Computational group theory problems arising from computational design theory

Leonard H. Soicher

1. DESIGN

The DESIGN package [9] for GAP [4] can construct, classify, partition and study block designs satisfying a very wide range of user-specified properties. The designs may be t-designs (simple or non-simple), but in general need not have constant block-size nor constant replication-number. The DESIGN package has already been used to generate, classify and study many new designs of interest to combinatorialists and statisticians; see, for example [1, 2, 3].

2. Linton's SmallestImageSet

In the course of developing the DESIGN package and using it to classify block designs, some interesting problems in (computational) group theory arose, the first being the need for algorithms to determine canonical orbit representatives. One very useful such algorithm I now use in design (and clique) classification is Steve Linton's `SmallestImageSet`, which, given a permutation group G on $\Omega = \{1, \ldots, n\}$, and a subset S of Ω, determines the lexicographically least set in the G-orbit of S (see [8]). The use of canonical set-orbit representatives allows pairwise G-isomorph-rejection to be accomplished by determining the canonical representative of each set under consideration, sorting these representatives, and removing duplicates.

I now suggest that for every action of a group G on a finite set Ω we should consider how best to define a canonical element in a G-orbit, and given such a definition, develop algorithms to determine:

- given $\alpha \in \Omega$, whether or not α is the canonical element in α^G;
- given $\alpha \in \Omega$, the canonical element in α^G;
- given $\alpha \in \Omega$, an element $g \in G$ such that α^g is the canonical element in α^G.

3. Friendly subgroups

When John Arhin (my PhD student) and I were classifying various designs invariant under given groups, the following concept naturally arose twice.

Definition A subgroup H of a group K is a *friendly* subgroup of K if every subgroup of K isomorphic to H is conjugate in K to H.

Proposition 1. *Suppose G acts on a set Ω, and let $\alpha, \beta \in \Omega$, with H a friendly subgroup of G_α and H a subgroup of G_β. Then α and β are in the same G-orbit if and only if they are in the same $N_G(H)$-orbit.*

Proof. The if-part is trivial. For the converse, suppose $x \in G$ with $\alpha^x = \beta$. Then $G_\beta = (G_\alpha)^x$, and so H^x is a friendly subgroup of G_β. Since $H \leq G_\beta$, it must be conjugate in G_β to H^x, and so there is a $y \in G_\beta$ with $H^{xy} = H$. We thus have $xy \in N_G(H)$ and $\alpha^{xy} = \beta^y = \beta$. □

Proposition 2. *Suppose G acts on a set Ω, and let $\alpha, \beta \in \Omega$, with H a friendly subgroup of G_α. Then if β is in the same G-orbit as α, every subgroup of G_β that is isomorphic to H is conjugate in G to H.*

Proof. Suppose $x \in G$ with $\alpha^x = \beta$. Then $G_\beta = (G_\alpha)^x$, and so H^x is a friendly subgroup of G_β. Thus, if $J \leq G_\beta$ with $J \cong H$, then J is conjugate in G_β to H^x, and so J is conjugate in G to H. □

When classifying H-invariant objects up to G-equivalence (that is, up to being in the same G-orbit), for a given $H \leq G$, Proposition 1 allows us to avoid many tests to determine G-equivalence when $N_G(H)$-orbit representatives of the H-invariant objects have been determined. (For such an $N_G(H)$-orbit representative α, if H is a friendly subgroup of G_α then no G-equivalence tests involving α are required.)

When classifying H_i-invariant objects for various pairwise isomorphic, but non-conjugate, subgroups H_i of G, Proposition 2 allows us to avoid many tests to determine when an H_i-invariant object is G-equivalent to an H_j-invariant one. (For a given H_i-invariant α, if H_i is a friendly subgroup of G_α, then α cannot be in the same G-orbit as an H_j-invariant object, when $i \neq j$.)

It is often possible to use cheap computational tests to confirm that a subgroup H of a finite group K is a friendly subgroup (when it is such a subgroup), making use of the following result.

Theorem 1. *Let K be a finite group and H a subgroup of K. Then H is a friendly subgroup of K if one or more of the following holds:*

(1) *$H = K$;*
(2) *K is cyclic;*
(3) *H is a Hall subgroup of K (i.e. $\gcd(|H|, |K : H|) = 1$) and H is supersoluble (see [7]);*
(4) *H is a nilpotent Hall subgroup of K (such as a Sylow subgroup), or more generally, H is a friendly subgroup of a nilpotent Hall subgroup of K (see [10]);*
(5) *K is soluble and H is a Hall subgroup of K, or more generally, K is soluble and H is a friendly subgroup of a Hall subgroup of K (see [6]).*

It is worth noting that F. Gross employs the Classification of Finite Simple Groups to prove that an odd-order Hall subgroup of a finite group is a friendly subgroup of that group (see [5]), but I prefer not to use this sledgehammer to crack the odd nut.

References

[1] R.A. Bailey, P.J. Cameron, P. Dobcsányi, J.P. Morgan and L.H. Soicher, *Designs on the web*, Discrete Math., to appear. Preprint available at: `http://designtheory.org/library/preprints/`

[2] P. Dobcsányi, D.A. Preece and L.H. Soicher, *On balanced incomplete-block designs with repeated blocks*, European J. Combinatorics, to appear. Preprint available at: `http://designtheory.org/library/preprints/`

[3] P. Dobcsányi and L.H. Soicher, *An online collection of t-designs*, 2005, `http://designtheory.org/database/t-designs/`

[4] The GAP Group, *GAP — Groups, Algorithms, and Programming*, Version 4.4; Aachen, St Andrews, 2004, `http://www.gap-system.org/`

[5] F. Gross, *Conjugacy of odd order Hall subgroups*, Bull. London Math. Soc. **19** (1987), 311–319.

[6] P. Hall, *A note on soluble groups*, J. London Math. Soc. **3** (1928), 98–105.

[7] P. Hall, *Theorems like Sylow's*, Proc. London Math. Soc. (3) **6** (1956), 286–304.

[8] S. Linton, *Finding the smallest image of a set*, ISSAC 2004, 229–234, ACM, New York, 2004.

[9] L.H. Soicher, *The DESIGN package for GAP*, Version 1.1, 2004, `http://designtheory.org/software/gap_design/`

[10] H. Wielandt, *Zum Satz von Sylow*, Math. Z. **60** (1954), 407–408.