MANCHESTER
1824

The University of Manchester

A Note on Involution Centralizers in Black Box Groups

Kelsey, Veronica and Rowley, Peter

2018

MIMS EPrint: **2018.21**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

A Note on Involution Centralizers in Black Box Groups

Veronica Kelsey, Peter Rowley

Abstract

Here we note a minor variation on the method in [1] which enables calculations of $C_H(t)$ for H a subgroup of a black box group G and t an involution of G.

In [1] Bray revealed a method for calculating centralizers of involutions in black box groups with an order oracle. This method extended one introduced earlier by R. Parker (see [9]). In recent times the Bray method has had many ramifications in computational group theory (for a fraction of these consult [2], [3], [4], [5], [6], [7], [8], [10], [12], [13]). The purpose of this short note is to observe a further twist to this story.

Suppose G is a black box group with an order oracle. Assume t is an involution of G. In [1] the elements $\mathcal{K}(t,g)$ of G are key. For $g \in G$ and letting n be the order of $[t,g]$ we define

$$\mathcal{K}(t,g) = \begin{cases} [t,g]^m & \text{if } n = 2m \\ [t,g]^m & \text{if } n = 2m+1. \end{cases}$$

These elements $\mathcal{K}(t,g)$ supply elements in $C_G(t)$. Those $\mathcal{K}(t,g)$ obtained when n is odd have the property observed by R. Parker that they are uniformly distributed throughout $C_G(t)$.

For $H \leq G$, set $\mathcal{O}_H = \{h \mid h \in H \text{ and } [t,h] \text{ is of odd order}\}$.

Lemma 0.1 *Suppose t is an involution in G, $H \leq G$ and let $c \in C_H(t)$. Then $|\{h \in \mathcal{O}_H \mid \mathcal{K}(t,h) = c\}|$ is independent of c.*

Proof Since $c \in C_H(t)$, $[t,h] = [t,ch]$ for all $h \in H$, so we only need prove the lemma for each right coset $C_H(t)h$ $(h \in H)$ for which $[t,h]$ has odd order. For $eh \in C_H(t)h$, we have

$$\mathcal{K}(t,eh) = eh[t,eh]^m = eh[t,h]^m = e\mathcal{K}(t,h),$$

where $[t,h]$ has order $2m+1$. Hence each such coset contributes 1 to $|\{h \in \mathcal{O}_H \mid \mathcal{K}(t,h) = c\}|$, so giving the lemma. $\square$

Theorem 3.1 of [1] is the case $H = G$, and its proof is virtually identical to that for Lemma 0.1. The point is that t does not need to be in H. So to compute $C_H(t)$ we may proceed as follows.

1. Fix $S := \{\ \}$.
2. Choose a random element $h \in H$.
3. Compute $\mathcal{K}(t,h)$.

4. Check whether $\mathcal{K}(t,h) \in H$; if yes then add $\mathcal{K}(t,h)$ to S.

5. Go to step 2.

Then $\langle S \rangle$ will be a subgroup of $C_H(t)$. All the analysis and caveats discussed in [1] will apply here. Lemma 0.1 shows that the set of elements passing test 4 will be uniformly distributed in $C_H(t)$. Also the membership problem raises its head in step 4 and the exact nature of H may help in resolving this. For example we may have $H = C_G(X)$ ($X \leq G$) in which case step 4 can be settled by checking whether $\mathcal{K}(t,h)$ commutes with a generating set for X. Suppose $H = C_G(s)$ where s is an involution of G (in fact, the situation that sparked this note), experimentally the following works well. In place of 2-5 do

2′. Compute $\mathcal{K}(s,g)$ where g is a random element of G (so applying the Bray method for $C_G(s)$).

3′. Compute $\mathcal{K}(t,\mathcal{K}(s,g))$.

4′. Check whether s and $\mathcal{K}(t,\mathcal{K}(s,g))$ commute; if yes then add $\mathcal{K}(t,\mathcal{K}(s,g))$ to S.

5′. Go to step 2′.

