Nordstrom-Robinson code and A_7-geometry

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

April 14, 2004

Abstract

The Nordstrom-Robinson code $\mathcal{NR}$ is a non-linear binary code of length 16, with 2^8 codewords and minimum distance 6. Its automorphism group is a semidirect product of an elementary abelian group of order 16 and the alternating group A_7. This group and the corresponding action of A_7 is also at the origin of the sporadic A_7-geometry. We construct this geometry and derive the Nordstrom-Robinson code from it.

1 Introduction

The Nordstrom-Robinson code was constructed in 1967 by A. W. Nordstrom and J. P. Robinson (see [9], reprinted in [1]). Its high degree of regularity and symmetry was observed early on. The original construction made use of a symmetry of order 7. $\mathcal{NR}$ is the uniquely determined $(16, 2^8, 6)_2$-code (binary, length 16, minimum distance $6, 2^8$ codewords) and it is optimal in the sense that no $(16, M, 6)_2$-code can have $M > 256$.

J. M. Goethals [7] gave a construction of $\mathcal{NR}$ based on the binary Golay code. The binary Golay code $\mathcal{G}$ is a self-dual $[24, 12, 8]_2$-code with 759 words of weight 8 (octads). Arrange notation such that the first 8 coordinates form an octad. Let π be the projection of $\mathcal{G}$ to the first 8 coordinates and $\mathcal{D}$ the kernel of π. The kernel of π still has minimum distance ≥ 8. By the Griesmer bound its dimension is ≤ 5. It follows that $\pi(\mathcal{G})$ has dimension $\geq 12 - 5 = 7$.

Because of self-duality we have equality: $\pi(\mathcal{G})$ is the all-even code $[8,7,2]_2$ and the projection of $\mathcal{D}$ to the last 16 coordinates is a $[16,5,8]_2$-code, a Reed-Muller code $\mathcal{R}$. Goethals defines the code $\mathcal{NR}$ as the union of 8 cosets of $\mathcal{R}$. More precisely a vector $x \in \mathbb{F}_2^{16}$ is in $\mathcal{NR}$ if and only if it is the projection onto the last 16 parameters of a codeword of $\mathcal{G}$ whose projection onto the first 8 parameters is either the 0-word or a word of weight 2 with a 1 in the first coordinate. It follows that $\mathcal{NR}$ has $2^5 \times 8 = 2^8$ codewords. As $\mathcal{G}$ has minimum distance 8 and only even weights it follows that $\mathcal{NR}$ has minimum distance 6 and that all distances are even.

The automorphism group of the binary Golay code $\mathcal{G}$ is the simple Mathieu group M_{24} of order

$$|M_{24}| = 24 \times 23 \times 22 \times 21 \times 20 \times 48$$

in its 5-transitive action on the 24 coordinates. As M_{24} is transitive on octads, the stabilizer of an octad has order $|M_{24}|/759$. The stabilizer of $\mathcal{NR}$ has index 8 in this group. It follows that $\mathcal{NR}$ admits an automorphism group of order $|M_{24}|/(759 \times 8) = 16 \times 7!$ This is a huge symmetry group. Its structure can be inferred from the embedding in $\mathcal{G}$ as well. The automorphism group of $\mathcal{NR}$ is a semidirect product of an elementary abelian group of order 16 and the alternating group A_7.

There are different approaches to the Nordstrom-Robinson code. The most recent one is based on Z_4-linear codes. Here $Z_4 = \mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$ is the ring of the integers mod 4. Consider the generator matrix

$$G = (I|P) = \left(\begin{array}{c|c} 1000 & 2111 \\ 0100 & 1213 \\ 0010 & 1321 \\ 0001 & 1132 \end{array}\right).$$

The quaternary Z_4-linear code $\mathcal{N}$ generated by G is known as the **octacode.** Observe that the factor ring $Z_4/(2)$ is the field $\mathbb{F}_2$. If we read the entries of G mod $(2) = \{0,2\}$ a generator matrix of a binary linear code is obtained. This binary code is the extended Hamming code $[8,4,4]_2$. The octacode can therefore be seen as a lifting of the Hamming code. Its codewords $x(a,b,c,d)$ are

