Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 41 (2000), No. 2, 303-323.

Automorphic Subsets of the n-dimensional Cube

Gareth Jones, Mikhail Klin[1]**, Felix Lazebnik**

Department of Mathematics, University of Southampton, Southampton SO17 1BJ,UK
e-mail: gaj@maths.soton.ac.uk

Department of Mathematics and Computer Science,
Ben-Gurion University of the Negev, P. O. Box 653, 84105 Beer-Sheva, Israel
e-mail: klin@cs.bgu.ac.il

Department of Mathematical Sciences, University of Delaware, Newark,Delaware, USA
e-mail: fellaz@math.udel.edu

Abstract. An automorphic subset of the n-dimensional cube Q_n is an orbit of a subgroup of $\mathrm{Aut}(Q_n)$, acting on the vertices. We develop a theory of such subsets, and we show that those containing 0 coincide with the cwatsets introduced by Sherman and Wattenberg in response to a statistical result of Hartigan. Using this characterisation, together with results from finite group theory and number theory, we answer two questions on cwatsets posed by Sherman and Wattenberg, and we complete the proofs of some results outlined by Kerr.

MSC 2000: 05C25, 20B25, 20E22.
Keywords: automorphic subset, cwatset, Hamming distance, n-dimensional cube, permutation group, subgraph, wreath product

1. Introduction

Let $V = \mathbf{Z}_2^n$, an n-dimensional vector space over the field $\mathbf{Z}_2 = \{0, 1\}$, or equivalently the vertex-set of the n-dimensional cube Q_n. Sherman and Wattenberg [18], motivated by a statistical result of Hartigan [11] (see also [1, 17]), introduced the concept of a *cwatset*, a set $C \subseteq V$ which is 'closed with a twist' (the precise definition is given in Section 5).

[1] Partially supported by research grant No. 6782-1-95 from the Israeli Ministry of Science and Arts, and by the Department of Mathematics and Computing Sciences, University of the South Pacific, Suva, Fiji Islands.

Their paper contains several open questions about the existence of cwatsets with certain properties. Our aim is to extend the notion of a cwatset to that of an *automorphic subset* of Q_n, namely an orbit of a subgroup of $\mathrm{Aut}(Q_n)$. We develop a general theory of such subsets, and characterise cwatsets as the automorphic subsets containing the vector $0 \in V$. We use this theory to construct infinite series of cwatsets which provide negative answers to two questions posed in [18], and to complete some of the results on cwatsets outlined by Kerr in [14]. An extended version of this paper, discussing links with other areas of combinatorics, is available from the authors [13].

In Section 2 we establish the necessary background about the n-dimensional cube Q_n and its automorphism group $\mathcal{E}_n$. Section 3 contains definitions of an automorphic subset of Q_n and of an automorphic orbit of $\mathcal{E}_n$, and discusses their properties. In Section 4 we prove some of the assertions in [14], and we use some deep results from group theory and number theory to construct an infinite series of counterexamples to one of the questions posed by Sherman and Wattenberg. In Section 5 we recall the definition and basic properties of cwatsets from [18]; in Theorem 5.2 we relate cwatsets to automorphic sets, and then we briefly consider their connections with binary linear codes and with hypergraphs. In Section 6 we first give some definitions and examples which refine the notions of cyclic cwatsets and direct sum decompositions in [14, 18]; we then give a negative answer to a second question of Sherman and Wattenberg, constructing an infinite series of cwatsets which are not direct sums of cyclic and group cwatsets.

2. Preliminaries

The *n-dimensional cube* is a graph $Q_n = (V, E)$ with vertex set $V = \mathbf{Z}_2^n$, an n-dimensional vector space over the field $\mathbf{Z}_2 = \{0, 1\}$ of integers mod (2); vertices $u, v \in V$ form an edge $\{u, v\} \in E$ if and only if the vectors u, v differ in exactly one coordinate. Thus each vertex v of Q_n has valency n, being adjacent to $v + e_i$ for $i = 1, \dots, n$, where $e_i = (0, \dots 0, 1, 0, \dots, 0)$ is the i-th standard basis vector of V.

The distance $d(u, v)$ between vertices $u, v \in V$ (the least number of edges in any path from u to v) is called the *Hamming distance.* If $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$ then $d(u, v)$ is the number of subscripts i such that $u_i \neq v_i$; equivalently, $d(u, v)$ is the weight (number of non-zero coordinates) of the vector $v - u$.

We define the *distance graphs* $Q_n^{(i)}$, where $i = 1, \dots, n$, to have vertex set $V = \mathbf{Z}_2^n$, with vertices u, v adjacent in $Q_n^{(i)}$ if and only if $d(u, v) = i$ in Q_n. In particular, $Q_n^{(1)} = Q_n$. Each $Q_n^{(i)}$ is a regular graph of valency $\binom{n}{i}$, and the edges of $Q_n^{(1)}, \dots, Q_n^{(n)}$ form a partition of the edges of the complete graph with vertex set V.

