Reconstructing Weighing Matrices From Their Automorphism Group

Giora Dula[1], Assaf Goldberger[2], Yossi Strassler[3]

[1] *Netanya Academic College, Israel, giora@netanya.ac.il*
[2] *Tel Aviv University, Israel assafg@post.tau.ac.il*
[3] *Dan Yishai, Israel danyishay@gmail.com*

A weighing matrix of order n and weight k, generally denoted by $W(n,k)$ is a $n \times n$ $\{0,1,-1\}$-matrix W such that $WW^T = kI_n$. We say that two matrices W_1 and W_2 in $W(n,k)$ are (Hadamard) equivalent, if $W_2 = LW_1R$ for monomial matrices L,R. The Automorphism group of a weighing matrix $W \in W(n,k)$ is the group

$$Aut(W) \ = \ \{(L,R)\ | LWR = W,\ L,R \text{ monomial}\}$$

with multiplication given by $(L,R)\cdot(L',R') := (LL',R'R)$.

Suppose now we are only given the group $Aut(W)$ and we would like to reconstruct W from it. Then $Aut(W)$ gives us a lot of information on W: The action of $Aut(W)$ on pairs (i,j), $1 \le i,j \le n$ splits the space of n^2 pairs into orbits, and a single entry in each orbit, determines all remaining entries in the orbit. This suggests a massive reduction in the search space for W.

Moreover, suppose for the moment that $Aut(W)$ acts bi-transitively on the rows of the matrix. Then for any candidate matrix W the resulting Gram matrix WW^T is constant (up to sign) off the diagonal. In particular, this value has fairly good chances to be zero, hence W will be a weighing matrix. Even when it is nonzero, in some cases there are augmenting constructions that can fix the problem.

To obtain such constructions, we first need to construct candidates for the automorphism groups. To this end we begin with two embeddings $L_0,R_0 : G \to S_n$ (considered as action of G on the rows and columns), and then lift them to embeddings $L,R : G \subset B_n$ using Group Cohomology. We now analyze the orbits of the action on pairs of row and column. Some orbits will result in conflicting signs, and must be given the value zero, the other orbits may be given any value in $\{0,1,-1\}$.

This method was applied to various cases: Some well known families such as Payley's Conference and Hadamard Matrices, as well as projective spaces are all a special case of this construction. We have also obtained some seemingly new families. We also can construct matrices from groups that are not doubly transitive.

We obtain gram matrices with some interesting structure, and they can serve as building blocks for weighing matrices.