A NOTE ON THE SUBGROUP MEMBERSHIP PROBLEM FOR $\mathrm{PSL}(2,p)$

DENIS XAVIER CHARLES

ABSTRACT. We show that there are infinitely many primes p such that the Subgroup Membership Problem for $\mathrm{PSL}(2,p)$ belongs to $\mathrm{NP} \cap \mathrm{coNP}$.

1. Introduction

One of the simplest computational questions we can pose in group theory is the subgroup membership problem: given a set of generators for a subgroup $H \subseteq G$, and an element $g \in G$ is $g \in H$? For arbitrary groups, this problem is already undecidable. So we can restrict our study to the case when G is a finite group.

Even in the finite case things apparently are not too easy (see [BS84], and [BB97] for a survey of results). Currently the best known result for subgroup membership in arbitrary finite groups is still from [BS84], where it is proved that the problem can be solved in $\mathrm{NP} \cap \mathrm{coAM}$. In the same paper a conjecture is framed for finite groups called the *Short Presentation Conjecture*, then it is shown that under this conjecture the subgroup membership problem can be solved in $\mathrm{NP} \cap \mathrm{coNP}$. There is a lot of evidence in favor of the conjecture, in particular in [BGKLP97] it is shown that if the conjecture holds for finite simple groups then it holds for all finite groups. Further, the conjecture has been verified for all finite simple groups except for three families of groups namely, the unitary groups $\mathrm{PSU}(3,q)$, the Suzuki groups $\mathrm{Sz}(q)$, and the Ree groups $R(q)$ (see [BGKLP97]). It follows from the results in that paper that if none of these exceptional families of groups occur as factor groups of composition series of subgroups of a group G, then the subgroup membership problem for G can be solved in $\mathrm{NP} \cap \mathrm{coNP}$. In this article we show that there are infinitely many primes p for which these exceptional families of groups do not occur as factor groups of the composition series of subgroups of $\mathrm{PSL}(2,p)$, thus proving the result.

If one were to look at the problem for $\mathrm{PSL}(2,\mathbb{F})$, where $\mathbb{F}$ is a field of characteristic 0, then even ZPP algorithms are known [BB93]. The problem with the characteristic p case has to do with *abelian obstacles*. For example $\mathrm{PSL}(2,p)$ contains a subgroup isomorphic to the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$, and the membership problem for this subgroup is not that easy. For example, the constructive version of this problem is the discrete log problem (see [BB97] §3.5). Algorithms for solvable matrix groups are given in [Lu92], however the running time of the membership algorithm is not polynomial in the bit-size of the input but depends also on the largest divisor of the order of the group other than the characteristic. For the infinite group $\mathrm{PSL}(2,\mathbb{Z})$ average case polynomial time algorithms are known for subgroup membership ([CFKL]).

2. Definitions and standard results

We recall some standard definitions and results regarding finite groups.
Let G be a finite group. If $S \subseteq G$, then $\langle S \rangle$, will denote the subgroup generated by the elements of S, in other words, it is the intersection of all subgroups of G which contain S. If $S \subseteq G$ and $g \in G$, then $S^g = \{gsg^{-1} \mid s \in S\}$, denotes the *conjugate* subset of S by g. If H is actually a subgroup then H^g is also a subgroup. If $S \subseteq G$, the *normalizer* of S in G is denoted by $N_G(S)$ and is defined to be:

$$N_G(S) = \{g \mid g \in G, S^g = S\}.$$

Department of Computer Science and Engineering, State University of New York at Buffalo, NY - 14260. Research supported in part by NSF grant CCR-9820140. E-mail: cdx@cse.buffalo.edu.

The normalizer is a subgroup of G. A subgroup H of G is called a *normal* subgroup of G if $N_G(H) = G$. Clearly G and 1 are trivially normal in G. If a group G has no non-trivial normal subgroups then G is called a *simple* group.
The *centralizer* of a subset S of G is defined as follows:

$$C_G(S) = \{g \mid g \in G, \forall s \in S \;:\; gsg^{-1} = s\}.$$

The centralizer of the group itself is called the *center* of the group and denoted by $Z(G) = C_G(G)$. Note that $C_G(S)$ is a normal subgroup of $N_G(S)$.