In many applications, another interpretation of V is useful. Let U denote the *power set* $\mathcal{P}(\mathbf{N}_n)$ of $\mathbf{N}_n = \{1, 2, \dots, n\}$. This is a group with respect to the operation of *symmetric difference* $A \triangle B := (A \backslash B) \cup (B \backslash A)$; the empty set $\emptyset$ is the identity element, and each $A \in U$ is its own inverse. For each $A \in U$ we define the *characteristic vector* $\chi(A) = (a_1, \dots, a_n) \in V$, where

$$a_i = \begin{cases} 1 & \text{if } i \in A, \\ 0 & \text{if } i \notin A. \end{cases}$$

This function $\chi : U \to V$ is an isomorphism between the groups $(U, \triangle)$ and $(V, +)$: if

$a = (a_1, \ldots, a_n) \in V$ then $\chi^{-1}(a) = A = \{i \in \mathbf{N}_n \mid a_i = 1\}$. By using χ to identify U with V, we can regard a vertex of Q_n as a vector or a subset of $\mathbf{N}_n$. If vertices a and b correspond to subsets A and B of N_n, then $d(A, B) = d(a, b) = |A \triangle B|$.

Another useful interpretation is to identify V with the set $\mathbf{Z}_2^{\mathbf{N}_n}$ of all functions $\phi : \mathbf{N}_n \to \mathbf{Z}_2$, by regarding each $a = (a_1, \ldots, a_n)$ as a function $i \mapsto a_i$, so that each subset $A \in U$ corresponds to its characteristic function χ_A; under point-wise addition mod (2) these functions form a group isomorphic to $(V, +)$. If vertices a and b correspond to functions $\phi = \chi_A$ and $\psi = \chi_B$, then $d(\phi, \psi)$ is the number of i such that $\phi(i) \neq \psi(i)$.

Our first goal is to describe the automorphism group $\mathrm{Aut}(Q_n)$ of the graph Q_n; this is well-known, but for completeness we include the result. If we think of vertices as vectors, then V acts on itself by addition, each $v \in V$ sending a vector $a \in V$ to $a + v$, while S_n acts on V by permuting coordinates: each $g \in S_n$ sends $a = (a_1, \ldots, a_n)$ to $a^g = b = (b_1, \ldots, b_n)$, where $b_j = a_i$ whenever $i^g = j$, that is, $(a_1, \ldots, a_n)^g = (a_{1^{g^{-1}}}, \ldots, a_{n^{g^{-1}}})$. Clearly V and S_n preserve the edges of Q_n, so we can regard them both as subgroups of $\mathrm{Aut}(Q_n)$. If $v \in V$ and $g \in S_n$ then (if we compose mappings from left to right) $g^{-1}vg$ sends a to $a + v^g$; thus $g^{-1}vg \in V$, so $Vg = gV$ and hence the subset $\mathcal{E}_n = S_nV$ of $\mathrm{Aut}(Q_n)$ is a subgroup. It has V as a normal subgroup, with $|S_n \cap V| = 1$, so $\mathcal{E}_n$ is a semi-direct product of V by S_n, a group of order $2^n n!$ with $\mathcal{E}_n/V \cong S_n$. The action of S_n by conjugation on $V = \mathbf{Z}_2^n$ is to permute the n direct factors $\langle e_i \rangle \cong \mathbf{Z}_2$ in the same way as it permutes $\mathbf{N}_n$, so $\mathcal{E}_n$ is isomorphic to the wreath product $\mathbf{Z}_2 \,\mathrm{wr}\, S_n \cong S_2 \,\mathrm{wr}\, S_n$ of S_2 by S_n. (Traditional Russian and western notations for this group are $S_n \wr S_2$ and $S_2 \wr S_n$; to avoid confusion we have used the notation in [6]. The action of the wreath product described here is its *primitive* action of degree 2^n, as opposed to its *imprimitive* action of degree $2n$ on $\mathbf{Z}_2 \times \mathbf{N}_n$.)

For a useful equivalent description of $\mathcal{E}_n$, we regard V as the set of functions $\phi : \mathbf{N}_n \to \mathbf{Z}_2$. Both S_n and S_2 have actions on $V = \mathbf{Z}_2^{\mathbf{N}_n}$, induced by their actions on $\mathbf{N}_n$ and $\mathbf{Z}_2$: each $g \in S_n$ sends a function $\phi : \mathbf{N}_n \to \mathbf{Z}_2$ to the function $\phi^g = g^{-1} \circ \phi : i \mapsto \phi(i^{g^{-1}})$, and each $f \in V = \mathbf{Z}_2^{\mathbf{N}_n}$ sends ϕ to $\phi^f = \phi + f : i \mapsto \phi(i) + f(i)$. The group of permutations of V generated by S_n and S_2 is their exponentiation $\mathcal{E}_n = S_2 \uparrow S_n$ [8]. Each element of $\mathcal{E}_n$ has a unique representation of the form $\sigma = gf$ where $g \in S_n$ and f $(\in V)$ is a function $\mathbf{N}_n \to \mathbf{Z}_2$, and its action on V is given by

$$\phi^\sigma = g^{-1} \circ \phi + f : i \mapsto \phi(i^{g^{-1}}) + f(i).$$

If we denote $\sigma = gf$ by the pair (g, f), then the group structure of $\mathcal{E}_n$ is given by

$$\begin{aligned} (g, f)(g', f') &= (gg', f^{g'} + f'), \\ (g, f)^{-1} &= (g^{-1}, f^{(g^{-1})}). \end{aligned}$$

