The array which has
d repeating pattern is
on is again optimal.
tended knight's move

1
5

o-dimensional binary
s with symbols from
C is a linear code;
ny code array in C
the matrix obtained
downwards is also in
ng such codes is by
yclic codes. As an
own in Figure 4.3,
) 1 1 1 0 1 1 1 0
to find the minimum
o-dimensional binary

e to the fact that a
weight and whose
derived by means of
ssible distinct Cayley
ue of theorem 3.2.1

| | | | |
|---|---|---|---|
| 0 0 0 | 1 0 1 | 1 1 0 | 0 1 1 |
| 0 0 0 | 0 1 1 | 1 0 1 | 1 1 0 |
| 0 0 0 | 1 1 0 | 0 1 1 | 1 0 1 |
| | | | |
| 0 1 1 | 1 0 1 | 0 1 1 | 1 1 0 |
| 1 0 1 | 0 0 0 | 0 0 0 | 0 0 0 |
| 1 1 0 | 1 0 1 | 0 1 1 | 1 1 0 |
| | | | |
| 1 1 0 | 0 0 0 | 0 0 0 | 0 0 0 |
| 0 1 1 | 1 0 1 | 0 1 1 | 1 1 0 |
| 1 0 1 | 1 0 1 | 0 1 1 | 1 1 0 |
| | | | |
| 1 0 1 | 1 0 1 | 0 1 1 | 1 1 0 |
| 1 1 0 | 1 0 1 | 0 1 1 | 1 1 0 |
| 0 1 1 | 0 0 0 | 0 0 0 | 0 0 0 |

Figure 4.3

of [DK], the minimum Hamming distance between any two arrays of the code is 2n. For convenience, we repeat our theorem here and we also illustrate our construction by giving in Figure 4.4 the two-dimensional non-binary cyclic code obtained when n = 3.

| | | | | | |
|---|---|---|---|---|---|
| 1 2 3 | 3 1 2 | 2 3 1 | 1 2 3 | 2 3 1 | 3 1 2 |
| 2 3 1 | 1 2 3 | 3 1 2 | 3 1 2 | 1 2 3 | 2 3 1 |
| 3 1 2 | 2 3 1 | 1 2 3 | 2 3 1 | 3 1 2 | 1 2 3 |
| | | | | | |
| 1 3 2 | 3 2 1 | 2 1 3 | 1 3 2 | 2 1 3 | 3 2 1 |
| 2 1 3 | 1 3 2 | 3 2 1 | 3 2 1 | 1 3 2 | 2 1 3 |
| 3 2 1 | 2 1 3 | 1 3 2 | 2 1 3 | 3 2 1 | 1 3 2 |

Figure 4.4

THEOREM 4.1 Two different Cayley tables, A and B, of a given group G of order n differ from each other in at least 2n places.

Proof. If no two corresponding rows of the two Cayley tables are the same then every row of A differs from the corresponding row of B in at least two places. Likewise, if no two corresponding columns of the two tables are the same, then every column of A differs from the corresponding column of B in at least two places. In either event, B differs from A in at least 2n places.

For the remaining part of the proof, we may suppose that at least one row and at least one column of B are the same as the corresponding row and column of A. Let us suppose that the equal rows are the u-th rows and that the equal columns are the v-th columns. Then, we have $a_{uv} = b_{uv}$, $a_{uj} = b_{uj}$ and $a_{iv} = b_{iv}$ whence, by the quadrangle criterion, $a_{ij} = b_{ij}$ for all pairs of indices i and j, and so A = B. Consequently, this case cannot occur. []

It was shown by E.N.Gilbert(1965) that the number of different Cayley tables of a given cyclic group G of order n is $n!(n-1)!(n-1)!/\phi(n)$, where $\phi(n)$ is Euler's function. For example, when n = 3, this number is 12, as in Figure 4.4.

Another class of two-dimensional arrays which arise in coding theory and which have connections with latin squares are the so-called Costas arrays.

A Costas array of order n is an n×n array of blanks and ones with the property that the $\frac{1}{2}n(n-1)$ vectors which connect pairs of ones in the matrix are all distinct as vectors. (For an example of order six, see Figure 4.5). Thus, a translation of the array without rotation produces at most one pair of superimposed cells both of which contain an entry one. Such arrays are of value in determining the range and velocity of a moving object by means of radar or sonar signals. A detailed account of the history of these arrays and of their applications will be found in J.P.Costas(1984).

A Costas array is called vertically singly-periodic (horizontally singly-periodic) if all its vertical translates (horizontal translates), when read cyclically as if on a horizontal (vertical) cylinder, are also Costas arrays. It is known that singly-periodic Costas arrays exist for all orders

S 46

.S.A.

, CA, U.S.A.
dge, MA, U.S.A.

# LATIN SQUARES

## New Developments in the Theory and Applications

J. DÉNES

*Industrial and Scientific Consultant*
*Formerly Head of Mathematics*
*Institute for Research and*
*Co-ordination of Computing Techniques (SZKI)*
*Budapest, Hungary*

*and*

A.D. KEEDWELL

*Department of Mathematical*
*and Computing Sciences*
*University of Surrey*
*Guildford, United Kingdom*

*With specialist contributions by*

G.B. BELYAVSKAYA
A.E. BROUWER
T. EVANS
K. HEINRICH
C.C. LINDNER
D.A. PREECE

NH
PC

1991

NORTH-HOLLAND – AMSTERDAM • NEW YORK • OXFORD • TOKYO

# CHAPTER 9

## LATIN SQUARES AND CODES (J.Dénes and A.D.Keedwell)

The codes which we consider in this chapter are those used for communication of messages of all kinds. The messages will be encoded into digital form for transmission and may also be ciphered so as to render them unintelligible to unauthorized interceptors. The primary message may be one-dimensional (for example, the message may consist of English sentences) or two-dimensional (for example, it may be required to transmit a picture by radio). In any event, the message has to be decoded at the receiving end and any errors of transmission detected and, if possible, corrected. For this reason, an error-detecting and correcting code will usually be used.

Suppose that we wish to transmit a sequence of digits $a_1, a_2, \ldots$ across a noisy channel : for example, through a telegraph cable or from a space satellite. Occasionally (in the case of a satellite, frequently), the channel noise will cause a transmitted digit $a_i$ to be mistakenly interpreted as a different digit $a_j$ with the result that the message received at the destination will differ from that which was transmitted.

Although it is not possible to prevent the channel from causing such errors, we can reduce their undesirable effects by sending with each "word" $(a_1, a_2, \ldots, a_k)$ of k information digits a sequence of r additional check digits $a_{k+1}, \ldots, a_{k+r}$ so that the codeword $(a_1\ a_2\ \ldots\ a_{k+r})$ actually transmitted is of length k+r. At the receiver, we hope to be able to use these additional digits to enable us to detect, and preferably also correct, errors in any of the digits of the lengthened word which we transmitted. In this way, we are able to recover the original message of k digits.

In a mobile radio telephone system, the area to be covered will be divided into smaller regions, each serviced by a local transmitter. If two such transmitters are allocated the same frequency, then there may be