Turkish Journal of Mathematics

Volume 40 | Number 4 Article 20

1-1-2016

A contribution to the analysis of a reduction algorithm for groups with an extraspecial normal subgroup

ABDULLAH ÇAĞMAN

NURULLAH ANKARALIOĞLU

Follow this and additional works at: https://journals.tubitak.gov.tr/math

 Part of the Mathematics Commons

Recommended Citation
ÇAĞMAN, ABDULLAH and ANKARALIOĞLU, NURULLAH (2016) "A contribution to the analysis of a reduction algorithm for groups with an extraspecial normal subgroup," *Turkish Journal of Mathematics*: Vol. 40: No. 4, Article 20. https://doi.org/10.3906/mat-1506-35
Available at: https://journals.tubitak.gov.tr/math/vol40/iss4/20

This Article is brought to you for free and open access by TÜBİTAK Academic Journals. It has been accepted for inclusion in Turkish Journal of Mathematics by an authorized editor of TÜBİTAK Academic Journals. For more information, please contact academic.publications@tubitak.gov.tr.

TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2016) 40: 914 – 923
© TÜBİTAK
doi:10.3906/mat-1506-35

A contribution to the analysis of a reduction algorithm for groups with an extraspecial normal subgroup

Abdullah ÇAĞMAN[1], **Nurullah ANKARALIOĞLU**[2,*]

[1]Department of Mathematics, Faculty of Science and Letters, Ağrı İbrahim Çeçen University, Ağrı, Turkey
[2]Department of Mathematics, Faculty of Science, Atatürk University, Erzurum, Turkey

Received: 10.06.2015 • **Accepted/Published Online:** 20.11.2015 • **Final Version:** 16.06.2016

Abstract: Reduction algorithms are an important tool for understanding structural properties of groups. They play an important role in algorithms designed to investigate matrix groups over a finite field. One such algorithm was designed by Brooksbank et al. for members of the class C_6 in Aschbacher's theorem, namely groups N that are normalizers in $GL(d,q)$ of certain absolutely irreducible symplectic-type r-groups R, where r is a prime and $d = r^n$ with $n > 2$. However, the analysis of this algorithm has only been completed when $d = r^2$ and when $d = r^n$ and $n > 2$, in the latter case under the condition that $G/RZ(G) \cong N/RZ(N)$. We prove that the algorithm runs successfully for some groups in the case of $d = r^3$ without any assumption.

Key words: Extraspecial group, matrix group,reduction algorithm, algorithm analysis

1. Introduction

In 1984, Aschbacher proved in his famous paper [2] that every subgroup of $GL(d,q)$ lies in at least one of nine classes $C_1, C_2, \ldots, C_9$.

This classification is regarded as the starting point of the matrix group recognition project. One of the first published articles related to this project is Neumann and Praeger's algorithm [14], which decides whether or not a matrix group over a finite field contains the special linear group. After this paper many algorithms were designed; some examples are [1, 3, 8, 13, 15]. For a more comprehensive list of references one can see [18], and the aim and frame of the project can be found in [12].

Given groups G and H, a reduction algorithm sets up a data structure for a homomorphism $\varphi : G \to H$ with nontrivial image. Reduction algorithms are not only an important tool for understanding structural properties of groups but also form an integral part of the matrix group recognition project. If we can design a reduction algorithm for the group G, then we can find a normal subgroup N and the factor group G/N. Repeating these steps recursively, we can form a composition tree for G in which the leaves of the tree are either simple groups or constructively recognized groups in other ways. Hence, this composition tree provides a data structure in which computation in the original group can be conducted.

Up to now, there have been two important reduction algorithms. One of them is an algorithm for the groups in the classes C_3 and C_5, which is fully analyzed and so has an important value in the literature [6].

*Correspondence: ankarali@atauni.edu.tr

2010 *AMS Mathematics Subject Classification:* 20G40, 20-04, 68Q87.

The other reduction algorithm is designed for the groups in the C_6 class [5], but this algorithm has not yet been fully analyzed.

In this paper, we extend the analysis of the algorithm given in [5]. We use the GAP system [20] (http://www.gap-system.org) in our analyses.

2. Essential preliminaries and process of the analyses

2.1. Normalizers of extraspecial groups

In [2], Aschbacher defined the class C_6 as subgroups of the normalizer in $GL(d,q)$ of symplectic-type r-groups R (r prime). Symplectic-type r-groups are closely related to the extraspecial groups due to the their structure. We will be concerned only with the symplectic-type r-groups with minimal exponent. The structures of these groups outlined in [11, 19] are given in Table 1.

