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 $K(t, g)$ of $G$ are key. For $g \in G$ and letting $n$ be the order of $[t, g]$ we define

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

These elements $K(t, g)$ supply elements in $C_G(t)$. Those $K(t, g)$ 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 $O_H = \{h \mid h \in H \text{ and } [t, h] \text{ is of odd order}\}$.

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

$$K(t, eh) = eh[t, eh]^m = eh[t, h]^m = eK(t, h),$$

where $[t, h]$ has order $2m + 1$. Hence each such coset contributes 1 to $|\{h \in O_H \mid K(t, h) = c\}|$, 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 $K(t, h)$. 


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 $|\langle S \rangle| = 2^{12} \cdot 3 \cdot 7$. 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


