Unitals and Codes

Anton Betten
Lehrstuhl Mathematik II
University of Bayreuth
95440 Bayreuth
Germany,

Dieter Betten
Mathematical Seminar
University of Kiel
Ludewig-Meyn-Str. 4
D-24098 Kiel
Germany,
and
Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931
USA

May 25, 2000

Abstract

A program is outlined for the enumeration of unital 2-(28,4,1) designs that uses tactical decompositions defined by vectors of certain weight in the dual binary code of a design. A class of designs with a spread that covers a codeword of weight 12 is studied in detail. A total of 909 nonisomorphic designs are constructed that include the classical hermitian and Ree unitals, as well as many other of the 145 previously known 2-(28,4,1) designs.

1 Introduction

We assume familiarity with the basics of combinatorial designs and linear codes (cf., e.g. [12]).

A *unital* in a projective plane of order $n = q^2$ is a set U of $q^3 + 1$ points that meets every line in either one or $q+1$ points. A classical example is the *hermitian unital* $H(q)$ defined by the absolute points of a unitary polarity in the desarguesian plane of order q^2, $PG(2, q^2)$. The points of U together with the line intersections of size $q + 1$ form a 2-$(q^3 + 1, q + 1, 1)$ design, called a *unital design* associated with U. More generally, any 2-$(q^3+1, q+1, 1)$ design is called a unital design, or a unital, regardless whether it is associated with any plane or not.

The *Ree unital* $R(q)$ is a design on $q^3 + 1$ points, $q = 3^{2m+1}$, $m \geq 0$, invariant under the Ree group [7].

Unital designs for $q = 3$, namely, 2-(28,4,1) designs, were studied by Brouwer [5] in connection with their embeddability in projective planes of order 9. Brouwer found 138 nonisomorphic unital 2-(28,4,1) designs, 12 of those being unitals in planes of order 9 [5]. Penttila and Royle [10] showed that up to isomorphism there are exactly 18 unitals in the projective planes of order 9. Seven more 2-(28,4,1) designs appear to have been found more recently, setting the record of known nonisomorphic 2-(28,4,1) designs to 145 [8]. Unitals were found in all known projective planes of order 16 by Stoichev and Tonchev [11].

The *binary code* of a design is the binary linear space spanned by the incidence vectors of the blocks. Brouwer [5] computed the binary codes of the 2-(28,4,1) designs he found, and made the conjecture that the Ree unital $R(3)$ is the only 2-(28,4,1) design with code of dimension 19, that is, with incidence matrix of 2-rank 19. Brouwer also noticed that the 2-rank of any other known 2-(28,4,1) design, including the hermitian unital $H(3)$, was 21 or larger.

Brouwer's conjecture was proved recently by McGuire, Tonchev and Ward [9]. More precisely, the 2-rank of the incidence matrix of any unital on 28 points is greater or equal to 19, and the Ree unital $R(3)$ is the only (up to isomorphism) example of rank 19 [9]. In addition, the 2-rank of any unital on 28 points without *ovals* (sets of 10 points that meet each block in at most 2 points) is greater or equal to 21, with equality if and only if the design is isomorphic to the hermitian unital $H(3)$ [9].

A computer search carried out by Jaffe and Tonchev [6] showed that there are no 2-(28,4,1) designs of 2-rank 20, and there are exactly 4 nonisomorphic 2-(28,4,1) designs of 2-rank 21: the hermitian unital $H(3)$ plus three other designs.

2 Binary codes and tactical decompositions

Binary codes were instrumental in the proof of Brouwer's conjecture [9], and for the enumeration of all 2-(28,4,1) designs of 2-rank 21 [6].

The code C of a 2-(28,4,1) design is the row space of the 63 by 28 block by point incidence matrix M. The row sums of M are even (equal to 4), and the column sums are odd (equal

to 9). This implies that all vectors in C are of even (Hamming) weight, the all-one vector $\bar{1}$ is in C as well as in the dual code $C^{\perp}$, and all weights in $C^{\perp}$ are also even. Any vector of weight w in $C^{\perp}$ corresponds to w linearly dependent columns of M. A simple counting argument shows that if $w > 0$ then $w \geq 10$, hence the possible nonzero weights in $C^{\perp}$ are 10, 12, 14, 16, 18 and 28. The sum of all columns of M is the zero column. Thus, the 2-rank of M ($rank_2(M)$ is at most 27, and by the results of [9], at least 19:

$$19 \leq rank_2(M) \leq 27.$$

If the 2-rank of M is 27 then C is the 27-dimensional vector subspace consisting of all even-weight vectors of length 28, and $C^{\perp}$ consists of the zero vector and the all-one vector only. Thus, the code does not provide any useful information about the structure of the design in this case.

