Discrete Mathematics 46 (1983) 95–98
North-Holland

NOTE

EXPONENTIAL NUMBERS OF TWO-WEIGHT CODES, DIFFERENCE SETS AND SYMMETRIC DESIGNS

William M. KANTOR*

Department of Mathematics, University of Oregon, Eugene, OR 97403-1222, USA

Received 7 June 1982

1. Introduction

The purpose of this paper is to obtain exponential lower bounds on the numbers of non-isomorphic linear codes or symmetric designs of certain types. This will be accomplished using a familiar—even mundane—object related to the desarguesian affine plane $AG(2, q^n)$. Namely, let V be a 2-dimensional vector space over $GF(q^n)$, and let Δ be its set of 1-spaces. We will use subsets Σ of Δ to define a code C_Σ and, when $q=2$, a difference set U_Σ and a symmetric design D_Σ. As in [5], we will then use Sylow's Theorem in order to deal with isomorphism questions.

2. Constructions

In order to construct C_Σ, regard V as a $2n$-dimensional vector space over $GF(q)$, fix a basis, and let $u\cdot v$ denote the usual dot product with respect to that basis. Let U_Σ denote the union of the members of Σ, so that $|U_\Sigma| = 1+|\Sigma|\,(q^n-1)$. Let $\langle u_1\rangle, \ldots, \langle u_N\rangle$ be all the 1-spaces contained in U_Σ. Set

$$C_\Sigma = \{(x\cdot u_1, \ldots, x\cdot u_N) \in GF(q)^N \mid x \in V\}.$$

Then C_Σ is a projective two-weight code of length N. We will assume that $2<|\Sigma|<q^n-1$, $n>2$, and $q^n \neq 2^6$. (Note that $\Sigma \subset \Delta$ where $|\Delta| = q^n+1$.) Then $\dim C_\Sigma = 2n$ and the weight distribution of C_Σ is completely determined by q, n and t. We refer to [1] for a discussion of this simple construction.

Theorem 1. *Let* $2<t<q^r-1$. *Then there are at least*

$$\binom{q^n+1}{t} \Big/ 2(q^n+1)q^{2n}(q^n-1)^2$$

* This research was supported in part by NSF Grant MCS 7903130

pairwise inequivalent projective linear $[t(q^n-1)/(q-1), 2n]$ *two-weight codes over* $\mathrm{GF}(q)$ *of the form* C_Σ *with* $\Sigma\subset\Delta$ *and* $|\Sigma|=t$.

For bounded $|\frac{1}{2}q^n-t|$ and large n, the number of codes is asymptotically at least $C2^{q^n}/q^{11n/2}$ for some constant C.

Next, let $q=2$ and $|\Sigma|=2^{n-1}+1$. Then U_Σ is a difference set in the additive group V (Dillon [3]). Its parameters are $v=2^{2n}$, $k=2^{2n-1}+2^{n-1}$, $\lambda=2^{2n-2}+2^{n-1}$.

Theorem 2. *There are at least*

$$\binom{2^n+1}{2^{n-1}}\Big/(2^n+1)2^n(2^n-1)^2n$$

pairwise inequivalent $(2^{2n}, 2^{2n-1}+2^{n-1}, 2^{2n-2}+2^{n-1})$ *difference sets in* V *of the form* U_Σ *with* $\Sigma\subset\Delta$.

Note that each U_Σ determines a symmetric (v, k, λ)-design. While these designs are undoubtedly not isomorphic when the corresponding U_Σ are inequivalent, this seems difficult to prove.

However, we have been able to deal with other symmetric designs having the same parameters. Let $q=2$ and $|\Sigma|=2^{n-1}+1$ once again. Consider all symmetric differences of U_Σ with the hyperplanes of $\mathrm{AG}(2n, 2)$. Each has size $k=|U_\Sigma|$ or $v-k$; and those of size k, together with U_Σ, form a symmetric design D_Σ (compare [3, 4, 6]).

Theorem 3. *There are at least*

$$\binom{2^n+1}{2^{n-1}}\Big/(2^n+1)2^n(2^n-1)^2n$$

pairwise non-isomorphic $(2^{2n}, 2^{2n-1}+2^{n-1}, 2^{2n-2}+2^{n-1})$ *designs* D_Σ *with* $\Sigma\subset\Delta$.

Note that the design D_Σ and the difference set design produced by U_Σ need not be isomorphic. It seems likely that they are isomorphic only if U_Σ is the set of zeros of a quadratic form (cf. [4]).

I am indebted to J.F. Dillon for posing the question that led to Theorem 2.

3. Sylow subgroups

Let q, n, V and Δ be as before. Let p be the prime dividing q. There is a prime power r^e (where r is prime) such that $r^e\mid q^n-1$ but $r^e\nmid p^i-1$ for $0<p^i-1<q^n-1$ (Zsigmondy [7]). Let R be a Sylow r-subgroup of the group of maps $(x, y)\to(\alpha x, \alpha y)$ belonging to $\Gamma\mathrm{L}(2, q^n)$. Then R sends each member of Δ to itself.

Proposition. *Let Σ, $\Sigma' \subset \Delta$. Assume that R is a Sylow subgroup of the stabilizer of Σ in $\Gamma L(2, q^n)$. If g is in the affine group $A\Gamma L(2n, q)$ of V, and if $(U_\Sigma)^g = U_{\Sigma'}$, then there is an element $h \in \Gamma L(2n, q)$ such that $(U_\Sigma)^{gh} = U_{\Sigma'}$ and $gh \in \Gamma L(2, q^n)$ (so that $\Delta^{gh} = \Delta$).*

Proof. First, note that the normalizer of R in $A\Gamma L(2n, q)$ is just $\Gamma L(2, q^n)$. For, R fixes exactly one vector, namely 0; and, in view of our choice of r, Δ is precisely the set of proper R-invariant subspaces of V. Thus, the normalizer fixes 0 and sends Δ to itself.