$$(a,b,c,d|2a+b+c+d, a+2b-c+d, a+b+2c-d, a-b+c+2d),$$

where a, b, c, d vary in Z_4. We have $\mathcal{N} = \mathcal{N}^\perp$ with respect to the dot product. The binary code $\mathcal{NR}$ is defined as the image of the octacode under the Gray map $\gamma : Z_4 \longrightarrow \mathbb{F}_2 \times \mathbb{F}_2$, which maps $0 \in Z_4$ to the 0-pair, the units of Z_4 to pairs of weight 1 and the zero divisor 2 to the pair 11 of weight 2. The only nonlinear element in this construction is the Gray map. As the nonzero codewords of the extended Hamming code have weights 4 and 8 it follows that all nonzero words of $\mathcal{NR}$ have even weight ≥ 4. It is not hard to see that weight 4 does not occur. A drawback of this construction is that it does not reveal the entire symmetry group of the Nordstrom-Robinson code. In fact the symmetry group of the octacode is a semidirect product of an elementary abelian group of order 16 and the simple group $GL(3, 2)$ of order 168. This constitutes a large automorphism group (of order 2688), but the automorphism group of $\mathcal{NR}$ is larger yet as we saw earlier (order $40, 320$). An advantage of the Z_4-linear approach is that it gives an explanation for some additional features of $\mathcal{NR}$, in particular that its dual distance distribution equals its distance distribution. This implies that $\mathcal{NR}$ behaves like a self-dual linear code in this respect. Most importantly it is an orthogonal array of strength 5. The Z_4-linear approach is described in [8]. A recent book on the subject is [10]. Another advantage of this description is that it generalizes to large families of codes, in particular to the Preparata codes and the Kerdock codes, two infinite families of non-linear codes which have $\mathcal{NR}$ as a member and behave like duals of one another in the sense that $\mathcal{NR}$ behaves like a self-dual linear code.

Yet another approach to $\mathcal{NR}$ and its generalizations uses finite geometries. It is based on quadratic forms and spreads. For a description see [3].

We present a construction of the Nordstrom-Robinson code based on the sporadic A_7-geometry. The virtue of this construction is that it explains the full automorphism group of $\mathcal{NR}$. In the next section we start from a self-contained introduction to this geometry.

2 The A_7-geometry

The **Fano plane** is the projective plane $PG(2, 2)$ of order 2. Let Ω be a 7-element set, $\Omega = \{x, 1, 2, 3, 4, 5, 6\}$. How many different Fano planes exist on Ω? As all Fano planes are isomorphic, they form one orbit under the action of the symmetric group S_7. The stabilizer of a Fano plane E in S_7 is by definition the automorphism group of E. This is the linear group $GL(3, 2)$, the simple group of order 168. It follows that the number of different Fano planes is $7!/168 = 30$. It is easy to confirm this result by a purely combinatorial argument. Now restrict to the alternating group A_7. As $GL(3,2)$ is a simple group, it is contained in A_7 (the commutator group of $GL(3,2)$ is contained in the commutator group of S_7, which is A_7, and the commutator group of the simple group $GL(3,2)$ is $GL(3,2)$ itself).

As $GL(3,2)$ has index 15 in A_7, the group A_7 has two orbits $\mathcal{E}_1$ and $\mathcal{E}_2$ of Fano planes, each of length 15.

Lemma 1. *There are* 30 *different Fano planes on a given* 7*-element set. They form one orbit under* S_7*, two orbits of length* 15 *each under* A_7*.*

Upon counting incident pairs of triples (3-subsets of Ω) and Fano planes, we see that every triple is a line of exactly 6 Fano planes, 3 from each A_7-orbit. Let $E \in \mathcal{E}_1$ be a Fano plane and $H \cong GL(3,2)$ its stabilizer. How does H act on the remaining 14 elements (Fano planes) of $\mathcal{E}_1$? The element of order 7 shows that H either is transitive or has two orbits of length 7. As $\binom{15}{2} = 105$ is odd, A_7 certainly is transitive on the unordered pairs from $\mathcal{E}_1$ (A_7 is 2-**homogeneous**). By counting triples (E, E', T), where E and E' are different Fano planes from $\mathcal{E}_1$ and T a triple, which is a line in both, we see that different Fano planes from the same A_7-orbit have exactly one line in common. This shows in particular that no more than two linewise disjoint Fano planes can be found.

