The Weight Distribution of the Self-Dual [128, 64] Polarity Design Code

Masaaki Harada, Ethan Novak*, and Vladimir D. Tonchev

August 27, 2015

Projective Geometry Designs

Notation

$PG_s(m, q)$ is the design having as points and blocks the points and s-dimensional subspaces of the projective geometry.

Projective Geometry Designs

Notation

$PG_s(m, q)$ is the design having as points and blocks the points and s-dimensional subspaces of the projective geometry.

Parameters

$PG_s(m, q)$ is a 2-(v, k, λ) design where $v = \dfrac{q^{m+1} - 1}{q - 1}$, $k = \dfrac{q^{s+1} - 1}{q - 1}$, and $\lambda = \begin{bmatrix} m-1 \\ s-1 \end{bmatrix}_q$.

Projective Geometry Designs

Notation

$PG_s(m, q)$ is the design having as points and blocks the points and s-dimensional subspaces of the projective geometry.

Parameters

$PG_s(m, q)$ is a 2-(v, k, λ) design where $v = \dfrac{q^{m+1} - 1}{q - 1}$, $k = \dfrac{q^{s+1} - 1}{q - 1}$, and $\lambda = \left[\begin{array}{c} m-1 \\ s-1 \end{array} \right]_q$.

Gaussian Coefficient

$$\left[\begin{array}{c} m \\ i \end{array} \right]_q = \frac{(q^m - 1)(q^{m-1} - 1)...(q^{m-i+1} - 1)}{(q^i - 1)(q^{i-1} - 1)...(q - 1)}$$

Affine Geometry Designs

Notation

$AG_s(m, q)$ is a 2-(v, k, λ) design having as points and blocks the points and s-dimensional subspaces of the m-dimensional affine geometry $AG(m, q)$.

Affine Geometry Designs

Notation

$AG_s(m, q)$ is a 2-(v, k, λ) design having as points and blocks the points and s-dimensional subspaces of the m-dimensional affine geometry $AG(m, q)$.

Parameters

The design $AG_s(m, q)$ has parameters $v = q^m$, $k = q^s$, and $\lambda = \begin{bmatrix} m-1 \\ s-1 \end{bmatrix}_q$.

Affine Geometry Designs

Notation

$AG_s(m,q)$ is a 2-(v,k,λ) design having as points and blocks the points and s-dimensional subspaces of the m-dimensional affine geometry $AG(m,q)$.

Parameters

The design $AG_s(m,q)$ has parameters $v = q^m$, $k = q^s$, and $\lambda = \begin{bmatrix} m-1 \\ s-1 \end{bmatrix}_q$.

$AG_s(m,2)$

When $q = 2$ and $s \geq 2$, $AG_s(m,2)$ is also a 3-design, with every set of three points contained in $\lambda_3 = \begin{bmatrix} m-2 \\ s-2 \end{bmatrix}_2$ blocks.

Codes from Geometries

Definition

A geometric code is a linear code being the null space of the incidence matrix of a geometric design $AG_s(m, q)$ or $PG_s(m, q)$.

Codes from Geometries

Definition

A geometric code is a linear code being the null space of the incidence matrix of a geometric design $AG_s(m, q)$ or $PG_s(m, q)$.

Properties

The codes over the field of p elements where $q = p^t$ for some t correspond to subfield subcodes of generalized Reed-Muller codes.

Codes from Geometries

Definition

A geometric code is a linear code being the null space of the incidence matrix of a geometric design $AG_s(m, q)$ or $PG_s(m, q)$.

Properties

The codes over the field of p elements where $q = p^t$ for some t correspond to subfield subcodes of generalized Reed-Muller codes.

In the binary case, the code corresponding to $AG_s(m, 2)$ is equivalent to the Reed-Muller code $R(m - s, m)$ of length 2^m and order $m - s$.

Codes from Geometries

Definition

A geometric code is a linear code being the null space of the incidence matrix of a geometric design $AG_s(m, q)$ or $PG_s(m, q)$.

Properties

The codes over the field of p elements where $q = p^t$ for some t correspond to subfield subcodes of generalized Reed-Muller codes.

In the binary case, the code corresponding to $AG_s(m, 2)$ is equivalent to the Reed-Muller code $R(m - s, m)$ of length 2^m and order $m - s$.

It is well known that the finite geometry codes admit majority-logic decoding.

Polarity Designs

Jungnickel and Tonchev used polarities in projective geometry to find a class of designs with the same parameters as the projective geometry design $PG_s(2s, q)$, $s \geq 2$, but are not isomorphic to $PG_s(2s, q)$.

