S_4 *if and only if* $p \equiv \pm 1 \bmod 8$
6. A_4 *if and only if* $p \equiv \pm 3 \bmod 10$ *and* $p \equiv \pm 3 \bmod 8$

where we use the convention that $|D_n| = n$.

In fact, Dickson studied all subgroups of $\mathrm{PSL}(2,p)$. One can find a modern version of his work in [6].

For the isolated cases when $p \in \{7, 11, 19, 31\}$, B. Nachman showed that $\mathrm{PSL}(2,p)$ satisfies RP in [10]. In the same paper, Nachman showed that for primes that are congruent to $+1 \bmod 8$, $\mathrm{PSL}(2,p)$ does not satisfy RP. Later, Ravi Fernando came up with the conjecture that is our Theorem 1.1.

Before we prove our main theorem, we state and prove some helpful lemmas.

Lemma 3.4. *If G is a simple group, M_1 and M_2 maximal subgroups of G, and there exists $N \neq \{1\}$ such that $N \trianglelefteq M_1, M_2$, then $M_1 = M_2$.*

Proof. Trivial. □

Lemma 3.5. *For a triple of maximal subgroups $S = (M_1, M_2, M_3)$ to be in general position it must be the case that:*

1. *all pairwise intersections are nontrivial*
2. *all of the maximal subgroups M_i must have 2 distinct chains of nontrivial subgroups of length at least 3 (where we say the length of a chain is the number of non-trivial subgroups involved, including M_i itself)*

Proof. The first statement is trivial. As for the second, let (M_1, M_2, M_3) be a sequence of maximal subgroups in general position. The chains $M_2 > M_1 \bigcap M_2 > M_1 \bigcap M_2 \bigcap M_3$ and $M_2 > M_3 \bigcap M_2 > M_1 \bigcap M_2 \bigcap M_3$ are distinct chains of length 3 as (M_1, M_2, M_3) are in general position. □

Lemma 3.6. *Let $G = \mathrm{PSL}(2,p)$. For $p > 5$, there does not exist an element of order p in $W(G)$.*

Proof. Suppose there exists some $x \in G$ with order p. Then x must lie in some maximal subgroup with order divisible by p. From Theorem 3.3, we can see that x must lie in a copy of $\mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}$. Hence, $\langle x \rangle \cong \mathbb{Z}_p \trianglelefteq \mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}$. But by Lemma 3.4, there is only one such maximal subgroup. Thus x cannot be in the intersection of 3 maximal subgroups in general position. Therefore $x \notin W(G)$. □

We can now return to our main theorem. Its proof is divided in several cases. In Proposition 3.7, we consider the case where, $p \equiv 3$ or $-3 \bmod 8$ and $p \equiv 3$ or $-3 \bmod 10$. In Proposition 3.12, we consider the rest of the cases.

Proposition 3.7. *If $p \equiv \pm 3 \bmod 8$ and $p \equiv \pm 3 \bmod 10$, then $\mathrm{PSL}(2,p)$ satisfies RP.*

Proof. According to Theorem 3.3, the possible maximal subgroups in this case are

1. $\mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}$
2. D_{p-1}
3. D_{p+1}
4. A_4

We will show that no triple of these maximal subgroups can be in general position while still having a nontrivial radical, thus proving the theorem by Proposition 3.1.

Firstly, looking at the subgroup lattice, all chains of nontrivial subgroups of length 3 in A_4 contain the unique normal subgroup $\mathbb{Z}_2 \times \mathbb{Z}_2$ as the middle term. Therefore, by Lemma 3.5, A_4 cannot appear in any triple of maximal subgroups in general position with nontrivial intersection.

