On m-specially resolvable BIB designs and q-ary constant weight codes

Leonid Bassalygo, Vladimir Lebedev, Victor Zinoviev

Harkevich Institute for Problems of Information Transmission, Moscow, Russia

Eighth International Workshop on Optimal Codes and Related Topics (OC 2017).
Sofia, Bulgary, July 10 - 14, 2017

Outline

Summary

We introduce m-specially resolvable BIB designs (SRB_m) which generalize known resolvable BIB designs. The coexistence theorem between SRB_m designs and some class of q-ary constant weight codes, satisfying the Johnson upper bound, is established. Several constructions of such designs and codes are developed based on Steiner systems and super-simple t-designs.

Introduction

Let $Q = \{0, 1, ..., q-1\}$. Any subset $C \subseteq Q^n$ is a code denoted by $(n, N, d)_q$ of length n, cardinality $N = |C|$ and minimum (Hamming) distance d. A code C is constant weight and denoted $(n, N, w, d)_q$ if every its codeword is of weight w.

Introduction

Let $Q = \{0, 1, ..., q-1\}$. Any subset $C \subseteq Q^n$ is a code denoted by $(n, N, d)_q$ of length n, cardinality $N = |C|$ and minimum (Hamming) distance d. A code C is constant weight and denoted $(n, N, w, d)_q$ if every its codeword is of weight w.
We recall the following two classical bounds for the size $N_q(n, d)$ of a q-ary $(n, N, d)_q$-code and for the size $N_q(n, d, w)$ of a q-ary constant weight $(n, N, w, d)_q$-code:

Introduction

Let $Q = \{0, 1, ..., q-1\}$. Any subset $C \subseteq Q^n$ is a code denoted by $(n, N, d)_q$ of length n, cardinality $N = |C|$ and minimum (Hamming) distance d. A code C is constant weight and denoted $(n, N, w, d)_q$ if every its codeword is of weight w.
We recall the following two classical bounds for the size $N_q(n, d)$ of a q-ary $(n, N, d)_q$-code and for the size $N_q(n, d, w)$ of a q-ary constant weight $(n, N, w, d)_q$-code:
Plotkin bound:

$$N_q(n, d) \leq \frac{qd}{qd - (q-1)n}, \quad \text{if } \; qd > (q-1)n, \tag{1}$$

Introduction

Let $Q = \{0, 1, ..., q-1\}$. Any subset $C \subseteq Q^n$ is a code denoted by $(n, N, d)_q$ of length n, cardinality $N = |C|$ and minimum (Hamming) distance d. A code C is constant weight and denoted $(n, N, w, d)_q$ if every its codeword is of weight w.
We recall the following two classical bounds for the size $N_q(n, d)$ of a q-ary $(n, N, d)_q$-code and for the size $N_q(n, d, w)$ of a q-ary constant weight $(n, N, w, d)_q$-code:
Plotkin bound:

$$N_q(n, d) \leq \frac{qd}{qd - (q-1)n}, \quad \text{if } \; qd > (q-1)n, \tag{1}$$

Johnson bound:

$$N_q(n, d, w) \leq \frac{(q-1)dn}{qw^2 - (q-1)(2w-d)n}, \quad \text{if } \; qw^2 > (q-1)(2w-d)n, \tag{2}$$

Introduction

Definition 1.

A $T(v, k, t, \lambda)$-design is an incidence structure (X, B), where $X = \{x_1, \ldots, x_v\}$ is a set of elements and B is a collection of blocks of size k, such that every t distinct elements of X are contained in exactly $\lambda > 0$ blocks of B (here $1 \leq t \leq k \leq v - 1$). If $\lambda = 1$ then $T(v, k, t, \lambda)$-design is called a Steiner system and denoted by $S(v, k, t)$.

Introduction

If $t = 2$ a design $T(v, k, 2, \lambda)$ is called also a balanced incomplete block-design (v, b, r, k, λ) and denoted $B(v, k, \lambda)$. Respectively, a Steiner system $S(v, k, 2)$ is a design $B(v, k, 1)$.
The other two parameters of a $B(v, k, \lambda)$ design are: $b = |B|$ (the number of blocks) and r (the number of blocks containing one fixed element):

$$b = \lambda \frac{v(v-1)}{k(k-1)}, \quad r = \lambda \frac{v-1}{k-1}. \tag{3}$$

Introduction

It is well known and quite evidently that a design $T(v,k,t,\lambda)$ with $t \geq 3$ is a design $B(v,k,\lambda_2)$ with parameters

$$\lambda_2 = \lambda \frac{\binom{v-2}{t-2}}{\binom{k-2}{t-2}}, \quad b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}, \quad r = \lambda \frac{\binom{v-1}{t-1}}{\binom{k-1}{t-1}}. \tag{4}$$

Introduction

A block-design $B(v, k, \lambda)$ is completely described by its *incidence matrix* $A = [a_{i,j}]$, where $a_{i,j} = 1$ if $a_i \in B_j$ and $a_{i,j} = 0$, otherwise. So A is a binary $(v \times b)$-matrix with columns of weight k, such that any two distinct rows contain exactly λ common nonzero positions.

