CORR 99-01

Applications of Combinatorial Designs to Communications, Cryptography, and Networking

C.J. Colbourn, J.H. Dinitz, & D.R. Stinson

Summary Combinatorial designs have long had substantial application in the statistical design of experiments, and in the theory of error-correcting codes. Applications in experimental and theoretical computer science have emerged, along with connections with the theory of cryptographic communication. In this paper, we focus on another collection of recent applications in the general area of communications, including cryptograph and networking. Applications have been chosen to represent those in which design theory plays a useful, and sometimes central, role. Moreover, applications have been chosen to reflect in addition the genesis of new and interesting problems in design theory in order to treat the practical concerns. Of many candidates, thirteen applications areas have been included. They are as follows:

1. Optical Orthogonal Codes
2. Synchronous Multiple Access to Channels
3. Group Testing and Superimposed Codes
4. Erasure Codes and Information Dispersal
5. Threshold and Ramp Schemes
6. Authentication Codes
7. Resilient and Correlation-immune Functions
8. Multidrop Networks
9. Channel Graphs and Interconnection Networks
10. Partial Match Queries on Files

11. Software Testing

12. Disk Layout and Striping

13. $(t,\ m,\ s)$-Nets and Numerical Intergration

Our conclusion is that the theory of combinatorial designs continues to grow, in part as a consequence of the variety of these applications and the increasing depth of the connections with challenging problems on designs.