Pseudo-Random Arrays and Codes and Designs Balanced for Residuals in Two Dimensions

I.M. Chakravarti
Department of Statistics
University of North Carolina
Chapel Hill, NC 27599-3260

A circular arrangement of the s^n letters using the s distinct letters of an alphabet S, such that every n-tuple occurs exactly once as a set of n consecutive symbols of the cycle, is usually called a deBruijn sequence.

Aardenne-Ehrenfest and deBruijn (1951) showed that the number of Eulerian circuits in a certain directed graph (called T-graphs by the authors) was the same as the number of such circular arrangements $P_n^{(s)} = s^{-n}(s!)^{s^{n-1}}$. deBruijn (1975) mentions that the counting problem for s=2 was solved by C. Flye Sainte-Marie in 1894 and gives references to numerous other contributions to the problems of construction and existence of such sequences.

An example with s=3 and n=2 is the cycle 11 22 33 13 2. There are 24 such cycles. A subset of these sequences can be generated by dividing 1 formally by a primitive polynomial f(x) of degree n in GF(s), s a prime power and by suitable modifications of the resultant power series.

These sequences called maximal period sequences (m-sequences) or pseudo-random sequences (see for instance, Birkhoff and Bartee (1970) and MacWilliams and Sloane (1977)) have been extensively used in the search for long period codes with good auto-correlation properties for satellite communication systems.

A $P_n^{(s)}$ cycle can be used to generate a serial factorial design where a factor with s levels is applied to s^n experimental units over s^n periods (Weidman (1975), Patterson (1968), Chakravarti (1978)). Over every n consecutive periods, one has a complete s^n factorial which can be analyzed to estimate direct effects and residual effects from (n-1) previous periods. In this context, instead of a complete factorial, a fractional factorial over n periods may be more useful and practicable.

A variant or a restriction of the $P_n^{(3)}$ cycle (de Bruijn, 1946) is the following:

Consider an n-tuple of digits {0,1,2} such that no two consecutive digits are the same, the last digit may be the same as the first digit. There are 3. 2^{n-1} such *admissible* n-tuples. Let $Q_n^{(3)}$ denote an ordered cycle of 3. 2^{n-1} digits from {0,1,2} such that each *admissible* n-tuple is represented *exactly once* by n consecutive digits of the cycle. For example, for n=3, s=3, 012 010 202 121 is such a $Q_3^{(3)}$ cycle.

By restricting the type of n-tuples that are to be exhibited in the cycle, the overall size of the experiment is reduced and also it may not be meaningful to have all the n-tuples repeated.

Two dimensional linearly recurring arrays as generalizations of maximal period linearly recurring sequences (m-sequences or pseudo-random sequences) or arrays with different types of window properties as two-dimensional analogues of deBruijn sequences have been studied by many authors (see, for instance, MacWilliams and Sloane (1976), Van Lint, MacWilliams and Sloane (1979) and Ma (1984)).

An array of 0's and 1's is said to have a certain type of uxv window property if each of the possible $2^{uv}-1$ non-null uxv arrays is seen exactly once, when one slides an uxv window over the array (to avoid trouble at the edges, the array is supposed to be written on a torus).

When every uxv array including the null array is allowed to appear exactly once, the array is a two-dimensional analogue of a deBruijn sequence.

Yet, another kind of array called an array with uxv horizontal window property is defined as one which permits every non-zero view once when a uxv window is moved horizontally across the array. The array is supposed to be written on a horizontal cylinder. An array with uxv vertical window property is defined in an analogous manner. Examples of two-dimensional arrays with the three types of window properties are given below.

Fig. 1

$$\begin{array}{cccc|c}
1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 \\
\hline
1 & 1 & 1 & 0 & 1
\end{array}$$

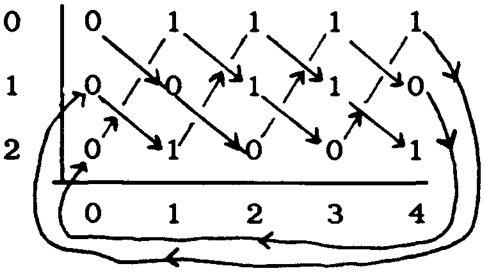
In Fig. 1 every 2x2 submatrix including the null submatrix occurs once, if the diagram is repeated as on a torus.

Fig. 2

$$\begin{array}{ccc@{\qquad}ccc@{\qquad}cc}
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{array}$$

In Fig. 2 the array has both the 3×1 horizontal and 1×3 vertical window properties. Row- and Column- complete and complete Latin squares exhibit various types of window properties.

Fig. 3



In Fig. 3, every non-null 2×2 subarray occurs exactly once, as a 2×2 window is slid over the array. This array was constructed by MacWilliams and Sloane (1976) by writing the m-sequence of length 2^4-1 (associated with x^4+x^3+1),

$$0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1$$

in a 3×5 rectangle in a special way.

Consider the ring $R = \{(a,b) : a \in GF(p^n),\ b \in GF(q^m)\}$ where p and q are primes such that $p^n+2 = q^m$. Addition and multiplication are defined by $(a_1,a_2) + (b_1,b_2) = (a_1+a_2,\ b_1+b_2)$ and $(a_1,b_1) \cdot (a_2,b_2) = (a_1a_2,\ b_1b_2)$ respectively, $a_i \in GF(p^n)$, $b_i \in GF(q^m)$.

Let x and y be respectively primitive elements of $GF(p^n)$ and $GF(q^m)$ and let $z = (x,y)$ and $s=p^n$. The order of $z = \text{l.c.m}\ (s-1,\ s+1) = (s^2-1)/2$. Then the set of elements

$$z^0,\ z^1,\ \ldots,\ z^{(s^2-3)/2},\ (0,0),\ (1,)\ \ldots\ (x^{s-2},0)$$

constitutes a difference set for the additive group R with $v = s(s+2)$, $k = \frac{v-1}{2}$, $\lambda = \frac{v-3}{4}$ (Stanton-Sprott, 1958).