Consider the action of H on $\mathcal{E}_2$. An element of order 7 has orbits of lengths $1, 7, 7$. Assume H stabilizes a (unique) Fano plane $E' \in \mathcal{E}_2$. This yields an orbit of length 7 under the action A_7 of pairs (E_1, E_2) such that $E_i \in \mathcal{E}_i$ and E_1, E_2 have the same stabilizer. Let E_1 and E_2 have x lines in common. and y the number of pairs (E_1, E_2) from the orbit having a given line in common. The usual counting argument shows $7 \times x = 35y$, hence $x = 5$. This is a contradiction as no two Fano planes have as many as 5 lines in common. We conclude that the stabilizer H of $E \in \mathcal{E}_1$ has two orbits of lengths 7 and 8, respectively, on $\mathcal{E}_2$. It follows that we have two orbits of pairs (E_1, E_2), where $E_i \in \mathcal{E}_i$ under the action of A_7, one of length $15 \times 7 = 105$, the other of length $15 \times 8 = 120$. Let pairs in the shorter orbit have x lines in common and y the number of lines which pairs in the longer orbit have in common. Count triples (E_1, E_2, T), where T is a common line. This yields $105x + 120y = 35 \times 9$. It follows that 7 divides y, consequently $y = 0$ and $x = 3$.

Theorem 1. *Let $\mathcal{E}_1$, $\mathcal{E}_2$ be the orbits of Fano planes under the action of A_7. Then A_7 is doubly transitive on $\mathcal{E}_1$ and on $\mathcal{E}_2$. There are two orbits of pairs (E_1, E_2) where $E_i \in \mathcal{E}_i$, of lengths 105 and 120. The number of common lines is 3 for the shorter, it is 0 for the longer orbit.*

Proof. It remains to prove the 2-transitivity of A_7 on $\mathcal{E}_1$. Choose

$$E = \{x12, x34, x56, 135, 146, 236, 245\}$$

$$E' = \{x12, x35, x46, 136, 145, 234, 256\}$$

$$E'' = \{x12, x36, x45, 235, 246, 134, 156\}$$

Then E, E', E'' are Fano planes. They belong to the same A_7-orbit as they pairwise have exactly one line 012 in common. The permutation $\sigma = (1,2)(3,4) \in A_7$ fixes E and maps $E' \leftrightarrow E''$. $\square$

It follows from Theorem 1 that the maximum number of linewise disjoint Fano planes which can be constructed on a given 7-set is 2. This result is attributed to Cayley [4].

Next we show how the action of A_7 on the orbit $\mathcal{E}_1$ (analogously on $\mathcal{E}_2$) can be used to obtain an embedding of A_7 in $GL(4, 2)$.

Definition 1. *Let $V = \{0\} \cup \mathcal{E}_1$. Define an addition on V with 0 as neutral element such that $v + v = 0$ for all $v \in V$ and the sum of any two different Fano planes from $\mathcal{E}_1$ is the third plane containing the line which the first two have in common.*

Observe that the Definition 1 makes sense as we know that two Fano planes from the same A_7-orbit have precisely one common line and there is exactly one further such Fano plane containing that line. As an example, the Fano planes E, E', E'' from the proof of Theorem 1 sum to 0.

Lemma 2. *A_7 is regular on the triples (E, F, G) of Fano planes from $\mathcal{E}_1$ where E, F, G are different and $G \neq E + F$. For each such triple the lines of pairwise intersection form a triangle. There is a uniquely determined point of Ω which is outside this triangle.*

Proof. The number of these triples is $15 \times 14 \times 12 = |A_7|$. It suffices to show that no nontrivial element of A_7 fixes such a triple. The stabilizer of E and F has order 12 and clearly is isomorphic to A_4. Let $1 \neq \sigma$ in the stabilizer of

E, F and G. Consider the three triples, which are the lines that two of our Fano planes have in common. As any two of them belong to a common Fano plane, they pairwise intersect in one point. Assume they form a triangle. Then σ is the identity, contradiction. On the other hand these triples cannot form a concurrent bundle as in this case E, F, G would have three lines in common. $\square$

Proposition 1. *V is an elementary abelian group of order* 16.

Proof. Addition is certainly commutative, and each element has order 2, by definition. Only associativity needs to be shown:

$$(E+F)+G = E+(F+G).$$

It can be assumed that E, F, G are different and nonzero, $G \neq E+F$. By Lemma 2 it suffices to check associativity for one special triple E, F, G of Fano planes. We are without restriction in the following situation:

$$E = \{x12, x34, x56, 135, 146, 236, 245\},\ F = \{x12, x35, x46, 136, 145, 234, 256\},$$

$$G = \{x34, x15, x26, 136, 124, 235, 456\}.$$

The triangle of pairwise intersection is $\{x12, x34, 136\}$ and 5 is the unique element of Ω not on this triangle. The Fano plane
$E+F = \{x12, x36, x45, 235, 246, 134, 156\}$ shares 136 with G. It follows

$$(E+F)+G = \{235, 2x4, 216, x56, x13, 346, 145\}.$$

On the other hand F and G share 136,
$F+G = \{136, 1x4, 125, x23, x56, 246, 345\}$ and finally

$$E+(F+G) = \{x56, x13, x24, 145, 126, 235, 346\}$$

which happens to coincide with $(E+F)+G$. $\square$

As the addition of V is respected by the action of A_7 we conclude that we have an embedding of A_7 in the linear group $GL(4,2)$, the group of automorphisms of an elementary abelian group of order 16, equivalently of a 4-dimensional vector space over $\mathbb{F}_2$.