The following is a basic result in finite group theory:

Theorem 2.1 (Lagrange). *If* G *is a finite group, and* H *is a subgroup of* G*, then* $|G| = |H||G : H|$.

Definition 2.2. Let G be a group. If we have a finite chain of subgroups of G

$$\mathcal{G} \;:\; G = G_0 \supset G_1 \supset \cdots \supset G_r = 1$$

such that for each $i, 1 \le i \le r$, G_i is a maximal normal subgroup of G_{i-1}, we say that $\mathcal{G}$, is a *composition series* of length r of G. The set of factor groups

$$\left\{\frac{G_0}{G_1}, \cdots, \frac{G_{r-1}}{G_r}\right\}$$

is said to be the set of *composition factors*.
Note that each composition factor is a simple group.

We define the group $PSL(2, p)$. The *special linear* group of dimension 2 over the finite field $\mathbb{Z}/p\mathbb{Z}$ denoted $SL(2, p)$ is the set of matrices:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad - bc \equiv 1 \mod p \right\}$$

together with ordinary matrix multiplication. $Z(SL(2, p)) = \{\pm I\}$, and the quotient group $SL(2, p)/\{\pm I\}$ is the *projective special linear* group $PSL(2, p)$.

We will define three other families of groups which will play a role in our discussion (see [Gor68] for details).

Let q be any prime power $GU(3, q)$ consists of all 3×3 unitary matrices with entries in $GF[q^2]$. A matrix X of $GL(3, q^2)$ is said to be unitary if $X^{-1} = (X^\sigma)^t$, where X^σ is the matrix obtained by applying the Frobenius autormorphism $\sigma(x) = x^q$ to each entry of the matrix X. The group modulo its center is the *projective unitary group*, $PGU(3, q)$, a subgroup of the projective general linear group $PGL(3, q^2)$. The *projective special unitary group* is the subgroup $PSU(3, q) = PGU(3, q) \cap PSL(3, q^2)$.

We now define the family of Suzuki groups $Sz(q)$ over $K = GF[q]$, where $q = 2^{2m+1}$ and $m > 0$. Let

$$T = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The field K has exactly one automorphism π such that $\pi^2(x) = x^2$ for all $x \in K$, namely $\pi(x) = x^{2^{m+1}}$. For $a, b \in K$, and $\lambda \in K^\times$, let

$$S(a, b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ b & \pi(a) & 1 & 0 \\ a^2(\pi(a)) + ab + \pi(b) & a\pi(a) + b & a & 1 \end{pmatrix}$$

and

$$M(\lambda) = \begin{pmatrix} \lambda^{1+2^m} & 0 & 0 & 0 \\ 0 & \lambda^{2m} & 0 & 0 \\ 0 & 0 & \lambda^{-2m} & 0 \\ 0 & 0 & 0 & \lambda^{-1-2^m} \end{pmatrix}.$$

The *Suzuki group* $\mathrm{Sz}(q)$ is defined to be the following subgroup of $\mathrm{GL}(4, q)$

$$\mathrm{Sz}(q) = \langle S(a, b), M(\lambda), T \mid a, b \in K, \lambda \in K^{\times} \rangle.$$

Another family of groups is the *Ree* groups denoted $\mathrm{R}(q), q = 3^{2m+1}, m > 0$; for whose definition we refer to [Ree61]. The Ree groups are obtained by following the Lie Algebra analogue of the definition of Suzuki groups in $\mathrm{GF}[3^{2m+1}]$.

The following is the basic fact we will use in our main theorem:

Theorem 2.3. *The orders of the families of groups* $\mathrm{PSL}(2, p), \mathrm{PSU}(3, q), \mathrm{Sz}(q)$ *and* $\mathrm{R}(q)$ *are as follows:*
(1) $|\mathrm{PSL}(2, p)| = \frac{p(p^2-1)}{2}$ *if* p *is an odd prime.*
(2) $|\mathrm{PSU}(3, q)| = \frac{q^3(q^2-1)(q^3+1)}{\gcd(3,q+1)}$*, where* q *is a power of a prime.*
(3) $|\mathrm{Sz}(q)| = q^2(q^2 + 1)(q - 1)$*, and* $q = 2^{2m+1}, m > 0$*.*
(4) $|\mathrm{R}(q)| = q^3(q^3 + 1)(q - 1)$*, where* $q = 3^{2m+1}, m > 0$*.*

3. The Short Presentation Conjecture

In [BS84] the following conjecture is formulated:

Conjecture: Every finite simple group of order n has a presentation by generators and relations of length $\leq \log^C n$, where $C > 0$ is a constant.

