Polarities, Quasi-Symmetric Designs, and Hamada's Conjecture

Vladimir D. Tonchev

Michigan Technological University

www.math.mtu.edu/∼tonchev/

Joint work with Dieter Jungnickel

D. Jungnickel and V. D. Tonchev: Polarities, quasi-symmetric designs, and Hamada's conjecture, *Designs, Codes and Cryptography*, 51, **May 2009**, 131-140.

Overview

- P-rank of incidence matrices and majority decoding
- Geometric designs and Hamada's conjecture
- Polarities and non-geometric designs with geometric parameters
- An infinite class of counter-examples to Hamada's conjecture
- An infinite class of quasi-symmetric designs.

Majority Decoding and Designs

Theorem. (Rudolph '67).
If the supports of vectors of weight w in the dual code of a linear $[n, k]$ code C over $GF(q)$ form a 2-(n, w, λ) design then C can correct by majority decoding up to e errors, where

$$e = \lfloor \frac{(n-1)\lambda + (w-1)(\lambda - 1)}{2\lambda(w-1)} \rfloor.$$

Majority Decoding and Designs

Theorem. (Rudolph ’67).
If the supports of vectors of weight w in the dual code of a linear $[n, k]$ code C over $GF(q)$ form a 2-(n, w, λ) design then C can correct by majority decoding up to e errors, where

$$e = \lfloor \frac{(n-1)\lambda + (w-1)(\lambda-1)}{2\lambda(w-1)} \rfloor .$$

The Majority Decoding algorithm evaluates r=$\lambda(n-1)/(w-1)$ linear functions of n variables for each of the n coordinates and chooses the predominant value by a majority vote.

Majority Decoding and Designs

Corollary. Rudolph's Theorem applies if C has a parity check matrix H being the incidence matrix of a 2-(n, w, λ) design.

Majority Decoding and Designs

Corollary. Rudolph's Theorem applies if C has a parity check matrix H being the incidence matrix of a 2-(n, w, λ) design.

Note. $\dim(C) = n - \mathrm{rank}_q H.$

Majority Decoding and Designs

Corollary. Rudolph's Theorem applies if C has a parity check matrix H being the incidence matrix of a 2-(n, w, λ) design.

Note. $\dim(C) = n - \mathrm{rank}_q H.$

Theorem. (Hamada '73).

$$\mathrm{rank}_q H \geq n - 1 \text{ if } \gcd(q, \frac{\lambda(n-w)}{w-1}) = 1.$$

Majority Decoding and Designs

Corollary. Rudolph's Theorem applies if C has a parity check matrix H being the incidence matrix of a 2-(n, w, λ) design.

Note. $\dim(C) = n - \operatorname{rank}_q H$.

Theorem. (Hamada '73).

$$\operatorname{rank}_q H \geq n - 1 \text{ if } \gcd(q, \frac{\lambda(n-w)}{w-1}) = 1.$$

Problem: Given n, w, λ and q, find a 2-(n, w, λ) design of minimum q-rank.

Designs from Finite Geometry

$$PG_d(n,q):\ 2-\left(\frac{q^{n+1}-1}{q-1},\frac{q^{d+1}-1}{q-1},\begin{bmatrix}n-1\\d-1\end{bmatrix}_q\right),$$

Designs from Finite Geometry

$$PG_d(n,q):\ 2-\left(\frac{q^{n+1}-1}{q-1},\frac{q^{d+1}-1}{q-1},\begin{bmatrix}n-1\\d-1\end{bmatrix}_q\right),$$

$$AG_d(n,q):\ 2-\left(q^n,q^d,\begin{bmatrix}n-1\\d-1\end{bmatrix}_q\right),1\le d\le n-1,$$

Designs from Finite Geometry

$$PG_d(n,q) : \; 2-\left(\frac{q^{n+1}-1}{q-1}, \frac{q^{d+1}-1}{q-1}, \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q\right),$$

$$AG_d(n,q) : \; 2-\left(q^n, q^d, \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q\right), 1 \le d \le n-1,$$

$$AG_d(n,2) : \; 3-\left(2^n, 2^d, \begin{bmatrix} n-2 \\ d-2 \end{bmatrix}_q\right), 1 \le d \le n-1,$$

where

$$\begin{bmatrix} n \\ i \end{bmatrix}_q = \frac{(q^n-1)\cdots(q^{n-i+1}-1)}{(q^i-1)\cdots(q-1)}.$$

1 P-ranks of Geometric Designs

$$\mathrm{rank}_2(AG_d(m,2)) = \mathrm{rank}_2(PG_{d-1}(m-1,2)) = \sum_{i=0}^{d} \binom{m}{i}.$$

Reed-Muller code $RM(d,m)$.

$$\mathrm{rank}_p(PG_1(2,p^m)) = \binom{p+1}{2}^m + 1.$$

In patricular, if $m = 1$

$$\mathrm{rank}_p(PG_1(2,p)) = \binom{p+1}{2} + 1.$$

Graham & MacWilliams '66.

> Note: The p-rank of the incidence matrix Π of any projective plane of a prime order p is equal to
> rank$_p(\Pi) = \binom{p+1}{2} + 1$.

$$\mathrm{rank}_p(PG_{n-1}(n,p^m)) = \binom{p+n-1}{n}^m + 1.$$

MacWilliams & Mann '68, Goethals & Delsarte '68, Smith '69.

