Note

Orthogonal Line Packings of $PG_{2m-1}(2)$

RonalD. Baker*

Department of Mathematical Sciences,
University of Delaware, Newark, Delaware 19711

Communicated by the Managing Editors

Received June 17, 1982.

Baker (Discrete Math. 15 (1976), 205–211) has shown that there exists a packing of the lines of each odd dimensional projective space over the field of two elements as a corollary to a theorem asserting the existence of a 2-resolution of the Steiner quadruple system of planes in an even dimensional affine space over the field of two elements. Two packings are orthogonal if any two of their spreads have at most one line in common. A variation of the previous construction gives alternate packings so that, for example, the existence of orthogonal packings of $PG_{2m-1}(2)$ when three does not divide $2m - 1$ can be demonstrated.

1. THE CONSTRUCTIONS

The notation follows [1]. $V = GF(2^{2m-1}) \times GF(2)$ is a $2m$-dimensional vector space over $GF(2)$, $(X, \mathscr{O})$ is the design of planes of the affine geometry $AG_{2m}(2)$ based on $V$, and $(Y, \mathscr{B})$ is the design of lines in the projective geometry $PG_{2m-1}(2)$ obtained by removing $\emptyset = (0,0)$. For any subset $S$ of $V$ and $i = 0, 1$, let $S_i = \{x: (x, i) \in S\}$. For any subset $F$ of $GF(2^{m-1})$ let $\sum F$ denote the sum of the $j$th powers of the elements of $F$. Let $\omega$ be a primitive element of $GF(2^{m-1})$ and $T_\omega$ the collineation of $AG_{2m}(2)$ (and $PG_{2m-1}(2)$) which maps $(a, i)$ onto $(\omega a, i)$.

The variation on the construction in [1] uses $u = 1 + 2^s$, $1 \leq s \leq 2m - 2$, in place of 3. Thus for each nonzero element $\alpha$ of $GF(2^{2m-1})$ let

$$\mathcal{A}_{\alpha, u} = \left\{ A \in \mathcal{A} : \sum A_0 + \sum A_1 + \left( \sum A_1 \right)^u = \alpha^u \right\}$$

and

$$\mathcal{B}_{\alpha, u} = \left\{ L \in \mathcal{B} : \sum L_0 + \sum L_1 + \left( \sum L_1 \right)^u = \alpha^u \right\}.$$

* The author was at North Carolina State University while preparing this article.
2. Resolutions and Packings

The results of [1] are immediately generalized to suitable \( u = 1 + 2^s \).

**Lemma 1.** The class \( \mathcal{A}_{a,u} \) is invariant under translation, i.e., if \( B = A + v \) for \( v \in V \), then

\[
\sum_{i=0}^{u-1} B_i + \left( \sum_{i=0}^{u-1} B_i \right)^u = \sum_{i=0}^{u-1} A_i + \left( \sum_{i=0}^{u-1} A_i \right)^u.
\]

**Lemma 2.** Suppose \( s \) and \( 2m - 1 \) are relatively prime. For any block \( A \) of \( \mathcal{A} \) the value of \( \sum_{i=0}^{u-1} A_i + \left( \sum_{i=0}^{u-1} A_i \right)^u \) is not zero.

**Lemma 3.** Suppose \( s \) and \( 2m - 1 \) are relatively prime. Let \( a, c \in GF(2^{2m-1}) \), \( a \neq 0 \), and suppose \( \bar{a} \) is such that \( \bar{a}^{2^{2m-1}-1} = a \). Then exactly one of the two polynomials \( x^{2^{u}} + ax + c \) and \( x^{2^{u}} + ax + c + a\bar{a} \) has roots in \( GF(2^{2m-1}) \), and it has exactly two roots.