Polarity Designs

Jungnickel and Tonchev used polarities in projective geometry to find a class of designs with the same parameters as the projective geometry design $PG_s(2s, q)$, $s \geq 2$, but are not isomorphic to $PG_s(2s, q)$.

When $q = p$ is a prime, the p-rank of the incidence matrix of the polarity design D is equal to that of $PG_s(2s, p)$.

Polarity Designs

Jungnickel and Tonchev used polarities in projective geometry to find a class of designs with the same parameters as the projective geometry design $PG_s(2s, q)$, $s \geq 2$, but are not isomorphic to $PG_s(2s, q)$.

When $q = p$ is a prime, the p-rank of the incidence matrix of the polarity design D is equal to that of $PG_s(2s, p)$.

This provides an infinite class of counterexamples to Hamada's conjecture.

Polarity Designs

Clark and Tonchev proved that a code obtained from a polarity design can correct by majority-logic decoding the same number of errors as the projective geometry code from $PG_s(2s, q)$.

Polarity Designs

Clark and Tonchev proved that a code obtained from a polarity design can correct by majority-logic decoding the same number of errors as the projective geometry code from $PG_s(2s, q)$.

When $q = 2$, the minimum distance of the code from the polarity design obtained from $PG(2s, 2)$ is 2^{s+1}.

Polarity Designs

Clark and Tonchev proved that a code obtained from a polarity design can correct by majority-logic decoding the same number of errors as the projective geometry code from $PG_s(2s, q)$.

When $q = 2$, the minimum distance of the code from the polarity design obtained from $PG(2s, 2)$ is 2^{s+1}.

All errors guaranteed by the minimum distance may be corrected.

Polarity Designs

Clark and Tonchev proved that a code obtained from a polarity design can correct by majority-logic decoding the same number of errors as the projective geometry code from $PG_s(2s, q)$.

When $q = 2$, the minimum distance of the code from the polarity design obtained from $PG(2s, 2)$ is 2^{s+1}.

All errors guaranteed by the minimum distance may be corrected.

Extending the binary code spanned by the blocks of a polarity design obtained from $PG(2s, 2)$ is a self-dual binary code of the same length, dimension, and minimum distance as the Reed-Muller code $R(s, 2s + 1)$.

Polarity Designs

Clark and Tonchev proved that a code obtained from a polarity design can correct by majority-logic decoding the same number of errors as the projective geometry code from $PG_s(2s, q)$.

When $q = 2$, the minimum distance of the code from the polarity design obtained from $PG(2s, 2)$ is 2^{s+1}.

All errors guaranteed by the minimum distance may be corrected.

Extending the binary code spanned by the blocks of a polarity design obtained from $PG(2s, 2)$ is a self-dual binary code of the same length, dimension, and minimum distance as the Reed-Muller code $R(s, 2s+1)$.

This code can correct the same number of errors as $R(s, 2s+1)$ of length 2^{2s+1} and order s.

The Smallest Case

When $s = 2$, the extended code of the polarity design from $PG(4, 2)$ is a doubly-even self-dual [32, 16, 8] code.

The Smallest Case

When $s = 2$, the extended code of the polarity design from $PG(4, 2)$ is a doubly-even self-dual [32, 16, 8] code.

This code has the same parameters and corrects the same number of errors as the Reed-Muller code $R(2, 5)$.

The Smallest Case

When $s = 2$, the extended code of the polarity design from $PG(4, 2)$ is a doubly-even self-dual [32, 16, 8] code.

This code has the same parameters and corrects the same number of errors as the Reed-Muller code $R(2, 5)$.

It also has the same weight distribution as $R(2, 5)$.

The Smallest Case

When $s = 2$, the extended code of the polarity design from $PG(4, 2)$ is a doubly-even self-dual [32, 16, 8] code.

This code has the same parameters and corrects the same number of errors as the Reed-Muller code $R(2, 5)$.

It also has the same weight distribution as $R(2, 5)$.

Both codes are extremal doubly-even self-dual codes, and thus must have the same weight distribution.

Goals for $PG_3(6,2)$

Consider the next case when $s = 3$.

Goals for $PG_3(6, 2)$

Consider the next case when $s = 3$.

Investigate the extended code of the polarity design obtained from $PG(6, 2)$.

Goals for $PG_3(6,2)$

Consider the next case when $s = 3$.

Investigate the extended code of the polarity design obtained from $PG(6,2)$.

Demonstrate that this doubly-even self-dual [128, 64, 16] code has the same weight distribution as the third order Reed-Muller code $R(3,7)$.

