BULL. AUSTRAL. MATH. SOC. 05B05
VOL. 37 (1988) [467–468]

THEORY OF COMBINATORIAL DESIGNS WITH APPLICATIONS TO ENCRYPTION AND THE DESIGN OF EXPERIMENTS

D.G. SARVATE

The main aim of this thesis is to prove that the necessary conditions are sufficient for the existence of various block designs with small block sizes and to explore the use of block designs in encryption and the design of experiments. Some general constructions and results are obtained.

The various designs studied are as follows.

In Chapter 1 block designs are introduced, using graphs, and a construction of PBIBD's, using n-partite graphs, is given.

Chapter 2 deals with directed and cyclic designs of block size 3 and 4. By generalizing results of Hanani, it is proved that the necessary conditions are sufficient for the existence of directed group divisible designs (GDD's) of block sizes 3, 4 and cyclic GDD's of block size 3 except $v = 6$ and group size $= 1$. Some general results are given. The existence of cyclic BIBD $(v, b, r, 4, (4t+2)^*)$ for $v \equiv 0, 1(\text{mod}4)$ and cyclic BIBD$(v, b, r, 4, 4t^*)$ for all $v \geqslant 4$ is established.

Chapter 3 is on equi-neighboured designs. One of the results proved is that every GDD of block size three, with $\lambda = 3t$, underlies an equi-neighboured GDD.

Chapter 4 is on simple designs. A theorem of R.G. Stanton and R.J. Collens is used to show that the necessary conditions are sufficient for the existence of simple balanced incomplete block designs (simple BIBD's) with block size three. Embedding theorems for simple BIBD's, based on a method of graph factorization, are given.

Coloured designs are in Chapter 5. Many new families of GDD's and BIBD's can be obtained by using construction based on coloured designs. One such construction and an existence theorem for coloured designs are given.

In Chapter 6 some general constructions, based on directed graphs and t–designs, for families of PBIBD's and BIBD's are given.

Generalised Bhaskar Rao designs and orthogonal designs are studied in Chapter 7. It is shown that neither BRD$(10, 4, 2)$ nor GBRD$(7, 4, 4; Z_2 \times Z_2)$ exists. It is

Received 11 September 1987
Thesis submitted to the University of Sydney, March 1987. Degree approved July 1987. Supervisor: Professor Jennifer Seberry

shown that the necessary conditions are sufficient for the existence of a GBRD(v, 3, $4t$; Z_4) except possibly when (v, t) = (27, 1) or (39, 1). Some new constructions for weighing matrices and orthogonal designs are obtained by extending a method of Kharaghani.

Chapter 8 gives some ideas about applications of designs in encryption. A systematic method to permute the message block, while scrambling, in the message, a number of arbitrary message symbols, is given.

Department of Mathematics
University of Papua New Guinea
P.O. Box 320
Papua New Guinea