If we identify V with $\mathcal{P}(\mathbf{N}_n)$, then the action of S_n on V is induced from its natural action on $\mathbf{N}_n$, while V acts on itself by symmetric difference; thus if $\sigma = (g, f)$, where f corresponds to $F = f^{-1}(1) \subseteq \mathbf{N}_n$, then $A^\sigma = A^g \triangle F$ for all $A \subseteq \mathbf{N}_n$.

Theorem 2.1. $\mathrm{Aut}(Q_n) = \mathcal{E}_n$.

Proof. We have shown that $\mathcal{E}_n \leq \mathrm{Aut}(Q_n)$; since $|\mathcal{E}_n| = 2^n n!$, it is therefore sufficient to prove that $|\mathrm{Aut}(Q_n)| \leq 2^n n!$. To do this, we regard the vertices of Q_n as the subsets of $\mathbf{N}_n$, with $0 = \emptyset$. Now $\mathrm{Aut}(Q_n)$ acts transitively on the vertices (since its subgroup V does), so $|\mathrm{Aut}(Q_n)| = 2^n|H|$ where H is the stabiliser in $\mathrm{Aut}(Q_n)$ of $\emptyset$. If we can prove that $H \leq S_n$ then $|H| \leq n!$, as required.

Suppose, therefore, that $h \in H$. For each k, let M_k denote the set of vertices at distance k from $\emptyset$ (the k-element subsets of $\mathbf{N}_n$). Since h fixes $\emptyset$, it permutes the set M_1 of vertices adjacent to $\emptyset$; these are the 1-element subsets of $\mathbf{N}_n$, so h acts on them as a permutation $g \in S_n$. Since $S_n \leq H$ we have $hg^{-1} \in H$. Now hg^{-1} fixes the vertices in $M_0 \cup M_1$, and by induction on k it fixes those in M_k for all k: if $A \in M_k$ with $k \geq 2$, then there are exactly k sets $B_1, \ldots, B_k \in M_{k-1}$ adjacent in Q_n to A, and A $(= B_1 \cup \cdots \cup B_k)$ is the only set in M_k adjacent to each B_i; by the induction hypothesis, the vertices $B_1, \ldots, B_k$ are fixed by hg^{-1}, and hence (by its uniqueness) so is A. Thus hg^{-1} fixes every vertex in V, so it is the identity permutation, giving $h = g \in S_n$ as required. □

Comments. 1. This shows that the stabiliser in $\mathrm{Aut}(Q_n)$ of the vertex $\emptyset = 0$ is the subgroup S_n.

2. The graph Q_n is *distance-transitive*, that is, if $u, v, u', v' \in V$ with $d(u, v) = d(u', v')$ then there exists $\sigma \in \mathrm{Aut}(Q_n)$ such that $u^\sigma = u'$ and $v^\sigma = v'$. This is because the subgroup V of $\mathcal{E}_n$ is transitive on the vertices, and S_n is transitive on the set M_k of vertices at each distance k from $\emptyset$.

3. Subgraphs of Q_n

If $X \subseteq V$, we define $\Gamma_i = \Gamma_i(X)$ to be the subgraph $Q_n^{(i)}(X)$ of $Q_n^{(i)}$ *generated* (or *induced*) by X. This graph has vertex set X, and its edges are those edges of $Q_n^{(i)}$ whose incident vertices both lie in X. If we regard the integers $i = 1, \ldots, n$ as colours, then by colouring the edges of each Γ_i with colour i we obtain the *complete coloured subgraph* $\Gamma = \Gamma(X)$ of Q_n generated by X.

For each $X \subseteq V$ we define $\mathrm{Stab}(X) := \{\sigma \in \mathcal{E}_n \mid X^\sigma = X\}$, the subgroup of $\mathcal{E}_n$ which stabilises X. Our definitions imply that each $\sigma \in \mathrm{Stab}(X)$, restricted to X, induces automorphisms of the subgraphs $\Gamma_i(X)$. The group $H = \mathrm{Stab}(X)$ induces a permutation group $(\overline{H}, X)$ on X, which is a homomorphic image of the permutation group (H, V).

The complete coloured graph $\Gamma = \Gamma(X)$ has automorphism group

$$G := \bigcap_{i=1}^{n} \mathrm{Aut}(\Gamma_i).$$

By our definitions, G contains $\overline{H}$, but in general these two groups may be different.