Table 1. Symplectic-type r-groups.

Structure of R	$\lvert R\rvert$	$\lvert Z(R)\rvert$	Notation
$\overbrace{R_0 \circ R_0 \circ \cdots \circ R_0}^{n}$	r^{1+2n}	r	r^{1+2n}
$\overbrace{D_8 \circ D_8 \circ \cdots \circ D_8}^{n}$	2^{1+2n}	2	2_+^{1+2n}
$\overbrace{D_8 \circ D_8 \circ \cdots \circ D_8}^{n-1} \circ Q_8$	2^{1+2n}	2	2_-^{1+2n}
$Z_4 \circ \overbrace{D_8 \circ D_8 \circ \cdots \circ D_8}^{n}$	2^{2+2n}	4	2^{2+2n}

In C_6 groups, the structures of the normalizers of the symplectic-type r-groups given in [5] are as follows:

$$Z\left(GL\left(d,q\right)\right) \circ r^{1+2n}.Sp\left(2n,r\right), \qquad r \text{ odd}$$

$$Z\left(GL\left(d,q\right)\right) \circ 2^{2+2n}.Sp\left(2n,2\right), \quad r=2 \text{ and } 4|q-1$$

$$Z\left(GL\left(d,q\right)\right) \circ 2_+^{1+2n}.O^+\left(2n,2\right), \qquad r=2$$

$$Z\left(GL\left(d,q\right)\right) \circ 2_-^{1+2n}.O^-\left(2n,2\right), \qquad r=2.$$

We are interested in extensions by $Sp(2n,r)$. If G is a C_6 group with $d=r^3$, then $G/(R\cap G) \cong GR/R \leq N/R \cong Sp(6,r)$. It is well known that if G is perfect, then all factor groups of G, especially $G/(R\cap G)$, are perfect. For a perfect C_6 group G, the factor group $G/(R\cap G)$ is a perfect subgroup of $Sp(6,r)$. To analyze the algorithm for perfect C_6 groups, we have to determine all perfect subgroups of the $Sp(6,r)$. These groups are firstly used in the analyses of the perfect C_6 groups and eventually in the generalization ($d=r^3$).

Any subgroup of a group G is contained in at least one of the maximal subgroups of G, and all perfect subgroups of G are contained in the soluble residual of G. We have to determine the soluble residuals of the

maximal subgroups of $Sp(6,r)$ and depending on these residuals we must find all the perfect subgroups of $Sp(6,r)$. Hence, using the maximal subgroups of $Sp(6,r)$ taken from [4, 11], the soluble residuals of maximal subgroups of $Sp(6,r)$ are determined and given in the Table 2.

Table 2. Soluble residuals of maximal subgroups of $Sp(6,r)$.

Soluble residuals of the maximal subgroups			
Maximal subgroups	$r=2$	$r=3$	$r\geq 5$
E_r^{1+4}: $((r-1)\times Sp(4,r))$	-	E_3^{1+4}:$Sp(4,3)$	E_r^{1+4}:$Sp(4,r)$
E_r^5: $((r-1)\times Sp(4,r))$	E_2^5:A_6	-	-
E_r^{3+4}: $(GL(2,r)\times Sp(2,r))$	[ ]	[ ]	E_r^{3+4}: $(SL(2,r)\times Sp(2,r))$
E_r^6:$GL(3,r)$	E_2^6:$GL(3,2)$	E_3^6:$SL(3,3)$	E_r^6:$SL(3,r)$
$Sp(2,r)\times Sp(4,r)$	A_6	$Sp(4,3)$	$Sp(2,r)\times Sp(4,r)$
$Sp(2,r)^3$:S_3	-	[ ]	$Sp(2,r)^3$
$GL(3,r).2$	-	$SL(3,3)$	$SL(3,r)$
$Sp(2,r^3):3$	$Sp(2,2^3)$	$Sp(2,3^3)$	$Sp(2,r^3)$
$GU(3,r).2$	-	$SU(3,3)$	$SU(3,r)$
$Sp(2,r)\circ GO(3,r)$	-	-	$Sp(2,r)\circ SO(3,r)$
$SO^+(6,r)$	$A_8\cong PSL(4,2)$	-	-
$SO^-(6,r)$	$PSp(4,3)\cong PSU(4,2)$	-	-
$2.A_5\cong SL(2,5)$	-	$2.A_5\cong SL(2,5)$	-
N_1	-	-	$PSU(3,3)$ $(r=11)$
$2.S_5^-$	-	-	$2.A_5\cong SL(2,5)$ $(r=7)$
$2.L_2(7).2^+$			
$2.L_2(13)$	-	$Sp(2,13)$	-
$U_3(3):2$	$PSU(3,3)$	-	-
$2\times U_3(3)$	-	-	$PSU(3,3)$ $(r=7)$
$(2\times U_3(3)).2$	-	-	$PSU(3,3)$ $(r=11)$
$2.J_2$	-	-	$2.J_2$ $(r=5)$
$2.L_2(q)$	-	-	$Sp(2,r)$ $(r\geq 7)$