Introduction

A block-design $B(v, k, \lambda)$ is completely described by its *incidence matrix* $A = [a_{i,j}]$, where $a_{i,j} = 1$ if $a_i \in B_j$ and $a_{i,j} = 0$, otherwise. So A is a binary $(v \times b)$-matrix with columns of weight k, such that any two distinct rows contain exactly λ common nonzero positions.
A $B(v, k, \lambda)$ design is *resolvable* (denoted $RB(v, k, \lambda)$) if its incidence matrix A looks as follows:

$$A = [A_1 \mid \cdots \mid A_r], \tag{5}$$

where for any $i \in \{1, \ldots, r\}$ the every row of A_i has the weight 1.

Preliminary results

Definition 2.

(Bassalygo-Lebedev-Zinoviev, 2017) A $B(v,k,\lambda)$ design is m-nearly resolvable ($NRB_m(v,k,\lambda)$ design) if its incidence matrix A can be presented as follows:

$$A = [A_1 \mid \cdots \mid A_n], \quad n = \frac{bk}{v-m}, \tag{6}$$

such that the following properties are valid:

Preliminary results

Definition 2.

(Bassalygo-Lebedev-Zinoviev, 2017) A $B(v,k,\lambda)$ design is m-nearly resolvable ($NRB_m(v,k,\lambda)$ design) if its incidence matrix A can be presented as follows:

$$A = [A_1 \mid \cdots \mid A_n], \quad n = \frac{bk}{v-m}, \tag{6}$$

such that the following properties are valid:
(1) the every submatrix A_j, of size $v \times \frac{v-m}{k}$ consists of rows of weight 1 with exception of m zero rows whose indices belong to the set V_j, $\quad |V_j| = m, \quad V_j \subset \{1,2,...,v\}$;

Preliminary results

Definition 2.

(Bassalygo-Lebedev-Zinoviev, 2017) A $B(v,k,\lambda)$ design is m-nearly resolvable ($NRB_m(v,k,\lambda)$ design) if its incidence matrix A can be presented as follows:

$$A = [A_1 \mid \cdots \mid A_n], \quad n = \frac{bk}{v-m}, \tag{6}$$

such that the following properties are valid:
(1) the every submatrix A_j, of size $v \times \frac{v-m}{k}$ consists of rows of weight 1 with exception of m zero rows whose indices belong to the set V_j, $\quad |V_j| = m, \quad V_j \subset \{1,2,...,v\}$;
(2) the sets $V_1,...,V_n$ (as a collection of n blocks of size m) induces a block design $B(v,m,\xi)$ (which we call accompanying design) for some ξ.

Preliminary results

It can be seen that in such m-nearly resolvable $NRB_m(v, k, \lambda)$ design, parameters λ and ξ look as follows:

$$\lambda = n\,\frac{(k-1)(v-m)}{v(v-1)}, \quad \xi = n\,\frac{m(m-1)}{v(v-1)}\,. \tag{7}$$

Preliminary results

It can be seen that in such m-nearly resolvable $NRB_m(v, k, \lambda)$ design, parameters λ and ξ look as follows:

$$\lambda = n\,\frac{(k-1)(v-m)}{v(v-1)}, \quad \xi = n\,\frac{m(m-1)}{v(v-1)}\,. \tag{7}$$

The case $m = 0$ corresponds to the mentioned above resolvable designs, and the case $m = 1$ gives near-resolvable designs (both widely considered in the literatures (see [Abel-Ge-Yin, 2007], [Beth-Jungnickel-Lenz, 1986], [Furino-Miao-Yin, 1996] and references there for resolvable and near-resolvabe designs).

Preliminary results

As well known [Beth-Jungnickel-Lenz, 1986], [Furino-Miao-Yin, 1996] block designs with blocks of two different sizes are also considered. Denote by $B(v, b, r, \{k_1, k_2\}, \lambda)$ such a design with blocks of two sizes k_1 and k_2. Denote for shortness $k_1 = m$ and $k_2 = k$.