$PG_3(6, 2)$

The polarity design D obtained from $PG(6, 2)$ is a 2-(127, 15, 155) design.

$PG_3(6,2)$

The polarity design D obtained from $PG(6,2)$ is a 2-(127, 15, 155) design.

D has the same parameters as the projective geometry design $PG_3(6,2)$.

$PG_3(6,2)$

The polarity design D obtained from $PG(6,2)$ is a 2-(127, 15, 155) design.

D has the same parameters as the projective geometry design $PG_3(6,2)$.

D has the same block intersections (sizes 1, 3, and 7) as $PG_3(6,2)$.

$PG_3(6,2)$

The polarity design D obtained from $PG(6,2)$ is a 2-(127, 15, 155) design.

D has the same parameters as the projective geometry design $PG_3(6,2)$.

D has the same block intersections (sizes 1, 3, and 7) as $PG_3(6,2)$.

D also has the same 2-rank as $PG_3(6,2)$. Namely, 64.

$PG_3(6, 2)$

The polarity design D obtained from $PG(6, 2)$ is a 2-(127, 15, 155) design.

D has the same parameters as the projective geometry design $PG_3(6, 2)$.

D has the same block intersections (sizes 1, 3, and 7) as $PG_3(6, 2)$.

D also has the same 2-rank as $PG_3(6, 2)$. Namely, 64.

These properties imply that the binary linear code C spanned by the block by point incidence matrix of D has minimum distance ≤ 15, and the extended code C^* is a doubly-even self-dual [128, 64] code of minimum distance $d \leq 16$.

$PG_3(6,2)$

The polarity design D obtained from $PG(6,2)$ is a 2-(127, 15, 155) design.

D has the same parameters as the projective geometry design $PG_3(6,2)$.

D has the same block intersections (sizes 1, 3, and 7) as $PG_3(6,2)$.

D also has the same 2-rank as $PG_3(6,2)$. Namely, 64.

These properties imply that the binary linear code C spanned by the block by point incidence matrix of D has minimum distance ≤ 15, and the extended code C^* is a doubly-even self-dual [128, 64] code of minimum distance $d \leq 16$.

From bounds on the minimum distance found by Clark and Tonchev, it follows that $d = 16$, and C^* admits majority-logic decoding that corrects up to 7 errors.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

The weight distribution of $R(3,7)$ was computed by Sugino, Ienaga, Tokura, and Kasami in 1971.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

The weight distribution of $R(3,7)$ was computed by Sugino, Ienaga, Tokura, and Kasami in 1971.

Find the weight distribution of the code C^* generated by the first k rows of the generator matrix.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

The weight distribution of $R(3,7)$ was computed by Sugino, Ienaga, Tokura, and Kasami in 1971.

Find the weight distribution of the code C^* generated by the first k rows of the generator matrix.

1. Considering 33 rows requires 2.14 minutes.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

The weight distribution of $R(3,7)$ was computed by Sugino, Ienaga, Tokura, and Kasami in 1971.

Find the weight distribution of the code C^* generated by the first k rows of the generator matrix.

1. Considering 33 rows requires 2.14 minutes.
2. Considering 34 rows requires 4.3 minutes.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

The weight distribution of $R(3,7)$ was computed by Sugino, Ienaga, Tokura, and Kasami in 1971.

Find the weight distribution of the code C^* generated by the first k rows of the generator matrix.

1. Considering 33 rows requires 2.14 minutes.
2. Considering 34 rows requires 4.3 minutes.
3. Considering 35 rows requires 8.6 minutes.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

The weight distribution of $R(3,7)$ was computed by Sugino, Ienaga, Tokura, and Kasami in 1971.

Find the weight distribution of the code C^* generated by the first k rows of the generator matrix.

1. Considering 33 rows requires 2.14 minutes.
2. Considering 34 rows requires 4.3 minutes.
3. Considering 35 rows requires 8.6 minutes.
4. ...
5. Considering 64 rows would require approximately 8750 years.

Finding the Weight Distribution

Now we demonstrate that C^* and $R(3,7)$ share the same weight distribution.

The weight distribution of $R(3,7)$ was computed by Sugino, Ienaga, Tokura, and Kasami in 1971.

Find the weight distribution of the code C^* generated by the first k rows of the generator matrix.

1. Considering 33 rows requires 2.14 minutes.
2. Considering 34 rows requires 4.3 minutes.
3. Considering 35 rows requires 8.6 minutes.
4. ...
5. Considering 64 rows would require approximately 8750 years.

This is not feasible, so we use another approach.