"[ ]" stands for the trivial group.
"–" means that there is no group in this case.
"notation" can be found in [4].

The perfect subgroups obtained from the soluble residuals stated in Table 2 are as follows:
A_5, $2.A_5\cong SL(2,5)$, $SL(2,9)\cong 2.A_6$, $2^5.A_5$, $2^2.(A_5\times A_5)$, $5^2.A_5 2^1$, $PSL(3,2)$, $3.A_6$, $3.A_7$, $PSL(2,11)$, $2.(A_5\times A_5)$, $2.(A_5\times L_2(11))$, $2^3.L_2(3)$, A_7, $Inn(\mathbb{Z}_2 wr A_5)$, $2^6.A_5$, $PSU(3,3)$ (the notation of [9] has been used for these groups).

2.2. Strategy of the analyses

In [5], the authors designed a reduction algorithm for C_6 groups and proved the following theorem:

Theorem 2.1 *[5] Let $G \leq N_{GL(d,q)}(R)$ be a C_6 group where R is an extraspecial r-group and $d = r^n$. Then there exists a reduction algorithm from G to H where H is a permutation or matrix group.*

The algorithm described in Theorem 2.1 relies on a procedure called BlindDescent, which takes as input a group $G \leq GL(d,q)$ and $\delta > 0$ and returns as output generators for a subgroup U for which $U/(UZ(G))$ is abelian. BlindDescent chooses a random element x in G and repeats a basic step up to $48nlog(1/\delta)$ times. In the basic step first another random element y in G is chosen. Depending on the properties of x and y, the element x might be modified. If during some repetition of the basic step a generating set for a subgroup is returned, we say that BlindDescent is *successful*; otherwise, the procedure *fails*. As the procedure for BlindDescent relies in turn on several subprocedures, we have not reproduced the procedure here and instead refer the reader to [5, p. 8]. We note that the analysis of the reduction algorithm in Theorem 2.1 in [5] was only completed for the case $d = r^2$ and for the cases $d = r^n$ with $n > 2$ under the additional assumption that $G/RZ(G) \cong N/RZ(N)$. For the case $d = r$ an analyzed algorithm exists as presented by [17]. We extend the analysis to the case $d = r^3$ without any further assumptions. We obtain our result by the following steps:

1. the analyses for the soluble C_6 groups,
2. the analyses for the perfect C_6 groups,
3. the analyses for the general case $d = r^3$.

3. Analysis of the algorithm "BlindDescent"

Hypothesis 1 *Let G be a C_6 group including R as an extraspecial r-group (r prime), $d = r^3$, and let δ be a reliability parameter.*

3.1. Soluble case

We know that the derived series of a finite group G terminates either in the trivial group, if G is soluble, or in a perfect group called the "soluble residual". Thus, we investigate groups in terms of their solubility and perfectness. For soluble linear groups of degree n, Zassenhaus determined an upper bound for the derived length of the group as a function of n [21]. This bound was improved by Huppert [10] and Dixon [7]. Ultimately, Newman [16] proved the following:

Let τ be the function defined on positive rational numbers by:

$$\tau(n) = \begin{cases} 5a(n), & \text{for} \quad 9^{a(n)} \leq n \leq 16.9^{a(n)-1} \\ 5a(n)+1, & \text{for} \quad 16.9^{a(n)-1} \leq n \leq 3.9^{a(n)} \\ 5a(n)+2, & \text{for} \quad 3.9^{a(n)} \leq n \leq 4.9^{a(n)} \\ 5a(n)+3, & \text{for} \quad 4.9^{a(n)} \leq n \leq 64.9^{a(n)-1} \\ 5a(n)+4, & \text{for} \quad 64.9^{a(n)-1} \leq n \leq 9^{a(n)-1} \end{cases}$$

where $a(n) = [\log_9 n\,]$ ($[x]$ is a largest integer that is less than or equal to x).