2 The general case

Theorem (N. Hamada '73).

(a)

$$\operatorname{rank}_p(PG_d(n,p^m)) = \sum_{t_0,\dots,t_m} \prod_{j=0}^{m-1} \sum_{i=0}^{[(t_{j+1}p-t_j)/p]} (-1)^i \binom{n+1}{i} \binom{n+t_{j+1}p-t_j-ip}{n}.$$

where summation is over all ordered sets $(t_0,\dots,t_m)$ of integers $t_0,\dots,t_m$ such that

$$t_m = t_0,\ d+1 \le t_j \le n+1,\ 0 \le t_{j+1}p - t_j \le (n+1)(p-1)$$

for each $j = 0, 1, \dots, m-1$.

(b)

$$\operatorname{rank}_p(AG_d(n,p^m) =$$

$$\operatorname{rank}_p(PG_d(n,p^m)) - \operatorname{rank}_p(PG_d(n-1,p^m)).$$

3 Hamada's Conjecture

The geometric designs $PG_d(n, q)$ and $AG_d(n, q)$ are characterized as the designs of minimum q-rank among all designs with the given parameters.

- The conjecture indicates that the geometric designs are the best (and practically unique) choice to use for designing majority-logic decodable codes in the given range of parameters.
  Note: The number of non-isomorphic designs having the same parameters as the classical geometric designs $PG_{n-1}(n, q)$ or $AG_{n-1}(n, q)$, $n \geq 3$, grows exponentially with linear growth of n (Jungnickel '84, Kantor '94, Lam^2 & VDT '00, '02). True also for $2 \leq d \leq n-2$ (Jungnickel & T, '09).

- The conjecture provides a computationally simple characterization of the geometric designs in terms of the p-rank of their incidence matrices.

- Hamada's conjecture implies that for any prime p, the only projective plane of order p is $PG(2, p)$.

4 The Proven Cases

Theorem 3.1 (Hamada and Ohmori '75).
(i) The 2-rank of the incidence matrix A of any 2-$(2^{n+1}-1, 2^n, 2^{n-1})$ design D satisfies the inequality

$$rank_2(A) \geq n+1,$$

with equality if and only if D is isomorphic to the complementary design of $PG_{n-1}(n, 2)$.

4 The Proven Cases

Theorem 3.2 (Hamada and Ohmori ’75).
(i) The 2-rank of the incidence matrix A of any 2-$(2^{n+1}-1, 2^n, 2^{n-1})$ design D satisfies the inequality

$$rank_2(A) \geq n+1,$$

with equality if and only if D is isomorphic to the complementary design of $PG_{n-1}(n,2)$.

(ii) The 2-rank of the incidence matrix A of any 2-$(2^n, 2^{n-1}, 2^{n-1}-1)$ design D satisfies the inequality

$$rank_2(A) \geq n+1,$$

with equality if and only if D is isomorphic to the design of the hyperplanes in $AG(n,2)$.

Theorem. *(Doyen, Hubaut and Vandensavel '78).*
(i) The 2-rank of the incidence matrix A *of any 2-*$(2^{n+1}-1,3,1)$ D *satisfies the inequality*

$$rank_2(A) \geq 2^{n+1} - n - 2,$$

with equality if and only if D *is isomorphic to the design* $PG_1(n,2)$ *of the lines in* $PG(n,2)$*.*

Theorem. *(Doyen, Hubaut and Vandensavel '78).*
(i) The 2-rank of the incidence matrix A of any 2-$(2^{n+1}-1, 3, 1)$ D satisfies the inequality

$$rank_2(A) \geq 2^{n+1} - n - 2,$$

with equality if and only if D is isomorphic to the design $PG_1(n, 2)$ of the lines in $PG(n, 2)$.

(ii) The 3-rank of the incidence matrix A of any 2-$(3^n, 3, 1)$ design D satisfies the inequality

$$rank_3(A) \geq 3^n - 1 - n,$$

with equality if and only if D is isomorphic to the design $AG_1(n, 3)$ of the lines in $AG(n, 3)$.

Theorem. *(Doyen, Hubaut and Vandensavel '78).*
(i) The 2-rank of the incidence matrix A of any 2-$(2^{n+1}-1,3,1)$ D satisfies the inequality

$$rank_2(A) \geq 2^{n+1} - n - 2,$$

with equality if and only if D is isomorphic to the design $PG_1(n,2)$ of the lines in $PG(n,2)$.

(ii) The 3-rank of the incidence matrix A of any 2-$(3^n,3,1)$ design D satisfies the inequality

$$rank_3(A) \geq 3^n - 1 - n,$$

with equality if and only if D is isomorphic to the design $AG_1(n,3)$ of the lines in $AG(n,3)$.

Theorem. (Teirlinck '80)*.*
The 2-rank of the incidence matrix A of a 3-$(2^n,4,1)$ design D satisfies the inequality

$$rank_2(A) \geq 2^n - 1 - n,$$

with equality if and only if D is isomorphic to the design $AG_2(n,2)$ of the planes in $AG(n,2)$.

5 A revised version: Generalized Incidence Matrices

A generalized incidence matrix has entries in $GF(q)$, with nonzero entries designating incidence.

5 A revised version: Generalized Incidence Matrices

A generalized incidence matrix has entries in $GF(q)$, with nonzero entries designating incidence.

