Chapter 5

Construction of Orthogonal Arrays from Codes

In this chapter we present some of the most important families of codes and the orthogonal arrays that are derived from them.

The first two sections describe some general constructions, and then Sections 5.3 to 5.10 describe specific classes of codes. One of our goals is to give explicit constructions for many of the orthogonal arrays that are mentioned in the tables in Chapter 12. These arrays are given in Sections 5.11, 5.12 and 5.13, corresponding to \( s = 2, 3 \) and 4 respectively. Most of these arrays are not well known in the statistics literature.

An important fact from the previous chapter is that if \( C \) is a \((k, N, d)_s\) linear code over \( GF(s) \), and if the dual code \( C^\perp \) has minimal distance \( d^\perp \), then the codewords of \( C^\perp \) can be used as the rows of an \( OA(N, k, s, d^\perp - 1) \).

While this chapter contains many fundamental and beautiful theorems and contributions from coding theory, a reader who wants to see detailed proofs and verifications would do well to keep a copy of MacWilliams and Sloane (1977) nearby.

5.1 Extending a Code by Adding More Coordinates

We begin by reminding the reader that, as we saw in Theorem 2.24, binary orthogonal arrays have a special property, not shared by arrays with greater numbers of levels: an \( OA(N, k, 2, 2u) \) exists if and only if an \( OA(2N, k + 1, 2, 2u + 1) \) exists.
Chapter 5. Construction of Orthogonal Arrays from Codes

There is a parallel theorem for codes — as we might expect, following the discussion in Section 4.6 — which states that a \((k, N, 2u+1)_2\) code exists if and only if a \((k+1, N, 2u+2)_2\) code exists — see MacWilliams and Sloane (1977), Chapter 2, Theorem 2.

Given a \((k, N, 2u+1)_2\) code, we obtain the \((k+1, N, 2u+2)_2\) code by appending a 0 to every codeword of even weight, and a 1 to every codeword of odd weight. This process is called extending a code, and the new code is called an extended code. This construction applies to both linear and nonlinear codes. If the original code was linear, so is the extended code.

For example, extending the \((7, 16, 3)_2\) code with generator matrix (4.7) yields an \((8, 16, 4)_2\) code with generator matrix

\[
\begin{bmatrix}
1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1
\end{bmatrix}.
\]

(5.1)

More generally, we say that a linear code has been extended whenever we modify it by adding columns to its generator matrix.

5.2 Cyclic Codes

A linear code over \(GF(s)\) is said to be cyclic if whenever

\[(c_0, c_1, \ldots, c_{k-2}, c_{k-1})\]

is a codeword, so also is

\[(c_1, c_2, \ldots, c_{k-1}, c_0).\]

(5.3)

As with most of the notions defined in this chapter, we will apply the same terminology to orthogonal arrays. Thus an \(OA(N, k, s, t)\) is cyclic if it is linear and if whenever (5.2) is a run, so is (5.3). For example, the \(OA(8, 7, 2, 2)\) and the \((7, 8, 4)_2\) code shown in (4.2) are both cyclic.

Cyclic codes and arrays have an even more economical description than linear codes. For one can show that any cyclic code or array can be described by a single vector (cf. MacWilliams and Sloane, 1977, Chapter 7, Theorem 1). Suppose the code contains \(N = s^n\) codewords, or the array contains \(N = s^n\) runs. Then there is always a single generating vector

\[g = (g_0, g_1, \ldots, g_{k-1})\]

(5.4)

such that the generator matrix consists of this vector and its first \(n - 1\) cyclic shifts. In the case of the orthogonal array and code in (4.2), for example, a generating vector is

\[g = (1110100),\]

(5.5)