Then

$$\rho(n)=\begin{cases}1, & \text{for} \quad n=1\\ 4, & \text{for} \quad n=2\\ 9+\tau((n-2)/8), & \text{for} \quad n\in\{6,7,17,59,60,61,62,63,64,65\}\\ 10+\tau((n-2)/8), & \text{other}\end{cases}$$

is an upper bound for the derived length of a soluble linear groups of degree n.

Lemma 3.1 *The derived length of a soluble subgroup of $Sp(6,r)$ is at most 7.*

Proof If $n=6$, then we need $\tau(1/2)$ to find $\rho(n)$. Since $a(1/2)=[\log_9 1/2]=-1$ we find $\tau(1/2)=-2$. Hence, we get $\rho(n)=7$. □

Theorem 3.1 *Suppose Hypothesis 1 holds. Assume that some iteration of the main loop in BlindDescent(G, δ) (BlindDescent is a part of the reduction algorithm [5], which has not yet been fully analyzed) generates a nonscalar $x\in H$ for some soluble subgroup H of group G. Then BlindDescent succeeds in at most eight further iterations with probability greater than $1-9\delta$.*

Proof In the main loop of BlindDescent, line 18 or 21 returns the suitable element x or generates elements x in subgroups of the derived series of H. Hence, we construct a correct x in at most seven iterations because the derived length of any soluble subgroup of $Sp(6,r)$ is at most 7 by Lemma 3.1, and so $H^{(7)}\leq R$. The probability of these iterations and the last normal subgroup computation is at least $1-9\delta$. □

3.2. Perfect case

We have to consider all soluble residuals of maximal subgroups of $Sp(6,r)$ because these subgroups are perfect, and then we analyze the other perfect subgroups of $Sp(6,r)$ obtained from these soluble residuals.

We need the following lemma to analyze the algorithms for an input group G for which $G/(R\cap G)$ is perfect.

Lemma 3.2 *Let G be a finite group and H an elementary abelian normal r-subgroup of G. If C is a fixed coset of H in G, then the conditional probability, $Prob([g,h]\neq 1|\ [g,h]\in H)$, is at least $1-1/r$ where h is a uniformly distributed random element of C and g is a fixed element of G acting nontrivially on H.*

Proof See [5, Lemma 5.1.ii]. □

Theorem 3.2 *Suppose Hypothesis 1 holds. If $S=R\cap G$ and $\overline{G}=G/S\cong A_6$ (in case $r=2$), then BlindDescent returns successfully with probability $1-\delta$ after at most $160\log(1/\delta)$ repetitions of a basic step.*

Proof Assume that the element assigned to x in any loop of BlindDecent is in $G\backslash R$ and y is the random element chosen just after this assignment. Let $\overline{x}=xS$ and $\overline{y}=yS$. One can easily see with a simple program that computes the proportion of commutative elements in A_6 that $Prob(\overline{y}\in C_{\overline{G}}(\overline{x}))\geq 1/80$. We know that:

$$\begin{aligned}Prob(\overline{y}\in C_{\overline{G}}(\overline{x})) &= Prob([\overline{x},\overline{y}]=S)\\ &= Prob(x^{-1}y^{-1}xyS=S)\\ &= Prob([x,y]\in S).\end{aligned}$$

Hence, we get $Prob\left([x,y]\in S\right)\geq 1/80$. Now let us calculate the probability of producing an element in $R\backslash Z(R)$ using BlindDescent with the aid of Lemma 3.2. If we assume that $b=xZ\left(S\right)$ and $h=yZ\left(S\right)\in gS/Z(S)$ with $g\in G$, then for any $kZ\left(S\right)\in S/Z(S)$ with $k\in S$,

$$\left(kZ\left(S\right)\right)^{b}=\left(xZ\left(S\right)\right)^{-1}kZ\left(S\right)xZ\left(S\right).$$