The 2-rank of M is smaller than 27 if and only if $C^{\perp}$ contains a vector x of weight w, such that $0 < w < 28$. The complementary vector $x + \bar{1}$ is also in $C^{\perp}$ and is of weight $28 - w$. The support of x corresponds to a set of w columns of M with even row sums, and the complementary set of $28 - w$ columns also has even row sums. Thus, every vector in $C^{\perp}$ of weight w, $0 < w < 28$, defines a tactical decomposition of M into submatrices with constant row sums.

There are three possible decompositions according to the value of w, listed in Table 1. Here n_i denotes the number of rows of the incidence matrix M that have row sum i ($i = 0$,

Case	w	n_0	n_2	n_4	$28 - w$	$\bar{n_0}$	$\bar{n_2}$	$\bar{n_4}$
A	10	18	45	0	18	0	45	18
B	12	12	48	3	16	3	48	12
C	14	7	49	7	14	7	49	7

Table 1: Tactical decompositions defined by vectors in $C^{\perp}$

2, or 4) in the columns indexed by the w nonzero positions of x, and $\bar{n_i}$ denotes the the number of rows of M with row sum i in the complementary $28 - w$ columns. Note that $\bar{n_i}$=n_{4-i}.

This paper reports some computational results on the enumeration of certain 2-(28,4,1) designs with a decomposition of type B, that is, designs whose dual code $C^{\perp}$ contains a vector of weight 12. It was noticed by Brouwer [5] that the set of nonzero positions of any vector of weight 12 in $C^{\perp}$ is the union of three disjoint blocks.

A *spread* (or parallel class) in a 2-(28,4,1) design is a set of 7 pairwise disjoint blocks that partition the point set. A *resolution* is a partition of the 63 blocks into 9 disjoint spreads.

We call a spread *special* if it contains three blocks whose union is the set of nonzero positions of a vector of weight 12 in $C^{\perp}$. It is seen by some of the computations in [5] that there are designs that contain spreads but do not have any special spread. Therefore, the

designs with a decomposition of type B and a special spread that contains the three disjoint blocks defining the decomposition, is a proper subclass of case B. We refer to this subclass as BP.

An algorithm developed by the first two authors ([2], [3], [4]) was used for finding refined decompositions of type BP and constructing designs from them. A set of 909 pairwise nonisomorphic 2-(28,4,1) designs were found by completing the search in some of these cases. Incidence matrices of these designs are available upon request from the authors electronically. Some statistics of these designs, such as 2-rank, automorphism group order, number of spreads and resolutions, are listed in the last section of the paper. The 909 designs include the hermitian unital, the Ree unital, as well as many other (but not all) of the 145 previously known 2-(28,4,1) designs.

The tactical decompositions A, B, C (Table 1) can be used as a starting point for the enumeration of all 2-(28,4,1) designs of 2-rank smaller than 27. The cases A, B, C are not disjoint in general. For example, the Ree unital $R(3)$ admits decompositions of type A, B and C. However, if the 2-rank of the incidence matrix is exactly 26, $C^{\perp}$ is of dimension 2 and consists of the zero vector, $\bar{1}$, a vector x of weight $0 < w < 28$, and the complementary vector $x + \bar{1}$ of weight $28 - w$, that yield exactly one of the decompositions A, B, or C.

3 Construction of Unital designs with a special spread

The unitals in cases A, B and C can be described by the following tactical decompositions (in the notation of [2]). Here the first column and the first line describe the partition of point set and the block set, and the entries in the matrix are the (constant) numbers of horizontal flags in the respective subrectangle:

A	45	18
10	9	0
18	5	4

,

B	12	3	48
16	3	0	6
12	0	1	8

,

C	7	49	7
14	2	7	0
14	0	7	2

Case B with a special parallel class has the following TD:

BP	4	3	8	48
16	1	0	2	6
12	0	1	0	8

We will concentrate in the following on the special case BP only. For the construction of the designs we use the same methods as in [2], [3], [4], and the reader is referred to these papers. Roughly, we proceed as follows: we start with some parameters or a parameter set, for instance with the scheme of a point tactical decomposition. Then we refine these parameters step by step. After having chosen a suitable step, we switch to the generator, i.e. we use a computer program which generates the designs from the parameters. Finally, we use a program to determine the isomorphism types of the constructed geometries. If

the parameters are too coarse, then the generating process will not work. If the parameters are too fine (the chosen step is too high), then the generator works well but we get too many cases. Somewhere in between is the best starting position, and we have to carry out experiments to find good approaches. We illustrate our method by two examples that we call *Approach 53* and *Approach 80*.