Next, suppose we have a sequence of maximal subgroups in general position $S = (M_1, M_2, M_3)$ where each M_i is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}$ or D_{p-1} and suppose there is a nontrivial element in $\mathrm{rad}(S)$. By Lemma 3.6, we know that this element can't have order p. Assume further that there exists an element $x \in M_1 \bigcap M_2$ such that $|x| > 2$. Then,

$$C_{M_1}(x), C_{M_2}(x) \leq C_G(x) \lneqq G. \tag{3.1}$$

In fact, we have $C_{M_1}(x) = C_{M_2}(x) = M_1 \bigcap M_2 = C_G(x)$. Now, if $\mathrm{rad}(S)$ or $M_1 \bigcap M_3$ contains an element of order larger than 2, then by the argument above we have that

$$M_1 \bigcap M_2 = M_1 \bigcap M_3 = \mathrm{rad}(S) \tag{3.2}$$

which contradicts the general position assumption. Now assume $\mathrm{rad}(S)$ contains only elements of order 2 and the identity. If we have $M_1 \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}$ then,

$$\mathrm{rad}(S) \lneqq M_1 \bigcap M_2, M_1 \bigcap M_3 \lneqq \mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}. \tag{3.3}$$

In particular, both $M_1 \bigcap M_2$ and $M_1 \bigcap M_3$ contains elements of order larger than 2. We again get the above contradiction. Now assume all maximal subgroups M_i are isomorphic to D_{p-1} and their pairwise intersections have no element of order larger than 2. Then, we must have that $M_i \bigcap M_j \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ for $i \neq j$ and $\mathrm{rad}(S) \cong \mathbb{Z}_2$. However, all isomorphic copies of $\mathbb{Z}_2 \times \mathbb{Z}_2$ in a dihedral group must contain the group's center. In particular,

$$Z(M_1) \subset M_1 \bigcap M_2, M_1 \bigcap M_3 \tag{3.4}$$

Hence, $Z(M_1) = Z(M_2) = \mathrm{rad}(S)$ which implies $\mathrm{PSL}(2,p)$ has a center, contradiction. The same arguments also applies to the cases where each M_i are isomorphic copies of D_{p+1} or $\mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}$.

Finally, we realize that D_{p-1} and D_{p+1} cannot appear in the same triple of maximal subgroups in general position with non-trivial radical since any intersection of D_{p-1} and D_{p+1} can have order at most 2, leaving the intersection with the third maximal subgroup to be trivial.

We have therefore showed that no triple of maximal subgroups from the list of possibilities can be in general position and have nontrivial radical simultaneously. The proof is thereby complete. □

Corollary 3.8. *Witnesses to failure in* $\mathrm{PSL}(2,p)$ *have order 2 or 3.*

Proof. Notice that in Proposition 3.7, we only used the criterion that $p \equiv \pm 3 \bmod 8$ and $p \equiv \pm 3 \bmod 10$ to build a list of possible maximal subgroups that could occur. Since we showed in the proof that no triple consisting of subgroups isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_{\frac{p-1}{2}}, D_{p-1}, D_{p+1}, A_4$ can constitute a triple of maximal subgroups in general position with nontrivial radical, we know (from Theorem 3.3) that any triple of maximal subgroups in general position with nontrivial radical must contain an S_4 or A_5. That is to say, any witness to failure must lie in some S_4 or A_5. Hence, a witness to failure can have order only 2, 3, 4, or 5.

To rule out elements of order 5, consider any triple of maximal subgroups in general position: (A_5, M_1, M_2). Suppose this triple corresponds to an irredundant generating sequence and does not intersect trivially, but contains some element x such that $|x| = 5$. Then $\langle x \rangle \cong \mathbb{Z}_5 \leq A_5$. The only chain of subgroups of A_5 containing $\mathbb{Z}_5$ is as follows:

$$\mathbb{Z}_5 \trianglelefteq D_{10} \leq A_5 \tag{3.5}$$

Thus, for the triple to be in general position, it must be the case that

$$A_5 \bigcap M_1 \bigcap M_2 \cong \mathbb{Z}_5 \tag{3.6}$$

and

$$A_5 \bigcap M_1 \cong D_{10}, \quad A_5 \bigcap M_2 \cong D_{10} \tag{3.7}$$

But $N_{A_5}(\mathbb{Z}_5) \cong D_{10}$, whence Lemma 3.4 implies that $A_5 \bigcap M_1 = A_5 \bigcap M_2 \cong D_{10}$ and hence,

$$A_5 \bigcap M_1 \bigcap M_2 \cong D_{10} \ncong \mathbb{Z}_5, \tag{3.8}$$

which is a contradiction.