As $x\in G\backslash R$, we know that $x\notin Z\left(S\right)$, so the element $x^{-1}kx$ is not always an element of $Z\left(S\right)$. Henceforth, the element b acts on $S/Z(S)$ nontrivially. From Lemma 3.2,

$$\begin{aligned}
&Prob\left([b,h]\neq Z\left(S\right)|\left[b,h\right]\in S/Z(S)\right)\geq 1-1/2\\
&\Rightarrow Prob\left(\left[xZ\left(S\right),yZ\left(S\right)\right]\neq Z\left(S\right)|\left[xZ\left(S\right),yZ\left(S\right)\right]\in S/Z(S)\right)\geq 1/2\\
&\Rightarrow Prob\left(x^{-1}y^{-1}xyZ\left(S\right)\neq Z\left(S\right)|x^{-1}y^{-1}xyZ\left(S\right)\in S/Z(S)\right)\geq 1/2\\
&\Rightarrow Prob\left([x,y]\notin Z\left(S\right)|\left[x,y\right]\in S\right)\geq 1/2.
\end{aligned}$$

Hence, from the definition of conditional probability ($P\left(A\mid B\right)=P(A\wedge B)/P(B)$),

$$Prob\left([x,y]\notin Z\left(S\right)\wedge\left[x,y\right]\in S\right)\geq Prob\left([x,y]\notin Z\left(S\right)|\left[x,y\right]\in S\right)\times Prob([x,y]\in S).$$

We get the probability that $[x,y]\in S\setminus Z(S)$ is at least $1/160$. For such an element y, line 11 reassigns x to a nonscalar element of R with $p=o_{y}$. Thus, BlindDescent produces a suitable x with probability $1-\delta$ after $160\log(1/\delta)$ elements y have been processed. □

Theorem 3.3 *Suppose Hypothesis 1 holds. If $S=R\cap G$ and $\overline{G}=G/S\cong 2\cdot A_{5}$, then BlindDescent returns successfully with probability $1-\delta$ after at most $30\log(1/\delta)$ repetitions of a basic step.*

Proof Let $\overline{N}{=}O_{\infty}(\overline{G})$ be the soluble radical of $\overline{G}$. In this case, we have $\overline{G}/\overline{N}\cong A_{5}$. Let $\overline{x}=xS$ and $\overline{y}=yS$ where x and y are elements of G produced by BlindDescent. If $\overline{x}\notin\overline{N}$, then $Prob\left(\overline{y}\overline{N}\in C_{\overline{G}/\overline{N}}\left(\overline{x}\overline{N}\right)\right)\geq 1/20$. One can see that

$$\begin{aligned}
Prob\left(\overline{y}\overline{N}\in C_{\overline{G}/\overline{N}}\left(\overline{x}\overline{N}\right)\right)&=Prob\left(\left[\overline{x}\overline{N},\overline{y}\overline{N}\right]=\overline{N}\right)\\
&=Prob\left(\overline{x}^{-1}\overline{y}^{-1}\overline{x}\ \overline{y}\overline{N}=\overline{N}\right)\\
&=Prob\left(\left[\overline{x},\overline{y}\right]\in\overline{N}\right)
\end{aligned}$$

and so we obtain $Prob\left(\left[\overline{x},\overline{y}\right]\in\overline{N}\right)\geq 1/20$.

We know that $\overline{N}\leq G/S$ and so from the Correspondence Theorem, there is a normal subgroup of G corresponding to $\overline{N}$ where this subgroup includes S. Let us show this group by N. Hence, one can see that $\overline{N}=N/S$. Also, since we can define an epimorphism (natural homomorphism) from $\overline{N}$ to N, the normal subgroup N is soluble. Then:

$$\begin{aligned}
Prob\left(\left[\overline{x},\overline{y}\right]\in\overline{N}\right)\geq 1/20&\Rightarrow Prob((xS)^{-1}(yS)^{-1}xSyS\in N/S\geq 1/20\\
&\Rightarrow Prob(x^{-1}y^{-1}xyS\in N/S)\geq 1/20\\
&\Rightarrow Prob([x,y]\in N)\geq 1/20.
\end{aligned}$$

