Pacific Journal of Mathematics

5-DESIGNS IN AFFINE SPACES

WILLIAM O'BANNON ALLTOP

Vol. 39, No. 3 July 1971

PACIFIC JOURNAL OF MATHEMATICS
Vol. 39, No. 3, 1971

5-DESIGNS IN AFFINE SPACES

W. O. ALLTOP

The n-dimensional affine group over $GF(2)$ is triply transitive on 2^n symbols. For $n \geqq 4$, $4 \leqq k \leqq 2^{n-1}$, any orbit of k-subsets is a 3-$(2^n, k, \lambda)$ design. In this paper a sufficient condition that such a design be a 4-design is given. It is also shown that such a 4-design must always be a 5-design. A 5-design on 256 varieties with block size 24 is constructed in this fashion.

We shall call $(\Omega, \mathscr{D})$ a t-(v, k, λ) design whenever $|\Omega| = v$, $\mathscr{D}$ is a family of k-subsets of Ω and every t-subset of Ω is contained in exactly λ members of $\mathscr{D}$. The design is nontrivial provided $\mathscr{D}$ is a proper subfamily of Σ_k, the family of all k-subsets of Ω. If G is a nontrivial t-ply transitive group acting on Ω, then an orbit of k-subsets under G yields a t-design. The design is nontrivial if G is not k-homogeneous (transitive on unordered k-subsets). The first known 5-designs arose from orbits under the quintuply transitive Mathieu groups M_{12} and M_{24}. Other 5-designs on 12, 24, 36, 48 and 60 varieties have been discovered (see [2; 3; 4]). In [1] a 5-design on $2^n + 2$ varieties is constructed for every $n \geqq 4$. Here we shall discuss 5-designs on 2^n varieties, giving one example for $n = 8$.

Let Ω be an n-dimensional vector space over $GF(2)$, $n \geqq 4$. Let L be the linear group $GL(n, 2)$ acting doubly transitively on $\Omega - \{0\}$ and T the group of translations t_α: $\omega \rightarrow \omega + \alpha$. The group $A = \langle L, T\rangle$ is the triply transitive affine group on Ω. Let Σ_4, Σ_5 denote the families of 4-, 5-subsets of Ω respectively. $(\Omega, \mathscr{S}_0)$ is a 3-$(2^n, 4, 1)$ design where $\mathscr{S}_0$ is the family of quadruples $\{\omega_i\}$ satisfying

$$\omega_1 + \omega_2 + \omega_3 + \omega_4 = 0 .$$

$\mathscr{S}_0$ is the orbit of affine planes in Ω. $\mathscr{S}_1$ is also an orbit, where $\mathscr{S}_1 = \Sigma_4 - \mathscr{S}_0$. Thus, A decomposes Σ_4 into only two orbits. From the design parameters of $(\Omega, \mathscr{S}_0)$ one establishes that

$$|\mathscr{S}_0| = \frac{1}{4}\binom{2^n}{3}$$

$$|\mathscr{S}_1| = (2^{n-2} - 1)\binom{2^n}{3} .$$

Suppose $Q \in \mathscr{S}_0$. The stabilizer of Q in A is transitive on $\Omega - Q$. Thus, $\mathscr{T}_0$ is an orbit under A, where $\mathscr{T}_0$ consists of those members of Σ_5 which contain a member of $\mathscr{S}_0$. Now suppose $R \in \Sigma_5 - \mathscr{T}_0$.

Clearly there exists a translate of R of the form

$$R_0 = \{0, \omega_1, \omega_2, \omega_3, \omega_4\} .$$

Since R_0 contains no member of $\mathscr{S}_0$, the ω_i's must be linearly independent in Ω considered as a vector space. Since L is transitive on linearly independent quadruples in $\Omega - \{0\}$, it follows that A must be transitive on the family $\mathscr{T}_1$, where $\mathscr{T}_1 = \Sigma_5 - \mathscr{T}_0$. Therefore, A also decomposes Σ_5 into only two orbits. From our knowledge of $|\mathscr{S}_0|$ we can deduce that

$$|\mathscr{T}_0| = (2^n - 4)\ |\mathscr{S}_0| ,$$

$$|\mathscr{T}_1| = \frac{1}{5}(2^n - 4)(2^n - 8)\ |\mathscr{S}_0| .$$

Geometrically $\mathscr{T}_0$ consists of the 5-subsets which generate 3-dimensional affine subspaces of Ω, while the members of $\mathscr{T}_1$ generate 4-dimensional subspaces. This classification of orbits in Σ_4 and Σ_5 will provide the information needed to investigate 4- and 5-designs which arise from orbits under A.