There is plenty of evidence for this conjecture, in particular the following results are proved in [BGKLP97]:

Theorem 3.1. *If the Short Presentation Conjecture holds for all finite simple groups with some constant* $C \geq 2$*, then every finite group* G *has a presentation of length* $O(\log^{C+1} G)$*.*

Theorem 3.2. *The Short Presentation Conjecture holds, with* $C = 2$*, for all finite simple groups, with the possible exception of the rank 1 twisted groups of Lie type, namely:* $\mathrm{PSU}(3, q)$*,* $\mathrm{Sz}(q)$ *and* $\mathrm{R}(q)$*.*

Conditional on the Short Presentation Conjecture the membership problem for a group can be checked in $\mathrm{NP} \cap \mathrm{coNP}$, more precisely:

Theorem 3.3 ([BS84],[BGKLP97])**.** *Let* G *be a finite group, such that none of its composition factors is one of the rank 1 twisted groups of Lie type. Then the group membership problem for* G *is in* $\mathrm{NP} \cap \mathrm{coNP}$*.*

4. Main Result

We will impose conditions on the prime p, such that none of the exceptional family of groups $\mathrm{PSU}(3, q)$, $\mathrm{Sz}(q)$, $\mathrm{R}(q)$ can occur as the composition factors of any subgroup H of $\mathrm{PSL}(2, p)$. Since the order of the composition factors of the subgroup H have to divide the order of $\mathrm{PSL}(2, p)$, an obvious way to ensure that these subgroups do not occur is to make sure that their orders cannot possibly divide the order of $\mathrm{PSL}(2, p)$ for the prime we select.

Suppose we pick primes p such that $p \equiv 3, 5 \mod 8$, then the largest power of 2 that can divide $|\mathrm{PSL}(2, p)|$ is 4, hence $\mathrm{Sz}(q)$ cannot occur in the composition factors (since 8 divides $|\mathrm{Sz}(q)|$). To exclude the possiblity that $\mathrm{R}(q)$ or $\mathrm{PSU}(3, q)$ occur as composition factors of subgroups of $\mathrm{PSL}(2, p)$ it suffices to pick primes p, such that both $p + 1$ and $p - 1$ are squarefree (in fact it suffices to pick them to be cube-free). We will now show that there are many such primes:

Theorem 4.1. *Let* $\mathcal{A} = \{p \leq x \mid p$ *a prime*$\}$. *Define* $\mathcal{A}_d$ *to be the set* $\{p \in \mathcal{A} \mid p \equiv \pm 1 \mod d^2\}$. *Let* $S(x)$ *be the number of primes* $p \leq x$ *such that* $p+1$ *and* $p-1$ *are not divisible by any prime* q^2, *where* $q > 2$. *Then*

$$S(x) = \left(2\prod_{p\neq 2}\left(1 - \frac{1}{p(p-1)}\right) - 1\right)\text{Li }(x) + o(\text{Li}(x)).$$

Proof : By inclusion-exclusion we can write the following expression for $S(x)$:

$$\begin{aligned} S(x) &= |\mathcal{A}| - \sum_{\substack{p^2 \leq x \\ p\neq 2}} |\mathcal{A}_p| + \sum_{\substack{(pq)^2 \leq x \\ p\neq 2, q\neq 2}} |\mathcal{A}_{(pq)}| - \cdots \\ &= |\mathcal{A}| + \sum_{\substack{4 < d^2 \leq x \\ \gcd(d,2)=1}} \mu(d)|\mathcal{A}_d| \end{aligned}$$

where $\mu(d)$ is the Möbius function.