We now consider some examples. For notational convenience, we will often write a vector $v = (v_1, \ldots, v_n) \in V$ as $v_1 \ldots v_n$. Even more concisely, we will sometimes denote v by the integer $\sum_{i=1}^{n} 2^{n-i} v_i$ whose binary representation is $v_1 v_2 \ldots v_n$; thus the vertex $(0, 1, 1)$ is denoted by 011, or by 3.

Example 3.1. Let $n = 3$ and $X = \{0, 3, 7\} \subset V$. The subgraphs Γ_i are shown in Figure 3.1. In this case G is the trivial group, and hence so is $\overline{H}$, while $H = \langle (0)(1,2)(3)(4)(5,6)(7) \rangle$ has order 2.

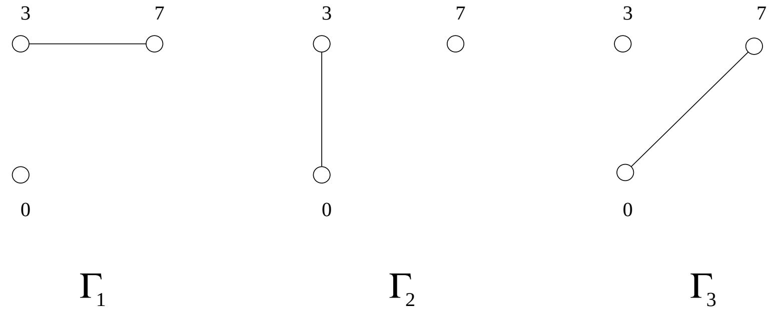

Figure 3.1

Example 3.2. Let $n = 4$ and $X = \{0101, 0110, 0011, 1010, 1001, 1100\}$. Each vertex in X has distance 4 from one vertex in X, and distance 2 from the remaining four. The subgraph Γ of Q_4 generated by X therefore has edges of colours 2 and 4, with Γ_2 an octahedron, and Γ_4 its complement $3K_2$ (the disjoint union of three complete graphs K_2); thus $G = \mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_2) = \mathrm{Aut}(\Gamma_4)$, and the latter is the wreath product $S_2 \,\mathrm{wr}\, S_3$, of order $(2!)^3 \cdot 3! = 48$, acting imprimitively with degree 6 on X.

To determine H we note that there are just two vertices of Q_4, namely $v = 0000$ and $w = 1111$, adjacent in $Q_4^{(2)}$ to every vertex in X. It follows that H acts transitively on $\{v, w\}$, so $|H : H_v| = 2$. It is easy to see that H_v can be identified with S_4 in its natural action on V (permuting coordinates), and H with $S_4 \times S_2$. Now H acts faithfully on X, so $|\overline{H}| = |H| = 48 = |G|$ and hence $\overline{H} \cong H \cong G$. As a corollary, we have proved that the octahedral group and the groups $S_2 \,\mathrm{wr}\, S_3$ and $S_4 \times S_2$ are mutually isomorphic; indeed, Theorem 2.1 gives $\mathrm{Aut}(Q_3) = \mathcal{E}_3 = S_2 \,\mathrm{wr}\, S_3$, so they are all isomorphic to $\mathcal{E}_3$.

Example 3.3. Our examples so far have all satisfied $\overline{H} = G$, but the following example shows that this is not always the case. Let $n = 7$, with

$$X = \{1100000, 1010000, 0110000, 0001100, 0001010, 0001001\}.$$

The coloured graph Γ generated by X has edges of colours 2 and 4, with $\Gamma_2 \cong 2K_3$ and Γ_4 its complement $K_{3,3}$ (a complete bipartite graph). Thus $G = \mathrm{Aut}(\Gamma) = S_3 \,\mathrm{wr}\, S_2$, a group of order $(3!)^2 \cdot 2! = 72$ acting imprimitively with degree 6 on X. One can easily check that 0 is the only vertex in Q_7 adjacent in $Q_7^{(2)}$ to every vertex in X, so H stabilises 0 and is therefore a subgroup of S_7 in its natural action on V. Now it is easy to see that $H \cong \overline{H} \cong S_3 \times S_3$, acting intransitively on X, so $\overline{H} < G$.
(This example is simply a variation on the Whitney-Jung Theorem on the isomorphism of line graphs [9].)

With each subset $X \subseteq V$ we associate its *orbit* $\mathrm{Orb}(X) := \{X^\sigma \mid \sigma \in \mathcal{E}_n\}$. The Orbit-Stabiliser Theorem gives

$$|\mathrm{Orb}(X)| = \frac{2^n n!}{|H|}.$$

In Example 3.1, for instance, $\mathrm{Orb}(X)$ contains 24 triples, each consisting of two vertices adjacent in Q_3 together with a vertex adjacent to neither of them. We will refer to two subsets in the same orbit, and their corresponding coloured complete subgraphs, as *internally isomorphic*, or *similar.*

A subset $X \subseteq V$ and its corresponding subgraph Γ are called *automorphic* if $(\overline{H}, X)$ is a transitive permutation group, in which case $\mathrm{Orb}(X)$ is an *automorphic orbit.* We are interested in classifying all automorphic subsets and subgraphs of Q_n up to (internal) isomorphism.