Suppose Δ is a k-subset of Ω and let $\mathscr{D}$ denote the orbit of Δ under A. Let σ_i, τ_i denote the number of members of $\mathscr{S}_i$, $\mathscr{T}_i$ contained in Δ respectively, $i = 0, 1$. Let λ_i, μ_i denote the number of members of $\mathscr{D}$ containing a fixed member of $\mathscr{S}_i$, $\mathscr{T}_i$ respectively, $i = 0, 1$. If $\lambda_0 = \lambda_1$ ($\mu_0 = \mu_1$), then $(\Omega, \mathscr{D})$ is a 4-design (5-design). The following equations relating the σ_i, τ_i, λ_i, μ_i are the result of straightforward counting arguments:

$$\sigma_i\,|\mathscr{D}| = \lambda_i\,|\mathscr{S}_i| \tag{1}$$

$$\tau_i\,|\mathscr{D}| = \mu_i\,|\mathscr{T}_i| \tag{2}$$

$$\tau_0 = \sigma_0(k - 4) . \tag{3}$$

From (1) and the fact that

$$|\mathscr{S}_0|/|\mathscr{S}_1| = 1/(2^n - 4)$$

we see that $(\Omega, \mathscr{D})$ is a 4-design if and olyn if

$$\sigma_1 = \sigma_0(2^n - 4) . \tag{4}$$

Likewise from (2) and the fact that

$$|\mathscr{T}_0|/|\mathscr{T}_1| = 5/(2^n - 8)$$

we see that $(\Omega, \mathscr{D})$ is a 5-design if and only if

$$\tau_1 = \tau_0(2^n - 8)/5 . \tag{5}$$

Since $\sigma_1 = \binom{k}{4} - \sigma_0$ and $\tau_1 = \binom{k}{5} - \tau_0$, we can use (3) to express σ_1, τ_0, τ_1 in terms of σ_0 and k. Substituting accordingly for σ_1, τ_0, τ_1 in (4) and (5) we obtain

$$(4') \qquad \binom{k}{4} - \sigma_0 = \sigma_0(2^n - 4)$$

$$(5') \qquad \binom{k}{5} - \sigma_0(k-4) = \sigma_0(k-4)(2^n - 8)/5 .$$

After simplifying the preceding equations we see that both (4′) and (5′) are equivalent to

$$(6) \qquad \sigma_0 = \binom{k}{4}\Big/(2^n - 3) .$$

We have in effect proved the following

THEOREM. *$(\Omega, \mathscr{D})$ is a 5-design whenever $(\Omega, \mathscr{D})$ is a 4-design. A necessary and sufficient condition for this to take place is that* $\sigma_0 = \binom{k}{4}\Big/(2^n - 3)$.

The first thing to note is that $2^n - 3$ must divide $\binom{k}{4}$ for such a 5-design to exist. This is not possible for $6 \leqq k \leqq 2^{n-1}$ if $2^n - 3$ is a prime power. Therefore, the first feasible value of n is eight. For $n = 8$, the values of $k \leqq 2^7$ for which $2^n - 3$ divides $\binom{k}{4}$ are 23, 24, 25, 46, 47 and 69. We pursue the case $n = 8$, $k = 24$.