Assume that $H=\overline{G}/Z(\overline{G})$ and $A=\overline{N}/Z(\overline{G})$ (here, the group $A=\overline{N}/Z(\overline{G})$ is an elementary abelian 2-group with order 2^5). If we take $b=\overline{x}Z(\overline{G})$, $h=\overline{y}Z(\overline{G})$, and $C=\overline{g}Z(\overline{G})(\overline{N}/Z(\overline{G}))$, then from Lemma 3.2, we get:

$$\begin{aligned}
&Prob\left(\left[\overline{x}Z\left(\overline{G}\right),\overline{y}Z\left(\overline{G}\right)\right]\neq Z\left(\overline{G}\right)\mid\ \left[\overline{x}Z\left(\overline{G}\right),\overline{y}Z\left(\overline{G}\right)\right]\in\overline{N}/Z(\overline{G})\right)\geq 1-1/3\\
&\Rightarrow Prob\left(\overline{x}^{-1}\overline{y}^{-1}\overline{x}\ \overline{y}Z\left(\overline{G}\right)\neq Z\left(\overline{G}\right)\mid\overline{x}^{-1}\overline{y}^{-1}\overline{x}\ \overline{y}Z\left(\overline{G}\right)\in\overline{N}/Z(\overline{G})\right)\geq 2/3\\
&\Rightarrow Prob\left([\overline{x},\overline{y}]\notin Z\left(\overline{G}\right)\mid\ [\overline{x},\overline{y}]\in\overline{N}\right)\geq 2/3\\
&\Rightarrow Prob\left(\overline{x}^{-1}\overline{y}^{-1}\overline{x}\ \overline{y}\notin Z\left(G/S\right)\mid x^{-1}y^{-1}xyS\in N/S\right)\geq 2/3\\
&\Rightarrow Prob\left(x^{-1}y^{-1}xyS\notin Z\left(N/S\right)\mid[x,y]\in N\right)\geq 2/3\\
&\Rightarrow Prob\left([x,y]\notin Z(N)\mid\ [x,y]\in N\right)\geq 2/3.
\end{aligned}$$

Then, from the definiton of conditional probability, we see that the probability that $[x,y]\in N\setminus Z(N)$ is at least $1/30$. Therefore, BlindDescent finds a suitable x with probability $1-\delta$ in line 11 with $p=o_y$ after $30\log(1/\delta)$ elements y have been processed. □

Theorem 3.4 *Suppose Hypothesis 1 holds. If $S=R\cap G$ and $\overline{G}=G/S\cong Inn(\mathbb{Z}_2wrA_5)$, then BlindDescent returns successfully with probability $1-\delta$ after at most $40\log(1/\delta)$ repetitions of a basic step.*

Proof In this case, $r=2$, $\overline{N}$ is an elementary abelian group of order 2^4, $Z(\overline{G})$ is the trivial subgroup, $H=\overline{G}/Z(\overline{G})$ and $A=\overline{N}/Z(\overline{G})\cong\overline{N}$. Let N be a subgroup of G that corresponds to $\overline{N}$. Then, as in Theorem 3.3, we get $Prob([x,y]\in N)\geq 1/20$. Hence, if we take $b=\overline{x}Z(\overline{G})$, $h=\overline{y}Z(\overline{G})$, and $C=\overline{g}Z(\overline{G})(\overline{N}/Z(\overline{G}))$, then by Lemma 3.2, we get:

$$\begin{aligned}
&Prob\left(\left[\overline{x}Z\left(\overline{G}\right),\overline{y}Z\left(\overline{G}\right)\right]\neq Z\left(\overline{G}\right)\mid\ \left[\overline{x}Z\left(\overline{G}\right),\overline{y}Z\left(\overline{G}\right)\right]\in\overline{N}/Z(\overline{G})\right)\geq 1-1/2\\
&\Rightarrow Prob\left(\overline{x}^{-1}\overline{y}^{-1}\overline{x}\ \overline{y}Z\left(\overline{G}\right)\neq Z\left(\overline{G}\right)\mid\overline{x}^{-1}\overline{y}^{-1}\overline{x}\ \overline{y}Z\left(\overline{G}\right)\in\overline{N}/Z(\overline{G})\right)\geq 1/2\\
&\Rightarrow Prob\left([\overline{x},\overline{y}]\notin Z\left(\overline{G}\right)\mid\ [\overline{x},\overline{y}]\in\overline{N}\right)\geq 1/2\\
&\Rightarrow Prob(\overline{x}^{-1}\overline{y}^{-1}\overline{x}\ \overline{y}\notin Z\left(G/S\right)\mid x^{-1}y^{-1}xyS\in N/S)\geq 1/2\\
&\Rightarrow Prob(x^{-1}y^{-1}xyS\notin Z\left(N/S\right)\mid[x,y]\in N)\geq 1/2\\
&\Rightarrow Prob([x,y]\notin Z(N)\mid\ [x,y]\in N)\geq 1/2.
\end{aligned}$$