Theorem 2. *A_7 possesses a* 2*-transitive permutation representation on the* 15 *nonzero vectors of a* 4*-dimensional vector space over $\mathbb{F}_2$. The stabilizer of a vector is $\cong GL(3,2)$. Moreover A_7 is regular (sharply transitive) on ordered triples (a, b, c) of linearly independent vectors.*

It follows from Theorem 2 that A_7 is a subgroup of $GL(4,2)$. The simple group $GL(4,2)$ acts on the 8 cosets of A_7. This yields an embedding of $GL(4,2)$ in S_8. As $GL(4,2)$ is simple it is embedded in A_8. These groups have the same order. It follows that these simple groups are isomorphic.

Theorem 3. *The simple groups $GL(4,2)$ and A_8 are isomorphic.*

How do we compute with the embedding of A_7 in $GL(4,2)$? It is combinatorially obvious that each bundle of 3 concurrent lines is contained in precisely 2 Fano planes, one from each A_7-orbit. Let E,F be Fano planes from the same orbit and $x12$ their common line. Assume E contains the bundle $\{x12,x34,x56\}$ and F contains $\{x12,x35,x46\}$. Then $E+F$ contains $\{x12,x36,x45\}$ and $E+F$ is the uniquely determined Fano plane from the same orbit that contains this bundle.

Let x be an element which is not on the line that E and F have in common. The bundle of lines of E through x defines a 1-factor of $\Omega\setminus\{0\}$, likewise for F. These two 1-factors together form a cycle of length 6 on $\Omega\setminus\{x\}$. The 1-factor determined by $E+F$ consists of the diagonals of this cycle. We have seen the following:

Proposition 2. *Let E,F be two Fano planes in the same A_7-orbit, defined on the ground set Ω. Let l be the line that E and F have in common and $a\in\Omega$.*

If $a\in l$ and $\{a,b,c\}$, $\{a,d,e\}$ are the lines $\neq l$ of E containing a, and $\{a,b,d\}$, $\{a,c,e\}$ the corresponding lines of F, then $E+F$ contains the lines $l,\{a,b,e\}$ and $\{a,c,d\}$.

If $a\notin l$, then the pairs collinear with a on a line of $E+F$ are the diagonals of the 6-cycle which the bundles of lines through a in E and in F define on $\Omega\setminus\{a\}$.

As an example consider the Fano planes E,F from the proof of Proposition 1. The first rule when applied to the element x shows $\{x12,x36,x45\}\subset E+F$. Apply the second rule to the element 6. The 1-factors on $\Omega\setminus\{6\}$ are $\{x5,14,23\}$ and $\{x4,13,25\}$. Together they define the cycle $(x,5,2,3,1,4)$ whose diagonals are $x3,15,24$. This shows that $E+F$ contains $\{x36,156,246\}$. Proposition 2 also suggests how the pairs and the 1-factors on a 6-set can be given an algebraic structure. Let $X=\{1,2,3,4,5,6\}$. Let W consist of 0 and of the unordered pairs from X. Here we write ij for $\{i,j\}$. Define an addition on W by $0+w=w,\ w+w=0$ and

$$12+13=23,\ 12+34=56$$

(the sum of two intersecting pairs is the third pair contained in the union, the sum of two disjoint pairs is the pair which is disjoint from the union). Then W is an elementary abelian group of order 16. This defines an embedding of S_6 in $GL(4,2)$. Moreover a symplectic bilinear form is defined by $(w_1, w_2) = 1$ if and only if the w_i are different pairs which intersect in a point of X. This symplectic form is respected by the action of S_6, defining an embedding of S_6 in the symplectic group $Sp(4,2)$. As these groups have the same order one obtains a second exceptional isomorphism: $S_6 \cong Sp(4,2)$.

