The Dimension of the Code of a Strongly Resolvable Design

Mavron, V. C.; McDonough, Thomas

Publication date:
2010

Citation for published version (APA):
Mavron, V. C., & McDonough, T. (2010). *The Dimension of the Code of a Strongly Resolvable Design*. 203-206.
http://hdl.handle.net/2160/5967

The Dimension of the Code of a Strongly Resolvable Design

T. P. McDonough V. C. Mavron

January 9, 2010

Abstract

This paper gives an explicit value for the dimension of the code of a strongly resolvable design over the field of prime order p in the case when p is not a divisor of $k - \rho$, where k is the block size of the design and ρ is the number of points in the intersection of two distinct blocks in the same resolution class.

Keywords: Codes, finite geometry, strongly resolvable and affine designs.

2010 Mathematics Subject Classification: Primary 94B05, 05B25, 94B27; Secondary 05B15, 94B65

1 Introduction

In this paper we consider some situations in which the dimension of the code of a strongly resolvable design over the field of prime order p may be determined explicitly. We show that there is such a form when p is not a divisor of $k - \rho$, where k is the block size of the design and ρ is the size of the intersection of two distinct blocks in the same resolution class.

The definitions and notation for designs that we shall need are outlined briefly here; more details can be found in the books by Assmus and Key [1] and by Beth, Jungnickel and Lenz [2].

A t-(v, k, λ) design $\mathcal{D}$, where t, v and k are positive integers, and λ is a non-negative integer, consists of a finite set $\mathcal{P}$ of order v, called the *points* of $\mathcal{D}$, together with a collection $\mathcal{B}$ of k-subsets of $\mathcal{P}$, called *blocks*, such that any two distinct points are contained in exactly λ blocks.

It is well-known that a t-design is also an s-design for any s with $0 < s \leq t$. The number of blocks through any point is therefore a constant and is usually denoted by r and called the *replication* number. The number of blocks $|\mathcal{B}|$ is denoted by b.

The design $\mathcal{D}$ is *symmetric* if $b = v$. A 2-design with $v > k > 1$ is symmetric if, and only if, any two distinct blocks meet in a constant number of points (the constant is necessarily λ); or equivalently the dual design is also a 2-design.

The design $\mathcal{D}$ is *resolvable* if it has a *resolution*; that is, $\mathcal{B}$ can be partioned into subsets, called *parallel classes*, such that each parallel class partitions $\mathcal{P}$. Blocks in the same parallel class are said to be *parallel*. It is easy to see that the number of parallel classes is r and that each parallel class has the same number $m = v/k$ of blocks.

If the resolution is such that any two non-parallel blocks meet in a constant number of points, say μ, then Π is said to be *affine*. In this case it is easy to show that $\mu = k/m = k^2/v$.

Affine 1-designs are also called *nets*. Some authors reserve the term net for affine designs with $\mu = 1$ only. Nets are also the dual designs of transversal designs and their existence is equivalent to that of certain types of orthogonal arrays. For more details, see Hedeyat, Sloane and Stufken [3].

The concept of strong resolvability is related to that of resolvability but is not quite a generalization of it.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a 1-(v, k, r) design, with $v > k$. Then $\mathcal{D}$ is said to be *strongly resolvable* if there exist constants ρ, σ, and μ, and a partition of $\mathcal{B}$, into m-subsets called *resolution classes*, such that:

- through any point there are exactly σ blocks from each resolution class;
- any two distinct blocks meet in either ρ or μ points together, according as they are or are not in the same resolution class.

We call ρ the *inner constant* and μ the *outer constant*.

We have the following arithmetical relations between these parameters: (i) $\rho = k(km - v)/v(m - 1)$, (ii) $\mu = k^2/v$, (iii) $\sigma = rm/b$. The number of resolution classes is r/σ. Some further relations are: (iv) $k + \rho(m - 1) = \mu m$, (v) $\mu b = rk$, (vii) $(k - \rho)(m - 1) = \sigma(v - k) = k(m - \sigma)$. Note that $0 \leq \rho < k$, $1 \leq \mu < k$ and $1 \leq \sigma < m$.

Affine designs are the strongly resolvable designs with $\rho = 0$, $\sigma = 1$ and, if $k > 1$, $\mu = k/m$.

Strongly resolvable designs with only one resolution class are precisely the dual designs of 2-designs. Therefore, symmetric 2-designs are precisely the strongly resolvable 2-designs with only one resolution class.

Let p be a prime and let $\mathbb{F}_p$ be the field of size p. Let V be the v-dimensional $\mathbb{F}_p$-space. The *code* $\mathbf{C}(\mathcal{D})$ of the design $\mathcal{D}$ over the field $\mathbb{F}_p$ is the subspace generated by the characteristic vectors of the blocks of the design, regarded as subsets of its point set, in $\mathbb{F}_p$-space. The *p-dimension* of $\mathbf{C}(\mathcal{D})$ is its dimension as a subspace of V.

2 The Dimension Theorem

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a strongly resolvable 1-(v, k, r) design, where $k < v$, with resolution classes of size $m > 1$, inner constant ρ and outer constant μ, and let $b = |\mathcal{B}|$.

Let p be a prime and let $\mathbb{F}_p$ be the field of size p. Let V be the $\mathbb{F}_p$-space with basis $\{v_P \colon P \in \mathcal{P}\}$ of size $|\mathcal{P}|$, and let $\mathbf{C} = \mathbf{C}(\mathcal{D})$ be the $\mathbb{F}_p$-code generated

by the blocks of $\mathcal{D}$, considered as characteristic vectors $\in V$; that is, $B \in \mathcal{B}$ is considered as $\sum_{P \in \mathcal{P},\, P\, I\, B} v_P$.