If X is an automorphic subset, then each Γ_i is a regular graph; we let k_i denote its valency, and define $k_0 = 1$. We also define $k = |X|$ and $b = |\mathrm{Orb}(X)|$. The distance-transitivity of Q_n implies that the following parameters are well-defined:

r is the number of subsets in $\mathrm{Orb}(X)$ containing a given vertex in V (such as 0);

λ_i is the number of subsets in $\mathrm{Orb}(X)$ containing a given pair u, v of elements of X such that the edge $\{u, v\}$ has colour i.

We now list some basic properties of these parameters; the proofs are simple exercises.

Proposition 3.1. *If X is an automorphic set in Q_n then*

(1) $1 \leq k \leq 2^n$;

(2) $b = 2^n n!/|H|$;

(3) k *divides* $|\overline{H}|, |H|$ *and* $2^n n!$;

(4) $\sum_{k=0}^{n} k_i = k$;

(5) $vr = bk$;

(6) $k_i r = \binom{n}{i}\lambda_i$. (Hint: show that $bkk_i = 2^n\binom{n}{i}\lambda_i$ and then apply (5).) □

One can enumerate the orbits of $\mathcal{E}_n$ on subsets of V using cycle indices. The *cycle index* of any permutation group G is the polynomial

$$z(G) = \frac{1}{|G|}\sum_{g\in G} z(g),$$

where

$$z(g) = x_1^{i_1} x_2^{i_2} \dots x_m^{i_m}$$

if g has i_k cycles of each length k. Replacing each variable x_i in $z(G)$ with $1 + x^i$, we obtain a generating function $f(x) = \sum_i a_i x^i$, where a_i is the number of orbits of G on i-element subsets.

Example 3.4. The cycle index of $\mathcal{E}_3$, acting on $V = \mathbf{Z}_2^3$, is

$$z(\mathcal{E}_3) = \frac{1}{48}(x_1^8 + 6x_1^4x_2^2 + 8x_1^2x_3^2 + 13x_2^4 + 8x_2x_6 + 12x_4^2),$$

so

$$f(x) = 1 + x + 3x^2 + 3x^3 + 6x^4 + 3x^5 + 3x^6 + x^7 + x^8,$$

and $\mathcal{E}_3$ has $f(1) - f(0) = 21$ orbits on the nonempty subsets of V. By detailed examination, one finds that only 10 of these 21 orbits are automorphic. In the following table, the set X in row i is an automorphic set from the i-th orbit; the elements of X are decimal representations of binary expansions.

#	k	X	b	r	k_1	k_2	k_3	λ_1	λ_2	λ_3	$\lvert\overline{H}\rvert$	$\lvert H\rvert$	$\lvert G\rvert$
1	1	{0}	8	1	0	0	0	0	0	0	1	6	1
2	2	{0,1}	12	3	1	0	0	1	0	0	2	4	2
3	2	{0,3}	12	3	0	1	0	0	1	0	2	4	2
4	2	{0,7}	4	1	0	0	1	0	0	1	2	12	2
5	3	{0,3,5}	8	3	0	2	0	0	2	0	6	6	6
6	4	{0,1,4,5}	6	3	1	2	0	2	1	0	8	8	8
7	4	{0,1,6,7}	6	3	1	1	1	1	1	3	8	8	8
8	4	{0,3,5,6}	2	1	0	3	0	0	1	0	24	24	24
9	6	{0,2,3,4,5,7}	4	3	2	2	1	2	2	3	12	12	12
10	8	V	1	1	3	3	1	1	1	1	48	48	48

Table 3.1: Automorphic orbits of $\mathcal{E}_3$

A natural problem is to find all possible sizes k of automorphic subsets of Q_n for each n. Proposition 3.1 shows that $k \leq 2^n$ and $k \mid 2^n n!$, but are these simple necessary conditions also sufficient? The answer is (trivially) yes for $n \leq 2$, and Table 3.1 confirms this for $n = 3$. For $n = 4$ the conditions are satisfied by $k = 1, 2, 3, 4, 6, 8, 12, 16$, and one can find a k-element automorphic subset in each case.

We will show that for $n \geq 5$ these conditions are insufficient. Our first counterexamples are based on simple combinatorial principles.

Proposition 3.2. *Let $k = 2^n - 2^{n-4}$, where $5 \leq n \leq 14$. Then $k \leq 2^n$ and k divides $2^n n!$, but there is no automorphic subset $X \subseteq V$ with k elements.*

Proof. Clearly $k \leq 2^n$, and $k = 2^{n-4} \cdot 15$ divides $2^n n!$ for all $n \geq 5$. If X is a k-element subset of V, then the subgraph $\Gamma(X)$ must have a vertex of valency less than the valency n of Q_n, for otherwise the connectedness of Q_n gives $X = V$. If X is automorphic then $\Gamma(X)$ is regular, of valency less than n, so each of the k vertices in X is adjacent in Q_n to a vertex $v \in V \setminus X$. Now there are 2^{n-4} such vertices v, each of valency n, so by counting edges we get $k \leq n2^{n-4}$ and hence $n \geq 15$, against our hypothesis. □

In Section 4 we will use more advanced methods to construct infinitely many counterexamples.

