Hadamard Codes

Ludmila Divišová

Spring school of algebra MFF UK

March 23, 2012

Introduction

Error-correcting codes

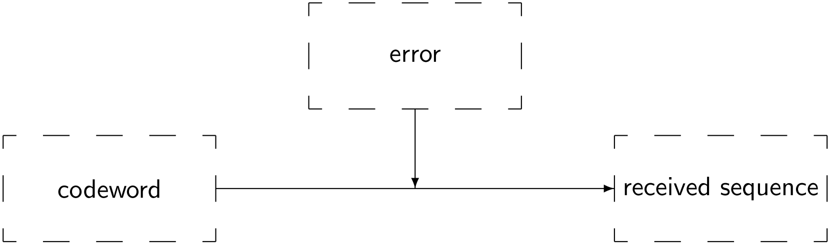
Hadamard codes

Construction of Hadamard codes

Designs

Hadamard 2-designs

Error-correcting codes



Code C is a set of codewords $c = (c_0, c_1, ..., c_{n-1})$, $|C| = M$.

- parameters(n,M,d)
- n length of codeword
- M count of all codewords
- d minimal distance = minimal count of positions, where two codewords differ

Error-correcting codes - Example

Example

Let us have code $C = \{(000), (011), (101), (110)\}$. Then

- $n = 3$
- $M = 4$
- $d = 2$

Hadamard codes

- big minimal distance
- large number number of codewords by a fixed minimum distance

Plotkin bound

Theorem

For any (n,M,d) code C for which $n < 2d$*,is*

$$M \leq 2\lfloor \frac{d}{2d-n} \rfloor$$

- $A(n,d)$...the largest M for any (n,M,d) code C

Lemma

$$A(n,d) = A(n+1, d+1)$$

Lemma

$$A(n,d) \leq 2A(n-1,d)$$

Plotkin bound

Theorem

1. *d even,* $n < 2d \Rightarrow A(n,d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$
2. *d even,* $n = 2d \Rightarrow A(2d,d) \leq 4d$
3. *d odd,* $n < 2d+1 \Rightarrow A(n,d) \leq 2\lfloor \frac{d+1}{2d+1-n} \rfloor$
4. *d odd,* $n = 2d+1 \Rightarrow A(2d+1,d) \leq 4d+4$

Construction of Hadamard codes

With use of Hadamard matrix H_n we can get

1. a (n-1,n,n/2) code A_n by deleting the first row and column
2. a (n-1, 2n, 1/2(n-1)) code B_n, which contains the words of A_n with their complements
3. a (n, 2n, n/2) code C_n, where we use the whole rows from H_n and their complements

I. construction method - Example

$$H_4 = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}$$

$A_n =$

1	0	1
0	1	1
1	1	0
0	0	0

- symbol $+$ was replaced by 0, - by 1
- A_n is a $(3, 4, 2)$ code and meets the Plotkin bound (1), because

$$M = 4 = 2\lfloor \frac{2}{2 * 2 - 3} \rfloor = 2\lfloor \frac{d}{2d - n} \rfloor$$