The dimension of a design D over $GF(q)$, $\dim_q(D)$, is defined as the minimum q-rank of all generalized incidence matrices of D over $GF(q)$.

5 A revised version: Generalized Incidence Matrices

A generalized incidence matrix has entries in $GF(q)$, with nonzero entries designating incidence.

The dimension of a design D over $GF(q)$, $\dim_q(D)$, is defined as the minimum q-rank of all generalized incidence matrices of D over $GF(q)$.

Example. The 3-rank of the incidence matrix of the unique 5-$(12, 6, 1)$ design D_{12} is 11, while

$$\dim_3(D_{12}) \leq 6.$$

Theorem. (T '99).
Let D be a 2-$((q^{n+1}-1)/(q-1), q^n, q^n - q^{n-1})$ design, $n \geq 2$. Then

$$\dim_q(D) \geq n+1.$$

The equality $\dim_q(D) = n+1$ holds if and only if D is isomorphic to the complementary design of $PG_{n-1}(n,q)$.

Theorem. (T '99).
Let D be a 2-$((q^{n+1}-1)/(q-1), q^n, q^n - q^{n-1})$ design, $n \geq 2$. Then

$$\dim_q(D) \geq n+1.$$

The equality $\dim_q(D) = n+1$ holds if and only if D is isomorphic to the complementary design of $PG_{n-1}(n,q)$.

Theorem. (T '99).
Let D be a 2-$(q^n, q^n - q^{n-1}, q^n - q^{n-1} - 1)$ design, $n \geq 2$. Then

$$\dim_q(D) \geq n+1.$$

The equality $\dim_q(D) = n+1$ holds if and only if D is isomorphic to the complementary design of $AG_{n-1}(n,q)$.

Theorem. (T '99).
Let D be a 2-$((q^{n+1}-1)/(q-1), q^n, q^n - q^{n-1})$ design, $n \geq 2$. Then

$$\dim_q(D) \geq n+1.$$

The equality $\dim_q(D) = n+1$ holds if and only if D is isomorphic to the complementary design of $PG_{n-1}(n,q)$.

Theorem. (T '99).
Let D be a 2-$(q^n, q^n - q^{n-1}, q^n - q^{n-1} - 1)$ design, $n \geq 2$. Then

$$\dim_q(D) \geq n+1.$$

The equality $\dim_q(D) = n+1$ holds if and only if D is isomorphic to the complementary design of $AG_{n-1}(n,q)$.

Example. Let D be a 2-$(121, 100, 99)$ design. Then

$$\dim_{11}(D) \geq 3,$$

with equality $\dim_{11}(D) = 3$ if and only if D is isomorphic to the complementary design of the Desarguesian affine plane of order 11, $AG(2,11)$.

6 Non-geometric designs having the same p-rank as geometric ones

(A) Deigns from self-dual codes

Theorem (T '86).

(i) There are exactly five non-isomorphic quasi-symmetric 2-$(31, 7, 7)$ designs (with block intersection numbers 1 and 3), one being $PG_2(4, 2)$, all five having the same 2-rank, 16.

(ii) There are exactly five non-isomorphic 3-$(32, 8, 7)$ designs with even block intersection numbers, one being $AG_3(5, 2)$, all five having the same 2-rank, 16.

6 Non-geometric designs having the same p-rank as geometric ones

(A) Deigns from self-dual codes

Theorem (T '86).

(i) There are exactly five non-isomorphic quasi-symmetric 2-$(31, 7, 7)$ designs (with block intersection numbers 1 and 3), one being $PG_2(4, 2)$, all five having the same 2-rank, 16.

(ii) There are exactly five non-isomorphic 3-$(32, 8, 7)$ designs with even block intersection numbers, one being $AG_3(5, 2)$, all five having the same 2-rank, 16.

Proof. *Use the classification of self-dual binary $[32, 16, 8]$ codes.*

6 Non-geometric designs having the same p-rank as geometric ones

(A) Deigns from self-dual codes

Theorem (T '86).

(i) There are exactly five non-isomorphic quasi-symmetric 2-$(31, 7, 7)$ designs (with block intersection numbers 1 and 3), one being $PG_2(4, 2)$, all five having the same 2-rank, 16.

(ii) There are exactly five non-isomorphic 3-$(32, 8, 7)$ designs with even block intersection numbers, one being $AG_3(5, 2)$, all five having the same 2-rank, 16.

Proof. *Use the classification of self-dual binary $[32, 16, 8]$ codes.*

Note. The non-geometric 2-$(31, 7, 7)$ design supported by the QR code of length 31 was mentioned in a paper by Goethals and Delsarte from 1968.

(B) Designs from codes of nets

A symmetric (μ, m)-net is a symmetric 1-$(m^2\mu, m\mu, m\mu)$ design D such that both D and its dual design D^* are affine resolvable.

(B) Designs from codes of nets

A symmetric (μ, m)-net is a symmetric 1-$(m^2\mu, m\mu, m\mu)$ design D such that both D and its dual design D^* are affine resolvable.

A symmetric (μ, m)-net is class-regular if it admits an automorphism group of order m that acts transitively on each block and point parallel class.

(B) Designs from codes of nets

A symmetric (μ, m)-net is
a symmetric 1-$(m^2\mu, m\mu, m\mu)$ design D
such that both D and its dual design D^* are
affine resolvable.

A symmetric (μ, m)-net is class-regular
if it admits an automorphism group of order m
that acts transitively on each block and point
parallel class.

