Construction of some subgroups in black box groups $\mathrm{PGL}_2(q)$ and $(\mathrm{P})\mathrm{SL}_2(q)$

Alexandre Borovik* and Şükrü Yalçınkaya†

Abstract

For the black box groups X encrypting $\mathrm{PGL}_2(q)$, q odd, we propose an algorithm constructing a subgroup encrypting Sym_4 and subfield subgroups of X. We also present the analogous algorithms for black box groups encrypting $(\mathrm{P})\mathrm{SL}_2(q)$.

1 Introduction

It becomes apparent that the groups $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$, q odd, play a fundamental role in the constructive recognition of black box groups of Lie type of odd characteristic [6]. This paper provides the fundamentals for the algorithms presented in [6], that is, we present polynomial time Las Vegas algorithms constructing black box subgroups encrypting Sym_4 and subfield subgroups of black box groups encrypting $\mathrm{PGL}_2(q)$. We also describe the corresponding algorithms for the black box groups encrypting $(\mathrm{P})\mathrm{SL}_2(q)$.

In this paper, we use description of $\mathrm{PGL}_2(q)$ as the semidirect product $\mathrm{PGL}_2(q) = \mathrm{PSL}_2(q) \rtimes \langle \delta \rangle$ where δ is a diagonal automorphism of $\mathrm{PSL}_2(q)$ of order 2. We refer the reader to [10, Chapter XII] or [21, Chapter 3.6] for the subgroup structure of $(\mathrm{P})\mathrm{SL}_2(q)$.

A black box group X is a black box (or an oracle, or a device, or an algorithm) operating with 0-1 strings of bounded length which encrypt (not necessarily in a unique way) elements of some finite group G. The functionality of the black box is specified by the following axioms: the black box

BB1 produces strings encrypting random elements from G;

BB2 computes a string encrypting the product of two group elements given by strings or a string encrypting the inverse of an element given by a string; and

BB3 compares whether two strings encrypt the same element in G.

*School of Mathematics, University of Manchester, UK; alexandre@borovik.net
†Nesin Mathematics Village, Izmir, Turkey; sukru.yalcinkaya@gmail.com

In this setting we say that black box group X *encrypts* G.

A typical example is provided by a group G generated in a big matrix group $\mathrm{GL}_n(p^k)$ by several matrices $g_1, \ldots, g_l$. The product replacement algorithm [9] produces a sample of (almost) independent elements from a distribution on G which is close to the uniform distribution (see the discussion and further development in [2, 3, 7, 11, 14, 16, 18, 17, 19]). We can, of course, multiply, invert, compare matrices. Therefore the computer routines for these operations together with the sampling of the product replacement algorithm run on the tuple of generators $(g_1, \ldots, g_l)$ can be viewed as a black box X encrypting the group G. The group G could be unknown—in which case we are interested in its isomorphism type—or it could be known, as it happens in a variety of other black box problems.

Unfortunately, an elementary task of determining the order of a string representing a group element involves either integer factorisation or discrete logarithm. Nevertheless black box problems for matrix groups have a feature which makes them more accessible:

BB4 We are given a *global exponent* of X, that is, a natural number E such that it is expected that $x^E = 1$ for all elements $x \in X$ while computation of x^E is computationally feasible.

Usually, for a black box group X arising from a subgroup in the ambient group $\mathrm{GL}_n(p^k)$, the exponent of $\mathrm{GL}_n(p^k)$ can be taken for a global exponent of X.

In this paper, we assume that all our black box groups satisfy assumptions BB1–BB4.

A randomized algorithm is called *Las Vegas* if it always returns a positive answer or fails with some probability of error bounded by the user, see [1] for a discussion of randomized algorithms.

We refer reader to [5] for a more detailed discussion of black box groups and the nature of the problems in black box group theory.

Our principal result is the following.

Theorem 1.1. *Let X be a black box group encrypting $\mathrm{PGL}_2(p^k)$ where p is a known odd prime and k is unknown. Then there exists a Las Vegas algorithm constructing a subgroup encrypting Sym_4 and, if $p \neq 5$, a black box subfield subgroup $\mathrm{PGL}_2(p)$.*

The running time of the algorithm is $O(\xi(\log\log q + 1) + \mu(k \log\log q \log q + \log q))$, where μ is an upper bound on the time requirement for each group operation in X and ξ is an upper bound on the time requirement, per element, for the construction of random elements of X.