For p=3, n=1, q=5, m=1, {(1,1,), (2,2), (1,4), (2,3); (0,0), (1,0), (2,0)} is a difference set for R. Further, the sets of differences from {(1,1), (2,2), (1,4), (2,3)} and {(0,0), (1,0), (2,0)} are disjoint.

In the array of Fig. 3 the coordinates of the element 0, namely, {(0,0), (1,0), (2,0); (1,1), (2,2), (1,4) (2,3) mod (3,5)} constitute the Stanton-Sprott difference set for the additive group G= {(a,b); mod(3,5)}.

Such difference sets are natural candidates for building blocks in the construction of uniquely decodable and delta-decodable codes for multiple access channels.

Arrays whose two-dimensional auto-correlation functions satisfy $\rho(0,0) = 1$, $\rho(i,j)$ small for $(i,j) \neq (0,0)$, have found applications in spectrometry, acoustics and cryptography for encrypting two-dimensional arrays such as images.

MacWilliams and Sloane (1976) have shown how to use pseudo-random sequences to obtain $n_1 \times n_2$ arrays with $\rho(0,0) = 1$, $\rho(i,j) = 1/n$ for $0 \leq i < n_1$, $0 \leq j < n_2$, $(i,j) \neq (0,0)$, where $n = 2^m-1 = n_1n_2$, provided n_1 and n_2 are relatively prime. Further, two-dimensional linearly recurring arrays or doubly periodic arrays over a finite field lead to two-dimensional cyclic codes which belong to the class of Abelian codes (see, for instance, Sakata 1981) and as such can be adapted for use in a two-user channel.

In clinical trials, agriculture and animal husbandry, research workers often encounter the situation where only a limited number of experimental units are available, each unit receives a prescribed sequence of treatments and a treatment applied to a unit in a previous state may influence statistically the observations on the same unit when it moves to another state. Designs for such experiments need to be planned so that efficient comparisons of *direct effects* adjusted for *residual effects* and estimation of residual effects can be made from the observations. If a *state* is defined in terms of levels of two factors, residuals will be specified in terms of two coordinates. In this context, designs balanced for two-dimensional residuals can be constructed from arrays with appropriate window properties.

Another application of such arrays will be in the design of experiments where a plant competes with neighbors of the same type and a second type (Gates, 1980; Azais 1987).

BIBLIOGRAPHY

Azais, J.M. (1987). Design of experiments for studying intergenotypic competition. *J. Roy. Statist. Soc. B*, 49 , 334-345.

van Aardenne - Ehrenfest, T. and N.G. de Bruijn (1951). Circuits and trees in oriented linear graphs. *Simon Stevin*, 28, 203-217.

Birkhoff, G. and T.C. Bartee (1970). *Modern Applied Algebra*, McGraw-Hill Co., (Ch. 13).

deBruijn, N.G. (1946). A combinatorial problem, *Nederl. Akad. Wetensch. Proc.* 49, 758-764, *Indag. Math.*, 9, 461-467.

deBruijn, N.G. (1975). Acknowledgement of priority to C. Flye Sainte-Marie on the counting of circular 2^n zeros and ones that show each n- letter word once. *Reports of the Technological University, Eindhoven*, Netherlands, Department of Mathematics, 1-14.

Chakravarti, I.M. (1978). Sainte-Marie, Aardenne-Ehrenfest, deBruijn sequences and their role in the construction of serially balanced factorial designs. *Bull. Inst. Math. Statist.* 7(5), 291-292.

Durup, H. (1967). Graphes et plan d'expériences temporels, mots circulaires et plan toriques. *Math. et Sciences Humaines, no.* 18, Centre de Mathématique Sociale et de Statistique EPHE, 1-31.

Gates, D.G. (1980) Competition between two types of plants with specified neighbor configurations. *Mathematical Biosciences* 48, 195-209.

Ma, S.L. (1984) A note on binary arrays with a certain window property. *IEEE Trans. on Information Theory*, IT-30(5), 774-775.

MacWilliams, F.J. and N.J.A. Sloane (1976) Pseudo-random sequences and arrays, *Proc. IEEE*, 64, 1715-1729.

MacWilliams, F.J. and N.J.A. Sloane (1977) The Theory of Error-Correcting Codes. *North Holland Publishing Co.*, New York and Amsterdam.

Patterson, H.D. (1968) Serial factorial designs. *Biometrika*, 55(1), 67-81.

Sakata, S. (1981) On determining the independent point set for doubly periodic arrays and encoding two dimensional cyclic codes and their duals. *IEEE Trans. Inf. Theory, IT-24, 719-730.*

Stanton, R.G. and D.A. Sprott (1958). A family of difference sets. *Canad. J. Math. 19*, 73-77.

van Lint, J.H., F.J. MacWilliams and N.J.A. Sloane (1979) On pseudo-random arrays. *SIAM J. Appl. Math.*, 36, 62-72.

Weidman, L. (1975) *Design and Analysis of Serial Experiments*. Institute of Statistics Mimeo Series No. 997. Department of Statistics, University of North Carolina at Chapel Hill.

RESUME

Dans cet article, nous avons d'abord étudié quelques propriétés combinatoires des tableaux doublement périodiques inscriptibles sur un tore (tableau torique selon Durup (1967)). Ensuite, nous constatons les utilités d'un tel tableau comme un code pour un canal a acces multiple et comme un plan d'expérience pour un essai ayant pour but l'estimation des effets directs compénses des effets residuels.