On the classification of unitals on 28 points of low rank

Alfred Wassermann

Department of Mathematics, Universität Bayreuth, Germany

joint work with Vladimir Tonchev

8ECM — Portorož, Slovenia — June 24, 2021

Designs

- $t, k, v, \lambda \in \mathbb{Z}_{\geq 0}$ and $0 \leq t \leq k \leq v$
- V: set of v points
- $\mathcal{B}$ is a collection of subsets of cardinality k (blocks) of V
- $\mathcal{D} = (V, \mathcal{B})$ is called a t-(v, k, λ) design on V if *each subset of cardinality t of V is contained in exactly λ blocks.*

t-(v, k, λ) design $\mathcal{D} = (V, \mathcal{B})$:

- $\#\mathcal{B} = \lambda\binom{v}{t}/\binom{k}{t}$
- Every point $P \in V$ appears in $r = \lambda\binom{v-1}{t-1}/\binom{k-1}{t-1}$ blocks
- r is called replication number

p-rank of a 2-(v, k, λ) design

- The *p-rank* of a design $\mathcal{D}(V, \mathcal{B})$ is the rank of the incidence matrix between the points $P \in V$ and the blocks $B \in \mathcal{B}$ of $\mathcal{D}$ over $\mathbb{F}_p$.
- Trivial upper bounds: p-rank $\leq v$ and $< v$ if $p \mid k$
- Design has low rank if the p-rank is $<$ trivial upper bound
- Code from a design: p-ary linear code spanned by the incidence matrix of the design.

  This code is only interesting if

$$p \mid r - \lambda$$

Unitals

- A 2-$(q^3+1, q+1, 1)$ design is called unital
- Classical examples:
  - Hermitian unital $H(q)$, defined by the absolute points and absolute lines of a unitary polarity in the desarguesian plane of order q^2
  - Ree unital $R(q)$ for $q = 3^{2m+1}$, invariant under the Ree group
- $q = 2$: 2-$(9, 3, 1)$ design – unique
- $q = 3$: 2-$(28, 4, 1)$ design – classification still incomplete

Rest of the talk: $q = 3$, i.e. unital $=$ 2-$(28, 4, 1)$ design

2-$(28, 4, 1)$ designs and their codes

- $\#\mathcal{B} = 63$, $r = 9$
- $\lambda = 1$: $r - \lambda = 8 \implies p = 2$

Let C be the binary linear code of a 2-$(28, 4, 1)$ design, $C^\perp$ the dual code of C.

- $\dim C \leq 27$
- C is self-complementary, i.e. contains the all-one vector $\implies$ all weights in $C^\perp$ are even
- $C^\perp$ is self-complementary
- Possible weights of $C^\perp$: 10, 12, 14, 16, 18, 28
- Codewords in $C^\perp$ of weight divisible by 4 form a subcode

Previous work on 2-$(28, 4, 1)$ designs

- Piper (1979)
- Brouwer (1981): Found 138 non-isomorphic unitals
- McGuire, Tonchev, Ward (1998): 2-rank ≥ 19, with equality achieved by the Ree unital only
- Jaffe, Tonchev (1998): There are
  - no unitals of rank 20
  - 4 non-isomorphic unitals of rank 21
- Krčadinac (2002): Classification of all (4466) 2-$(28, 4, 1)$ designs with non-trival automorphisms
- Betten, Betten, Tonchev (2003): Classification of all (909) 2-$(28, 4, 1)$ designs containing a special spread
- Kaski, Östergård (2009): Classification of all (7) resolutions of 2-$(28, 4, 1)$ designs
- Here: Classification of unitals of rank 22, 23, and 24

Classification method

The computer classification method is in the spirit of the work of Jaffe, Tonchev (1998) – using different tools:

- Fix a rank $\mathtt{rk} \geq 19$
- Classify the binary linear codes $[28, 28 - \mathtt{rk}, \geq 10]$ codes $C^{\perp}$ with all known restrictions
- For each code $C^{\perp}$:
  - Compute the set of all codewords of C of weight 4, i.e. all possible blocks of such a unital
  - Enumerate all unitals for this set of blocks
  - Classify the unitals
- Classify all unitals
- Result: **all** unitals of rank $\leq \mathtt{rk}$

Comment: We did this for $\mathtt{rk} = 22, 23, 24$ and compared the outcome with previous results, i.e. checked if the determined number of unitals of rank $< \mathtt{rk}$ is correct.

The code C from a unital

The code from a unital of rank $\mathtt{rk}$

- C is an even self-complementary $[28, \mathtt{rk}]$ code
- $C^{\perp}$ is an even self-complementary $[28, 28 - \mathtt{rk}, \geq 10]$ code, containing a doubly-even self-complementary $[28, t, 12]$ code for some $t \leq 28 - \mathtt{rk}$.