Preliminary results

Definition 3.

A $B(v, b, r, \{m, k\}, \lambda)$ design we call m-specially resolvable if the incidence matrix A can be presented as follows:

$$A = [A_1 \mid \cdots \mid A_r], \tag{8}$$

such that the following properties are valid:

Preliminary results

Definition 3.

A $B(v, b, r, \{m, k\}, \lambda)$ design we call m-specially resolvable if the incidence matrix A can be presented as follows:

$$A = [A_1 \mid \cdots \mid A_r], \tag{8}$$

such that the following properties are valid:
(1) the every submatrix A_j, of size $v \times \frac{v-m}{k}$ consists of rows of weight 1 and of columns of weight k with exception that one column is of weight m;

Preliminary results

Definition 3.

A $B(v, b, r, \{m, k\}, \lambda)$ design we call m-specially resolvable if the incidence matrix A can be presented as follows:

$$A = [A_1 \mid \cdots \mid A_r], \tag{8}$$

such that the following properties are valid:
(1) the every submatrix A_j, of size $v \times \frac{v-m}{k}$ consists of rows of weight 1 and of columns of weight k with exception that one column is of weight m;
(2) the sets $V_1, ..., V_r$ formed by the elements of blocks of the size m (one block from every submatrix A_i) induces a constant weight code.

Preliminary results

It is strightforward to check (by the standard counting of ones and of pairs of ones in the matrix A) that in a such m-specially design $B(v, b, r, \{m, k\}, \lambda)$ the parameters r and b are defined by v, k, m, λ as follows:

$$r = \frac{\lambda v(v-1)}{m(m-1) + (v-m)(k-1)}, \quad b = \frac{\lambda v(v-1)(v-m+k)}{k(m(m-1) + (v-m)(k-1))}. \tag{9}$$

Preliminary results

It is strightforward to check (by the standard counting of ones and of pairs of ones in the matrix A) that in a such m-specially design $B(v, b, r, \{m, k\}, \lambda)$ the parameters r and b are defined by v, k, m, λ as follows:

$$r = \frac{\lambda v(v-1)}{m(m-1) + (v-m)(k-1)}, \quad b = \frac{\lambda v(v-1)(v-m+k)}{k(m(m-1) + (v-m)(k-1))}. \tag{9}$$

So, denote an m-specially resolvable design $B(v, b, r, \{m, k\}, \lambda)$ by $SRB_m(v, k, \lambda)$.

Preliminary results

It is strightforward to check (by the standard counting of ones and of pairs of ones in the matrix A) that in a such m-specially design $B(v, b, r, \{m, k\}, \lambda)$ the parameters r and b are defined by v, k, m, λ as follows:

$$r = \frac{\lambda v(v-1)}{m(m-1) + (v-m)(k-1)}, \quad b = \frac{\lambda v(v-1)(v-m+k)}{k(m(m-1) + (v-m)(k-1))}. \tag{9}$$

So, denote an m-specially resolvable design $B(v, b, r, \{m, k\}, \lambda)$ by $SRB_m(v, k, \lambda)$.

The concept of m-specially resolvable designs is also a variant of generalization of frames [Furino-Miao-Yin, 1996], which are used for construction of resolvable and near-resolvable designs. Now we have the following simple relations between concepts introduced above.

Preliminary results

Lemma 1.

(1) Let D be a resolvable RB(v, k, λ) design. Then this design implies the existence of a $(k-1)$-specially resolvable design $SRB_{k-1}(v-1, k, \lambda)$.
(2) Let $D^{(1)}$ be a m-nearly resolvable $NRB_m(v, k, \lambda)$-design and let $D^{(0)}$ be its accompanying $B(v, m, \xi)$ design, formed by the sets $V_1, ..., V_n$. Then the design $D^{(1)}$ implies the existence of m-specialy resolvable $SRB_m(v, k, \lambda + \xi)$ design.

Preliminary results

We recall the following known results, connecting q-ary optimal equidistant codes meeting the upper bounds (1) and (2) and resolvable and m-nearly resolvable designs $B(v, k, \lambda)$, respectively.

Theorem 1.

([8]) *An optimal equidistant $(n, d, N)_q$ code meeting the Plotkin bound (1) exists if and only if there exists a resolvable $RB(v, k, \lambda)$ design, where*

$$q = v/k, \quad n = \lambda(v-1)/(k-1), \quad N = v, \quad d = n - \lambda. \tag{10}$$

Preliminary results

Theorem 2.