Corollary 1.2. *Let X be a black box group encrypting $\mathrm{(P)SL}_2(p^k)$ where p is a known odd prime and k is unknown. Then there exists a Las Vegas algorithm constructing a subgroup encrypting*

(i) Alt_4 *or* Sym_4 *when* $q \equiv \pm 3 \ mod\ 8$ *or if* $q \equiv \pm 1\ mod\ 8$*, respectively, if* $X \cong \mathrm{PSL}_2(p^k)$*, and the normalizer* N *of a quaternion group, if* $X \cong \mathrm{SL}_2(p^k)$*; and*

(ii) *if* $p \neq 5, 7$ *a subfield subgroup* $\mathrm{(P)SL}_2(p)$*.*

The running time of the algorithm is $O(\xi(\log\log q + 1) + \mu(k \log\log q \log q + \log q))$*, where* μ *is an upper bound on the time requirement for each group operation in* X *and* ξ *is an upper bound on the time requirement, per element, for the construction of random elements of* X*.*

Corollary 1.3. *Let* X *be a black box group encrypting* $\mathrm{PGL}_2(p^k)$ *or* $\mathrm{(P)SL}_2(p^k)$ *where* p *is a known odd prime with known* k*. Then, for any divisor* $a > 1$ *of* k*, there exists a Las Vegas algorithm constructing a black box subgroup encrypting a subfield subgroup* $\mathrm{PGL}_2(p^a)$ *or* $\mathrm{(P)SL}_2(p^a)$*, respectively.*

2 Subfield subgroups and Sym_4 in $\mathrm{PGL}_2(p^k)$

Let $G \cong \mathrm{PGL}_2(q)$, $q = p^k$, p an odd prime. Note that G has two conjugacy classes of involutions, say $\pm$-type involutions, where the order of the centralizer of a $+$-type involution is $2(q-1)$ and the order of the centralizer of a $-$-type involution is $2(q+1)$. Notice that $C_G(i) = T \rtimes \langle w \rangle$ where T is a torus of order $(q \pm 1)$ and w is an involution inverting T. Throughout the paper, we consider the involutions of $+$-type if $q \equiv 1 \bmod 4$ and $-$-type if $q \equiv -1 \bmod 4$ so that the order of the torus T is always divisible by 4; we call them involutions of *right type*.

We set 5-tuple

$$(i, j, x, s, T) \tag{1}$$

where $i \in G$ is an involution of right type, $T < G$ is the torus in $C_G(i)$, $j \in G$ is an involution of right type which inverts T, $x \in G$ is an element of order 3 normalising $\langle i, j \rangle$ and $s \in T$ is an element of order 4. We also set $k = ij$ and note that k is also of right type. Clearly $V = \langle i, j \rangle$ is a Klein 4-subgroup and $\langle i, j, x \rangle \cong \mathrm{Alt}_4$. Moreover, we have $\langle i, j, x, s \rangle \cong \mathrm{Sym}_4$.

An alternative and slightly easier construction of Sym_4 in $\mathrm{PGL}_2(q)$ is as follows. Let $i, j \in G \cong \mathrm{PGL}_2(q)$ be involutions of right type where j inverts the torus in $C_G(i)$, choosing the elements t_i, t_j of order 4 in the tori in $C_G(i)$ and $C_G(j)$, respectively, we have $\mathrm{Sym}_4 \cong \langle t_j, t_j \rangle$. However, such a construction of Sym_4 in $\mathrm{PGL}_2(q)$ does not cover the corresponding construction of Alt_4 in $\mathrm{PSL}_2(q)$ when $q \equiv \pm 3 \bmod 8$, see Remark 2.1 (1). For the sake of completeness, we follow the setting in (1).

Remark 2.1.

(1) If $G \cong \mathrm{PSL}_2(q)$, then G has only one conjugacy classes of involutions and $C_G(i) = T \rtimes \langle w \rangle$ where $|T| = (q-1)/2$ if $q \equiv 1 \bmod 4$, and $|T| = (q+1)/2$ if $q \equiv -1 \bmod 4$. Therefore T contains element of order 4 if and

only if $q \equiv \pm 1 \bmod 8$. Thus, we can construct subgroups isomorphic to Sym_4 in G precisely when $q \equiv \pm 1 \bmod 8$. Otherwise, the subgroup Alt_4 will be constructed. We shall note here that Alt_4 or Sym_4 are maximal subgroups of $\mathrm{PSL}_2(p)$ if $p \equiv \pm 1 \bmod 8$ or $p \equiv \pm 3 \bmod 8$, respectively [13, Proposition 4.6.7].