We also rule out an element's having order 4 by the same argument by realizing that the only chain of subgroups of S_4 of length 3 ending with a subgroup that contains an element of order 4 is

$$\mathbb{Z}_4 \trianglelefteq D_8 \leq S_4$$

□

Corollary 3.9. *The groups* $\mathrm{PSL}(2,p)$ *with* $p \in \{7, 11, 19, 31\}$ *satisfy RP.*

Proof. By Theorem 3.2, $m(\mathrm{PSL}(2,p)) = 4$ for these primes, it suffices by the Proposition 3.1 that any sequence of maximal subgroup in general position of length 4 would have a trivial radical. Similar considerations as of Corollary 3.8 and of Lemma 3.5 leads to the following observation. Any sequence of maximal subgroup of length 3 in general position with non-trivial radical must

have $\mathbb{Z}_2$ or $\mathbb{Z}_3$ as its radical. Hence any sequence of maximal subgroups of length 4 must have trivial radical. □

We will actually be able to refine Corollary 3.8 using techniques discussed in the following proofs. Even though we will use explicit knowledge about the subgroup lattice of the groups of the type $\mathrm{PSL}(2,p)$, a similar conclusion can be drawn using the character table. The main tool in this case would be Mackey's theorem and similar work can be found in [7].

It remains to show that *RP* fails for $\mathrm{PSL}(2,p)$ in the remaining cases. To begin this endeavor, we quote a lemma from King [6]:

Lemma 3.10.
1. *There are* $\frac{p(p^2-1)}{12}$ *subgroups of PSL(2, p) isomorphic to* S_3.
2. *If* $p \equiv \pm 1 \bmod 10$, *there are* $\frac{p(p^2-1)}{20}$ *subgroups of PSL(2, p) isomorphic to* D_{10}.
3. *If* $p \equiv \pm 1 \bmod 8$, *then there are* $\frac{p(p^2-1)}{24}$ *subgroups of PSL(2, p) isomorphic to* S_4.
4. *If* $p \equiv \pm 1 \bmod 10$, *then there are* $\frac{p(p^2-1)}{60}$ *subgroups of PSL(2, p) isomorphic to* A_5.

A simple consequence of Lemma 3.10 that is used in subsequent proofs follows:

Lemma 3.11. *For* $p \equiv \pm 1 \bmod 8$ *(resp.* $p \equiv \pm 1 \bmod 10$*),* $\mathrm{PSL}(2,p)$ *always contains two isomorphic copies of* S_4*,(resp.* A_5*) that intersect in a copy* S_3 *(resp.* D_{10}*).*

Proof. We know that for $p \equiv \pm 1 \bmod 8, \mathrm{PSL}(2,p)$ has $\frac{p(p^2-1)}{24}$ distinct subgroups isomorphic to S_4 (item 3 of Lemma 3.10). Further, each S_4 has four distinct copies of S_3. Suppose all these copies of S_3 were distinct. Then there would be at least

$$4 \cdot \frac{p(p^2-1)}{24} = \frac{p(p^2-1)}{6}$$

subgroups of $\mathrm{PSL}(2,p)$ isomorphic to S_3. This contradicts item 1 of Lemma 3.10. Therefore, there exist two copies of S_4 must intersect in an S_3. The same line of arguments with corresponding parts of Lemma 3.11 shows that when $p = \pm 1 \bmod 10$ there exist two copies of A_5 that must intersect in an D_{10}. □