Alternatively we can use the 15 1-factors on X to define an elementary abelian group W', where

$$(12)(34)(56) + (12)(35)(46) = (12)(36)(45),$$

$$(12)(34)(56) + (13)(25)(46) = (16)(24)(35)$$

and a symplectic form where two 1-factors have symplectic product $= 1$ if and only if they do not have a pair in common. Using the pairs of X as points and the 1-factors as lines, with the obvious incidence, we obtain a geometry which is known as the S_6-**generalized quadrangle**. Generalized quadrangles are geometries of points and lines such that all lines have the same number of points, all points are on the same number of lines, any two points are on at most one common line, and which satisfy the following main axiom: given a line l and a point $P \notin l$ there is precisely one point $Q \in l$ which is on a common line with P. It is obvious that are geometry of 15 points (the pairs from X) and 15 lines (the 1-factors on X) satisfy these axioms.

We can define the famous A_7-geometry:

Definition 2. *The points of our geometry are the* 7 *elements of the ground set* Ω, *the lines are the* $\binom{7}{3} = 35$ *triples from* Ω, *the* 15 *planes are the Fano planes from one* A_7*-orbit* $\mathcal{E}_1$. *Incidence is defined in the natural way.*

Theorem 4. *The* A_7*-geometry is a diagram geometry, with diagram as given in Figure 1.*

Proof. The meaning of the term *diagram geometry* is explained in the proof. First of all we have a **rank** 3 **geometry,** meaning that we have 3 types of objects, points, lines and planes. Fix a plane E. This really is a Fano

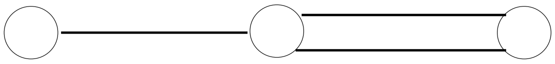

Figure 1: The A_7-geometry

plane. The **residual geometry** consists of the points and lines of E. We conclude that the residual geometry of each plane is a projective plane. This is represented by drawing a single line between the nodes representing points and lines.

Fix a line of our geometry. This is a triple T of Ω. The corresponding residual geometry consists of the three elements of Ω on T and of the Fano planes from our orbit having T as a line. All of those objects are incident. The residual geometry of T (a rank 2 geometry) is a complete bipartite graphs. These are represented by not joining the corresponding nodes of the diagram. In our diagram the nodes representing points and planes are not joined.

Most interesting is the residual geometry corresponding to a fixed element $a \in \Omega$. The points of the residual geometry are the 15 triples containing a, its lines are the 15 Fano planes from orbit $\mathcal{E}_1$. We saw above that this residual geometry is the S_6-generalized quadrangle. The graphical representation of a generalized quadrangle is a double line connecting the corresponding nodes. $\square$

Another famous structure is related to the A_7-geometry, the Hoffman-Singleton graph which we denote by Γ. Recall that we constructed a model of $PG(3,2)$ whose 35 lines are the triples from the ground set Ω of 7. There are at least 3 types of pairs of lines, according to the size of intersection of the triples $(0, 1$ or $2)$ in Ω. Under the full $GL(4,2)$ there are of course only two types of pairs of lines.

The 50 vertices of Γ are the 15 points and the 35 lines of $PG(3,2)$. Two points are never neighbours. A point and a line form an edge if in $PG(3,2)$ the point is on the line. Two lines are neighbours if the corresponding triples are disjoint. Observe that this is **not** equivalent with the corresponding lines of $PG(3,2)$ being parallel.

Each vertex of point type has valency 7 as a point of $PG(3,2)$ is on 7 lines. A vertex of line type has 3 neighbours of point type and $\binom{4}{3} = 4$ neighbours of line type. It follows that Γ is regular of valency 7.

Theorem 5. *The Hoffman-Singleton graph Γ is a* **Moore graph.** *This means*

- Γ *is regular (of valency 7).*
- *There are no triangles in* Γ
- *Any two non-adjacent vertices have precisely one common neighbour.*

Proof. We know the valency, and the absence of triangles is obvious: two disjoint triples cannot be on a common Fano plane. In order to check the final axiom several cases have to be distinguished. Two vertices of point type are on precisely 1 line of $PG(3,2)$. Let T_1, T_2 be triples intersecting in cardinality 1. Then there is precisely one point of $PG(3,2)$ (Fano plane from $\mathcal{E}_1$) containing both as lines. If T_1, T_2 intersect in cardinality 2 there is no such point (Fano plane), but there is exactly one triple disjoint from T_1 and T_2. Finally, let a triple T and a point $P \in PG(3,2)$ be given, where $P \notin T$. In our A_7-language this means we are given a Fano plane E (the projective point) and three points of X forming a triangle in E. The complementary set of 4 points from X contains exactly one line of E. $\square$

We remark that the Moore geometries have more or less been classified. Each Moore geometry either is the Petersen graph or the Hoffman-Singleton graph or possibly a certain graph on 3250 vertices, of valency 56 whose existence is in doubt.