(2) If $G \cong \mathrm{SL}_2(q)$, then i, j are pseudo-involutions (whose squares are the central involution in $\mathrm{SL}_2(q)$) and $V = \langle i, j \rangle$ is a quaternion group. Moreover, if $q \equiv \pm 3 \bmod 8$ ($q \equiv \pm 1 \bmod 8$, respectively), the subgroup $\langle i, j, x \rangle$ ($\langle i, j, s, x \rangle$, respectively) is $N_G(V)$, where s is an element of order 8 in $C_G(i)$.

The main ingredient of the algorithm in the construction of Sym_4 and subfield subgroups of $G \cong \mathrm{PGL}_2(q)$ is to construct an element $x \in G$ of order 3 permuting some mutually commuting involutions $i, j, k \in G$ of right type. The following lemma provides explicit construction of such an element.

Lemma 2.2. *Let $G \cong \mathrm{PGL}_2(q)$, q odd, i, j, k mutually commuting involutions of right type. Let $g \in G$ be an arbitrary element. Assume that $h_1 = ij^g$ has odd order m_1 and set $n_1 = h_1^{\frac{m_1+1}{2}}$ and $s = k^{gn_1^{-1}}$. Assume also that $h_2 = js$ has odd order m_2 and set $n_2 = h_2^{\frac{m_2+1}{2}}$. Then the element $x = gn_1^{-1}n_2^{-1}$ permutes i, j, k and x has order* 3.

Proof. Observe first that $i^{n_1} = j^g$ and $j^{n_2} = s$. Then, since $s = k^{gn_1^{-1}}$, we have $j^{n_2} = k^{gn_1^{-1}}$. Hence $j = k^{gn_1^{-1}n_2^{-1}} = k^x$. Now, we prove that $j^x = i$. Since $j^{gn_1^{-1}} = i$, we have $j^x = j^{gn_1^{-1}n_2^{-1}} = i^{n_2^{-1}}$. We claim that $h_2 \in C_G(i)$, which implies that $n_2 \in C_G(i)$, so $j^x = i^{n_2^{-1}} = i$. Now, since $j \in C_G(i)$, $h_2 = js \in C_G(i)$ if and only if $s = k^{gn_1^{-1}} \in C_G(i)$. Recall that $i^{n_1} = j^g$. Therefore $s \in C_G(i)$ if and only if $k^g \in C_G(j^g)$, equivalently, $k \in C_G(j)$ and the claim follows. It is now clear that $i^x = k$ since $ij = k$. It is clear that $x \in N_G(V)$ where $V = \langle i, j \rangle$ and x has order 3. □

Lemma 2.3. *Let G, h_1 and h_2 be as in Lemma* 2.2. *Then the probability that h_1 and h_2 have odd orders is bounded from below by $1/2 - 1/2q$.*

Proof. We first note that the subgroup $\langle i, x \rangle \cong \mathrm{Alt}_4$ is a subgroup of $L \leq G$ where $L \cong \mathrm{PSL}_2(p)$, so the involutions i, j, k belong to a subgroup isomorphic to $\mathrm{PSL}_2(q)$. Therefore it is enough to compute the estimate in $H \cong \mathrm{PSL}_2(q)$. Notice that all involutions in H are conjugate. Therefore the probability that h_1 and h_2 have odd orders is the same as the probability of the product of two random involutions from H to be of odd order.

We denote by a one of these numbers $(q \pm 1)/2$ which is odd and by b the other one. Then $|H| = q(q^2 - 1)/2 = 2abq$ and $|C_H(i)| = 2b$ for any involution $i \in H$. Hence the total number of involutions is

$$\frac{|H|}{|C_H(i)|} = \frac{2abq}{2b} = aq.$$

Now we shall compute the number of pairs of involutions (i, j) such that their product ij belongs to a torus of order a. Let T be a torus of order a. Then $N_H(T)$ is a dihedral group of order $2a$. Therefore the involutions in $N_H(T)$ form the coset $N_H(T)\backslash T$ since a is odd. Hence, for every torus of order a, we have a^2 pairs of involutions whose product belong to T. The number of tori of order a is $|H|/|N_H(T)| = 2abq/2a = bq$. Hence, there are bqa^2 pairs of involutions whose product belong to a torus of order a. Thus the desired probability is

$$\frac{bqa^2}{(aq)^2} = \frac{b}{q} \geqslant \frac{q-1}{2q} = \frac{1}{2} - \frac{1}{2q}.$$

□

For the subfield subgroups isomorphic to $\mathrm{PGL}_2(p^a)$ of $G \cong \mathrm{PGL}_2(q)$, $q = p^k$, p an odd prime, we extend our setting in (1) and set 6-tuple

$$(i, j, x, s, r, T) \tag{2}$$

where $r \in T$ has order $(p^a \pm 1)$ where $(p^a \pm 1)/2$ is even. Notice that if a is a divisor of k, then the torus T contains an element r of order $(p^a \pm 1)$ where $(p^a \pm 1)/2$ is even. The following lemma provides explicit generators of the subfield subgroups of G.