The classical class-regular (q, q)-net:

Points and planes of $AG(3, q)$ that
do not contain lines from a given parallel class.

A $(4, 4)$-net consists of 64 points and 64 blocks, each block of size 16 and each point in 16 blocks, so that the blocks (as well as and points) are partitioned into 16 parallel classes of size 4, and any two non-parallel blocks share 4 points.

A $(4,4)$-net consists of 64 points and 64 blocks, each block of size 16 and each point in 16 blocks, so that the blocks (as well as and points) are partitioned into 16 parallel classes of size 4, and any two non-parallel blocks share 4 points.

Theorem. (Harada, Lam, & T, '05).

(i) Up to isomorphism, there are exactly 239 class-regular $(4,4)$-nets.

A $(4, 4)$-net consists of 64 points and 64 blocks, each block of size 16 and each point in 16 blocks, so that the blocks (as well as and points) are partitioned into 16 parallel classes of size 4, and any two non-parallel blocks share 4 points.

Theorem. (Harada, Lam, & T, ’05).

(i) Up to isomorphism, there are exactly 239 class-regular $(4, 4)$-nets.
(ii) The 2-rank a symmetric class-regular $(4, 4)$-net is greater than or equal to 16.

A $(4,4)$-net consists of 64 points and 64 blocks, each block of size 16 and each point in 16 blocks, so that the blocks (as well as and points) are partitioned into 16 parallel classes of size 4, and any two non-parallel blocks share 4 points.

Theorem. (Harada, Lam, & T, '05).

(i) Up to isomorphism, there are exactly 239 class-regular $(4,4)$-nets.
(ii) The 2-rank a symmetric class-regular $(4,4)$-net is greater than or equal to 16.
(iii) The binary codes of length 64 of three of the class-regular $(4,4)$-nets support affine 2-$(64,16,5)$ designs of 2-rank 16:

A $(4,4)$-net consists of 64 points and 64 blocks, each block of size 16 and each point in 16 blocks, so that the blocks (as well as and points) are partitioned into 16 parallel classes of size 4, and any two non-parallel blocks share 4 points.

Theorem. (Harada, Lam, & T, '05).

(i) Up to isomorphism, there are exactly 239 class-regular $(4,4)$-nets.
(ii) The 2-rank a symmetric class-regular $(4,4)$-net is greater than or equal to 16.
(iii) The binary codes of length 64 of three of the class-regular $(4,4)$-nets support affine 2-$(64,16,5)$ designs of 2-rank 16:

- *The code of the classical $(4,4)$-net supports the geometric design $AG_2(3,4)$.*
- *Two other nets support non-geometric 2-$(64,16,5)$ designs having the same 2-rank as $AG_2(3,4)$.*

(C) Designs from polarities

in $PG(2k-1, q)$

The motivating example:

A quasi-symmetric 2-(31,7,7) design with the following structure:

$15+16$

$2-(15,7,3)$ Planes in $PG(3,2)$	$2-(15,3,1)\times 4$ Lines in $PG(3,2)$
$\emptyset$	$3-(16,4,1)$ Planes in $AG(4,2)$

(C) Designs from polarities

in $PG(2k-1, q)$

The motivating example:

A quasi-symmetric 2-(31,7,7) design with the following structure:

$$15+16\left\{\begin{array}{|c|c|}\hline 2-(15,7,3) & 2-(15,3,1)\times 4 \\ \text{Planes in } PG(3,2) & \text{Lines in } PG(3,2) \\ \hline \emptyset & 3-(16,4,1) \\ & \text{Planes in } AG(4,2) \\ \hline \end{array}\right.$$

Note: $PG_2(4,2)$ and one other design share this structure.

Polarities in $PG(n, q)$

Polarities in $PG(n, q)$

A polarity α of $PG(n, q)$ is an involutory isomorphism between $PG(n, q)$ and its dual space:

Polarities in $PG(n,q)$

A polarity α of $PG(n,q)$ is an involutory isomorphism between $PG(n,q)$ and its dual space:

$$\begin{array}{rcl} \alpha: \ \text{point} & \longleftrightarrow & \text{hyperplane}, \ldots, \\ \text{i}-\text{subspace} & \longleftrightarrow & \text{(n-1-i)}-\text{subspace} \\ & \ldots & \end{array}$$

Polarities in $PG(n, q)$

A polarity α of $PG(n, q)$ is an involutory isomorphism between $PG(n, q)$ and its dual space:

$$\begin{array}{rcl} \alpha: \text{ point} & \longleftrightarrow & \text{hyperplane}, \ldots, \\ \text{i}-\text{subspace} & \longleftrightarrow & \text{(n-1-i)}-\text{subspace} \\ & \ldots & \end{array}$$

Example: The null polaity:

$$\begin{array}{rcl} \text{point} & \longleftrightarrow & \text{hyperplane} \\ (a_0, \ldots, a_n) & \longleftrightarrow & a_0x_0 + \cdots + a_nx_n = 0. \end{array}$$

A generalization to $PG(4,q)$

A polarity α of $PG(3,q)$:

$$\alpha:\ \text{point} \longleftrightarrow \text{plane};\ \textbf{line} \longleftrightarrow \textbf{line}$$

$$PG_2(4,q)\left\{\begin{array}{|c|c|}\hline PG_2(3,q) & PG_1(3,q)\\ \text{Planes} & \text{Lines}\\ \hline & AG_2(4,q)\\ \emptyset & \text{Planes}\\ \hline\end{array}\right.$$