3.1 Approach 53

Since the scheme BP is too coarse for generation, we try to refine it. Note that in the set of lower 12 points there are three disjoint 4-blocks. Each pair of them is joined by 16 blocks. Isolating these blocks we get the left scheme of Figure 1, which in fact shows the transposed decomposition. From this situation we calculate the next parameter step which is a point

	4	4	4	16
4	0	0	0	4
1	4	0	0	0
1	0	4	0	0
1	0	0	4	0
8	0	0	0	4
16	1	1	0	2
16	1	0	1	2
16	0	1	1	2

$\mapsto$

	4	1	1	1	8	16	16	16
16	1	0	0	0	2	2	2	2
4	0	1	0	0	0	4	4	0
4	0	0	1	0	0	4	0	4
4	0	0	0	1	0	0	4	4

Figure 1: Refinement of the Scheme BP

tactical decomposition scheme. It turns out that it is even a decomposition scheme (i.e. it is point tactical and row tactical), see figure right.

Combining two of the 16-subsets of blocks to a 32-subset, we get a tactical decomposition, which is a bit coarser:

	4	1	2	8	16	32
16	1	0	0	2	2	4
4	0	1	0	0	8	0
8	0	0	1	0	4	4

From this situation (our approach 53), we started the generation. Since it was difficult to proceed up to line 16 we took subcases with respect to the 52 ranges (non-isomorphic partial designs) on line 8. But these subcases mix, therefore we had to merge the resulting packages afterwards. We did only some of the ranges, and the numbers of designs found are in Table 2.

range no.	generated	merged
1-8		537
17	626	136
18-20	104	35
21	20	8
merge-all		592

Table 2: Some of the Subcases of Approach 53

3.2 Approach 80

We tried another approach by looking at the 4 disjoint 4-blocks in the 16 point subset. We group them into 2 and 2 and get a partition of these 16 points into two 8-subsets. These 8-subsets are joined by 32 of the 48 4-blocks and we get the block-tactical decomposition of Fig. 2 (left scheme). Refinement of the parameters yields 26 point tactical decomposition schemes. The first of these is shown in the figure (right) From those 26 parameter situations

	8	8	12
2	4	0	0
2	0	4	0
3	0	0	4
8	2	2	0
8	2	0	2
32	1	1	2
8	0	2	2

$\mapsto$

	2	2	3	8	8	32	8
8	1	0	0	2	2	4	0
8	0	1	0	2	0	4	2
2	0	0	1	0	4	0	4
8	0	0	1	0	1	6	1
2	0	0	1	0	0	8	0

Figure 2: Another Refinement of the Scheme BP

(our approch no. 80) we started again the generating process. Here it is easy to proceed up to line 16: all 26 cases have the same 16 first lines and there are 53 ranges at line 16, which can be constructed quickly. But now it is in some cases much more difficult to go from line 16 to the end. Table 3 lists the numbers of designs constructed by this approach. The cases are noted by 80.1., ... ,80.26. A third number refers to the range at line 16, for instance 80.26.1. means the first range at line 16 of case 80.26.

4 Some resolvable designs

We are particularly interested in Steiner Systems on 28 points which admit a resolution (also called a parallelism). This situation may be described by the following

case	# designs
80.1.	442
80.2.-80.5.	0
80.6.	63
80.7.	65
80.8.	40
80.9.	7
80.10.	4
80.11.	0
80.12.	188
80.13.	42
80.14.	357
80.15.	24
80.16.	75
80.17.	3
...	...
80.26.1.	176
merged:	825

Table 3: Some of the Subcases of Approach 80

Story:

> 28 hale and hearty pensioners go for 9 days holiday using cars, 4 persons in each car: it is required to arrange them daily, so that no two sit twice in the same car.