II. construction method - Example

- B_n is a $(3, 8, 1)$ code
- meets the Plotkin bound (4), because

$$M = 8 = 4 * 1 + 4 = 4d + 4$$

$$H_4 = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}$$

$B_n =$

1	0	1
0	1	1
1	1	0
0	0	0
0	1	0
1	0	0
0	0	1
1	1	1

III. construction method - Example

- C_n is a $(4, 8, 2)$ code
- meets the Plotkin bound (2), because

$$M = 8 = 4 * 2 = 4d$$

$$H_4 = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}$$

$C_n =$

0	1	0	1
0	0	1	1
0	1	1	0
0	0	0	0
1	0	1	0
1	1	0	0
1	0	0	1
1	1	1	1

Design

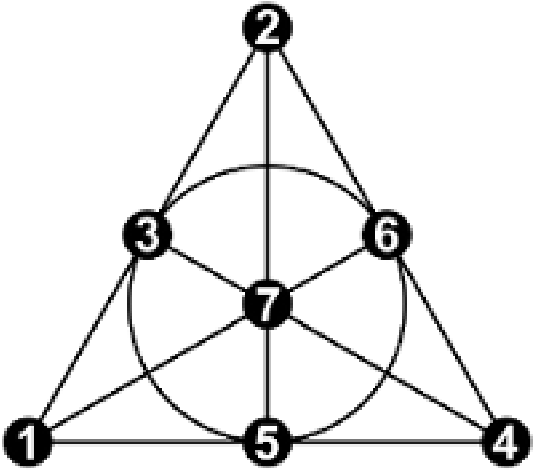
Definition

A *t-design* with parameters(v,k,λ) is a set of v 'points', and its subsets of cardinality k called 'blocks', where any t points are contained in λ blocks.

Example

Fano plane.

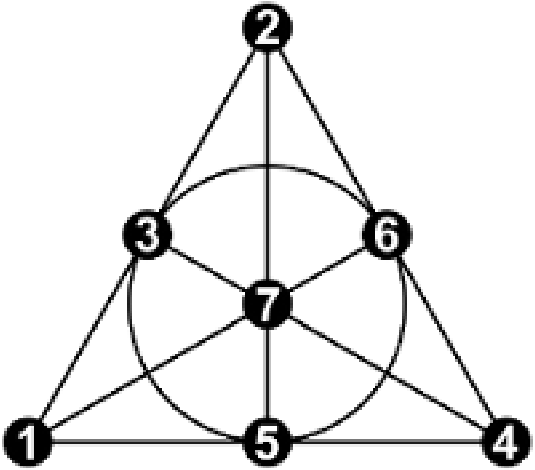
- 2-(7,3,1) design
- Points are vertexes of graph.
- Blocks are the lines.
- Each pair of points is in one block.



Square Design

Definition

Square 2-design is a 2-design, where $v < k$ and every two blocks have λ common points.



Incidence matrix of design

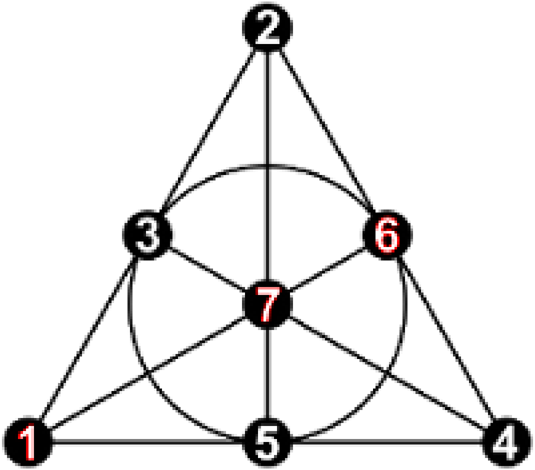
Definition

An *incidence matrix* of a design is a matrix M, where $M_{ij} = 1$ if the j-th point belongs to the i-th block. Otherwise $M_{ij} = 0$.

Example

Incidence matrix of Fano plane.

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$



Incidence matrix of design - Conclusion

Incidence matrices of square 2-designs with parameters $(4t-1, 2t-1, t-1)$ corresponds with the Hadamard matrices without their first row and column.

Example

Hadamard matrix H_8

$$\begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{pmatrix}$$

- symbol $+$ was replaced by 1, - by 0

Incidence matrix of Fano plane, a 2-(7,3,1) design.

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Hadamard 2-designs

Definition

A square 2-design with parameters $(n-1, \frac{1}{2}(n-1), \frac{1}{4}(n-1))$ is called *Hadamard design*.

Theorem

There exists a Hadamard matrix of order $n > 2$ if and only if there exists a Hadamard design $(n-1, \frac{1}{2}(n-1), \frac{1}{4}(n-1))$.

Conclusion

- Hadamard codes can be constucted from Hadamard matrices in three ways
- Hadamard codes have a large number of codewords by their length and minimal distance, they meet the Plotkin bound
- There is a relationship between Hadamard codes and Hadamard 2-designs