A generalization to $PG(4,q)$

A polarity α of $PG(3,q)$:

$$\alpha: \text{ point} \longleftrightarrow \text{plane; } \textbf{line} \longleftrightarrow \textbf{line}$$

$$PG_2(4,q) \left\{ \begin{array}{|c|c|} \hline PG_2(3,q) & PG_1(3,q) \\ \text{Planes} & \text{Lines} \\ \hline & AG_2(4,q) \\ \emptyset & \text{Planes} \\ \hline \end{array} \right.$$

Theorem. Permuting the lines of a hyperplane

$$H = PG(3,q) \subset PG(4,q)$$

via a polarity α transforms $PG_2(4,q)$ into another **non-geometric** quasi-symmetric design.

A generalization to $PG(4,q)$

A polarity α of $PG(3,q)$:

$$\alpha : \text{ point} \longleftrightarrow \text{plane; } \textbf{line} \longleftrightarrow \textbf{line}$$

$$PG_2(4,q) \left\{ \begin{array}{|c|c|} \hline \begin{array}{c} PG_2(3,q) \\ \text{Planes} \end{array} & \begin{array}{c} PG_1(3,q) \\ \text{Lines} \end{array} \\ \hline \emptyset & \begin{array}{c} AG_2(4,q) \\ \text{Planes} \end{array} \\ \hline \end{array} \right.$$

Theorem. Permuting the lines of a hyperplane

$$H = PG(3,q) \subset PG(4,q)$$

via a polarity α transforms $PG_2(4,q)$ into another **non-geometric** quasi-symmetric design.

Note: Lines of $PG(4,q)$ which meet $H = PG(3,q)$ in one point are transformed by α into ”lines” of size 2.

A generalization to $PG(2k, q)$

$PG_k(2k, q)$

$PG_k(2k-1, q)$	$PG_{k-1}(2k-1, q)$
$\emptyset$	$AG_k(2k, q)$

A generalization to $PG(2k, q)$

$$PG_k(2k,q) \left\{ \begin{array}{|c|c|} \hline PG_k(2k-1,q) & PG_{k-1}(2k-1,q) \\ \hline \emptyset & AG_k(2k,q) \\ \hline \end{array} \right.$$

Note. Any polarity α of $PG(2k-1, q)$ maps any $(k-1)$-subspace to a $(k-1)$-subspace.

A generalization to $PG(2k, q)$

$$PG_k(2k,q)\left\{\begin{array}{|c|c|}\hline PG_k(2k-1,q) & PG_{k-1}(2k-1,q)\\ \hline \emptyset & AG_k(2k,q)\\ \hline\end{array}\right.$$

Note. Any polarity α of $PG(2k-1, q)$ maps any $(k-1)$-subspace to a $(k-1)$-subspace.

Theorem. Permuting the $(k-1)$-subspaces of a hyperplane

$$H = PG(2k-1, q) \subset PG(2k, q)$$

via a polarity α transforms $D = PG_k(2k, q)$ to a non-geometric design $\alpha(D)$ having the same parameters and block intersection numbers as $PG_k(2k, q)$.

The q-ranks of the new designs

Theorem.

Let α be a polarity in $PG(2k-1,q)$, where $q = p^s$ and p is a prime.

The q-ranks of the new designs

Theorem.

Let α be a polarity in $PG(2k-1,q)$, where $q=p^s$ and p is a prime.

- The p-rank the design $\alpha(D)$ satisfies the inequalities

$$\mathrm{rank}_p(D) \le \mathrm{rank}_p(\alpha(D)) \le \frac{1}{2}\Big(\frac{q^{2k+1}-1}{q-1}+1\Big),$$

  where $\mathrm{rank}_p(D)$ is the p-rank of the geometric design $D = PG_k(2k,q)$.

- If $q=p$ is a prime number then

$$\mathrm{rank}_p(D) = \mathrm{rank}_p(\alpha(D))$$

The q-ranks of the new designs

Theorem.

Let α be a polarity in $PG(2k-1,q)$, where $q=p^s$ and p is a prime.

- The p-rank the design $\alpha(D)$ satisfies the inequalities

$$\mathrm{rank}_p(D) \le \mathrm{rank}_p(\alpha(D)) \le \frac{1}{2}\Big(\frac{q^{2k+1}-1}{q-1}+1\Big),$$

  where $\mathrm{rank}_p(D)$ is the p-rank of the geometric design $D = PG_k(2k,q)$.

- If $q=p$ is a prime number then

$$\mathrm{rank}_p(D) = \mathrm{rank}_p(\alpha(D))$$

Note. If $q=4=2^2$, $k=2$,

$$\mathrm{rank}_2(PG_2(4,4)) = 146 < \mathrm{rank}_2(\alpha(D)) = 154 <$$

$$< ((4^5-1)/(4-1)+1)/2 = 171.$$

Hamada's formula for $r_p = \mathrm{rank}_p(PG_k(2k, p))$, p prime, as simplified by Hirschfeld and Shaw '94:

Hamada's formula for $r_p = \mathrm{rank}_p(PG_k(2k,p))$, p prime, as simplified by Hirschfeld and Shaw '94:

$$r_p = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1}(-1)^i \binom{(k-i)(p-1)-1}{i}\binom{k+(k-i)p}{2k-i}.$$