Doubly-even subcodes of an even code

General result: [Lemma 2.4 in Jaffe, Tonchev (1998)]

In an even binary linear $[n, k]$ code:

- D: set of codewords of weight divisible by 4
- t: maximum dimension of a doubly-even subcode
- Then:

$$\#D \in \{2^{k-1} - 2^t, 2^{k-1}, 2^{k+1} + 2^{t-1}\}$$

Case of unitals:

D is a doubly-even subcode of $C^\perp$ of maximum dimension t

$\implies$ 2^t is one of the above numbers

Results

Unitals of rank 22

$\dim C = 22$, $\dim C^{\perp} = 6$

1. Classify the self-compl. doubly-even $[28, 4, 12]$ codes:
   - 4 codes
   - Software: enumeration: `solvediophant` by the author, classification: `codecan` by Feulner
2. Extend the codes to self-compl. even $[28, 6, \geq 10]$ codes:
   - 1. step: there are 128 self-compl. even $[28, 5, \geq 10]$ codes
   - 2. step: there are 15 007 self-compl. even $[28, 6, \geq 10]$ codes
   - Again, we used `solvediophant` and `codecan`
3. Find all unitals in the 15 007 $[28, 22]$ codes:
   - 661 504 unitals from 124 codes with `dlx` by Knuth
   - 17 isomorphy classes with `GAP design` package by Soicher

Result:

- 1 unital of rank 19
- 4 unitals of rank 21
- 12 unitals of rank 22

Unitals of rank 23

$\dim C = 23$, $\dim C^\perp = 5$

1. Classify the self-compl. doubly-even $[28, 3, 12]$ codes:
   - 2 codes
2. Extend the codes to self-compl. even $[28, 5, \geq 10]$ codes:
   - 1. step: there are 34 self-compl. even $[28, 4, \geq 10]$ codes
   - 2. step: there are 880 self-compl. even $[28, 5, \geq 10]$ codes
3. Find all unitals in the 880 $[28, 23]$ codes:
   - 16 911 unitals from 126 codes
   - 95 isomorphy classes

Result:

- 1 unital of rank 19
- 4 unitals of rank 21
- 12 unitals of rank 22
- 78 unitals of rank 23

Unitals of rank 24

$\dim C = 24$, $\dim C^{\perp} = 4$

1. Classify the self-compl. doubly-even $[28, 2, 12]$ codes:
   - 1 code
2. Extend the codes to self-compl. even $[28, 4, \geq 10]$ codes:
   - 1. step: there are 9 self-compl. even $[28, 3, \geq 10]$ codes
   - 2. step: there are 82 self-compl. even $[28, 4, \geq 10]$ codes
3. Find all unitals in the 82 $[28, 24]$ codes:
   - 7 663 704 unitals from 39 codes
   - 393 isomorphy classes

Result:

- 298 unitals of rank 24

Intermediate computations

- Rank 22: straightforward
- Rank 23:
  - Classify the derived designs with regard to point 28 under the stabilizer of 28 of the automorphism group of the code, i.e. fix 9 blocks
  - Try to extend each derived design to unitals
- Rank 24:
  - Determine transversal of all block orbits of blocks containing point 28 under the stabilizer of 28 of the automorphism group of the code
  - For each block, classify the derived designs with regard to point 28 that contain that block.
  - Try to extend each derived design to unitals
- Computations with automorphism groups were done with GAP

Summary

There are:

- 1 unital of rank 19 (non-rigid)
- 4 unitals of rank 21 (all non-rigid)
- 12 unitals of rank 22 (all non-rigid)
- 78 unitals of rank 23 (4 rigid, 74 non-rigid)
- 298 unitals of rank 24 (38 rigid, 260 non-rigid)

The numbers of non-rigid unitals coincide with the results of Krčadinac

Open questions

- Rank 25:
  - 1 self-compl. doubly-even $[28, 2, 12]$ codes
  - 9 self-compl. even $[28, 3, \geq 10]$ codes
- Rank 26: ?
- Complete classification of 2-$(28, 4, 1)$ designs
- Unitals for $q = 4$, i.e. 2-$(65, 5, 1)$ designs

Thank you for your attention!

References

- A. Betten, D. Betten, V. Tonchev, *Unitals and codes*, Discr. Math. (2003)
- A. E. Brouwer, *Some unitals on 28 points and their embedding in projective planes of order 9*, Springer LNMS 893, (1981)
- G. McGuire, V. Tonchev, H. N. Ward, *Characterizing the Hermitian and Ree unitals on 28 points*, DCC (1998)
- D. B. Jaffe, V. Tonchev, *Computing linear codes and unitals*, DCC (1998)
- P. Kaski, P. R. J. Östergård, *Classification of resolvable balanced incomplete block designs – The unitals on 28 points*, Mathematica Slovaca 59 (2009),
- V. Krčadinac, *Steiner 2-designs $S(2,4,28)$ with nontrivial automorphisms*, Glasnik Matematički (2002)
- F. Piper, *Unitary block designs*, Research notes in mathematics (1979)