Theorem 2.1 (The Dimension Theorem) *Suppose that $p \nmid k - \rho$.*
If $p \nmid \sigma$ also then $\mathbf{C}$ has dimension $1 + r(m-1)/\sigma$.
If $p \mid \sigma$ then $\mathbf{C}$ has dimension $r(m-1)/\sigma$.

Proof. Since each point is on σ blocks of each class, the sum of the m blocks of any resolution class is $\sigma\mathbf{j}$, where $\mathbf{j}$ is the all one vector. If $p \nmid \sigma$, then $\mathbf{j} \in \mathbf{C}$. If $p \mid \sigma$, then the m blocks in a resolution class are linearly dependent. Therefore, $\mathbf{C}$ is generated by any set $\mathcal{S} = \mathcal{S}' \cup \mathcal{S}''$, where $\mathcal{S}'$ is any set of $b - b/m$ vectors consisting of any $m-1$ blocks from each of the b/m block classes, and $\mathcal{S}''$ is $\{\mathbf{j}\}$ or $\emptyset$ according as $p \nmid \sigma$ or $p \mid \sigma$.

Let

$$\lambda'\mathbf{j} + \sum_{\mathbf{v} \in \mathcal{S}'} \lambda_{\mathbf{v}} \mathbf{v} = \mathbf{0} \tag{1}$$

be an $\mathbb{F}_p$-linear relation involving only the vectors in $\mathcal{S}$. If $p \mid \sigma$, set $\lambda' = 0$.

Given any two blocks $\mathbf{u}$ and $\mathbf{v}$, their inner product is k, or ρ, or μ, according as the two blocks are equal, or distinct and in the same resolution class, or in different resolution classes.

Let $\mathcal{T}$ be a resolution class of $\mathcal{D}$ and let $\mathcal{T}' = \mathcal{T} \cap \mathcal{S}'$. Let $\mathbf{u} \in \mathcal{T}'$. Taking the inner product with $\mathbf{u}$ of both sides of the (1), we get

$$k\lambda' + k\lambda_{\mathbf{u}} + \rho \sum_{\mathbf{v} \in \mathcal{T}' - \{\mathbf{u}\}} \lambda_{\mathbf{v}} + \mu \sum_{\mathbf{v} \in \mathcal{S}' - \mathcal{T}'} \lambda_{\mathbf{v}} = 0. \tag{2}$$

Thus

$$k\lambda' + \rho \sum_{\mathbf{v} \in \mathcal{T}'} \lambda_{\mathbf{v}} + \mu \sum_{\mathbf{v} \in \mathcal{S}' - \mathcal{T}'} \lambda_{\mathbf{v}} = -(k - \rho)\lambda_{\mathbf{u}}. \tag{3}$$

Now let $\mathbf{u}' \in \mathcal{T} - \mathcal{T}'$. Taking the inner product with $\mathbf{u}'$ of both sides of the (1), we get

$$k\lambda' + \rho \sum_{\mathbf{v} \in \mathcal{T}'} \lambda_{\mathbf{v}} + \mu \sum_{\mathbf{v} \in \mathcal{S}' - \mathcal{T}'} \lambda_{\mathbf{v}} = 0. \tag{4}$$

From (3) and (4),

$$(k - \rho)\lambda_{\mathbf{u}} = 0. \tag{5}$$

Since $p \nmid k - \rho$, $\lambda_{\mathbf{u}} = 0$ for all $\mathbf{u} \in \mathcal{S}'$. If $p \mid \sigma$, we have established that the relation in (1) is trivial. If $p \nmid \sigma$, the relation in (1) becomes $\lambda'\mathbf{j} = \mathbf{0}$. So $\lambda' = 0$ and the relation is trivial. This completes the proof. ■

The proof of the following corollary is straightforward.

Corollary 2.2 *Suppose that $\mathcal{D}$ is an affine 1-$(\mu m^2, \mu m, r)$ design (i.e a net) and that $p \nmid \mu m$. Then $\mathbf{C}$ has dimension $1 + r(m-1)$.*

The case when p divides $k - \rho$ is more difficult, though it is the more interesting case for coding theorists. The Smith normal form of the incidence matrix of the design may give some insight as to why the cases differ. For example, consider

the case of the unique net with $\mu = 2$ and $m = 4$. (We are indebted to Vladimir Tonchev for the information that there is only one net with these parameters and for computing the Smith normal form of its 32×32 incidence matrix.) The invariant factors of the incidence matrix consist of 13 ones, 4 twos, 6 fours and 2 eights.

This explains why the p-dimension of the code of this net is 13 if $p = 2$ and is 25 otherwise.The latter number agrees with that given by the corollary.

References

[1] E. F. Assmus, Jr and J. D. Key, *Designs and their Codes*, Cambridge: Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[2] T. Beth, D. Jungnickel and H. Lenz, *Designs and their Codes*, Cambridge: Cambridge University Press, 1992, Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[3] *Orthogonal Arrays*, New York: Springer-Verlag, 1999.

Institute of Mathematics and Physics, Aberystwyth University, Aberystwyth, Ceredigion SY23 3BZ, U.K.
E-mail: **tpd@aber.ac.uk**

Institute of Mathematics and Physics, Aberystwyth University, Aberystwyth, Ceredigion SY23 3BZ, U.K.
E-mail: **vcm@aber.ac.uk**