BULL. AUSTRAL. MATH. SOC. 05B05
VOL. 59 (1999) [175–175]

Trades and defining sets with applications to access schemes

BRENTON GRAY

A block design, D, is a collection of k-subsets (blocks) of a v-set, V, such that every element of V occurs in the same number of blocks of D. If each t-subset of V occurs in the same number of blocks, then D is a t-design. The study of t-designs has led to applications in coding theory, cryptography and the planning of agricultural experiments.

The focus of the thesis is on two types of structures related to t-designs, namely *trades* and *defining sets*. A trade $T = (T_1, T_2)$ of volume m consists of two disjoint collections T_1 and T_2 each containing m blocks such that every t-subset is contained in the same number of blocks of T_1 and of T_2. A defining set is a collection of blocks which can be completed to only one t-design with given parameters. Trades and defining sets are intimately related.

Trades are investigated in the first half of the thesis. Considerable progress is made in understanding the possible volumes and structures of certain trades.

Defining sets and their relationship to trades are studied in the second half of the thesis. Using this relationship, results regarding defining sets of well known families of designs are presented.

An *access scheme* is a method of sharing a *password* amongst a group of people so that the password can only be reconstructed by a sufficiently large section of the group acting in agreement. Typical users include the military and banks. A critical analysis of an access scheme which uses trades and defining sets concludes this thesis.

39 Boundary Rd
Indooroopilly Qld 4068
Australia

Received 7th October, 1998.
Thesis submitted to The University of Queensland November 1997. Accepted August 1998. Supervisor: Professor Anne Street.