$([B-Z,2017],[B-L-Z,2017])$ *Any m-nearly resolvable $NRB_m(v,k,\lambda)$-design with accompanying $B(v,m,\xi)$ design induces a q-ary equidistant constant weight $(n,N,w,d)_q$ code C with parameters*

$$q=\frac{v-m}{k}+1,\quad n=\lambda\frac{v(v-1)}{(k-1)(v-m)},\quad N=v,\quad w=\lambda\frac{k-1}{v-1},\quad d=\lambda\frac{v}{}$$

meeting the Johnson bound (2) with additional property that its n blocks of size $m=(n-w)N/n$, formed by indices of zero positions, defines a $B(v,m,\xi)$ design.

Preliminary results

Conversely, any q-ary equidistant constant weight $(n, N, w, d)_q$ code C, satifying Johnson bound (2), whose n blocks of size $m = (n - w)N/n$, formed by indices of zero positions, defines a $B(v, m, \xi)$-design, induces an m-nearly resolvable $NRB_m(v, k, \lambda)$-design with parameters

$$v = N, \quad k = \frac{wN}{(q-1)n}, \quad \lambda = \frac{w(wN - (q-1)n)}{n(q-1)(N-1)}, \quad m = \frac{(n-w)N}{n}.$$

Main results

First we formulate the main equivalence theorem, which is a natural extension of Theorem 2, involving a wider class of q-ary constant weight codes satisfying the Johnson upper bound (2).

Main results

First we formulate the main equivalence theorem, which is a natural extension of Theorem 2, involving a wider class of q-ary constant weight codes satisfying the Johnson upper bound (2).

Theorem 3.

Any m-specially resolvable $SRB_m(v,k,\lambda)$ design D induces a q-ary equidistant constant weight $(n,N,w,d)_q$ code C with parameters

$$q = \frac{v-m+k}{k},\ n = \frac{\lambda v(v-1)}{m(m-1)+(v-m)(k-1)},\ N = v,\ w = n\frac{v-r}{v}$$

meeting the Johnson bound (2).

Main results

Conversely, any q-ary equidistant constant weight $(n, N, w, d)_q$ code C, satisfying Johnson bound (2), induces an m-specially resolvable design $SRB_m(v, k, \lambda)$, where

$$v = N, \quad m = \frac{(n-w)N}{n}, \quad k = \frac{wN}{(q-1)n}, \quad \lambda = n - d\,.$$

Main results

In [B-L-Z, 2017] we derived several constructions of m-nearly resolvable designs (based on Steiner systems and super-simple designs) and corresponding q-ary equidistant constant weight codes meeting Johnson bound (2). In all that cases we obtain, according to Theorem 3, the corresponding m-specially resolvable designs $SRB_m(v, k, \lambda)$. In particularly, we have the following

Main results

In [B-L-Z, 2017] we derived several constructions of m-nearly resolvable designs (based on Steiner systems and super-simple designs) and corresponding q-ary equidistant constant weight codes meeting Johnson bound (2). In all that cases we obtain, according to Theorem 3, the corresponding m-specially resolvable designs $SRB_m(v, k, \lambda)$. In particularly, we have the following

Theorem 4.

Any Steiner system $S(v, k, t)$ induces a $(t-1)$-specially resolvable design $SRB_{t-1}(v, k-t+1, \lambda)$, where

$$\lambda = \frac{m(m-1) + (v-m)(k-1)}{v(v-1)} \binom{v}{t-1}. \tag{11}$$

Main results

The interesting question is, of course, the existence of m-specially resolvable $SRB_m(v, k, \lambda)$.

Main results

The interesting question is, of course, the existence of m-specially resolvable $SRB_m(v, k, \lambda)$.
For the simplest case $k = 2$ and $\lambda = 1$ we can write out the parameters of the putative infinite family of such designs:

$$v = (m-1)^3 + 1, \quad k = 2, \quad \lambda = 1, \quad m = 3, 4, 5, \ldots. \tag{12}$$

and corresponding q-ary codes with $q = m(m-1)(m-2)/2 + 1$:

$$n = (m^2 - 3m + 3)(m-1), \; N = (m-1)^3 + 1, \; w = (m-1)^2(m-2), \; d = n- \tag{13}$$

Main results

We give the two first $(6, 9, 4, 5)_4$ codes C_1 and C_2 from this family for the cases $m = 3$ and $m = 4$:

Main results

We give the two first $(6, 9, 4, 5)_4$ codes C_1 and C_2 from this family for the cases $m = 3$ and $m = 4$:

$$C_1 = \left\{ \begin{array}{cccccc} (0 & 1 & 1 & 0 & 2 & 1) \\ (0 & 2 & 2 & 1 & 0 & 2) \\ (0 & 3 & 3 & 2 & 1 & 0) \\ \hline (1 & 0 & 1 & 1 & 3 & 0) \\ (2 & 0 & 2 & 0 & 1 & 3) \\ (3 & 0 & 3 & 3 & 0 & 1) \\ \hline (1 & 1 & 0 & 2 & 0 & 3) \\ (2 & 2 & 0 & 3 & 2 & 0) \\ (3 & 3 & 0 & 0 & 3 & 2) \end{array} \right\}$$

Main results

The second $(21, 28, 18, 20)_{13}$ code C_2 of this family (for the case $(m = 4)$ also exists.

Main results

The second $(21, 28, 18, 20)_{13}$ code C_2 of this family (for the case $(m = 4)$ also exists. The code matrix can be presented as the following 4×3 matrix C_2,

Main results

The second $(21, 28, 18, 20)_{13}$ code C_2 of this family (for the case $(m = 4)$ also exists. The code matrix can be presented as the following 4×3 matrix C_2,

$$C_2 = \begin{bmatrix} P_1 & P_2 & P_3 \\ P_4 & P_5 & P_6 \\ P_7 & P_8 & P_9 \\ P_{10} & P_{11} & P_{12} \end{bmatrix}$$

consisting of the 12 circulant matrices $P_1, \ldots, P_{12}$ of order 7.

Main results

We give the first rows p_i of these matrices (the other rows are cyclic shifts of the first one):

$$p_1 = (0,1,2,3,3,2,1), \qquad p_2 = (0,6,5,4,3,2,1),$$
$$p_3 = (0,1,2,3,4,5,6), \qquad p_4 = (0,4,5,6,6,5,4),$$
$$p_5 = (1,2,10,9,8,0,7), \qquad p_6 = (1,7,0,8,9,10,2),$$
$$p_7 = (0,7,8,9,9,8,7), \qquad p_8 = (6,12,11,0,5,8,9),$$
$$p_9 = (6,9,8,5,0,11,12), \qquad p_{10} = (0,10,11,12,12,11,10),$$
$$p_{11} = (10,0,3,11,12,7,4), \qquad p_{12} = (10,4,7,12,11,3,0).$$

Main results

We conjecture that for the case m, when $m^2 - 3m + 3$ is a prime power number, the corresponding code (13) and design (12) exist.

References

- *R.J.R. Abel, G. Ge, J. Yin*, Resolvable and near-resolvable designs// *Handbook of Combinatorial Designs*. 2nd edition. Ed. by Colbourn C.J., Dinitz J.H., Boca Raton: Chapman and Hall/CRC Press, 2007. VI. 7. P. 124 - 132.
- *P. Adams, D.E. Bryant, A. Khodkar*, On the existence of super-simple designs with block size 4// Aequationes Math., 1996, vol. 51, pp. 230 - 246.
- *L. A. Bassalygo*, New upper bounds for error-correctng codes// Problems of Information Transmission. 1965. vol. 1, No. 1. pp. 41 - 44.
- *L. A. Bassalygo, V. S. Lebedev, V. A. Zinoviev*, On m-nearly resolvable BIB designs and q-ary optimal constant weight codes// in: "10th International Workshop on Coding and Cryptography. WCC 2017", Saint Petersburg, Russia, September 18 - 22, 2017.

References

- *L. A. Bassalygo, V. A. Zinoviev*, A note on balanced incomplete block-designs, near-resolvable block-designs, and q-ary optimal constant-weight codes// Problems of Information Transmissions, 2017. vol. 53. No. 1. P. 55-58.
- T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, London, 1986.
- *S. Furino, Y. Miao, J. Yin*, Frames and Resolvable Designs, CRC Press, Boca Raton - New York - London - Tokyo. 1996.

References

- *N. V. Semakov, V. A. Zinoviev*, Equidistant q-ary codes with maximal distance and resolvable balanced incomplete block-designs// Problems of Information Transmission, 1968, vol. 4. No. 2, pp. 3 - 10.
- *N. V. Semakov, V. A. Zinoviev*, Constant weight codes and tactical configurations// Problems of Information Transmission, 1969, vol. 5. No. 3, pp. 28 - 36.
- *G. T. Bogdanova, V. A. Zinoviev, T. J. Todorov*, On construction of q-ary equidistant codes// Problmes of Information Transmission, 2007, vol. 43, No. 4, pp. 13 - 36.