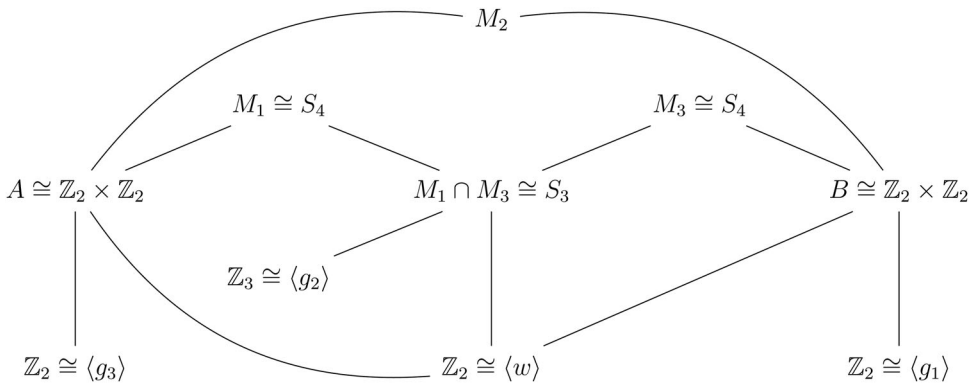
We can now prove the rest of Theorem 1.1. Our strategy for the proof will be to use the maximal subgroups in Lemma 3.11 and their intersections to construct irredundant generating sequences of length 3 that fail to replace an element.

Proposition 3.12. *If* $p \equiv \pm 1 \bmod 8$ *or* $p \equiv \pm 1 \bmod 10$ *and* $p \notin \{7, 11, 19, 31\}$, *then* $\mathrm{PSL}(2,p)$ *fails RP.*

Proof. Case 1: $p \equiv \pm 1 \bmod 8$:

We take two subgroups M_1 and M_3 isomorphic to S_4 such that their intersection is isomorphic to S_3. Consider w an element of order 2 contained in $M_1 \bigcap M_3$. Then there is only one subgroup A of M_1 that is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and contains w. There is also a unique subgroup $B \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ of M_3 containing w. We now take as M_2 a maximal subgroup of $\mathrm{PSL}(2,p)$ containing the centralizer of w. More precisely, we take as M_2 the only subgroup isomorphic to $D_{p\mp 1}$ (plus or minus sign according to $p \equiv \pm 1 \bmod 8$)[6] that contains both A and B, namely, M_2 is the centralizer of w. It is clear that the maximal subgroups M_1, M_2, and M_3 are in general position and have nontrivial intersection.

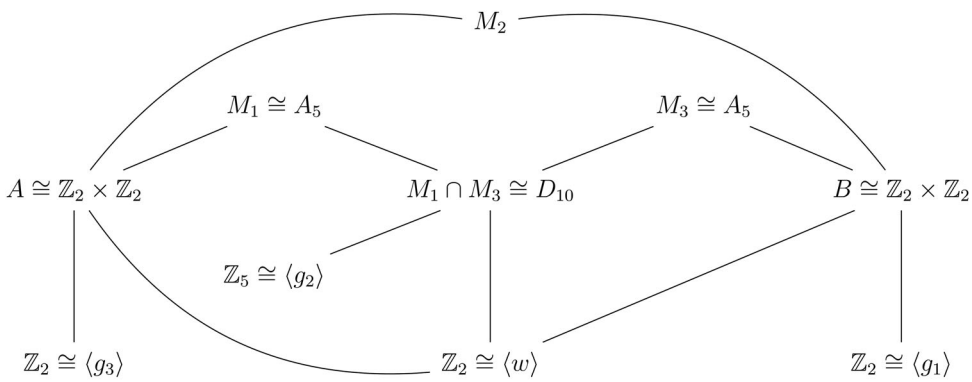
We take g_1 to be the element of order 2 in B distinct from w that is conjugate to w in M_3. We take $1 \neq g_3 \neq w$ in A. Let g_2 be an element of order 3 in $M_1 \bigcap M_3$. Then $g_i \in \bigcap_{j \neq i} M_j \setminus M_i$ and (g_1, g_2, g_3) is an irredundant generating sequence of $\mathrm{PSL}(2,p)$ since it is irredundant by construction and $\langle g_1, g_2 \rangle = M_3$, which is a maximal subgroup not containing g_3. Finally, note that (g_1, g_2, g_3) does not satisfy the replacement property as $\langle \{g_j\}_{j \neq i} \cup \{w\} \rangle \leq M_i$.