Finding the Weight Distribution

Since C^* is a doubly-even self-dual [128, 64, 16] code, we can find the weight distribution from the values of a_{16} and a_{20} using Gleason's Theorem.

Finding the Weight Distribution

Since C^* is a doubly-even self-dual [128, 64, 16] code, we can find the weight distribution from the values of a_{16} and a_{20} using Gleason's Theorem.

The weight enumerator $W(x) = \sum_{i=0}^{128} a_i x^i$ can be expressed entirely in terms of a_{16} and a_{20}.

Finding the Weight Distribution

Since C^* is a doubly-even self-dual [128, 64, 16] code, we can find the weight distribution from the values of a_{16} and a_{20} using Gleason's Theorem.

The weight enumerator $W(x) = \sum_{i=0}^{128} a_i x^i$ can be expressed entirely in terms of a_{16} and a_{20}.

$a_{16} = 94488$ and $a_{20} = 0$ were computed quickly using Magma.

Finding the Weight Distribution

Since C^* is a doubly-even self-dual [128, 64, 16] code, we can find the weight distribution from the values of a_{16} and a_{20} using Gleason's Theorem.

The weight enumerator $W(x) = \sum_{i=0}^{128} a_i x^i$ can be expressed entirely in terms of a_{16} and a_{20}.

$a_{16} = 94488$ and $a_{20} = 0$ were computed quickly using Magma.

Computing $a_{24} = 74078592$ took several days.

Table of Weights

The Weight Distribution of C^* and $R(3,7)$	
$a_0 = a_{128}$	1
$a_{16} = a_{112}$	94488
$a_{20} = a_{108}$	0
$a_{24} = a_{104}$	74078592
$a_{28} = a_{100}$	3128434688
$a_{32} = a_{96}$	312335197020
$a_{36} = a_{92}$	18125860315136
$a_{40} = a_{88}$	552366841342848
$a_{44} = a_{84}$	9491208609103872
$a_{48} = a_{80}$	94117043084875944
$a_{52} = a_{76}$	549823502398291968
$a_{56} = a_{72}$	1920604779257215744
$a_{60} = a_{68}$	4051966906789380096
a_{64}	5193595576952890822

The weight distribution of the doubly-even, self-dual code C^* was computed from $a_{16} = 94488$ and $a_{20} = 0$ using Gleason's Theorem and is identical to that of $R(3,7)$ computed in 1971.

Conclusion

Theorem

The weight distribution of the extended [128, 64, 16] code C^* of the code C spanned by the incidence vectors of the blocks of the polarity design D obtained from $PG(6,2)$ is identical with the weight distribution of the 3rd order Reed-Muller code $R(3,7)$.

Conjecture

The extended code of the polarity design from $PG(4,2)$ is a doubly-even self-dual code with the same weight distribution as $R(2,5)$.

Conjecture

The extended code of the polarity design from $PG(4,2)$ is a doubly-even self-dual code with the same weight distribution as $R(2,5)$.

The extended code of the polarity design from $PG(6,2)$ is a doubly-even self-dual code with the same weight distribution as $R(3,7)$.

Conjecture

The extended code of the polarity design from $PG(4,2)$ is a doubly-even self-dual code with the same weight distribution as $R(2,5)$.

The extended code of the polarity design from $PG(6,2)$ is a doubly-even self-dual code with the same weight distribution as $R(3,7)$.

Conjecture

Professor Tonchev conjectures that the extended code of the polarity design obtained from $PG(2s,2)$ has the same weight distribution as the Reed-Muller code $R(s,2s+1)$ for every $s \geq 2$.

Conjecture

The extended code of the polarity design from $PG(4,2)$ is a doubly-even self-dual code with the same weight distribution as $R(2,5)$.

The extended code of the polarity design from $PG(6,2)$ is a doubly-even self-dual code with the same weight distribution as $R(3,7)$.

Conjecture

Professor Tonchev conjectures that the extended code of the polarity design obtained from $PG(2s,2)$ has the same weight distribution as the Reed-Muller code $R(s,2s+1)$ for every $s \geq 2$.

Verifying the next case ($s = 4$) is currently computationally infeasible.

References

D. Clark, D. Jungnickel, and V. D. Tonchev, Affine geometry designs, polarities, and Hamada's conjecture, *J. Combin. Theory Ser. A* **118** (2011), 231-239.

D. Clark and V. D. Tonchev, A new class of majority-logic decodable codes derived from polarity designs, *Adv. Math. Commun.* **7** (2013), 175-186.

Thank you!

Thank you for your time and attention!