4. Group-theoretic analysis of automorphic subsets

The mapping $\varphi : \mathcal{E}_n \to S_n$, $\sigma = (g, f) \mapsto g$ is an epimorphism, with $\ker(\varphi) = V$. For any $H \leq \mathcal{E}_n$, let $\tilde{H}$ denote $\varphi(H)$. The Orbit-Stabiliser Theorem implies that if X is an automorphic subset and $H = \mathrm{Stab}(X)$, then

$$k = |X| = |H : H_x|$$

where H_x is the subgroup of H fixing some $x \in X$.

Lemma 4.1. $k = |\tilde{H} : \tilde{H}_x| \cdot |H \cap V|$.

Proof. Using $\ker(\varphi|_H) = H \cap V$ and $\ker(\varphi|_{H_x}) = \{0\} \subset V$, we have

$$k = |H : H_x| = \frac{|H|}{|H_x|} = \frac{|\tilde{H}| \cdot |\ker(\varphi|_H)|}{|\tilde{H}_x| \cdot |\ker(\varphi|_{H_x})|} = \frac{|\tilde{H}|}{|\tilde{H}_x|} \cdot |\ker(\varphi|_H)| = |\tilde{H} : \tilde{H}_x| \cdot |H \cap V|. \qquad \square$$

Corollary 4.2. *If k is odd then $H \cap V = \{0\}$ and $k = |\tilde{H} : \tilde{H}_x|$.*

Proof. Since $H \cap V$ is a subgroup of V, its order is a power of 2, so Lemma 4.1 gives $|H \cap V| = 1$ and the result follows. □

The subgroup S_n of $\mathcal{E}_n$ is the stabiliser of 0, and as such it is conjugate in $\mathcal{E}_n$ to the stabiliser of any other vertex, so we have a conjugacy class of subgroups isomorphic to S_n. There are 2^{n-1} subgroups in this conjugacy class, each fixing two antipodal vertices. We are interested in whether this is the only conjugacy class of subgroups isomorphic to S_n.

Example 4.1. When $n = 2$ we have $\mathcal{E}_2 \cong D_4$, the dihedral group of order 8 (the symmetry group of a square). This has five subgroups isomorphic to S_2, forming three conjugacy classes: one consists of the two stabilisers of vertices, and the other two consist of one and two subgroups of V.

Example 4.2. If $n = 3$ then, in addition to the conjugacy class of vertex-stabilisers, $\mathcal{E}_3$ has a second class of subgroups isomorphic to S_3. If we regard Q_3 as the vertices and edges of a regular solid in $\mathbf{R}^3$, then its symmetry group is $\mathcal{E}_3 \cong S_4 \times S_2$ (see Example 3.2). The rotation group, corresponding to S_4, acts naturally on the four diagonals (edges in $Q_3^{(3)}$), so it has four subgroups isomorphic to S_3, each preserving a diagonal. These subgroups have orbits of length 2 and 6 on V, so they are not vertex-stabilisers.

Example 4.3. The above example generalises to higher dimensions, though the concept of a rotation is no longer valid. The stabiliser in $\mathcal{E}_n$ of the vertex 0 consists of the automorphisms $\sigma = (g, 0)$ with $g \in S_n$. If v denotes the vector $11 \ldots 1$ at maximum distance n from 0, then the elements of $\mathcal{E}_n$ preserving the diagonal $\{0, v\}$ are those of the form $\sigma = (g, f)$ where $g \in S_n$ and $f \in \{0, v\}$, forming a subgroup isomorphic to $S_n \times S_2$; those σ with g even and $f = 0$, or with g odd and $f = v$, form a subgroup isomorphic to S_n which does not stabilise any vector. We have therefore found two conjugacy classes of subgroups of $\mathcal{E}_n$ isomorphic to S_n; in each case, the normaliser of such a subgroup is $S_n \times S_2$, so the number of subgroups in each conjugacy class is equal to the index $|\mathcal{E}_n : S_n \times S_2| = 2^{n-1}$.

Theorem 4.3. *If $n = 3$ or $n \geq 5$, then the subgroups described in Example 4.3 are the only subgroups $S \leq \mathcal{E}_n$ isomorphic to S_n. If $n = 4$ then there are 16 additional subgroups $S \cong S_4$, each satisfying $|S \cap V| = 4$.*

Proof. We will use the cohomology of groups; [2] or [12, I.16–I.17] are good references.