3 From the A_7-geometry to $\mathcal{NR}$.

In the preceding section we constructed a semidirect product $G = VA$, where V is elementary abelian of order 16 and $A \cong A_7$ in its 2-transitive action on V. We write V additively, as a 4-dimensional vector space over $\mathbb{F}_2$, with basis v_1, v_2, v_3, v_4. In terms of Fano planes we can make the following choice:

$$v_1 = x12, x34, x56, 135, 146, 236, 245.$$

$$v_2 = x12, x35, x46, 136, 145, 234, 256.$$

$$v_3 = x34, x15, x26, 124, 136, 235, 456.$$

$$v_4 = 135, 1x4, 126, x25, x36, 234, 456.$$

The normal subgroup V acts by translation on the vectors from V. The action of V is transitive. Let $\tau(v)$ denote translation by $v \in V$. The stabilizer of vector $0 \in V$ is $A \cong A_7$, which is 2-transitive on the 15 nonzero vectors (see Theorem 2). It follows that G acts 3-transitively. In particular each orbit of G in its action on subsets of V defines a 3-design. Let us use the parameters introduced in [2]. The **dimension** of a subset $S \subseteq V$ is the dimension of the affine subspace generated by S. One point has dimension 0, two points have dimension 2 and a 3-point set has dimension 3. A k-set is **in general position** if it has dimension $k-1$.

Lemma 3. *G is regular on the ordered 4-tuples in general position.*

Proof. This follows from Theorem 2. □

A 4-set in general position is $V_1 = \{0, v_1, v_2, v_3\})$. This defines the orbit $\mathcal{V}_1$ of length $16 \times 15 \times 14 \times 12/24 = 16 \times 15 \times 7$. As G is 3-transitive and each triple is contained in precisely one 4-set of dimension 2 (its elements sum to 0), the 4-sets of dimension 2 form an orbit $\mathcal{V}_2$ of length 140, with representative $V_2 = \{0, v_1, v_2, v_1 + v_2\}$. As $|\mathcal{V}_1| + |\mathcal{V}_2| = \binom{16}{3}$ these are all the orbits on 4-sets. The elements of $\mathcal{V}_2$ form a Steiner quadruple system $S(3, 4, 16)$. It follows from Lemma 3 that the stabilizer $G(V_1)$ of V_1 under the action of G is the symmetric group S_4. We have

$$G(V_1) = \langle r, z, \tau(v_1)h \rangle$$

where $r = (x, 1, 3)(2, 6, 4),\ z = (x, 1)(4, 6),\ h = (1, 2)(3, 4)$. The action of these linear operations on V is described by

$$r : v_1 \mapsto v_2 \mapsto v_3 \mapsto v_1,\ v_4 \mapsto v_2 + v_3 + v_4,$$

$$z : v_1 \leftrightarrow v_2,\ v_3 \mapsto v_3,\ v_4 \leftrightarrow v_3 + v_4,$$

$$h : v_1 \mapsto v_1,\ v_2 \leftrightarrow v_1 + v_2,\ v_3 \leftrightarrow v_1 + v_3,\ v_4 \leftrightarrow \sum v_i.$$

The group $G(V_1)$ has two orbits on the set of 8 points complementing V_1 to a 5-set in general position. These orbits are $\{v_2 + v_4, v_1 + v_3 + v_4\}$ and the remaining 6 points. Let

$$H = \{0, v_1, v_2, v_3, v_2 + v_4, v_1 + v_3 + v_4\}$$

and denote by $\mathcal{H}$ the orbit containing H. The 6-sets of this orbit are the **hexads.** Observe that $G(V_1)$ is contained in the stabilizer of H. Another element of $G(H)$ is $\tau(v_2+v_4)l$, where $l=(x,6,1,2,4)$. The action of l on V is described by

$$l: v_1 \mapsto v_1+v_2,\ v_2 \mapsto v_1+v_3,\ v_3 \mapsto v_1+v_2+v_4,\ v_4 \mapsto v_3$$

and $\tau(v_2+v_4)l$ acts on H as a 5-cycle, with fixed point $v_1+v_3+v_4$. The group generated by $G(V_1)$ and $\tau(v_2+v_4)l$ clearly is A_6. It follows $|\mathcal{H}| \leq |G|/|A_6| = 16\times 7$. All 4-sets contained in H are from $\mathcal{V}_1$. By double counting it follows that we have equality and V_1 is contained in precisely one hexad.