Case 2: $p \equiv \pm 1 \bmod 10$:

We consider two subgroups M_1 and M_3 isomorphic to A_5 such that $M_1 \bigcap M_3 \cong D_{10}$. Let w be an element of order 2 contained in $M_1 \bigcap M_3$. Then there is only one subgroup A of M_1 isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and contains w. There is also a unique subgroup $B \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ of M_3 that contains w. We now take as M_2 a maximal subgroup of $\mathrm{PSL}(2,p)$ containing the centralizer of w in $\mathrm{PSL}(2,p)$. More precisely, we take as M_2 the only subgroup isomorphic to $D_{p\mp 1}$ (here the order of this dihedral group depends on $p \equiv \pm 1 \bmod 4$)[6] which is the centralizer of w and contains both A and B. It is clear that the maximal subgroups M_1, M_2, and M_3 are in general position and have nontrivial intersection.

We take $g_1 \neq w$ an element of order 2 in B. We take $1 \neq g_3 \neq w$ in A. Let g_2 be an element of order 5 in $M_1 \bigcap M_3$. Then $g_i \in \bigcap_{j \neq i} M_j \setminus M_i$ and (g_1, g_2, g_3) is an irredundant generating sequence of $\mathrm{PSL}(2,p)$ since it is irredundant by construction and $\langle g_1, g_2 \rangle = M_3$, which is a maximal subgroup not containing g_3. Similarly, (g_1, g_2, g_3) does not satisfy the replacement property.



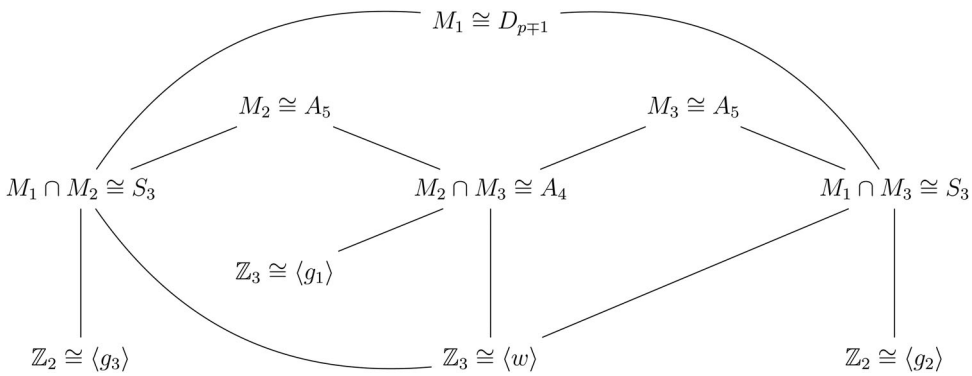
□

From the last proof it follows that:

Corollary 3.13. *If the replacement property fails for* $\mathrm{PSL}(2,p)$, *then there is a witness to failure of order 2.*

Proposition 3.14. $\mathrm{PSL}(2,p)$ *has a witness to failure of order 3 if and only if* $p \equiv \pm 1 \bmod 10$.