We can view such a resolution as a linear space. Take for each of the 9 parallel classes an extra point which extends the 4-blocks to 5-blocks and define a new line at infinity containing these 9 points. Then one gets a linear space on 37 points having 63 blocks of length 5 and one block of length 9. In terms of tactical decomposition schemes this extension process may be described by the schemes:

	63
28	9

$\mapsto$

	63	1
28	9	0
9	7	1

If we concentrate on the class PB wich has some special parallel class, then it is adequate to look for resolutions which extend this special parallel class. Extending the block tactical decomposition we started with (approach 80), we get the following block tactical decomposition scheme for the corresponding linear space on 37 points:

	8	8	12	8	1
2	4	0	0	0	1
2	0	4	0	0	1
3	0	0	4	0	1
8	2	2	0	1	0
8	2	0	2	1	0
32	1	1	2	1	0
8	0	2	2	1	0
1	0	0	0	8	1

From this situation we calculate the parameters one step further and then start the generator. We get the following

Result:
The Steiner Systems of type BP admit exactly 5 pairwise non-isomorphic resolutions which extend the special parallel class. The distribution of their automorphism group orders is $48^2, 168^1, 432^1, 1512^1$.

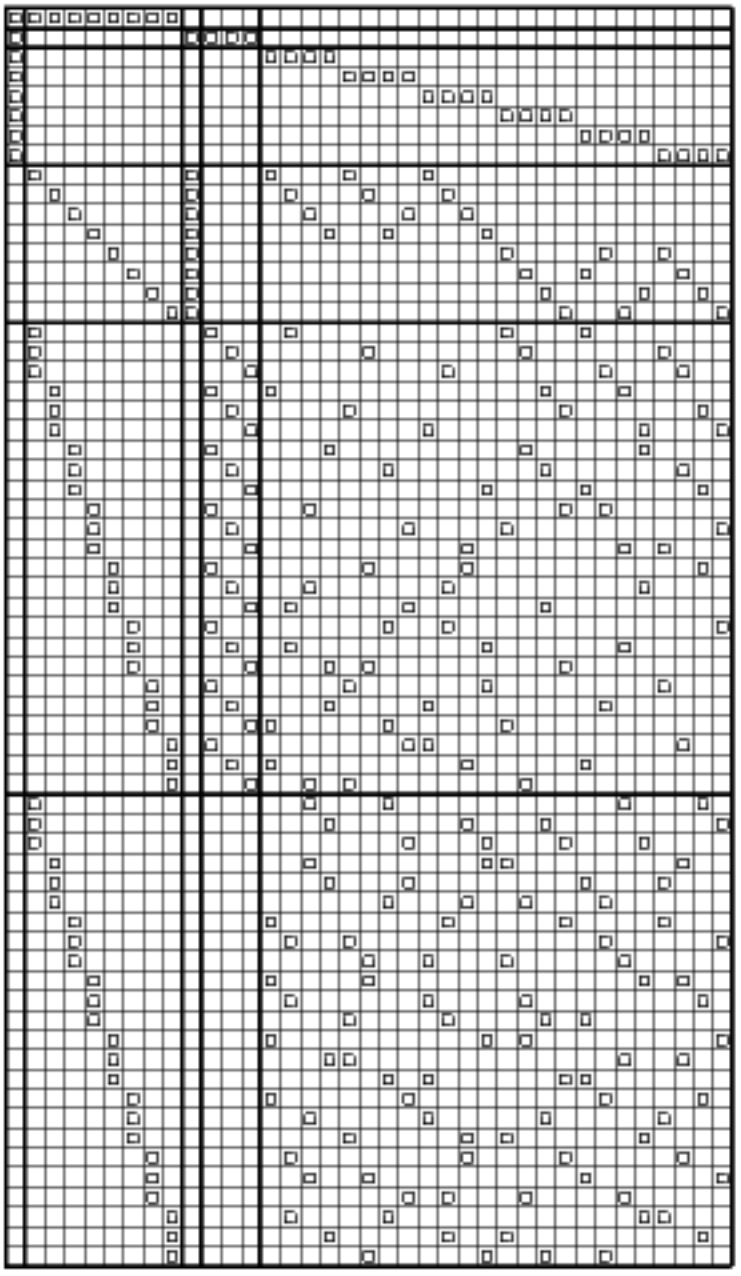
Remark:
The Ree unital, i. e., the unique 2-(28,4,1) design with full automorphism group of order 1512 has exactly 10 resolutions, one of them fixed under the automorphism group, the other 9 being an orbit under the automorphism group. Hence, by distinguishing a resolution one gets an automorphism group of order 1512 or $1512/9 = 168$ respectively. The classical (hermitian) unital 2-(28,4,1) design has automorphism group of order 12096 and 28 resolutions, all equivalent with respect to the automorphism group. Therefore, distinguishing one of the resolutions, one gets a group of order $12096/28 = 432$. Thus, three of the constructed resolutions belong to these two designs. The other two belong to designs with automorphism group order 48. The tactical decomposition defined by the orbits of the automorphism group (TDA) for one of them is displayed in Figure 3. The other one looks quite similar, though not being isomorphic to the first one.