Proposition 3. *Let $\mathcal{H}$ be the G-orbit of 6-sets containing $H=\{0,v_1,v_2,v_3,v_2+v_4,v_1+v_3+v_4\}$ (the hexads). There are $112=16\times 7$ hexads, and each 4-set in general position is contained in precisely one hexad.*

Let us describe the completion of a 4-set in general position to its uniquely determined hexad in a combinatorial way. Start from V_1. By Lemma 2 the lines of pairwise intersection of v_1,v_2,v_3 form a triangle. This is the triangle $\{x12,x34,136\}$. Let v be one of the two elements of V (Fano planes) that complement V_1 to a hexad. The vertices of the intersection triangle form a line $x13$ of v. The line through x and 6 contains either 2 or 4, similarly for the other pairs of opposite points in the triangle. Choose $x62$ as a line of v. The same rule shows that 324 and 146 are lines of v, which by now is uniquely determined:

$$v=v_2+v_4=\{x13,x62,324,146,x45,356,125\}.$$

The choice of $x64$ as a line leads to

$$v=v_1+v_3+v_4=\{x13,x64,142,326,x25,156,345\}$$

These two completion points are the Fano planes $\neq v_1+v_2+v_3$ from orbit $\mathcal{E}_1$ containing $x13$ as a line.

Another orbit we are going to need are the **affine hyperplanes.** These are the subgroups of order 8 of V and their complements. There are 30 affine hyperplanes and clearly they form an orbit.

Definition 3. *Use the elements of V as coordinates of the vector space $\mathbb{F}_2^{16}$. Identify each vector from $\mathbb{F}_2^{16}$ with its support, a subset of V. The* **Nordstrom-Robinson code** $\mathcal{NR}$ *is the union of the following words:*

- *The* 0*-word and the* 1*-word,*
- *The affine hyperplanes,*
- *the hexads and their complements.*

The number of codewords of $\mathcal{NR}$ is $2+30+112+112 = 2^8$. By definition $\mathcal{NR}$ admits G as a group of automorphisms. The constant words and the affine hyperplanes together form a linear subcode. As any two different affine hyperplanes have either 0 or 4 points in common, this is a $[16,5,8]_2$-code, the Reed-Muller code $\mathcal{R}$.

Lemma 4. *The hexads define a* $3-(16,6,4)$*. A hexad and an affine hyperplane intersect either in* 4 *or in* 2 *points. For each hexad there are* 15 *affine hyperplanes meeting it in* 4 *points.*

Proof. The parameters of the design follow from double counting. Let H be a hexad. Each of the 15 4-subsets of H is in exactly one affine hyperplane E, and E meets H in precisely those 4 points. The complements of those 15 affine hyperplanes intersect H in 2 points. ☐

Proposition 4. $\mathcal{NR}$ *is the union of* 8 *cosets of* $\mathcal{R}$*. If* H *is a hexad, then the coset* $H+\mathcal{R}$ *consists of the images of* H *under the translation subgroup* V *and their complements.*

In order to prove Proposition 4 it suffices to prove the last claim, which itself is a consequence of the following lemma.

Lemma 5. *Let* H *be a hexad and* E *an affine hyperplane.*

If $|E\cap H| = 4$*, then* $H+E = H+a+b$*, where* a, b *are the points of* H *which are not in* E*.*

If $|E\cap H| = 2$*, then* $H+E$ *is the complement of* $H+a+b$*, where* $E\cap H = \{a,b\}$*.*

Proof. Considering complements it suffices to prove the first rule. Let $h+a$ or $h=b$. Then $h+a+b \in H\setminus E \subset H+E$. If $h\in H\setminus\{a,b\}$, then $h+a+b\in E$ but $h+a+b\notin H$ as H does not contain a 4-set of dimension 2. It follows $h+a+b\in H+E$ also in this case. As the cardinalities are the same we are done. ☐

Definition 4. *Let* $x\in\mathbb{F}_2^{16}$*. Denote by* $A_i(x)$ *the number of codewords of* $\mathcal{NR}$ *at distance* i *from* x*.*

Theorem 6. *For each $x \in \mathcal{NR}$ we have*

$$A_0(x) = A_{16}(x) = 1,\ A_6(x) = A_{10}(x) = 112,\ A_8(x) = 30.$$

In particular $\mathcal{NR}$ is a $(16, 2^8, 6)$-code.