Our theorem tells us that for $|\Delta| = 24$, $(\Omega, \mathscr{D})$ is a 5-design provided $\sigma_0 = 42$. We must select a 24-subset Δ which contains exactly 42 members of $\mathscr{S}_0$. One example of such a Δ is the following. Let $(u_1, u_2, u_3, v_1, v_2, v_3, w_1, w_2)$ be a basis for the vector space Ω. We define 3-dimensional vector subspaces of Ω:

$$\begin{aligned} U_0 &= (u_1, u_2, u_3) \\ V_0 &= (v_1, v_2, v_3) \\ W_0 &= (u_1 + v_1, u_2 + v_2, u_3 + v_3) . \end{aligned}$$

Now let $\Delta = U \cup V \cup W$, where

$$\begin{aligned} U &= U_0 + w_1 \\ V &= V_0 + w_2 \\ W &= W_0 + (w_1 + w_2) . \end{aligned}$$

For this Δ it is clear that $\sigma_0 \geqq 42$ since each of the 3-dimensional affine subspaces U, V, W contains 14 members of $\mathscr{S}_0$. Suppose Δ contains additional members of $\mathscr{S}_0$. There exists $Q \in \mathscr{S}_0$ such that Q meets at least two members of $\{U, V, W\}$. In order to decrease the number of cases to be considered we investigate the action of the stabilizer of Δ on $\{U, V, W\}$. Let $x, y \in L$ be defined by

$$x\colon \begin{cases} u_i \longrightarrow v_i \longrightarrow (u_i + v_i) \longrightarrow u_i, & 1 \leqq i \leqq 3 \\ w_1 \longrightarrow w_2 \longrightarrow (w_1 + w_2) \longrightarrow w_1 \end{cases}$$

$$y\colon \begin{cases} u_i \longrightarrow v_i \longrightarrow u_i, & 1 \leqq i \leqq 3 \\ w_1 \longrightarrow w_2 \longrightarrow w_1 \,. \end{cases}$$

Letting x^*, y^* denote the action of x, y on $\{U, V, W\}$, we have

$$\begin{aligned} x^*\colon &\quad U \rightarrow V \rightarrow W \rightarrow U \\ y^*\colon &\quad U \rightarrow V \rightarrow U, \quad W \rightarrow W \,. \end{aligned}$$

Hence, $\langle x^*, y^* \rangle$ acts as the symmetric group S_3 on $\{U, V, W\}$. We must only consider the cases where the partition of Q induced by (U, V, W) is of the form $(2, 2, 0)$, $(3, 1, 0)$ or $(2, 1, 1)$. These three cases are easily seen to be impossible, so no such Q exists. It follows that $\sigma_0 = 42$, and we have a 5-design on 256 varieties with blocks of size 24.

One wonders in how many affine spaces Ω such 5-designs exist. Since 143 divides $2^n - 3$ whenever $n \equiv 28 \pmod{60}$, there are infinitely many values of n for which $2^n - 3$ is not a prime power. For fixed k, n, with $6 \leqq k \leqq 2^{n-1}$, let us consider the problem heuristically. Suppose we select Δ from Σ_k randomly, each member of Σ_k having probability $1\Big/\binom{2^n}{k}$ of being selected. Now σ_0 is a random variable on the probability space Σ_k. The expectation of σ_0 is

$$E = \binom{k}{4}\Big/(2^n - 3) \,.$$

A 5-design of the type under consideration exists if and only if σ_0 achieves its expectation in Σ_k. When E is an integer, it does not seem unreasonable that σ_0 would achieve its expectation.

The author has not investigated the construction of designs in affine spaces over $GF(2)$ by using more than one orbit under A.

References

1. W. O. Alltop, *An infinite class of 5-designs*, to appear.
2. E. F. Assmus, Jr., and H. F. Mattson, Jr., *New 5-designs*, J. Combinatorial Theory, **6** (1969), 122–151.
3. D. R. Hughes, *On t-designs and groups*, Amer. J. Math., **87** (1965), 761–778.

4. Vera Pless, *On a new family of symmetry codes and related new 5-designs*, Bull. Amer. Math. Soc., **75** (1969), 1339–1342.

Received February 16, 1970. Part of the results in this paper were presented to a meeting of Navy Mathematicians at Colorado State University, Fort Collins, Colorado, August 20, 1970.

MICHELSON LABORATORIES, CHINA LAKE, CALIFORNIA

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. The editorial "we" must not be used in the synopsis, and items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in duplicate if possible, may be sent to any one of the four editors. Please classify according to the scheme of Math. Rev. Index to Vol. **39**. All other communications to the editors should be addressed to the managing editor, Richard Arens, University of California, Los Angeles, California, 90024.

50 reprints are provided free for each article; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is $8.00; single issues, $3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues $1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics

Vol. 39, No. 3 July, 1971