**Theorem 1.** Suppose \( s \) and \( 2m - 1 \) are relatively prime. The partition of \( \mathcal{A} \) into the \( \mathcal{A}_{a,u} \) is a 2-resolution of \( (X, \mathcal{A}) \) and the partition of \( \mathcal{B} \) into the \( \mathcal{B}_{a,u} \) is a packing of spreads in \( (Y, \mathcal{B}) \). Both partitions are cyclically generated by \( T_0 \).

The proofs of these results are essentially those given in [1] for \( u = 3 \). The condition that \( s \) and \( 2m - 1 \) be relatively prime gives the existence of unique \( u \)th and \( (u - 2) \)th roots in \( GF(2^{2m-1}) \). If \( y \) is a root of \( x^{2^{u}} + x + 1 \), then \( y^{2^{2m-1}} + y^{2^{2m-2}} + \cdots + y \) is a root of \( x^{2} + x + 1 \). In proving Theorem 1 the line \( L \) on \( (a, 0) \) in \( \mathcal{B}_{a,u} \) is \( L = \{(a, 0), (b, i), (c, i)\} \) for \( b, c \) the roots of \( x^{2^{u}} + a^{2^{u-1}}x + a^{-1}a^{u} + ia^{2^{u}} \) for \( i = 0 \) or 1. Likewise the line on \( (b, 1) \) is \( L = \{(b + (b, 1), ((b^{u} + a^{u})^{1/u}, 1)\} \), which illustrates the need for unique \( u \)th roots.

3. Orthogonal Packings

Two packings of \( PG_{2m-1}(2) \) are orthogonal if any two of their spreads have at most one line in common. The existence of a pair of orthogonal packings of \( PG_{2m-1}(2) \) is equivalent to the existence of a square array of side \( 2^{2m-1} - 1 \) whose cells contain the lines of \( PG_{2m-1}(2) \) subject to the restrictions that, (i) each cell contains at most one line and each line is in exactly one cell, and (ii) each row and each column of the array contains the lines of a spread. Theorem 1 provides many orthogonal pairs of packings, including the series of Theorem 2.
ORTHOGONAL LINE PACKINGS OF $PG_{2m-1}(2)$

**Theorem 2.** If $m \not\equiv 2 \pmod{3}$, then $PG_{2m-1}(2)$ admits a pair of orthogonal packings. In particular the packings for $u = 1 + 2^{m-1}$ and $1 + 2^{m-2}$ are orthogonal.

**Proof:** Let $u = 1 + 2^{m-1}$, $u' = 1 + 2^{m-2}$, and note that both provide packings by Theorem 1 when $m \not\equiv 2 \pmod{3}$. Now suppose $L, L' \subseteq \mathcal{F}_{a, u} \cap \mathcal{F}_{b, u}$, for some $a, b \in GF(2^{2m-1})$. To show $L = L'$ it suffices to show that the symmetric difference $L \Delta L'$ is empty or contains at least eight elements ($L, L'$ lines implies $|L \Delta L'| \leq 6$). Let $X = (L \Delta L'_0) + \delta$ and $Y = L_1 \Delta L'_1$, where $\delta = \sum_1^{11} L_0$. Direct computation shows that $\sum_0^{11} X = \sum_0^{11} Y = 0$, $\sum_1^{11} X = \sum_1^{11} Y$, $\sum_{u'} X + \sum_{u'} Y + (\sum_1^{11} X)^u = 0$, and $\sum_{u'} X + \sum_{u'} Y + (\sum_1^{11} X)^{u'} = 0$. Now these conditions are symmetric in the roles of $X$ and $Y$, while Lemma 1 shows that $(X + Y, Y + b)$ satisfies the conditions if $(X, Y)$ does. If $Y = \emptyset$, then $\sum_0^{11} X = \sum_0^{11} Y = \sum_0^{11} X = \sum_{u'} Y = 0$. If $Y = \{0, a\}$ then $\sum_0^{11} X = \sum_{u'} X = \sum_{u'} Y = 0$ and $\sum_1^{11} X = a$. The proof of the theorem is completed by Lemma 4.