Observe that Lemma 0.1 applied twice shows that these will be uniformly distributed in $C_G(t) \cap C_G(s)$. Of course we could determine generating sets for $C_G(t)$ and $C_G(s)$ using the Bray method and then attempt to compute $C_G(t) \cap C_G(s)$. In computationally hard groups the latter step may prove impossible.

To illustrate this with an example, take $G = E_6(2)$, as given in the electronic ATLAS [14] in its 27-dimension $GF(2)$ representation. There $G = \langle a, b \rangle$ where a has order 2, b has order 3 with ab of order 62. So taking $t = a$ and $s = (ab)^{31}$, using the method discussed here (that is, steps 1, 2′, 3′, 4′, 5′) with 10000 random elements $g \in G$ we get $\langle S \rangle = C_G(s) \cap C_G(t)$ with $|\langle S \rangle| = 2^{12}.3.7$. This is done in the blink of an eye whereas first calculating $C_G(s)$ and $C_G(t)$ (which is quick) and then $C_G(s) \cap C_G(t)$ takes forever (1552 seconds on a 16×1248MHz machine running MAGMA version 222-10). This disparity will be even greater for larger groups.

Finally, we observe that the above process for the centralizer of two involutions may be iterated so as to find $C_G(H)$ where H is generated by involutions.

References

[1] Bray, John. *An improved method for generating the centralizer of an involution.* Arch. Math. (Basel) 74 (2000).

[2] Bray, John. Bäärnhielm, Henrik. *A new method for recognising Suzuki groups.* J. Algebra 493 (2018), 483–499.

[3] Ballantyne, John. Bates, Chris. Rowley, Peter. *The maximal subgroups of $E_7(2)$.* LMS J. Comput. Math. 18 (2015), no. 1, 323–371.

[4] Bäärnhielm, Henrik; Holt, Derek. Leedham-Green, Charles. O'Brien, Eamonn. *A practical model for computation with matrix groups.* J. Symbolic Comput. 68 (2015), part 1, 27–60.

[5] Dietrich, Heiko. Leedham-Green, Charles. O'Brien, Eamonn. *Effective black-box constructive recognition of classical groups.* J. Algebra 421 (2015), 460–492.

[6] Dixon, John. Praeger, Cheryl. Seress, Ákos. *Strong involutions in finite special linear groups of odd characteristic.* J. Algebra 498 (2018), 413–447.

[7] Farooq, Adeel. Norton, Simon. Wilson, Robert. *A presentation of the monster and a set of matrices which satisfy it.* J. Algebra 379 (2013), 432–440.

[8] Kantor, William. Magaard, Kay. *Black box exceptional groups of Lie type II.* J. Algebra 421 (2015), 524–540.

[9] Norton, Simon. *The construction of J_4.* In: Proceedings of the Santa Cruz Group Theory Conference. Cooperstein and Mason eds., pp. 271 - 278, Proc. Sympos. Pure Math. 37, Amer. Math. Soc. (1980).

[10] Norton, Simon. Wilson, Robert. *A correction to the 41-structure of the Monster, a construction of a new maximal subgroup $L_2(41)$ and a new Moonshine phenomenon.* J. Lond. Math. Soc. (2) 87 (2013), no. 3, 943–962.

[11] Parker, Christopher. Wilson, Robert. *Recognising simplicity of black-box groups by constructing involutions and their centralisers.* J. Algebra 324 (2010), no. 5, 885–915.

[12] Wilson, Robert. *Every $PSL_2(13)$ in the Monster contains 13A-elements.* LMS J. Comput. Math. 18 (2015), no. 1, 667–674.

[13] Wilson, Robert. *Classification of subgroups isomorphic to $PSL_2(27)$ in the Monster.* LMS J. Comput. Math. 17 (2014), no. 1, 33–46.

[14] Wilson, Robert. Walsh, Peter. Tripp, John. Suleiman, Ibrahim. Parker, Richard. Norton, Simon. Nickerson, Simon. Linton, Stephen. Bray, John. Abbot, Rachel. *Atlas of finite group representations, version 3.* `http://brauer.maths.qmul.ac.uk/Atlas/v3/`