Hamada's formula for $r_p = \mathrm{rank}_p(PG_k(2k,p))$, p prime, as simplified by Hirschfeld and Shaw '94:

$$r_p = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1}(-1)^i \binom{(k-i)(p-1)-1}{i}\binom{k+(k-i)p}{2k-i}.$$

What we need is

$$r_p = \frac{1}{2}\Big(\frac{p^{2k+1}-1}{p-1}+1\Big).$$

Hamada's formula for $r_p = \mathrm{rank}_p(PG_k(2k,p))$, p prime, as simplified by Hirschfeld and Shaw '94:

$$r_p = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1}(-1)^i \binom{(k-i)(p-1)-1}{i}\binom{k+(k-i)p}{2k-i}.$$

What we need is

$$r_p = \frac{1}{2}\Big(\frac{p^{2k+1}-1}{p-1} + 1\Big).$$

Claim.

$$\frac{1}{2}\left(\frac{p^{2k+1}-1}{p-1} + 1\right) = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1}(-1)^i \binom{(k-i)(p-1)-1}{i}\binom{k+(k-i)p}{2k-i}.$$

Hamada's formula for $r_p = \mathrm{rank}_p(PG_k(2k,p))$, p prime, as simplified by Hirschfeld and Shaw '94:

$$r_p = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1} (-1)^i \binom{(k-i)(p-1)-1}{i} \binom{k+(k-i)p}{2k-i}.$$

What we need is

$$r_p = \frac{1}{2}\Big(\frac{p^{2k+1}-1}{p-1} + 1\Big).$$

Claim.

$$\frac{1}{2}\left(\frac{p^{2k+1}-1}{p-1} + 1\right) = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1} (-1)^i \binom{(k-i)(p-1)-1}{i} \binom{k+(k-i)p}{2k-i}.$$

J. L. W. V. Jensen: Sur une identité d'Abel et sur d'autres formules analogues, *Acta Math.* **26** (1902), 307-318.

Hamada's formula for $r_p = \mathrm{rank}_p(PG_k(2k,p))$, p prime, as simplified by Hirschfeld and Shaw '94:

$$r_p = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1} (-1)^i \binom{(k-i)(p-1)-1}{i} \binom{k+(k-i)p}{2k-i}.$$

What we need is

$$r_p = \frac{1}{2}\Big(\frac{p^{2k+1}-1}{p-1} + 1\Big).$$

Claim.

$$\frac{1}{2}\left(\frac{p^{2k+1}-1}{p-1} + 1\right) = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1} (-1)^i \binom{(k-i)(p-1)-1}{i} \binom{k+(k-i)p}{2k-i}.$$

J. L. W. V. Jensen: Sur une identité d'Abel et sur d'autres formules analogues, *Acta Math.* **26** (1902), 307-318.

M. E. Larsen: *Summa Summarum*, CMS Treatises in Mathematics, Canadian Mathematical Society, Ottawa, ON; A K Peters, Ltd., Wellesley, MA (2007).

Thank You!

We will need two lemmas for the proof of Theorem **??**.

Lemma 3.3 *Let α be a polarity in $PG(2k-1,q)$, where $q=p^s$ and p is a prime. The p-rank $r_p(\alpha)$ of the incidence matrix of the design $\alpha(\mathcal{D})$ from Theorem* **??** *satisfies the inequalities*

$$r_p(\mathcal{D}) \leq r_p(\alpha) \leq \frac{1}{2}\Big(\frac{q^{2k+1}-1}{q-1}+1\Big), \qquad (1)$$

where $r_p(\mathcal{D})$ is the p-rank of the geometric design $\mathcal{D}=PG_k(2k,q)$.

By the construction described in Section 2, the design $\alpha(\mathcal{D})$ has an incidence matrix of the form

$$M = \left(\begin{array}{c|c} M_1 & M_2 \\ \hline 0 & M_3 \end{array}\right),$$

where M_1 is a point by block incidence matrix of the geometric design $PG_k(2k-1,q)$, and M_3 is a point by block incidence matrix of the geometric design $AG_k(2k,q)$. Thus, we have

$$r_p(M_1)+r_p(M_3) \leq r_p(\alpha).$$

On the other hand, it follows from [1, Corollary 5.7.3, page 186], that

$$r_p(PG_k(2k,q)) = r_p(PG_k(2k-1,q)) + r_p(AG_k(2k,q))$$

Hence, we have

$$r_p(\mathcal{D}) = r_p(M_1) + r_p(M_3).$$

This proves the left-hand side inequality in (1). To prove the right-hand side inequality in (1), we consider the complementary design $\overline{\alpha(\mathcal{D})}$. By Lemma **??**, the design $\alpha(\mathcal{D})$ has the same intersection numbers as $\mathcal{D} = PG_k(2k,q)$, that is, $(q^i-1)/(q-1)$ for i in the range $1 \le i \le k$. Consequently, the block intersection numbers of the complementary design $\overline{\alpha(\mathcal{D})}$ are

$$\frac{q^i(q^{2k+1-i} - 2q^{k+1-i} + 1)}{q-1}, \ 1 \le i \le k.$$

Note that all these numbers are divisible by q, and that the blocks of $\overline{\alpha(\mathcal{D})}$ are of size

