Finite geometry codes, generalized Hadamard matrices, and Hamada and Assmus' conjectures

Vladimir D. Tonchev[a]

Department of Mathematical Sciences

Michigan Technological University

Houghton, Michigan 49931, USA

tonchev@mtu.edu, www.math.mtu.edu/∼tonchev

[a]Speaker's participation sponsored by Fulbright Grant #1868.

Overview

- All generalized Hadamard matrices of order 16 over a group of order 4 are classified up to equivalence.
- The quaternary codes spanned by these matrices and the binary linear codes spanned by the incidence matrices of related symmetric nets are computed and classified.

- The binary codes include the affine geometry $[64, 16, 16]$ code spanned by the planes in $AG(3, 4)$ and two new codes that support non-isomorphic designs with the same 2-rank as the classical affine design in $AG(3, 4)$, hence provide counter-examples to Hamada's and Assmus' conjectures.
- Many of the F_4-codes spanned by generalized Hadamard matrices yield quantum error-correcting codes, including some codes with optimal parameters.

Designs

A t-(v, k, λ) design $\mathcal{D}$ is a set X of v *points* together with a collection $\mathcal{B}$ of b k-subsets of X called *blocks* such that every t-subset of X is contained in exactly λ blocks.

A design is symmetric if $v = b$.

Two designs are isomorphic if there exists a bijection between their point sets that maps the blocks of the first design into blocks of the second design.

Incidence Matrices

An incidence matrix of $\mathcal{D}$ is a $b \times v$ $(0,1)$ matrix $A = (a_{ij})$ with rows indexed by the blocks, and columns indexed by the points, where $a_{ij} = 1$ if the ith block contains the jth point and $a_{ij} = 0$ otherwise.

The dual design $\mathcal{D}^*$ of $\mathcal{D}$ is the design with incidence matrix A^T.

Resolvable Designs

A parallel class in a t-(qk, k, λ) design is a set of q pairwise disjoint blocks.
A resolution is a partition of the collection of blocks into disjoint parallel classes.
A design is resolvable if it admits a resolution.
A resolvable design is affine resolvable or affine, if every two blocks that belong to different parallel classes of $\mathcal{R}$ intersect in a constant number of $\mu = k^2/v$ points.
The classical affine 2-$(q^n, q^{n-1}, (q^{n-1} - 1)/(q - 1))$ design has the hyperplanes in the affine geometry $AG(n, q)$ as blocks.

Symmetric Nets

A **symmetric (μ, q)-net** is a symmetric 1-$(\mu q^2, \mu q, \mu q)$ design $\mathcal{D}$ such that both $\mathcal{D}$ and $\mathcal{D}^*$ are affine.

A symmetric (μ, q)-net is **class-regular** if it admits a group of automorphisms G of order q that acts transitively on every point and block parallel class.

The Classical Nets

The classical class-regular (q, q)-net, where q is a prime power, is obtained from the 3-dimensional affine space $AG(3, q)$ over the field of order q as follows:

Choose a class $\mathcal{P}$ of q^2 parallel lines in $AG(3, q)$, that is, $\mathcal{P}$ consists of a given 1-dimensional vector subspace and its cosets in $GF(q)^3$, and consider as blocks of the net the q^3 planes in $AG(3, q)$ that do not contain any line from $\mathcal{P}$. The group of bitranslations G in this case is an elementary Abelian group of order q.

Generalized Hadamard matrices

A generalized Hadamard matrix $H(\mu, G) = (h_{ij})$ over a group G of order q is a $q\mu \times q\mu$ matrix with entries from G with the property that for every i, j, $1 \le i < j \le q\mu$, the multi-set

$$\{h_{is}h_{js}^{-1} \mid 1 \le s \le q\mu\}$$

contains every element of G exactly μ times.

A generalized Hadamard matrix over the multiplicative group of order two $G = \{1, -1\}$ is an ordinary Hadamard matrix.

GH Matrices and Nets

Every generalized Hadamard matrix $H = H(\mu, G)$ over a group G of order q determines a class-regular symmetric (μ, q)-net N as follows: let $\bar{G}$ be a group of q by q permutation matrices isomorphic to G, and let ϕ be an isomorphism between G and $\bar{G}$. Replacing each element h_{ij} of H by $\phi(h_{ij})$ gives a $(0,1)$-incidence matrix of a class-regular symmetric (μ, q)-net N.