5 Quotient structures

A 2-(28,4,1) design with a parallel class may described by the following tactical decomposition scheme:

	7	56
28	1	8

If we identify each of the seven 4-blocks of the parallel class to a point we get a quotient structure on 7 points with the parameters $v = 7, b = 56, r = 32, k = 4, \lambda = 16$. The complementary design has the parameters $v = 7, b = 56, r = 24, k = 3, \lambda = 8$. This is no. 357 of the list in the handbook [8] with 5413 solutions.



$|Aut| = 48$

Figure 3: A Resolvable 2-(28,4,1) Design

Now let us carry out this process for the parallel class of the special situation BP. Here we get the following TD-scheme:

	8	48
4	8	24
3	0	32

This scheme generates exactly (up to isomorphisms) 30 designs with $\lambda = 16$. This is only a small portion of the 5431 quotient structures in the general case.

6 Some statistics

Table 4 displays some statistics of the designs. We show the distribution of the 2-rank, the order of the automorphism groups, the number of spreads and resolutions.

2-rank	#
19	1
21	4
22	12
23	74
24	238
25	406
26	174

$\lvert Aut \rvert$	#
1	187
2	401
3	6
4	231
6	16
8	29
12	1
16	10
24	9
32	2
48	12
64	1
192	2
1512	1
12096	1

# spreads	#
1	217
2	139
3	319
4	65
5	54
6	17
7	53
8	1
9	11
11	22
15	7
27	1
31	1
45	1
63	1

# resolutions	#
1	2
10	1
28	1

Table 4: Statistics of the Designs

References

[1] L. M. Batten and A. Beutelspacher: The theory of finite linear spaces. Cambridge University Press, Cambridge 1993.

[2] A. Betten and D. Betten: Linear spaces with at most 12 points. *J. of Combinatorial Designs* **7** (1999), 119–145.

[3] A. Betten and D. Betten: The Proper Linear Spaces on 17 Points. *Discrete Applied Mathematics* **95** (1999), 83–108.

[4] A. Betten and D. Betten: Tactical decompositions and some configurations v_4. *J. of Geom.* **66** (1999), 27–41.

[5] A.E. Brouwer, Some unitals on 28 points and their embedding in projective planes of order 9, in: "Geometries and Groups", M. Aigner and D. Jungnickel eds., *Lecture Notes in Mathematics* **893** (1981), pp. 183-188.

[6] D. Jaffe and V.D. Tonchev, Computing linear codes and unitals, *Designs, Codes and Cryptography* **14** (1998), 39-52.

[7] H. Lüneburg, Some remarks concerning the Ree group of type (G_2), *J. Algebra* **3** (1966), 256-259.

[8] R. Mathon, A. Rosa, "2-(v, k, λ) designs of small order", in: "The CRC Handbook of Combinatorial Designs", C.J. Colbourn and J.H. Dinitz eds., CRC Press, New York 1996, pp. 3-41.

[9] G. McGuire, V.D. Tonchev, and H.N. Ward, Characterizing the Hermitian and Ree unitals on 28 points, *Designs, Codes and Cryptography* **13** (1998), 57-61.

[10] T. Penttila, G.F. Royle, Sets of type (m, n) in the affine and projective planes of order 9, *Designs, Codes and Cryptography* **6** (1995), 229-245.

[11] S. Stoichev and V.D. Tonchev, Unital designs in planes of order 16, *Discrete Applied Math.* (to appear)

[12] V.D. Tonchev, "Combinatorial Configurations", Longman, Wiley, New York 1988.