



# Self-orthogonal Codes Derived from Generalized Weighing Matrices

Vladimir D. Tonchev

Michigan Technological University, Houghton, MI 49931, USA

tonchev@mtu.edu

# Abstract

Generalized weighing matrices, Bhaskar-Rao designs, and generalized Hadamard matrices over a finite field of order  $q$  are used for the construction of self-orthogonal linear codes. Certain matrices of minimum rank yield optimal codes. In the special case when  $q = 4$ , the codes yield quantum error-correcting codes.

# Generalized Weighing Matrices

A **generalized weighing matrix** over a multiplicative group  $G$  of order  $g$  is a  $v \times b$  matrix  $M = (m_{ij})$  with entries from  $G \cup \{0\}$  such that for every two rows  $(m_{i1}, \dots, m_{ib}), (m_{j1}, \dots, m_{jb})$ ,  $i \neq j$ , the multi-set

$$\{m_{is}m_{js}^{-1} \mid 1 \leq s \leq b, m_{js} \neq 0\} \quad (1)$$

contains every element of  $G$  the same number of times.

# Bhaskar-Rao Designs

A generalized weighing matrix with the additional properties that every row contains precisely  $r$  nonzero entries, each column contains exactly  $k$  nonzero entries, and for every two distinct rows the multi-set (1) contains every group element exactly  $\lambda/g$  times is known as a **generalized Bhaskar-Rao design**  $GBRD(v, b, r, k, \lambda; G)$ .

# Generalized Hadamard Matrices

A **balanced generalized weighing matrix**  $BWG(v, k, \lambda)$  is a generalized Bhaskar-Rao design with  $r = k$  and  $v = b$ .

A **generalized Hadamard matrix**  $GH(\lambda, g)$  over a group  $G$  of order  $g$  is a balanced generalized weighing matrix with  $v = b = k = \lambda$ .

# Codes

A linear  $q$ -ary  $(n, k)$  **code**  $C$  is a  $k$ -dimensional subspace of the  $n$ -dimensional vector space over the field  $GF(q)$  of order  $q$ .

A **generator matrix** of an  $(n, k)$  code  $C$  is any matrix of rank  $k$  whose rows are vectors from  $C$ .

The Hamming **distance** between two vectors  $x = (x_1, \dots, x_n)$ ,  $y = (y_1, \dots, y_n)$  is the number of  $i$  such that  $x_i \neq y_i$ .

A code with minimum distance  $d$  detect up to  $d - 1$  errors, and correct up to  $(d - 1)/2$  errors.

# Self-Orthogonal Codes

The **dual** code  $C^\perp$  of an  $(n, k)$   $C$  is the  $(n, n - k)$  code being the orthogonal space of  $C$  with respect to a specified inner product.

A code  $C$  is **self-orthogonal** if  $C \subseteq C^\perp$ .

The ordinary inner product in  $GF(q)^n$  is defined as

$$x \cdot y = x_1y_1 + \dots + x_ny_n, \quad (2)$$

while the *hermitian* inner product in  $GF(q)^n$  ( $q \geq 4$ ) is defined as

$$(x, y) = x_1y_1^{q-2} + \dots + x_ny_n^{q-2}. \quad (3)$$

# Codes from Generalized Weighing M

## Proposition.

Let  $q = p^s \geq 4$  be a power of a prime number  $p$ , and let  $M$  be a  $v \times b$  generalized weighing matrix over the multiplicative group of  $GF(q)$  such that the Hamming weight of every row of  $M$  is a multiple of  $p$ . Then the rows of  $M$  span a linear code  $C$  of length  $b$  which is self-orthogonal with respect to the hermitian product.

# Balanced Generalized Matrices

Balanced generalized weighing matrices

$$BGW((q^t - 1)/(q - 1), q^{t-1}, q^{t-1} - q^{t-2})$$

over the multiplicative group of  $GF(q)$  are known to exist for every prime power  $q$  and every integer  $t \geq 2$ .

Constructions using traces of elements in  $GF(q)$  are known that give many monomially inequivalent

$BGW((q^t - 1)/(q - 1), q^{t-1}, q^{t-1} - q^{t-2})$  for various  $q$  and  $t$ .

# Codes from Balanced Matrices

## Theorem 1.

Let  $q \geq 4$  be a prime power and  $t \geq 2$  be an integer. The code  $C$  spanned by the rows of a  $BGW((q^t - 1)/(q - 1), q^{t-1}, q^{t-1} - q^{t-2})$  over  $GF(q)$  is a hermitian self-orthogonal code of length  $n = (q^t - 1)/(q - 1)$ , dimension  $k \geq t$ , and dual distance  $d^\perp \geq 3$ .

# Generalized Hadamard Matrices

Let  $q$  be a prime power. A generalized Hadamard  $q^t \times q^t$  matrix  $GH(q^{t-1}, q)$  over the elementary abelian group  $E_q$  of order  $q$  is known to exist for every  $t \geq 1$ .

The rank of a  $q^t \times q^t$  matrix  $GH(q^{t-1}, q)$  over  $GF(q)$  is at least  $t$ . For any given prime power  $q$  and any  $t \geq 1$ , there exists a unique (up to a permutation of rows and columns) matrix  $M = GH(q^{t-1}, q)$  of minimum  $q$ -rank equal to  $t$ .

# Codes from Additive H-Matrices

## Theorem 2.

The rows of an additive generalized Hadamard matrix  $M = GH(q^{t-1}, q)$  over  $GF(q)$  of minimum  $q$ -rank span a linear hermitian self-orthogonal code.

# An Application to Quantum Codes

Calderbank, Rains, Shor and Sloane described a method for the construction of quantum codes from quaternary hermitian self-orthogonal codes.

Theorem 1 implies the following.

**Theorem 3.** Let  $t \geq 2$  be an integer. The code  $C$  over  $GF(4)$  spanned by the rows of a matrix  $M = BGW((4^t - 1)/3, 4^{t-1}, 4^{t-1} - 4^{t-2})$  yields a quantum code with parameters  $[[((4^t - 1)/3, (4^t - 1)/3 - 2k, d \geq 3)]]$ , where  $k$  is the rank of  $M$  over  $GF(4)$ .

# Optimality

The codes of Theorem 3 in the case when the matrices are of minimum rank meet the sphere-packing bound for quantum  $[[n, k, d = 2e + 1]]$  codes:

$$\sum_{j=0}^e 3^j \binom{n}{j} \leq 2^{n-k}. \quad (4)$$

# References

G. Berman, Families of generalized weighing matrices, *Canadian J. Math.* **30** (1978), 1016-1028.

A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Quantum error correction via codes over  $GF(4)$ , *IEEE Trans. Information Theory* **44** (1998), 1369-1387.

V. D. Tonchev, On generalized Hadamard matrices of minimum rank, *Finite Fields and their Appl.* **10** (2004), 522-529.

**THANK YOU!**