Codes and combinatorial designs

Codes and Combinatorial Designs

J.H. van Lint
Eindhoven University of Technology

IN MEMORY OF MARSHALL HALL, JR.

Abstract

An expository lecture on a few recent results connecting coding theory with the theory of combinatorial designs.

1 Introduction

It is by now well known that there are many connections between coding theory and the theory of combinatorial designs. During the past ten years Marshall Hall was extremely interested in some of these connections. His interest presumably originated with the celebrated result of MacWilliams, Sloane, and Thompson [17] that the code generated by the rows of the incidence matrix of a projective plane of order 10 (if it exists) can have no words of weight 15 (cf.,[6]). Hall contributed to the attack on this projective plane in a paper on configurations in a plane of order 10 [8]. As we all know, these methods and an extensive computer search led to the "proof" of the nonexistence of the plane of order 10; for an account of this proof see [12].

Hall and several coauthors used similar methods for the plane of order 12 [10],in an attempt to show that a 2-(22,8,4) design does not exist [4], [9], and by such methods discovered a new block design, namely a 2-(41,16,6) design [4]. The methods, based on one of the most important results in coding theory: MacWilliams' Theorem (cf.,[13, 17]), are by now well known and occur in text books (e.g.,[7]). The equally important Assmus-Mattson Theorem (cf.,[6, 16]), which depends on MacWilliams' Theorem, led to several new 5-designs constructed from codes. At the time of their discovery these designs were quite sensational. Again, this is by now fairly well known. For an excellent survey of some of the "older" links between coding theory and combinatorics we refer to [1].

In this expository lecture we wish to concentrate on a few less well known links between these theories, including some recent results. Also we shall illustrate a few personal favorites from this still growing area of research. We shall assume that the reader is familiar with the standard definitions and theorems from coding theory and from the theory of combinatorial designs. Standard references are [6, 7, 13, 16].

2 The uniqueness of $S(5,8,24)$

First some well known facts. The famous [23, 12, 7] binary Golay code, a perfect code, is unique and so is its extension $\mathcal{G}_{24}$, a [24, 12, 8] code. The equally famous Steiner system $S(5,8,24)$ is also unique and it can be obtained from $\mathcal{G}_{24}$ as the set of words of weight 8. Not well known is the following uniqueness proof, starting with the extended Golay code.

Theorem 2.1 *Let C be a binary code of length 24 with minimum distance 8, and suppose that $\mathbf{0} \in C$ and $|C| = 2^{12}$. Then C is $\mathcal{G}_{24}$ (i.e. the extended Golay code is unique).*

Proof.

(i) Puncturing on any position leads to a $(23, 2^{12}, 7)$ code. Since such a code is perfect, its weight enumerator is determined. In fact $A_0 = A_{23} = 1$, $A_7 = A_{16} = 253$, $A_8 = A_{15} = 506$, $A_{11} = A_{12} = 1288$. This immediately implies that the code C only has words of weight 0,8,12,16, and 24. However, the same is true for the code $C + \mathbf{c}$ for any $\mathbf{c} \in C$. Therefore not only all the weights in C are divisible by 4 but also all the distances between codewords are divisible by 4. This implies that $\langle \mathbf{c}, \mathbf{c}' \rangle = 0$ for any two codewords $\mathbf{c}$, $\mathbf{c}'$ in C. So, the words of C span a (doubly even) self-orthogonal code. Such a code has dimension at most 12 and thus we see that the code C was already linear!

(ii) Take any codeword $\mathbf{c}$ of weight 12 as a basis vector for C. The residual code must have dimension 11 and it has only even weights. So, the residual code is the [12, 11, 2] even-weight code. Therefore C has a generator matrix G of the form

$$G = (I_{12}\ P), \quad \text{where} \quad P = \begin{pmatrix} 0 & 1 \\ \mathbf{1}^{\mathsf{T}} & A \end{pmatrix}, \tag{1}$$

(so A is of size 11 by 11).

(iii) Since C has minimum distance 8, every row of A has at least six 1's. From the top row of G we see that every row of A therefore must have exactly six 1's. Clearly, any two rows of A have at most three 1's in common. Again using the top row, we see that any two rows of A have exactly three 1's in common. This forces A to be the incidence matrix of a 2-(11,6,3) design. The uniqueness of that design is well known (easily proved by hand). □

From the words of weight 8 of $\mathcal{G}_{24}$ one finds a Steiner system $S(5,8,24)$. We show that only one such design exists.