Lemma 2.4. *Let $G \cong \mathrm{PGL}_2(q)$, $q = p^k$ for some $k \geqslant 2$ and (i, j, x, s, r, T) be as in* (2)*. Then $\langle r, x\rangle \cong \mathrm{PGL}_2(p^a)$ except when $a = 1$ and $p = 5$.*

Proof. Let $L = \langle i, j, x, s\rangle \cong \mathrm{Sym}_4 \cong \mathrm{PGL}_2(3)$. Observe that L is a subgroup of some $H \leqslant G$ where $H \cong \mathrm{PGL}_2(p)$. Now assume first that $a = 1$. Since $r \in C_G(i)$, the order of the subgroup $T \cap H$ is $p \pm 1$. Since T is cyclic, it has only one subgroup of order $p \pm 1$ so $r \in H$. Thus $\langle r, x\rangle \leqslant H$. By the subgroup structure of $\mathrm{PGL}_2(p)$, the subgroup $L \cong \mathrm{Sym}_4$ is either a maximal subgroup or contained in a maximal subgroup of H isomorphic to $\mathrm{Sym}_4 \rtimes \langle\delta\rangle$ where δ is a diagonal automorphism of $\mathrm{PSL}_2(q)$. Hence, if $|r| \geqslant 7$, or equivalently $p \geqslant 7$, then we have $\langle r, x\rangle = H$ since such a maximal subgroup does not contain elements of order bigger than 7. As we noted above, if $p = 3$, then $L \cong \mathrm{Sym}_4 \cong \mathrm{PGL}_2(3)$.

Observe that if $a > 1$ and a is a divisor of k, then an element r of order $p^a \pm 1$, where $(p^a \pm 1)/2$ is even, belongs to a subgroup $H \cong \mathrm{PGL}_2(p^a)$ hence the lemma follows from the same arguments above. □

Remark 2.5.

(1) Following the notation of Lemma 2.4, observe that if $a = 1$ and $p = 5$, then $|r| = 4$ and $\langle r, x\rangle \cong \mathrm{Sym}_4$.

(2) If $G \cong \mathrm{PSL}_2(q)$, then, there is one more exception in the statement of Lemma 2.4, that is, $a = 1$ and $p = 7$. This extra exception arises from the fact that the torus $T \cap H$ in the proof of Lemma 2.4 has order $(p \pm 1)/2$ and the element r has order 4. Again, we are in the situation that $\langle r, x\rangle \cong \mathrm{Sym}_4 < \mathrm{PSL}_2(7)$.

(3) If $G \cong \mathrm{SL}_2(q)$, then, by considering the pseudo-involutions, the same result in Lemma 2.4 holds with the exceptions $a = 1$ and $p = 5$ or 7.

3 The algorithm

In this section we present an algorithm for the black box group encrypting $\mathrm{PGL}_2(p^k)$ and the corresponding algorithm for the groups $(\mathrm{P})\mathrm{SL}_2(p^k)$ follows from Remarks 2.1 and 2.5.

In order to cover the algorithm in Corollary 1.3, we assume below that a divisor a of k is given as an input. Observe that such an input is not needed for the construction of a subfield subgroup $\mathrm{PGL}_2(p)$.

Algorithm 3.1. *Let X be a black box group isomorphic to $\mathrm{PGL}_2(q)$, $q = p^k$, p an odd prime.*

Input:
- *A set of generators of X.*
- *The characteristic p of the underlying field.*
- *An exponent E for X.*
- *A divisor a of k.*

Output:
- *A black box subgroup encrypting Sym_4.*
- *A black box subgroup encrypting $\mathrm{PGL}_2(p^a)$ except when $a = 1$ and $p = 5$.*

Outline of Algorithm 3.1 (a more detailed description follows below):

1. Find the size of the field $q = p^k$ (This step is not needed for Corollary 1.3).
2. Construct an involution $i \in X$ of right type from a random element together with a generator t of the torus $T < C_X(i)$ and a Klein 4-group $V = \langle i, j \rangle$ in X where j is an involution of right type.
3. Construct an element x of order 3 in $N_X(V)$.
4. Set $s = t^{|T|/4}$ and deduce that $\langle s, x \rangle \cong \mathrm{Sym}_4$.
5. Set $r = t^{|T|/(p^a \pm 1)}$ where $(p^a \pm 1)/2$ is even and deduce that $\langle r, x \rangle \cong \mathrm{PGL}_2(p^a)$ except when $a = 1$ and $p = 5$.