**Lemma 4.** Let $u = 1 + 2^{m-1}$, $u' = 1 + 2^{m-2}$, and $S \subseteq GF(2^{2m-1})$, $S \neq \emptyset$. If $\sum_0^{11} S = \sum_{u'} S = \sum_{u} S = 0$, then $|S| > 6$, and if additionally $\sum_1^{11} S = 0$, then $|S| > 8$.

**Proof:** It suffices to show that $S \neq \emptyset$ and $\sum_{u} S = \sum_{u'} S = 0$ imply $|S| > 5$, and if additionally $\sum_1^{11} S = 0$ that $|S| > 7$. For $y \in GF(2^{2m-1})$, $T(y) = y + y^2 + \cdots + y^{2^{2m-2}}$ is the trace function. For $x \in GF(2^{2m-1})$ let $f_S(x) = \sum_{i=0}^{2^{2m-2}} \sum_{a \in S} a^{1 + 2^i} x^{2^i}$. On the other hand $f_S(x) = \sum_{a \in S} a T(ax)$, which shows that the range of $f_S(x)$ is spanned by $S$. Now if $f_S(x)$ is the zero polynomial then $\sigma_0 = \sigma_1 = \sigma_2 = 0$, which means $\sum_1^{11} S = \sum_2^{11} S = \sum_1^{11} S = \sum_2^{11} S = \sum_2^{11} S = \sum_1^{11} S = 0$ (using the Frobenius automorphism). Let $\hat{a} = (a, a^2, a^3, a^4, a^5, a^6)$ for $a \in S$, and note the vectors $\{\hat{a}: a \in S\}$ are linearly dependent in this case (they sum to the zero vector). But if $|S| \leq 6$ the vectors $\hat{a}$ are rows of a nonsingular (Vandermonde) matrix, a contradiction. Hence $|S| > 7$, when $f_S(x)$ is the zero polynomial. For $\sum_{u'} S = \sum_{u} S = 0$ it follows that $\sigma_{m-2} = \sigma_{m-1} = \sigma_0 = \sigma_{m+1} = 0$. Using $x_2^{2m-1} = x$ for $x \in GF(2^{2m-1})$, $(f_S(x))_2^{2m-3} = \sigma_0^{m-3} X^{2m-3} + \cdots + \sigma_{m-3}^{m-3} x_2^{2m-3} + \sigma_{m-2}^{m-2} x + \cdots + \sigma_2^{m-2} x^{2m-4}$, so that $\text{kernel} f_S(x) \leq 2^{2m-6}$. This implies $|\text{range} f_S(x)| \geq 2^5$, and hence $|S| \geq 5$ by the observation that $S$ spans the range of $f_S(x)$. Moreover $|S| = 5$ if and only if $S$ is a basis for the range of $f_S(x)$. Thus if $\sigma_0 = 0$, as well as $\sigma_{m-2} = \sigma_{m-1} = \sigma_0 = \sigma_{m+1} = 0$, then $|S| \geq 6$. Suppose $|S| = 6$, say $S = \{a_1, a_2, \ldots, a_6\}$ and consider the set $\tilde{S} = \{a_1 + a_6, a_2 + a_5, a_3 + a_6\}$. Direct computation shows $\sum_1^{11} \tilde{S} = \sum_{u'} \tilde{S} = \sum_{u'} \tilde{S} = 0$, whence $|\tilde{S}| > 6$ by the above argument, a contradiction. Thus $|S| > 7$ whenever $\sum_{u} S = \sum_{u'} S = 0$, as claimed.
The proof of Lemma 4 is due to R. M. Wilson, and has been used in coding theory (see [2]). Indeed the argument of Lemma 4 can be applied to other pairs of indices in both the context of orthogonal packings and in the context of generalizing Goethal’s nonlinear triple-error-correcting codes.

References

1. R. D. Baker, Partitioning the planes of $AG_{2m}(2)$ into $2$-designs, *Discrete Math.* 15 (1976), 205–211.