Since $\gcd(p+1, p-1) = 2$ if p is odd, we have $|\mathcal{A}_d| = |\{p \leq x \mid p \equiv 1 \mod d^2\}| + |\{p \leq x \mid p \equiv -1 \mod d^2\}|$. We know by the prime number theorem in arithmetic progressions that each of these terms is well approximated by the function $\frac{1}{\varphi(d^2)}\text{Li }(x)$. Thus we set

$$|\mathcal{A}_d| = \frac{2}{\varphi(d^2)}\text{Li }(x) + E_d(x), d > 1$$

and

$$|\mathcal{A}| = \text{Li }(x) + E(x).$$

Where $E_d(x)$ is the error term in this approximation. Substituting in the expression for $S(x)$ we get:

$$\begin{aligned} S(x) &= \text{Li }(x) + \text{Li }(x)\sum_{4<d^2\leq x}\frac{2\mu(d)}{\varphi(d^2)} + \sum_{d^2\leq x} E_d(x) \\ &= \text{Li }(x)\left\{\left(2\prod_{p\neq 2}\left(1-\frac{1}{p(p-1)}\right) - 1\right) - \sum_{d^2>x}\frac{2\mu(d)}{\varphi(d^2)}\right\} + \sum_{d^2\leq x} E_d(x). \end{aligned}$$

Now

$$2\sum_{d^2>x}\frac{\mu(d)}{\varphi(d^2)} \leq 2\sum_{d^2>x}\frac{1}{\varphi(d^2)}.$$

Also

$$\begin{aligned} \varphi(n) &= n\prod_{p\backslash n}(1-\frac{1}{p}) \\ &\geq n\prod_{p\leq x}(1-\frac{1}{p}). \end{aligned}$$

By Mertens theorem $\prod_{p\leq x}(1-\frac{1}{p}) \asymp \frac{1}{\log\log n}$, so we have $\varphi(n) = \Omega(\frac{n}{\log\log n})$. Thus

$$\begin{aligned} \sum_{d^2>x}\frac{1}{\varphi(d^2)} &= O\left(\sum_{d^2>x}\frac{\log\log d}{d^2}\right) \\ &= O\left(\sum_{d^2>x}\frac{1}{d^{1.5}}\right) \\ &= O\left(\frac{1}{x^{\frac{1}{4}}}\right). \end{aligned}$$

Thus

$$S(x) = \left(2\prod_{p\neq 2}\left(1-\frac{1}{p(p-1)}\right)-1\right)\text{Li }(x) + o(\text{Li }(x)) + \sum_{d^2\leq x} E_d(x).$$

We can split up the error term as follows:

$$\sum_{d^2\leq x} E_d(x) = \sum_{d^2\leq \frac{\sqrt{x}}{\log^D x}} E_d(x) + \sum_{\frac{\sqrt{x}}{\log^D x}<d^2\leq x} E_d(x).$$

The famous Bombieri result states that for any $C > 1$, there is a $D > 0$ such that

$$\sum_{d\leq \frac{\sqrt{x}}{\log^D x}} E_d(x) = O\left(\frac{x}{\log^C x}\right)$$

(see for example [Dav00] chapter 28).

Thus applying this we get that the first sum is $o(\text{Li }(x))$. Now clearly $E_d(x) = O\left(\frac{x}{d^2}\right)$, so

$$\begin{aligned}\sum_{\frac{\sqrt{x}}{\log^D x}<d^2\leq x} E_d(x) &= O\left(\sum_{\frac{x^{\frac{1}{4}}}{\log^D x}<d\leq\sqrt{x}} \frac{x}{d^2}\right)\\ &= O\left(x\sum_{\frac{x^{\frac{1}{4}}}{\log^D x}<d\leq\sqrt{x}} \frac{1}{d^2}\right)\\ &= O\left(x^{\frac{3}{4}}\log^E x\right) \text{ where } E>0 \text{ is a constant.}\end{aligned}$$

Thus the theorem follows. □

The following results can be proved similarly:

Theorem 4.2. *Let* $\mathcal{A}_a = \{p \leq x \mid p$ *a prime*, $p \equiv a \mod 8\}$, $(a \in \{3,5\})$, *and* $S(x) = |\{p \in \mathcal{A}_a \mid p - 1$ *and* $p+1$ *are not divisible by* $p^2, p > 2\}|$. *Then*

$$S(x) = \frac{\text{Li }(x)}{4}\left(2\prod_{p\neq 2}\left(1-\frac{1}{p(p-1)}\right)-1\right) + o(\text{Li }(x)).$$