Proof. By definition this is true for $x = 0$. Proposition 4 shows that it holds for all $x \in \mathcal{R}$ and it suffices to prove the statement for a hexad of our choice. Let H be a hexad. It follows from Lemma 4 that the distances from H to the elements of $\mathcal{R}$ are 6 and 10, each occurring 16 times. We need to know how hexads intersect. As each 4-set in general position is in precisely one hexad, the intersection sizes are ≤ 3. As the hexads form a $3-(16, 6, 4)$, there are precisely $\binom{6}{3} \times 3 = 60$ hexads intersecting H in 3 points. The usual counting arguments show that 15 hexads meet H in 2 points and 36 meet it in precisely one point. As $1+60+15+36 = 112$ this exhausts all hexads. We conclude that precisely 15 hexads are at distance 8 from H, while all other hexads $\neq H$ are at distance 6 or 10. The presence of the all-1-word shows that our claim is true. $\square$

Finally let us consider the embedding of $\mathcal{NR}$ in ambient space. There are 2^8 vectors at distance 0, $2^8 \times 16$ vectors at distance 1 and $2^8 \times 120$ vectors at distance 2 from $\mathcal{NR}$. Each vector x at distance 3 from some word of $\mathcal{NR}$ is at distance 3 from $\mathcal{NR}$ and there are precisely 5 codewords at distance 3. The number of vectors at distance 3 from $\mathcal{NR}$ is therefore $2^8 \times \binom{16}{3}/5 = 2^8 \times 112$. Let $x \in \mathcal{NR}$. The 112 vectors $x + u$ where u varies over the words in $\mathcal{NR}$ at distance 6 from x intersect pairwise in at most 3 points. Any three points are contained in at most 4 and in an average of 4 such vectors. It follows that we have equality: the $x+u$ as above form the 112 blocks of an $3-(16, 6, 4)$. These blocks cover 112×15 sets of size 4. The remaining $\binom{16}{4} - 112 \times 15 = 140$ sets v of size 4 represent the vectors $x + v$ at distance 4 from x which are also at distance 4 from the code. The number of codewords at distance 4 from $x + v$ is $1+3+4\times 4 = 20$. The number of vectors at distance 4 from $\mathcal{NR}$ is therefore $2^8 \times 140/20 = 2^8 \times 7$. We count a grand total of $2^8(1+16+120+112+7) = 2^{16}$ vectors at distances at most 4 from $\mathcal{NR}$. The covering radius is 4.

Theorem 7. *G is the full automorphism group of $\mathcal{NR}$.*

Proof. Let $S \subset S_{16}$ be the full automorphism group. If S_{16} is 4-homogeneous, then there must be elements of $\mathcal{V}_2$ contained in hexads, which is not the case. It follows that $\mathcal{V}_1$ and $\mathcal{V}_2$ are the orbits of S on 4-sets. Let S_0 be the stabilizer of 0. As the 4-tuples from $\mathcal{V}_2$ form an $S(3,4,16)$ and $a+b$ is the unique element completing $\{0,a,b\}$ to an element of $\mathcal{V}_2$, it follows that S_0 acts as a subgroup of $GL(4,2)$. Assume S properly contains G. Then S_0 properly contains $A \cong A_7$. As A_7 is a maximal subgroup of $GL(4,2)$ it follows that $S_0 = GL(4,2)$, which is clearly not the case. $\square$

References

[1] E. R. Berlekamp (ed): *Key papers in the development of coding theory,* IEEE Press, NY 1974.

[2] J. Bierbrauer: *An infinite family of* 7*-designs,* *Discrete Mathematics* **240** (2001), 1-11.

[3] P. J. Cameron and J. H. van Lint: *Designs, Graphs, Codes and their Links, Cambridge University Press* 1991.

[4] A. Cayley: *On the triadic arrangements of seven and fifteen things, London, Edinburgh and Dublin Philos. Mag and J.Sci* **37** (1850),50-53.

[5] J. H. Conway and N. J. A. Sloane: *Orbit and coset analysis of the Golay and related codes, IEEE Transactions on Information Theory* **36** (1990), 1038-1050.

[6] G. D. Forney, N. J. A. Sloane, M. D. Trott: *The Nordstrom-Robinson code is the binary image of the octacode, DIMACS/IEEE Workshop on Coding and Quantization, 1992, AMS 1993,* 19-26.

[7] J. M. Goethals: *On the Golay perfect binary code,* *Journal of Combinatorial Theory* **11** (1971), 178-186.

[8] A.R. Hammons, P.V. Kumar, A.R.Calderbank, N.J.A.Sloane, P. Solé: *The Z_4-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Transactions on Information Theory* **40** (1994), 301-319.

[9] A. W. Nordstrom and J. P. Robinson: *An optimum nonlinear code, Information and Control* **11** (1967), 613-616.

[10] Z. X. Wan: *Quaternary codes,* World Scientific 1997.