Proof. If $p \equiv \pm 1 \bmod 10$, then a similar argument to the one used in the previous proof shows that there exist three maximal subgroups in general position such that $M_1 \cong D_{p\mp 1}$ (here the order of this dihedral group depends on $p \equiv \pm 1 \bmod 3$), $M_2 \cong A_5, M_3 \cong A_5, M_2 \bigcap M_3 \cong A_4, M_1 \bigcap M_3 \cong S_3, M_1 \bigcap M_2 \cong S_3$ and $\bigcap_{i=1}^{3} M_i \cong \mathbb{Z}_3$. This allows to construct an irredundant generating sequence (g_1, g_2, g_3) with a witness to failure w of order 3 such that $g_i \in \bigcap_{j \neq i} M_j \setminus M_i, \langle g_1 \rangle \neq \langle w \rangle$ and $\langle g_1, g_3 \rangle = M_2$.



Conversely, if there is an irredundant generating sequence (g_1, g_2, g_3) with a witness to failure w of order 3 and $p \not\equiv \pm 1 \bmod 10$, then one of the maximal subgroups of the corresponding sequence of maximal subgroups in general position must be isomorphic to S_4 (without loss of generality, M_1). This leads to a contradiction as both $M_1 \bigcap M_2$ and $M_1 \bigcap M_3$ would have to be equal to the only copy of D_3 containing $C_3 \cong \langle w \rangle$. □

Acknowledgement

The authors are thankful to R. K. Dennis for patiently and carefully teaching us the requisite information needed for this paper and for guiding our inquiries in fruitful directions. Further thanks goes to the math department at Cornell University for hosting the SPUR/REU program and of course to our group mates without whom progress would have been far slower and less enjoyable. Finally, we would like to thank the referee for providing useful comments on how to improve the paper.

Funding

The first author is grateful to María Cristina Masaveu Peterson Foundation for their funding. The second author would also like to acknowledge and thank the Science Scholars Program at Temple University for summer funding. The third author would like to thank The Crossing Paths for their traveling grant.

References

[1] Cameron, P. J., Cara, P. (2002). Independent generating sets and geometries for symmetric groups. *J. Algebra* 258(2):641–650. DOI: 10.1016/S0021-8693(02)00550-1.

[2] Dan, C. (2010). Generating sequences of finite groups senior. Thesis. Cornell University. http://pi.math.cornell.edu/m/sites/default/files/imported/Research/SeniorTheses/2010/collinsThesis.pdf

[3] Dickson, L. E. (1958). *Linear Groups: With an Exposition of the Galois Field Theory*. New York: Dover Publications, Inc.

[4] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.9.2 (2018). https://www.gap-system.org

[5] Jambor, S. (2013). The minimal generating sets of $\mathrm{PSL}(2,p)$ of size four. *LMS J. Comput. Math.* 16: 419–423.

[6] King, O. H. (2005). The subgroup structure of finite classical groups in terms of geometric configurations. In *Surveys in Combinatorics 2005, Volume 327 of London Math. Soc. Lecture Note Ser.* Cambridge: Cambridge Univ. Press, pp. 29–56.

[7] Komissartschik, E. A., Tsaranov, S. V. (1986). Intersections of maximal subgroups in simple groups of order less than 10^6. *Commun. Algebra* 14(9):1623–1678. DOI: 10.1080/00927878608823389.

[8] Lam, H. P. G. The replacement property of $\mathrm{PSL}(2,p)$ and $\mathrm{PSL}(2,p^2)$. *arXiv e-Prints*. page arXiv:1709.08745, September 2017.

[9] Lucchini, A. Finite soluble groups satisfying the replacement property. *arXiv e-Prints*. page arXiv:1710.00582, October 2017.

[10] Nachman, B. (2014). Generating sequences of $\mathrm{PSL}(2,p)$. *J. Group Theory* 17(6):925–945.

[11] Tarski, A. (1975). An interpolation theorem for irredundant bases of closure structures. *Discr. Math.* 12(2): 185–192. DOI: 10.1016/0012-365X(75)90033-3.