Theorem 2.2 *The Steiner system $S(5,8,24)$ is unique.*

Proof.

(i) Let S be such a system. The intersection numbers of such a design show that the code C spanned by the blocks of S is self-orthogonal and doubly even (if two distinct blocks of S meet, then in two or four points). To see that C has minimum distance 8, observe that $C^{\perp}$ must have minimum distance at least 6. This follows from the fact that the blocks of S assume all possible 0-1 configurations on a given 5-set of points.

(ii) Fix three points. The derived design with respect to these points is a 2-(21,5,1) design, i.e. the plane $PG(2,4)$. Again, it is well known that the rows of the incidence matrix of $PG(2,4)$ span a code of dimension 10 (cf.,[6]). This implies that C has dimension 12 and by Theorem 1 we are done. □

For more details and several more facts about the related designs, we refer to [5, 22].

We remark that Tonchev [23] has shown that if we replace I_{12} by I_{36} in (1) and replace A by the incidence matrix of a 2-(35,18,9) Hadamard design, the resulting code is again doubly even with minimum weight at least 8 and self-orthogonal. If however the minimum weight were 16, then we would have found a solution to a famous open problem, namely the existence of a [72,36,16] extremal selfdual code. In a recent preprint it was shown that such a code does not exist but the latest news is that there is an error in a calculation in the preprint. It appears that the problem is still open. We do not know if the construction of the extremal code using a Hadamard design has been tried in a systematic way.

3 Designs from quadratic residue codes

Several authors have generalized the quadratic residue codes. A simple description was given in [14]. There the codes have length $q = p^m$ $(m > 1)$ and the alphabet is $\mathsf{F} = GF(l)$, where for odd m it is required that l is a quadratic residue of p. Codewords are described as elements $\sum c_g g$ of $\mathsf{F}G$, where G is the additive group of $GF(q)$. As usual, the sets U, respectively V, of squares, respectively nonsquares, in $GF(q)$ play a special rôle. First, a special character ψ_1 from G into the set of p-th roots of unity over F is defined and then, for $h \in G$, we define $\psi_h(g) := \psi_1(gh)$. The character is extended in the obvious way to $\mathsf{F}G$. Generalized quadratic residue codes (GQR codes) are defined as follows.

Definition 1 *The code A^+ consists of all $\mathbf{c} = \sum c_g g$ for which $\psi_u(\mathbf{c}) = 0$, for all $u \in U$. The code B^+ is defined in the same way, replacing U by V.*

It is clear that these codes have dimension $\frac{1}{2}(q+1)$. These codes are extended to codes of length $q+1$ by adding a "parity check" symbol in a new coordinate position labeled ∞. This is done in such a way that the extended

codes are invariant under a group of monomial transformations, of which the permutation part is $PSL(2,q)$.

This work (done in 1978) led to a sequence of 3-designs but only for the special case $q = p^2$.

Theorem 3.1 *Let A_∞, B_∞ be the extended GQR codes of length p^2+1. Each of these codes contains $\frac{1}{2}p(p^2+1)(l-1)$ codewords of minimum weight $p+1$. The supports of these codewords form a 3-$(p^2+1, p+1, 1)$ design.*

In order to prove this theorem for the case p^{2t} $(t > 1)$, we needed a proof of the following conjecture.

Conjecture 1 *If A is a subset of $GF(q^2)$ with $|A| = q$, $0 \in A$, $1 \in A$, and such that for all $x \in A$ and all $y \in A$, the difference $x - y$ is a square in $GF(q^2)$, then $A = GF(q)$.*

We, and subsequently several others, tried in vain to prove this conjecture. In 1984 A. Blokhuis [2] found an ingenious and elegant proof. The result and the proof deserve to be better known than they seem to be. We formulate the result in geometric terms.