Set $H = \{h \in A\Gamma L(2n, q) \mid (U_\Sigma)^h = U_\Sigma\}$, and define H' similarly. Clearly, $R \leq H \cap H'$.

We claim that R is a Sylow r-subgroup of H. For otherwise, there is an r-subgroup R_1 of H with $R_1 \rhd R$. Then $R_1 \leq \Gamma L(2, q^n)$, so that R_1 preserves both Δ and U_Σ. But then R_1 also preserves Σ, contrary to the hypothesis of the proposition.

Now $R^g = g^{-1}Rg$ is a Sylow r-subgroup of $H^g = H'$. By Sylow's Theorem, $(R^g)^h = R$ for some $h \in H'$. Then $gh \in \Gamma L(2, q^n)$ and $(U_\Sigma)^{gh} = (U_{\Sigma'})^h = U_{\Sigma'}$, as required.

4. Theorems 1, 2 and 3

Proof of Theorem 1. Let Σ, $\Sigma' \subset \Delta$ with $|\Sigma| = |\Sigma'| = t$. If U_Σ and $U_{\Sigma'}$ are inequivalent under $GL(2n, q)$, then C_Σ and $C_{\Sigma'}$ are inequivalent (see, e.g., [1, §2B]). By the proposition, we only need to find a lower bound for the number of $\Gamma L(2, q^n)$-orbits of subsets Σ of size t.

Let $\Sigma \subset \Delta$ with $|\Sigma| = t$, and assume that some r-subgroup R_1 of $\Gamma L(2, q^n)$ preserves Σ, where $R_1 > R$. Then R_1 fixes exactly two members of Δ. Thus, if $t \not\equiv 0, 1, 2 \pmod r$, then no such R_1 can exist In this situation, the proposition asserts that the number of inequivalent sets U_Σ is at least

$$\binom{q^n+1}{t} \Big/ |P\Gamma L(2, q^n)| = \binom{q^n+1}{t} \Big/ (q^n+1)q^n(q^n-1)^2 \log_p q^n,$$

where p is the prime dividing q.

Now consider the cases $t \equiv \varepsilon \pmod r$ with $\varepsilon = 0$, 1 or 2. We will estimate the number of t-element subsets Σ of Δ fixed by a subgroup R_1 of $P\Gamma L(2, q^n)$ of order r. The number of R_1 is $(q^n+1)q^n/2(2, q-1)$, and R_1 fixes exactly

$$\binom{(q^n+1-\varepsilon)/r}{(t-\varepsilon)/r}\delta$$

t-sets Σ, where $\delta = 1$ if $\varepsilon = 0$ or 2, but $\delta = 2$ if $\varepsilon = 1$. Thus, we must avoid at most

$$\binom{(q^n+1-\varepsilon)/r}{(t-\varepsilon)/r}\delta \cdot (q^n+1)q^n/2(2, q-1)$$

t-sets Σ in order to apply the proposition. Splitting the remaining ones into orbits under $\mathrm{P\Gamma L}(2, q^n)$, we obtain at least

$$\left\{\binom{q^n+1}{t}-\binom{(q^n+1-\varepsilon)/r}{(t-\varepsilon)/r}\frac{\delta\cdot(q^n+1)q^n}{2(2,q-1)}\right\}\Big/(q^n+1)q^n(q^n-1)^2\log_p q^n$$

different orbits, and hence at least that many inequivalent sets U_Σ. The preceding number is at least as large as the required bound.

Proof of Theorem 2. Two difference sets U_Σ and $U_{\Sigma'}$ are (by definition) equivalent if and only if there is an element of $\mathrm{A\Gamma L}(2n, 2)$ taking the first to the second. But $|\Sigma| = 2^{n-1}+1 \not\equiv 0, 1, 2 \pmod r$; for example, if $2^{n-1}+1 \equiv 0 \pmod r$, then $2^{2n-2} \equiv 1 \equiv 2^n \pmod r$ and hence $2^2 \equiv 1 \pmod r$. Thus, the proposition applies as above

Proof of Theorem 3. Consider all the symmetric differences of pairs of distinct blocks, and the complements of these symmetric differences. These sets of points constitute all the hyperplanes of $\mathrm{AG}(2n, 2)$. Thus, any isomorphism between designs D_Σ induces (and is then induced by) a collineation of $\mathrm{AG}(2n, 2)$. Consequently, we can proceed exactly as before.

Remark. The case $n = 2$ can be handled very similarly. Note that all proofs applied so long as $q+1$ was not a power of 2; but that case does not create any significant difficulties.

References

[1] R. Calderbank and W.M. Kantor, The geometry of two-weight codes (submitted)
[2] P. Dembowski, Finite Geometries (Springer-Verlag, Berlin, 1968)
[3] J.F. Dillon, Elementary Hadamard difference sets, in: Proc. 6th S. E. Conf. Combinatorics, Graph Theory and Computing (Utilitas Math., Winnipeg, 1975) 237–249
[4] W.M. Kantor, Symplectic groups, symmetric designs, and line ovals, J. Algebra 33 (1975) 43–58
[5] W.M. Kantor, On the inequivalence of generalized Preparata codes, IEEE Trans. Inf. Theory, to appear.
[6] O.S. Rothaus, On 'bent' functions, J. Combin. Theory (A) 20 (1976) 300–305
[7] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys. 3 (1892) 265–284