Thus, from the definition of conditional probability, we obtain that the probability that $[x,y]\in N\setminus Z(N)$ is at least $1/40$. BlindDescent finds a suitable x with probability $1-\delta$ in line 11 with $p=o_y$ after $40\log(1/\delta)$ elements y have been processed. □

Theorem 3.5 *Suppose Hypothesis 1 holds. If $S=R\cap G$ and $\overline{G}=G/S\cong 3.A_6$, then BlindDescent returns successfully with probability $1-\delta$ after at most $200\log(1/\delta)$ repetitions of a basic step.*

Proof In this situation, $r=5$, $\overline{N}\cong C_3$ (cyclic group of order 3), $H=\overline{G}/Z(\overline{G})$, and $A=\overline{N}/Z(\overline{G})$. One can see easily that A is the trivial group, so A can be taken as an elementary abelian 5-group. Hence, if we take

N as a subgroup of G corresponding to $\overline{N}$, then:

$$Prob([x,y] \in N) \geq 1/80$$

and

$$Prob([x,y] \notin Z(N) |\ [x,y] \in N) \geq 4/5.$$

We get the probability that $[x,y] \in N \setminus Z(N)$ is at least $1/200$. Therefore, BlindDescent produces a suitable x with probability $1-\delta$ in line 11 with $p = o_y$ after $200\log(1/\delta)$ elements y have been processed. □

Theorem 3.6 *Suppose Hypothesis 1 holds. If $S = R \cap G$ and $\overline{G} = G/S \cong PSL(3,2)$, then BlindDescent returns successfully with probability $1-\delta$ after at most $60\log(1/\delta)$ repetitions of a basic step.*

Proof In this case, $r = 3$ and $Prob(\,[x,y] \in S) \geq 1/40$. So, since

$$Prob\left([x,y] \notin Z\left(S\right) |\ [x,y] \in S\right) \geq 2/3,$$

we obtain:

$$Prob\left([x,y] \notin Z\left(S\right) \wedge [x,y] \in S\right) \geq 1/60.$$

□

If we know that any involution of a finite group G is in the center of G, then at least half of the elements of G have even order. For example, let t be a central involution of G and let y be an arbitrary element of G. Then one of y and yt has even order. If y has even order, then the statement is clearly true. Assume that y has odd order, i.e. $|y| = 2k+1$. In this case, $|yt| = lcm(|y|,|t|) = 2.(2k+1)$. Thus, yt has even order. Also, the number of pairs y, yt of elements different from each other is equal to half of the order of G. Thus, at least half of the elements of G have even order.

Taking advantage of this property of finite groups, the analysis in [5] was done for $Sp(2,r)$, which is a perfect subgroup of $Sp(4,r)$. One can see in [4, 11] that this subgroup is also a perfect subgroup of $Sp(6,r)$. Thus, this analysis is also valid for $Sp(6,r)$.

Theorem 3.7 *Suppose Hypothesis 1 holds. If $S = R \cap G$ and $\overline{G} = G/S \cong Sp(2,r)^3$, then BlindDescent returns successfully with probability $1-\delta$ after at most $324\log(1/\delta)$ repetitions of a basic step.*

Proof It is well known that the order of the center of $Sp(2,r)^3$ is equal to 8 and all involutions of these groups are central. Thus, at least half of the elements of any of these groups have even order. In $Sp(2,r)$, the proportion of elements of order equal to 6 modulo 8 is at least $1/6$. Hence, the proportion of even ordered and noncentral elements of the form $\overline{y} = (\overline{y_1}, \overline{y_2}, \overline{y_3})$ in $\overline{G} = Sp(2,r)^3$ for which $\overline{y}$ is determined by the elements mentioned in previous sentence is at least $1/216$. For $y \in G$ for which the image of y is $\overline{y}$, the image of $y^{o_y/2}$ is an involution and central. Then we get:

$$\begin{aligned} & xSy^{o_y/2}S = y^{o_y/2}SxS \\ & \Rightarrow x^{-1}S(y^{o_y/2})^{-1}SxS = S \\ & \Rightarrow [x, y^{o_y/2}] \in S. \end{aligned}$$