$$\frac{q^{k+1}(q^k-1)}{q-1},$$

which is also divisible by q. Thus, the incidence vectors of the blocks of $\overline{\alpha(\mathcal{D})}$ span a linear self-orthogonal code of length $(q^{2k+1}-1)/(q-1)$ over $GF(p)$. Hence, the p-rank of the incidence matrix $(J-M)$ of $\overline{\alpha(\mathcal{D})}$, where J denotes the all-one matrix of appropriate size, does not exceed $(\frac{q^{2k+1}-1}{q-1}-1)/2$ (note that the number of points of $\alpha(\mathcal{D})$, $(q^{2k+1}-1)/(q-1)$ is an odd number). The columns of $J-M$ have 0 and 1 entries, and the number of 1's in each column is a multiple of p. Therefore, each column of $J-M$ is orthogonal (over $GF(p)$) to the all-one column **j**, and consequently, the whole column space is orthogonal to **j**. Since **j** is not orthogonal to itself, **j** is not in the column space of $J-M$. On the other hand, **j** is a nonzero multiple of the sum of columns of M over $GF(p)$. This implies

$$r_p(M) = r_p(J-M)+1,$$

and therefore

$$r_p(M) \leq \frac{1}{2}\Big(\frac{q^{2k+1}-1}{q-1}-1\Big)+1 = \frac{1}{2}\Big(\frac{q^{2k+1}+1}{q-1}+1\Big).$$

This proves the right-hand side inequality in (1).

A summation formula for the p-rank of the incidence matrix of a geometric design $PG_r(n,q)$,

$1 \leq r \leq n-1$, $q = p^t$, p a prime, was found by Hamada [8]. If $r \neq 1, n-1$, Hamada's formula involves some parameters that have to be computed. A simplified formula for the case when $q = p$ is a prime was found by Hirschfeld and Shaw [13, Theorem 5.10]. In particular, the p-rank of $\mathcal{D} = PG_k(2k, p)$ is given by:

$$r_p(\mathcal{D}) = \frac{p^{2k+1}-1}{p-1} - \sum_{i=0}^{k-1} (-1)^i \binom{(k-i)(p-1)-1}{i} \Bigg(\tag{2}$$

If $p = 2$, the linear code spanned by the blocks of $\mathcal{D} = PG_k(2k, 2)$ is a punctured Reed-Muller code of length $v = 2^{2k+1} - 1$ and order k [1, Proposition 5.3.2], so we have an alternative formula for $r_2(\mathcal{D})$ which can be written in a simple closed form, namely

$$r_2(\mathcal{D}) = \sum_{i=0}^{k} \binom{2k+1}{i} = 2^{2k}.$$

Note that $2^{2k} = (v+1)/2$, so the inequalities in (1) are replaced by equalities:

$$r_2(\mathcal{D}) = r_2(\alpha) = 2^{2k} = (v+1)/2.$$

Thus, the pseudo-geometric designs from Section 2 for $q = p = 2$ are counter-examples to the “only if” part of Hamada’s conjecture.

In addition, the two formulas for $r_2(\mathcal{D})$ imply the following identity:

$$2^{2k} - 1 = \sum_{i=0}^{k-1} (-1)^i \binom{k-i-1}{i} \binom{3k-2i}{2k-i}. \quad (3)$$

It turns out that a similar closed formula for $r_p(\mathcal{D})$ holds for any prime number p.

Lemma 3.4 *If p is any prime, the p-rank of $\mathcal{D} = PG_k(2k, p)$ is equal to*

$$r_p(\mathcal{D}) = \frac{1}{2}\Big(\frac{p^{2k+1} - 1}{p-1} + 1\Big). \quad (4)$$

We will use the following result by Hirschfeld and Shaw [13, Corollary 5.5]): if p is a prime and $C^*(k, n, p)$ is the dual of the linear code over $GF(p)$ spanned by the incidence vectors of the k-dimensional subspaces of $PG(n, p)$, $1 \le k \le n-1$, then

$$\dim C^*(k, n, p) + \dim C^*(n-k, n, p) = \frac{p^{n+1} - 1}{p-1} - 1. \quad (5)$$

In the special case $n = 2k$, (5) implies that

$$\dim C^*(k, 2k, p) = \frac{1}{2}\Big(\frac{p^{2k+1}-1}{p-1} - 1\Big).$$

Note that $C^*(k, 2k, p)$ is the code having the incidence matrix of $\mathcal{D}$=$PG_k(2k, p)$ as a parity check matrix, hence

$$r_p(\mathcal{D}) = \frac{p^{2k+1}-1}{p-1} - \dim C^*(k, 2k, p) = \frac{1}{2}\Big(\frac{p^{2k+1}-1}{p-1}$$

Now Theorem **??** follows from Lemmas 3.3 and 3.4. We note that comparing (2) and (4) gives the following identity, which generalizes (3):

$$\frac{1}{2}\Big(\frac{p^{2k+1}-1}{p-1} - 1\Big) = \sum_{i=0}^{k-1} (-1)^i \binom{(k-i)(p-1)-1}{i} \Big(\qquad (6)$$

It was pointed to us by one of the reviewers, that equation (6) is actually true for all positive integers p and not just for primes; it follows from a formula of J.L.W.V. Jensen [14, Equation (18)], which is given a modern setting in [21, Section 14.1]. Of course, with (11) in hand, Lemma 3.4 is an immediate consequence of (2).