EXAMPLE

$$H(2,2) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \; 1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; -1 \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$H(2,2) \to N = \left(\begin{array}{cc|cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right).$$

Class-Regular (q, q)-Nets: Classifica

q	Group	Class-regular nets	Total # nets
2	Z_2	1	1
3	Z_3	2	4
4	Z_4	**13**	≥ 239
4	$Z_2 \times Z_2$	**226**	≥ 239

The Class-Regular $(4, 4)$-Nets

- There are 13 non-isomorphic $(4, 4)$-nets with group Z_4.
- There are 226 non-isomorphic $(4, 4)$-nets with group $Z_2 \times Z_2$.

These nets give rise to 13 inequivalent generalized Hadamard matrices of order 16 over the cyclic group Z_4 of order 4, and 226 such matrices over the elementary Abelian group $Z_2 \times Z_2$.

Hamada's Conjecture

Conjecture (**N. Hamada, 1973**):

A geometric design having as points and blocks the points and subspaces of a given dimension of a finite affine or projective space over $GF(q)$ is characterized as the unique design with the given parameters having minimum q-rank of its incidence matrix.

The Proven Cases

Hamada's conjecture was proved to be true in the following cases:

- Classical (hyperplane) designs in $AG(n, 2)$ and $PG(n, 2)$ (Hamada and Ohmori '75);
- Lines in $PG(n, 2)$ and $AG(n, 3)$ (Doyen, Hubaut and Vandensavel '78);
- Planes in $AG(n, 2)$ (Teirlinck '80).

Counter-Examples

The only previously known counter-examples of Hamada's conjecture were five 3-$(32, 8, 7)$ designs supported by extremal doubly-even self-dual $[32, 16, 8]$ codes (one being the second order Reed-Muller, or affine geometry code), and their derived 2-$(31, 7, 7)$ designs supported by the shortened codes, all having 2-rank 16 (V.D. Tonchev 1986).

Assmus Conjecture

Assmus' Conjecture:

Hamada's conjecture is true for designs with classical parameters.

Theorem. (V.D. Tonchev 1999).
The Assmus conjecture is true for generalized incidence matrices with entries over $GF(q)$.

Binary Codes from $(4, 4)$-Nets

The binary linear codes spanned by the 64×64 incidence matrices of the $(4, 4)$-nets were computed and classified.

Three codes (C_1, C_{20} and C_{36}), have the following weight enumerator:

$$W(y) = 1 + 84y^{16} + 3360y^{24} + \cdots + y^{64}.$$

New Counter-Examples

- The vectors of weight 16 in each of the codes C_1, C_{20} and C_{36} support an affine 2-$(64, 16, 5)$ design.
- The design in C_1 is isomorphic to the classical design of the planes in $AG(3, 4)$.
- The 2-(64,16,5) designs in C_{20} and C_{36} are the only known designs with classical parameters that are not geometric but have the same p-rank as a geometric design.
- These designs are counter-examples to both Hamada's and Assmus' conjectures.

Quantum Codes

The **hermitian product** of $x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n)$ over $GF(4)$:

$$(x, y) = x_1 y_1^2 + x_2 y_2^2 + \cdots + x_n y_n^2$$

Theorem. **Calderbank, Rains, Shor and Sloane, 1998**:

A hermitian self-orthogonal $GF(4)$*-code* C *of length* n *with dual distance* $d(C^{\perp})$ *(where* $C^{\perp}$ *is the hermitian dual code of* C*) yields a quantum error-correcting code with parameters* $[[n, k = n - 2\mathrm{dim}C, d = d(C^{\perp})]]$.

Quantum Codes from GH Matrices

- Normalizing a generalized Hadamard matrix of order 16 over $Z_2 \times Z_2$ gives a generator matrix of a self-orthogonal code of length 15 over $GF(4)$.
- Among these codes, 150 are hermitian self-orthogonal, hence give rise to quantum codes.
- The matrix related to the classical net yields an optimal quantum $[[15, 11, 2]]$ code.
- Several matrices give optimal quantum $[[15, 7, 3]]$ codes.

REFERENCES

- A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.
- N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes, *Hiroshima Math. J.* **3** (1973), 153–226.
- M. Harada, C. Lam and V.D. Tonchev, Symmetric $(4,4)$-nets and generalized Hadamard matrices over groups of order 4, *Designs, Codes and Cryptography* **34** (2005), 71-87.
- V.D. Tonchev, Quasi-symmetric 2-(31,7,7) designs and a revision of Hamada's conjecture, *J. Combin. Theory, Ser. A* **42** (1986), 104-110.
- V.D. Tonchev, Linear perfect codes and a characterization of the classical designs, *Designs, Codes and Cryptography* **17** (1999), 121-128.

Thank You!