Let $n \geq 3$ and let S be any subgroup of $\mathcal{E}_n$ isomorphic to S_n. Now V is a normal subgroup of $\mathcal{E}_n$, so $S \cap V$ is a normal subgroup of S; being a subgroup of V, it has order a power of 2. For $n \neq 4$ the only proper normal subgroups of S_n are the alternating group A_n (of order $n!/2$) and the trivial subgroup, while S_4 also has a normal Klein four-group K, so either $|S \cap V| = 1$ or $S \cap V \cong K$ with $n = 4$.

Suppose first that $|S \cap V| = 1$. Now V is normal in $\mathcal{E}_n$, so SV is a subgroup of $\mathcal{E}_n$ of order $|S| \cdot |V|/|S \cap V| = 2^n n!$; thus $SV = \mathcal{E}_n$, so S is a complement for V in $\mathcal{E}_n$. In general, conjugacy classes of complements for abelian normal subgroups can be studied using cohomology theory, as follows.

Any group G, acting by automorphisms on an abelian group A (so that A is a G-module) determines a sequence of cohomology groups $H^i(G, A)$, $i \geq 1$; in particular, if GA denotes the semi-direct product (split extension) of A by G, then the conjugacy classes of complements for A in GA are in one-to-one correspondence with the elements of $H^1(G, A)$ (see [2, IV.2.3] or [12, I.17.3(a)]). In our case, this implies that the conjugacy classes of complements for V in $\mathcal{E}_n = S_n V$ correspond to the elements of $H^1(S_n, V)$. Now S_n acts on $V = \mathbf{Z}_2^n$ by conjugation, permuting the n standard basis vectors, so that V is the natural permutation module for S_n over $\mathbf{Z}_2$. The permutation module M for any transitive group G is isomorphic to the induced G-module N^G obtained from the trivial 1-dimensional module N for a point-stabiliser in G, so in our case $V \cong \mathbf{Z}_2^{S_n}$, where $\mathbf{Z}_2$ is a trivial S_{n-1}-module. Shapiro's Lemma [2, III.6.2] states that if a G-module A is the induced module B^G obtained from some H-module B, where $H \leq G$, then $H^1(G, A) \cong H^1(H, B)$. (Strictly speaking, Shapiro's Lemma applies to co-induced modules, but for finite groups G these are the same as induced modules [2, III.5.9].) In our case, we therefore have $H^1(S_n, V) \cong H^1(S_{n-1}, \mathbf{Z}_2)$. If B is a trivial H-module, then $H^1(H, B) \cong \mathrm{Hom}\,(H, B)$, the group of homomorphisms $H \to B$ [2, III.1, Exercise 2]. For $n \geq 3$ there are just two homomorphisms $S_{n-1} \to \mathbf{Z}_2$, so $|H^1(S_n, V)| = 2$ and there are just two conjugacy classes of complements for V in $\mathcal{E}_n$; these are the classes described in Example 4.3, and we have shown that for $n \neq 4$ they provide the only subgroups of $\mathcal{E}_n$ isomorphic to S_n.

There remains the case where $n = 4$ and $S \cap V$ is a Klein four-group normal in S. Then $\varphi(S) \cong SV/V \cong S/(S \cap V) \cong S_3$, so $SV = \varphi^{-1}(T)$ where T is a subgroup of S_4 isomorphic to S_3. There are four such subgroups $T \leq S_4$, namely the stabilisers of $1, 2, 3$ and 4, so there are four corresponding subgroups $SV \leq \mathcal{E}_4$, each a semi-direct product TV of V by T. Since T acts on V by fixing one of its four standard basis vectors and permuting the other three as S_3, it follows that $TV \cong S_2 \times (S_2 \operatorname{wr} S_3) \cong S_2 \times S_2 \times S_4$ (see Example 3.2 for the last isomorphism). This group has four subgroups isomorphic to S_4: in addition to the direct factor S_4, three others may be obtained from this one by multiplying the elements of $S_4 \setminus A_4$ by one of the three involutions in the factor $S_2 \times S_2$ (this is an adaptation of the construction in Example 4.3). Since each such subgroup S is contained in a unique subgroup $SV = TV$, we obtain 16 subgroups S with $|S \cap V| = 4$; each has normaliser SV, of index 4 in $\mathcal{E}_4$, so there are four groups in each of four conjugacy classes of such subgroups. □

The combinatorial interpretation of the extra subgroups for $n = 4$ is that there are four ways of expressing V as a direct sum $V_1 \oplus V_3$ of 1- and 3-dimensional subspaces by choosing a partition $1+3=4$ of its standard basis vectors; in each case there is a subgroup $\mathcal{E}_1 \times \mathcal{E}_3$ of $\mathcal{E}_4$ preserving this decomposition, with $\mathcal{E}_3$ (the symmetry group $S_2 \operatorname{wr} S_3 \cong S_4 \times S_2$ of a cube) containing two subgroups isomorphic to S_4, and two others obtained by composing the elements of $S_4 \setminus A_4$ with the non-identity element of $\mathcal{E}_1 \cong S_2$.