Acknowledgments. The second author wishes to thank the University of Augsburg, Germany, for the hospitality during his visit. He is also grateful for the support provided by a grant of the Alexander von Humboldt Foundation. The authors wish to thank James Hirschfeld for providing them with a copy of [13], Jenny Key for valuable references to [2], and the reviewers for their detailed work.

References

[1] E. F. Assmus, Jr., and J. D. Key: *Designs and their Codes*. Cambridge University Press, Cambridge (1992).

[2] E. F. Assmus, Jr., and J. D. Key: Polynomial codes and finite geometries. In: *Handbook of Coding Theory, Vol. II* (Eds. V. Pless and W. C. Huffman). North Holland, Amsterdam (1998), pp.1269–1343.

[3] A. Baartmans and S. Sane: A characterization of projective sub- spaces of codimension two as quasi-symmetric designs with good blocks. *Discr. Math.* **306** (2006), 1493–1501.

[4] T. Beth, D. Jungnickel and H. Lenz: *Design Theory (2nd edition)*. Cambridge University Press (1999).

[5] C. J. Colbourn and J. H. Dinitz: *Handbook of Combinatorial Designs (2nd edition)*. CRC Press, Boca Raton (2007).

[6] J.-M. Goethals and P. Delsarte: On a class of majority-logic decodable cyclic codes, *IEEE Trans. Inform. Theory* **14** (1968), 182-188.

[7] J. Doyen, X. Hubaut and M. Vandensavel: Ranks of incidence matrices of Steiner triple systems. *Math. Z.* **163** (1978), 251–259.

[8] N. Hamada: On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its application to error correcting codes. *Hiroshima Math. J.* **3** (1973), 154–226.

[9] N. Hamada and H. Ohmori: On the BIB-design having the minimum p-rank. *J. Combin. Theory Ser. A* **18** (1975), 131–140.

[10] M. Harada, C. W. H. Lam and V. D. Tonchev: Symmetric (4,4)-nets and generalized Hadamard matrices over groups of order 4. *Des. Codes Cryptogr.* **34** (2005), 71–87.

[11] J. W. P. Hirschfeld: *Projective Geometries over Finite Fields (2nd edition).* Oxford University Press (1998).

[12] J. W. P. Hirschfeld: *Finite Projective Spaces of Three Dimensions.* Oxford University Press (1985).

[13] J. W. P. Hirschfeld and R. Shaw: Projective geometry codes over prime fields. In: *Finite Fields: Theory, Application and Algorithms*. Contemporary Math **168** (1994), pp. 151–163. Amer Math. Soc., Providence, R.I.

[14] J. L. W. V. Jensen: Sur une identité d'Abel et sur d'autres formules analogues, *Acta Math.* **26** (1902), 307-318.

[15] D. Jungnickel: The number of designs with classical parameters grows exponentially. *Geom. Dedicata* **16** (1984), 167–178.

[16] D. Jungnickel and V. D. Tonchev: Polarities, quasi-symmetric designs, and Hamada's conjecture, *Designs, Codes and Cryptography*, **51** (2009), 131-140.

[17] D. Jungnickel and V. D. Tonchev: The Number of Designs with Geometric Parameters Grows

Exponentially, *Designs, Codes and Cryptography*, submitted.

[18] W. M. Kantor: Automorphisms and isomorphisms of symmetric and affine designs. *J. Algebraic Combin.* **3** (1994), 307–338.

[19] C. Lam, S. Lam and V. D. Tonchev: Bounds on the number of affine, symmetric, and Hadamard designs and matrices. *J. Combin. Theory Ser. A* **92** (2000), 186–196.

[20] C. Lam and V. D. Tonchev: A new bound on the number of designs with classical affine parameters. *Des. Codes Cryptogr.* **27** (2002), 111–117.

[21] M. E. Larsen: *Summa Summarum*, CMS Treatises in Mathematics, Canadian Mathematical Society, Ottawa, ON; A K Peters, Ltd., Wellesley, MA (2007).

[22] V. C. Mavron, T. P. McDonough and M. S. Shrikhande: Quasi-symmetric designs with good blocks and intersection number one. *Des. Codes Cryptogr.* **28** (2003), 147–162.

[23] V. C. Mavron, T. P. McDonough and V. D. Tonchev: On affine designs and Hadamard designs with line spreads. *Discrete Math.* **308** (2008), 2742–2750.

[24] T. P. McDonough and V. C. Mavron: Quasi-symmetric designs with good blocks. *J. Comb. Des.* **3** (1995), 433–441.

[25] M. Rahman and I. F. Blake: Majority logic decoding using combinatorial designs. *IEEE Trans. Inform. Theory* **21** (1975), 585–587.

[26] L. D. Rudolph: A class of majority-logic decodable codes. *IEEE Trans. Inform. Theory* **23** (1967), 305–307.

[27] S. S. Sane and M. S. Shrikhande: Some characterizations of quasi-symmetric designs with a spread. *Des. Codes Cryptogr.* **3** (1993), 155–166.

[28] M. S. Shrikhande and S. S. Sane: *Quasi-symmetric Designs*. Cambridge University Press, Cambridge (1991).

[29] L. Teirlinck: On projective and affine hyperplanes. *J. Combin. Theory Ser. A* **28** (1980), 290–306.

[30] 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.

[31] V. D. Tonchev: Linear perfect codes and a characterization of the classical designs. *Des. Codes Cryptogr.* **17** (1999), 121–128.