Theorem 3.2 *Consider the affine plane $AG(2,q)$ as (the additive structure of) $GF(q^2)$. Let A be a subset of the plane with $|A| = q$, $0 \in A$, and such that the difference $x - y$ of any two elements x, y of A is a square in $GF(q^2)$. Then A is a line through the origin.*

The result implies that Theorem 3.1 is true if we replace p by p^t, i.e. consider GQR codes of length $p^{2t}+1$.

A possibly interesting case of designs derived from words of minimum weight in a GQR code is length 7^3 because $7^3 = 18^2 + 18 + 1$ and an optimist would be tempted to try to find a plane of order 18 in this way. In fact it was suggested that it might be possible to find an abelian group difference set that would yield the plane. The following theorem of Jungnickel and Vedder [11] and Wilbrink [24] rules that out.

Theorem 3.3 *If a projective plane of order $n \equiv 2 \pmod 4$ has an abelian regular automorphism group, then it is the plane of order 2.*

By now, the theorem has at least four different proofs. Pless [19] pointed out that for the cyclic case, the theorem can be proved using methods from coding theory.

4 Nonembeddable quasi-residual designs

In [15] a sequence of nonembeddable quasi-residual designs was constructed. We illustrate the method by an example.

Let A be the 10 by 30 incidence matrix of a 2-(10,3,2) design. Denote by E_i a 10 by 11 matrix with 1's in row i and 0's elsewhere. The permutation matrix corresponding to the permutation $(1, 2, \ldots, 11)$ is denoted by C. Define B by

$$B := \begin{pmatrix} A & E_1 & E_2 & \cdots & E_{10} \\ O & I+C & I+C^2 & \cdots & I+C^{10} \end{pmatrix}. \tag{2}$$

The complement $\overline{B}$ is the 21 by 140 incidence matrix of a quasi-residual design corresponding to a symmetric 2-(141,120,102) design. Suppose that $\overline{B}$ is embeddable in a design

$$\begin{pmatrix} \mathbf{0} & \overline{B} \\ \mathbf{j} & D \end{pmatrix}$$

Let $\mathcal{C}$ be the binary code generated by the rows of $\overline{B}$. Since $\lambda = 102$ is even, every row of D is a codeword in $\mathcal{C}^\perp$. From (2) we see that the sum of the first 10 rows of $\overline{B}$ is $\mathbf{1}$. Hence every word in $\mathcal{C}^\perp$ has even weight. However, every row of D has weight 119, a contradiction.

This is a rather simple application of ideas from coding theory. Nevertheless, there are many situations where clever use of a code, its dual, and the all-one vector has led to nice results.

5 Memories with restrictions

A fairly new area of research is the construction of "codes" for memories for which there are certain restrictions on updates. We shall discuss two such problems and for each of them show an interesting connection to design theory.

A *Write-Once-Memory* (WOM) of length n consists of n so-called *wits* (write once bit positions). Each of these is initially 0. At each writing wits that are 0 can be updated to 1 but the process is irreversible. An example is paper tape for a computer into which holes are punched or a compact disc on which pits are created by a laser. Conventional write-once-memories are used only once. The idea of reusing such memories was introduced by Rivest and Shamir [20].

Let there be M "messages" $m_1, \ldots, m_M$ that can be stored in the WOM. Suppose that we wish to use the WOM on t successive occasions. An update consists of changing certain 0's to 1's. In order to describe this, we define for $\mathbf{x} \in \mathbb{F}_2^n$, $\mathbf{y} \in \mathbb{F}_2^n$

$$\mathbf{x} \leq \mathbf{y} \quad \text{if} \quad \{i : x_i = 1\} \subseteq \{i : y_1 = 1\}. \tag{3}$$

Sometimes it is convenient to interpret elements of $\mathbb{F}_2^n$ as characteristic functions of subsets of $N := \{1, 2, \ldots, n\}$. Then (3) states that $\mathbf{x}$ is a subset of $\mathbf{y}$.

As a first rule we state that if message m_i is stored in the WOM and at the next usage one wishes to store the same message, then one simply does

not change the WOM. What we need is to associate with each message m_i a list L_i^ν $(1 \leq \nu \leq t)$, where $L_i^\nu \subseteq L_i^{\nu+1}$ $(1 \leq \nu < t)$ and any two lists with different lower indices are disjoint. If the memory contains an element from a list with lower index i then we interpret this as message m_i. The requirement that we should always be able to update implies that if $\mathbf{x} \in L_i^\nu$ and $\nu < t$, then for any j $(1 \leq j \leq M)$ there is a $\mathbf{y} \in L_j^{\nu+1}$ such that $\mathbf{x} \leq \mathbf{y}$. Note that we do not require to be able to determine "time" from the memory (because of our first rule).