Thus, we find that $Prob([x, y^{o_y/2}] \in S) = 1$. Here $r \geq 3$ and so, from Lemma 3.2, we obtain:

$$Prob([x, y^{o_y/2}] \notin Z(S) | \ [x, y^{o_y/2}] \in S) \geq 2/3.$$

Hence, we get:

$$Prob([x, y^{o_y/2}] \notin Z(S) \wedge [x, y^{o_y/2}] \in S) \geq 1.\frac{2}{3}.\frac{1}{216}$$
$$\Rightarrow Prob([x, y^{o_y/2}] \notin Z(S) \wedge [x, y^{o_y/2}] \in S) \geq \frac{1}{324}.$$

BlindDescent thus produces a suitable x with probability $1 - \delta$ in line 11 with $p = 2$. □

3.3. Integration

If the input group G is soluble, then BlindDescent runs successfully by Theorem 3.1. If the input group G is nonsoluble, then we take a preparatory step of replacing G by its soluble residual. If the soluble residual of G is one of the groups considered in Section 3.2, then BlindDescent gives the result successfully.

Acknowledgement

We would like to express our gratitude to the anonymous referee for a very careful review and for suggestions that improve the readability of the paper. We also thank Akos Seress who inspired us for the research.

References

[1] Ankaralıoğlu N, Seress Á. Computing tensor decompositions of finite matrix groups. Discret Math Theor C 2011; 13: 5-14.

[2] Aschbacher M. On the maximal subgroups of finite classical groups. Invent Math 1984; 76: 469-514.

[3] Beals R, Leedham-Green CR, Niemeyer AC, Praeger CE, Seress Á. Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules. J Algebra 2005; 292: 4-46.

[4] Bray J, Holt D, Rooney-Dougal C. The Maximal Subgroups of the Low Dimensional Finite Classical Groups. Cambridge, UK: Cambridge University Press, 2013.

[5] Brooksbank P, Niemeyer AC, Seress Á. 2006. A reduction algorithm for matrix groups with an extraspecial normal subgroup. In: Hulpke A, editor. Finite Geometries, Groups and Computation. New York, NY, USA: de Gruyter, 2006, pp. 1-16.

[6] Carlson J, Neunhöffer M, Rooney-Dougal C. A polynomial-time reduction algorithm for groups of semilinear or subfield class. J Algebra 2009; 322: 613-637.

[7] Dixon JD. The solvable length of a solvable linear group. Math Z 1968; 121: 151-158.

[8] Gül K, Çağman A, Ankaralıoğlu N. An algorithm for projective representations of some matrix groups. Life Science Journal 2014; 11: 1005-1009.

[9] Holt DF, Plesken W. 1989. Perfect Groups. Oxford, UK: Clarendon Press, 1989.

[10] Huppert B. Lineare auflösbare Gruppen. Math Z 1957; 67: 479-518 (in German).

[11] Kleidman P, Liebeck M. The Subgroup Structure of the Finite Classical Groups. Cambridge, UK: Cambridge University Press, London Mathematical Society Lecture Notes, 1990.

[12] Leedham-Green CR. The computational matrix group project. Groups and computation III (Colombus, OH, 1999). Ohio State Univ Math Res Inst Publ 2001; 8: 229-247.

[13] Murray SH, Rooney-Dougal CM. Constructive homomorphisms for classical groups. J Symb Comput 2011; 46: 371-384.

[14] Neumann PM, Praeger CE. A recognition algorithm for special linear groups. P Lond Math Soc 1992; 65: 555-603.

[15] Neunhöffer M, Seress Á. A data structure for a uniform approach to computations with finite groups. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation, pp. 254-261.

[16] Newman MF. The soluble length of soluble linear groups. Math Z 1972; 126: 59-70.

[17] Niemeyer AC. A constructive recognition algorithm for normalisers of small extra-special groups as matrix groups. Int J Algebr Comput 2005; 15: 367-394.

[18] O'Brien EA. Towards effective algorithms for linear groups. In: Hulpke A, editor. Finite Geometries, Groups and Computation. New York, NY, USA: de Gruyter, 2006, pp.163-190.

[19] Suzuki M. Group Theory II. New York, NY, USA: Springer Verlag, 1986.

[20] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.7.8, 2015.

[21] Zassenhaus H. Beweis eines Satzes über diskrete Gruppen. Abh Math Sem Univ Hamburg 1938; 12: 289-312 (in German).