Hadamard codes III

Ludmila Divišová

One of applications of *Hadamard matrices* are error-correcting codes, called Hadamard codes. An *error-correcting code* is used to protect a message from corruption by errors during transmission through an information channel. The stucture of an error-correcting code enables us to remove the errors after receiving the message. The code consists of codewords, n-tuples of symbols over some set called alphabet. For classic Hadamard matrices we get binary Hadamard codes, but there also exists a q-ary generalization.

The most significant properties of the code are expressed in parameters $[n, M, d]$, where n is the length of codeword, M is the count of all codewords and d is the minimal distance of code. We often want a code to be linear, that means that every codeword can be expressed as a linear combination of another codewords.

Hadamard codes are generally nonlinear. However, there is a good reason to use them, because these codes can correct a maximal number of errors for a given length of codeword. On the other hand, we can get more codewords by a fixed minimum distance than with a linear code. Actually, Hadamard codes meet the *Plotkin bound*.

Because of their large error capability they were used in space exploration. Pictures of Jupiter, Saturn, Uranus and Neptune sent by Mariner and Voyager space probes were coded in this way.

There are three possibilities of how to construct Hadamard codes from the normalized Hadamard matrices. From a matrix H_n we can get

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

Example. The first construction method gives us for matrix

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

following $[3, 4, 2]$ code,

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

where the codewords are in the rows, symbol + was replaced by 0, − by 1 and all 0's word is added.

Another possibility, how to create Hadamard codes comes from design theory.

Definition 1. 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.

Designs can be characterized by a *incidence matrix* M, where 1 at position M_{ij} means, that the j-th point belongs to the i-th block. Otherwise $M_{ij} = 0$.

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