Now we give a more detailed description of Algorithm 3.1.

Step 1: We compute the size q of the underlying field by Algorithm 5.5 in [22].

Step 2: Let $E = 2^k m$ where $(2, m) = 1$. Take an arbitrary element $g \in X$. If the order of g is even, then the last non-identity element in the following sequence is an involution

$$1 \neq g^m, g^{2m}, g^{2^2 m}, \ldots, g^{2^k m} = 1.$$

Let $i \in X$ be an involution constructed as above. Then, we construct $C_X(i)$ by the method described in [4, 8] together with the result in [20].

To check whether i is an involution of right type, we construct a random element $g \in C_X(i)$ and consider $g^{q\pm1}$. If $|g| > 2$ and $g^{q+1} \neq 1$, then i is of $+$-type. We follow the analogous process to check whether i is of $-$-type. We have $C_X(i) = T \rtimes \langle w \rangle$ where T is a torus of order $q \pm 1$ and w is an involution which inverts T. Observe that the coset Tw consists of involutions inverting T, so half of the elements of $C_X(i)$ are the involutions inverting T and half of the involutions in Tw are of the same type as i. We check whether j has the same type as i by following the same procedure above. Let $j \in C_X(i)$ be such an involution, then, clearly, $V = \langle i, j \rangle$ is a Klein 4-group. For the construction of a generator of T, notice that a random element of $C_X(i)$ is either an involution inverting T or an element of T and, by [15], the probability of finding a generator of a cyclic group of order $q \pm 1$ is at least $O(1/\log\log q)$. Since $|T|$ is divisible by 4, we can find an element $t \in C_X(i)$ such that $t^2 \neq 1$ and $t^{|T|/2} \neq 1$ with probability at least $O(1/\log\log q)$ and such an element is a generator of T.

Step 3: By Lemmas 2.2 and 2.3, we can construct an element x of order 3 normalizing $V = \langle i, j \rangle$ with probability at least $1/2 - 1/2q$.

Step 4: Since the order T is divisible by 4, we set $s = t^{|T|/4}$ and we can deduce that $\langle s, x \rangle \cong \mathrm{Sym}_4$ from the discussion in the beginning of Section 2.

Step 5: It follows from Lemma 2.4 that the subgroup $\langle r, x \rangle$ encrypts a black box group $\mathrm{PGL}_2(p^a)$ except when $a = 1$ and $p = 5$.

Following the arguments in Remarks 2.1 and 2.5, we have the corresponding algorithms for the black box groups encrypting $(\mathrm{P})\mathrm{SL}_2(q)$.

3.1 Complexity

Let μ be an upper bound on the time requirement for each group operation in X and ξ an upper bound on the time requirement, per element, for the construction of random elements of X.

We outline the running time of Algorithm 3.1 for each step as presented in the previous section. For simplicity, we assume that $E = |X| = |\mathrm{PGL}_2(q)| = q(q^2 - 1)$.

Step 1 First, random elements in X belong to a torus of order $q-1$ or $q+1$ with probability at least $1 - O(1/q)$. Then, in each type of tori, by [15], we can find an elements of order $q-1$ and $q+1$ with probability $c/\log\log q$ for some constant c. Therefore, producing $m = O(\log\log q)$ elements $g_1, \ldots, g_m$, we assume that one of g_i has order $q-1$ and g_j has order $q+1$. Now, checking each $g_i^{p(p^{2\ell}-1)} = 1$ involves at most $\log p^{2\ell+1}$ group operations making the overall cost to determine the exact power of p involving in $q = p^k$,

$$\sum_{\ell=1}^{k} \log(p^{2\ell+1}) = \log p^{k^2+2k} = (k+2)\log q.$$

Hence the size of the field can be computed in time $O(k\mu \log\log q \log q + \xi \log\log q)$.