Rivest and Shamir called such a set of lists a $\langle M \rangle^t/n$ WOM code and used the notation $w(\langle M \rangle^t)$ for the least n for which such a WOM code exists. They derived lower bounds for $w(\langle M \rangle^t)$. In particular they showed that $w(\langle 7 \rangle^4) \geq 7$ and $w(\langle 8 \rangle^4) \geq 8$. Note that in conventional (not reusable) write-once-memories we would require twelve bits to store one of seven messages on four successive occasions (only the number of the message is stored of course). So a WOM code of length 7 would mean a saving of nearly 50%. The following example, due to one of my former students F. Merkx [18], has turned out to be a particularly good "motivating" example in a discrete mathematics course for computer science students.

Example 1 *A $\langle 7 \rangle^4/7$ WOM code.*

We number the seven wits with the points $P_1, P_2, \ldots, P_7$ of the Fano plane. We proceed as follows. Since the memory is not changed for successive storages of the same message, we only have to show what to do if a different message is to be stored. We list the configurations that the reading device can encounter, with their interpretation. The reader should convince himself that all updates are possible.

Generation 1: a point P_i represents m_i;
Generation 2: two points P_i, P_j represent m_k if $\{P_i, P_j, P_k\}$ is a line of the plane.
Generation 3: a line $\{P_i, P_j, P_k\}$ and a fourth point P_l represents m_l.
Generation 4: two lines that intersect at P_i represent m_i and this message is also represented by the complement of the set $\{P_i\}$.

Note that there are 7^4 possible sequences of messages that can be stored although only $2^7 - 2$ states of the memory occur. This is possible because the "memory" actually does not remember the previous state. In the same paper [18], several other nice applications of finite geometries to WOM codes are given.

Our next example concerns so-called WUM codes. Now we are interested in a write-unidirectional-memory. The motivation for these memories came from the updating of magneto-optical discs. In the early versions, the updating depended on a magnetic field for which reorientation was a slow process. This implied that for an update one could either only change 0's to 1's or only 1's to 0's. For an introduction see [3, 25].

Suppose that we have a memory of n bits and that we wish to store one of M possible messages at each usage. Again we interpret codewords as subsets of N. For each message m_i we must have a subset S_i of $\mathbb{F}_2^n$ such that

(i) $S_i \cap S_j = \emptyset$ i i $\neq j$,

(ii) for all $i \neq j$ and all $\mathbf{x} \in S_i$ there is a $\mathbf{y} \in S_j$ with $\mathbf{x} \leq \mathbf{y}$ or $\mathbf{y} \leq \mathbf{x}$.

The rate R of a WUM code is defined as $R := n^{-1} \log_2 M$. Borden [3] showed that $R < \frac{1}{2}\log_2(1+\sqrt{5})$ if $n \geq 5$. He also showed that $R = \frac{1}{2}$ is trivially achievable if $n = 2k$. Simply define

$$S_i := \{(\mathbf{1}, \mathbf{x}_i); (\mathbf{x}_i + \mathbf{1}, \mathbf{0})\}$$

for each $\mathbf{x}_i \in \mathbb{F}_2^k$.

Although it is no longer a record holder for R we mention the following interesting example due to Simonyi [21].

Example 2 *A WUM code with* $R = 0.525...$

Let $k|n$. Then it is well known (Baranyai's Theorem) that the design of all k-subsets of an n-set is resolvable. Now we take $n = k(k+1)$, $M = \binom{n-1}{k-1}$ and with each message m_i we associate the $k+1$ blocks of a parallel class and their complements (each of course interpreted as its characteristic function). To show that updating is possible we can, by symmetry, assume that a block B in class i is stored in the memory and that we wish to update to a message corresponding to class j ($j \neq i$). Since $|B| = k$, there is a block B' in class j that does not meet B, i.e. B is a subset of the complement of B'. This shows that the update is possible by a 0 to 1 writing. In fact the argument still goes through if we pick one of the points of the n-set and remove it from all the subsets (so the memory now has length $n-1$). For $k = 3$ we find $M = \binom{11}{2} = 55$ messages storable in a memory of length 11, corresponding to a rate 0.525...