Theorem 4.3. *Let* $\mathcal{A}_a = \{p \leq x \mid p$ *a prime*, $p \equiv a \mod 8\}$, $(a \in \{3,5\})$, *and* $S(x) = |\{p \in \mathcal{A}_a \mid p - 1$ *and* $p+1$ *are not divisible by* $p^3, p > 2\}|$. *Then*

$$S(x) = \frac{\text{Li }(x)}{4}\left(2\prod_{p\neq 2}\left(1-\frac{1}{p^2(p-1)}\right)-1\right) + o(\text{Li }(x)).$$

Thus we have proved the following result:

Theorem 4.4. *If* p *is a prime* $p \equiv 3,5 \mod 8$ *such that* $p-1$ *and* $p+1$ *are not divisible by any cube, then the subgroup membership problem for* $\text{PSL}(2,p)$ *is in* $\text{NP}\cap\text{coNP}$. *Further the number of such primes below a bound* x *is asymptotic to*

$$\frac{\text{Li }(x)}{2}\left(2\prod_{p\neq 2}\left(1-\frac{1}{p^2(p-1)}\right)-1\right).$$

Since $\left(2\prod_{p\neq 2}\left(1-\frac{1}{p^2(p-1)}\right)-1\right) > 0.86$, we have that for nearly half of all the primes the subgroup membership problem for $\text{PSL}(2,p)$ is in $\text{NP}\cap\text{coNP}$.

5. Conclusion

We have shown that there are a lot of primes for which the subgroup membership problem for $\mathrm{PSL}(2,p)$ is in $\mathrm{NP} \cap \mathrm{coNP}$. The problem is unlikely to be easier than this since there are conections with the discrete log problem over prime fields. The natural question to ask is whether for every prime p the subgroup membership problem for $\mathrm{PSL}(2,p)$ is in $\mathrm{NP} \cap \mathrm{coNP}$. This might be true independent of verifying the Short Presentation Conjecture for the exceptional family of groups. We have used only a trivial property of $\mathrm{PSL}(2,p)$ namely its order to exclude having the exceptional family of groups in the composition factors. One could try to use more structural information of both $\mathrm{PSL}(2,p)$ and the exceptional groups. For example, the 2-Sylow subgroup of the Ree groups $R(q)$ is elementary abelian of order 8, whereas the 2-Sylow subgroup of $\mathrm{PSL}(2,p)$, where $p \equiv 3, 5 \mod 8$ is of order 4, so the Ree groups can be directly excluded from consideration. Another direction to proceed would be to completely characterize *all* groups that can have one of the exceptional groups in their composition series and thereby explicitly find all families of groups for which the membership problem is provably in $\mathrm{NP} \cap \mathrm{coNP}$.

References

[BB93] Babai, L; Beals, R.; *Las Vegas algorithms for matrix groups.*, Proc. 34th IEEE FOCS, 427 - 436, 1993.

[BB97] Babai, L; Beals, R.; *A Polynomial-time theory of black-box groups I*, Proceedings of Groups St. Andrews 1997. 30-64, Lond. Math. Soc. Lecture Notes Series. 260, Cambridge Univ. Press, 1999.

[BGKLP97] Babai, L.; Goodman, A., J.; Kantor, W., M.; Luks, E., M., and Pálfy, P., P.; *Short Presentations for Finite Groups*, J. Algebra, **(194)**, no. 1, 79-112, 1997.

[BS84] Babai Lászlo and M. Szemerédi. *On the complexity of matrix group problems I.* Proc. 25th IEEE Symposium on Foundations of Computer Science, 229-240, 1984.

[CFKL] Cai, Jin-Yi; Fuchs, Wolfgang H.; Kozen, Dexter; and Liu, Zicheng; *Efficient Average-Case Algorithms for the Modular Group*, Proc. 35th IEEE. Symp. Foundations of Computer Science, Nov. 1994.

[Dav00] Davenport, Harold; *Multiplicative Number Theory*, 3rd ed., Springer-Verlag, 2000.

[Gor68] Gorenstein, Daniel. *Finite Groups*, Harper & Row publishers, 1968.

[Lu92] Luks, E. M.; *Computing in solvable matrix groups*, Proc. 33rd IEEE FOCS, 111-120, 1992.

[Ree61] Ree, R; *A family of simple groups associated with the simple Lie algebra of type* (G_2), Amer. J. Math., **(83)**, 432-462, 1961.