Step 2 By [12, Corollary 5.3], random elements in X have even order with probability at least 1/4. Then, construction of an involution i from a random element and checking whether an element of the form ii^g has odd order for a random element involves constant number of construction of a random element in X and $C_X(i)$ and $\log E \leq \log q^3$ group operations by repeated square and multiply method. Checking whether an involution is of desired type involves $\log E$ group operations. By [15], we can find a generator for the torus $T \leq C_X(i)$ with probability $O(1/\log\log q)$ and checking whether it is indeed a generator of T involves $\log q$ group operations. Hence we can construct involutions i, j of desired type and a generator t of the torus T in time $O(\xi(1 + \log\log q) + \mu \log\log q \log q)$.

Step 3 By Lemma 2.3 the elements $h_1 = ij^g$ and $h_2 = jk^{gu_1^{-1}}$ have odd orders m_1 and m_2 with probability $1/2 - 1/2q$. Checking both elements for having odd order and construction of elements $h_1^{\frac{m_1+1}{2}}$ and $h_2^{\frac{m_2+1}{2}}$ involves $\log E$ group operations making overall cost $O(\xi + \mu \log q)$ to construct an element x of order 3 permuting the involutions i, j, k of right type.

Step 4 The element s can be constructed in time $O(\mu \log q)$.

Step 5 The element r can be constructed in time $O(\mu \log q)$.

Combining the running times of the steps above, the overall running time of the algorithm for the construction of Sym_4 and $\mathrm{PGL}_2(p^k)$ is $O(\xi(\log\log q + 1) + \mu(k \log\log q \log q + \log q))$.

Observe that the algorithm presented in Section 3 together with Remarks 2.1 and 2.5 and the computation of the complexity above gives a proof of Theorem 1.1 and Corollaries 1.2 and 1.3.

References

[1] L. Babai, *Randomization in group algorithms: conceptual questions*, Groups and Computation II (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, RI, 1997, pp. 1–17.

[2] L. Babai and I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000) (New York), ACM, 2000, pp. 627–635.

[3] L. Babai and I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, J. Algorithms **50** (2004), no. 2, 215–231, SODA 2000 special issue.

[4] A. V. Borovik, *Centralisers of involutions in black box groups*, Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 7–20.

[5] A. V. Borovik and Ş. Yalçınkaya, *Fifty shades of black*, Available at arXiv:1308.2487.

[6] A. V. Borovik and Ş. Yalçınkaya, *Revelations and reifications: Adjoint representations of black box groups* $\mathrm{SL}_2(q)$, in preparation.

[7] S. Bratus and I. Pak, *On sampling generating sets of finite groups and product replacement algorithm (extended abstract)*, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC) (New York), ACM, 1999, pp. 91–96.

[8] J. N. Bray, *An improved method for generating the centralizer of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245.

[9] F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien, *Generating random elements of a finite group*, Comm. Algebra **23** (1995), no. 13, 4931–4948.

[10] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover Publications Inc., New York, 1958.

[11] A. Gamburd and I. Pak, *Expansion of product replacement graphs*, Combinatorica **26** (2006), no. 4, 411–429.

[12] I. M. Isaacs, W. M. Kantor, and N. Spaltenstein, *On the probability that a group element is p-singular*, J. Algebra **176** (1995), no. 1, 139–181.

[13] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.

[14] A. Lubotzky and I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363.

[15] D. S. Mitrinović, J. Sándor, and B. Crstici, *Handbook of number theory*, Mathematics and its Applications, vol. 351, Kluwer Academic Publishers Group, Dordrecht, 1996.

[16] I. Pak, *The product replacement algorithm is polynomial*, 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000), IEEE Comput. Soc. Press, Los Alamitos, CA, 2000, pp. 476–485.

[17] I. Pak, *The product replacement algorithm is polynomial*, Proc. FOCS'2000, The 41st Ann. Symp. on Foundations of Comp. Sci. (2001), 476–485.

[18] I. Pak, *What do we know about the product replacement algorithm?*, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 301–347.

[19] I. Pak and A. Żuk, *On Kazhdan constants and mixing of random walks*, Int. Math. Res. Not. (2002), no. 36, 1891–1905.

[20] C. W. Parker and R. A. Wilson, *Recognising simplicity of black-box groups by constructing involutions and their centralisers*, J. Algebra **324** (2010), no. 5, 885–915.

[21] Michio Suzuki, *Group theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin, 1982.

[22] Ş. Yalçınkaya, *Black box groups*, Turkish J. Math. **31** (2007), no. suppl., 171–210.