At present better codes exist. These were constructed with methods that are not of a combinatorial nature. Our goal was to interest the reader in these subjects and to show how designs and codes often influence each other.

References

[1] E.F. Assmus, Jr. and H.F. Mattson, Jr., Coding and combinatorics, *SIAM Review* **16** (1974) 349–388.

[2] A. Blokhuis, On subsets of $GF(q^2)$ with square differences, *Proc. Kon. Ned. Akad. v. Wetensch.* (A) **87** (1984) 369–372.

[3] J.M. Borden, Coding for write-unidirectional memories, *IEEE Trans. Inform. Theory*, submitted.

[4] W.M. Bridges, M. Hall, Jr. and J.L. Hayden, Codes and Designs, *J. Comb. Theory* (A) **31** (1981) 155–174.

[5] A.E. Brouwer, The Witt designs, Golay codes and Mathieu groups, to appear in *Handbook of Combinatorics* (in preparation).

[6] P.J. Cameron and J.H. van Lint, *Graphs, codes and designs*, London Math. Soc. Lecture Note Series **43**, Cambridge University Press, London, 1980.

[7] M. Hall, Jr., *Combinatorial Theory*, Wiley Interscience, New York, 1986.

[8] M. Hall, Jr., Configurations in a plane of order ten, *Annals of Discrete Math.*, **6** (1980) 157–174.

[9] M. Hall, Jr., R. Roth, G.H.J. van Rees and S.A. Vanstone, On Designs (22,33,12,8,4), *J. Comb. Theory* (A) **47** (1988) 157–175.

[10] M. Hall, Jr. and J. Wilkinson, Termary and Binary Codes for a Plane of Order 12, *J. Comb. Theory* (A) **36** (1984) 183–203.

[11] D. Jungnickel and K. Vedder, On the geometry of planar difference sets, *Eur. J. Comb.* **5** (1984) 143–148.

[12] C.W.H. Lam, The search for a finite projective plane of order 10, *Amer. Math. Monthly* **98** (1991) 305–318.

[13] J.H. van Lint, *Introduction to Coding Theory*, Graduate Texts in Mathematics **86**, Springer Verlag, New York, 1982.

[14] J.H. van Lint and F.J. MacWilliams, Generalized Quadratic Residue Codes, *IEEE Trans. Inform. Theory* **IT-24** (1978) 730–737.

[15] J.H. van Lint and V.D. Tonchev, Nonembeddable Quasi-residual Designs with Large K, *J. Comb. Theory* (A) **37** (1984) 359–362.

[16] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

[17] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, On the Existence of a Projective Plane of Order 10, *J. Comb. Theory* (A) **14** (1973) 66–78.

[18] F. Merkx, Womcodes constructed with projective geometries, *Traitement du Signal* **1** (1984) 227–231.

[19] V. Pless, Cyclic Projective Planes and Binary Extended Cyclic Self-Dual Codes, *J. Comb. Theory* (A) **43** (1986) 331–333.

[20] R.L. Rivest and A. Shamir, How to reuse a Write-Once-Memory, *Information and Control* **55** (1982) 1–19.

[21] G. Simonyi, On Write-Unidirectional Memories, *IEEE Trans. Inform. Theory* **IT-35** (1989) 663–669.

[22] V.D. Tonchev, A Characterization of Designs Related to Dodecads in the Witt System $S(5,8,24)$, *J. Comb. Theory* (A) **43** (1986) 219–227.

[23] V.D. Tonchev, Self-Orthogonal Designs and Extremal Doubly Even Codes, *J. Comb. Theory* (A) **52** (1989) 197–205.

[24] H.A. Wilbrink, A Note on Planar Difference Sets, *J. Comb. Theory* (A) **38** (1985) 94–95.

[25] F.M.J. Willems and A.J. Vinck, Repeated recording for an optical disk, in *Proc. 7th Symp. Inform. Theory in the Benelux* (1986) 49–53.