Lemma 4.4. *If G is a subgroup of $\mathcal{E}_n$ with an orbit of odd length in V, then G fixes a vertex $v \in V$.*

Proof. For each subset X of V, define $v(X) = \sum_{x \in X} x \in V$. Each $g \in S_n$ acts on V as a linear transformation, so

$$v(X^g) = \sum_{x \in X} x^g = \Big(\sum_{x \in X} x\Big)^g = v(X)^g.$$

Each $f \in V$ acts on V as a translation $x \mapsto x + f$, so

$$v(X+f) = \sum_{x \in X}(x+f) = \Big(\sum_{x \in X} x\Big) + |X|f = \begin{cases} v(X) & \text{if } |X| \text{ is even,} \\ v(X)+f & \text{if } |X| \text{ is odd.} \end{cases}$$

Thus if $|X|$ is odd and $\sigma = (g,f) \in \mathcal{E}_n$ then $v(X^\sigma) = v(X)^\sigma$, and in particular if σ leaves X invariant then it fixes $v(X)$. It follows that if a subgroup G of $\mathcal{E}_n$ has an orbit X of odd length then $v(X)$ is fixed by G. □

(This result is a discrete analogue of the classical result that any finite group of isometries of $\mathbf{R}^n$ has a fixed-point: this is the centroid, or average, of the points in some orbit, found by adding these points and then dividing by the number of them. In our case, with coefficients in $\mathbf{Z}_2$ rather than $\mathbf{R}$, we need the number of points to be odd in order that this averaging can take place. The proof we have given is an adaptation of an earlier proof shown to us by M. Muzychuk.)

Theorem 4.5. (Kerr's bound) *If X is an automorphic subset of Q_n and $|X|$ is odd, then*

$$|X| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

Proof. Let G be the stabiliser of X in $\mathcal{E}_n$. Since $|X|$ is odd, Lemma 4.4 implies that G has a fixed-point in V. By replacing G with a suitable conjugate we may assume that this point is 0. Then G is contained in the stabiliser S_n of 0, so X, which is an orbit of G, is contained in an orbit of S_n on V. These orbits are the sets M_i of i-element subsets of $\mathbf{N}_n$ for $0 \leq i \leq n$, with $|M_i| = \binom{n}{i}$, so $|X|$ is bounded above by the greatest of these binomial coefficients, which corresponds to $i = \lfloor n/2 \rfloor$. □

This result was stated, though without a complete proof, in [14]. For example, it implies that there are no automorphic k-element subsets of Q_n for

a. $n=5,\ k=15$,

b. $n=6,\ k=45$,

c. $n=7,\ k=45, 63, 105$,

and so on, even though these values of n and k satisfy the conditions $k \leq 2^n$ and $k \mid 2^n n!$ given by Proposition 3.1.

In the remainder of Section 4 we use more advanced results on finite groups to improve on Kerr's non-existence result. For background details, see [6, 16, 19].

For each prime p the *affine general linear group* $AGL_1(p)$ consists of the *affine transformations*

$$\sigma = \sigma_{a,b} : x \mapsto ax + b$$

of the field $\mathbf{Z}_p$, where $a, b \in \mathbf{Z}_p$ and $a \neq 0$. This is a doubly transitive permutation group of degree p and order $p(p-1)$. If K is any subgroup of the multiplicative group $\mathbf{Z}_p^* = \mathbf{Z}_p \setminus \{0\}$, then

$$H = \{\sigma_{a,b} \mid a \in K,\, b \in \mathbf{Z}_p\}$$

is a transitive group of degree p and order kp, where $k = |K|$ divides $p - 1$; such groups H, called *affine* groups, are in a sense the most 'typical' transitive groups of prime degree. More precisely, we have:

Burnside's Theorem. *Each transitive permutation group of prime degree is an affine group or is doubly transitive.*

(Note that $AGL_1(p)$ is affine and doubly transitive.) This theorem was first proved by Burnside in [3] (see also [4]), using representation theory. The most elementary proof is in [7] which, together with the editorial remarks in [20], gives further references and historical details.

Proposition 4.6. *Let p be any prime distinct from* 11 *and* 23*, and not of the form* $(q^d - 1)/(q-1)$ *where q is a prime-power and $d \in \mathbf{N}$, $d \geq 2$. Then the only transitive permutation groups of degree p are S_p, A_p and affine groups.*

Proof. One consequence of the classification of finite simple groups is that the doubly transitive finite permutation groups are all known [5, 6]. Among them, the only groups of prime degree p are the affine group $AGL_1(p)$, the symmetric group S_p, the alternating group A_p, three groups $PSL_2(11), M_{11}$ and M_{23} of degrees $p = 11, 11$ and 23 respectively, and certain subgroups of $P\Gamma L_d(q)$ where $p = (q^d - 1)/(q-1)$ for some prime-power q and $d \geq 2$. (Full details of these groups can be found in the sources given above.) Burnside's Theorem now completes the proof. □

Lemma 4.7. *There are infinitely many primes p satisfying the hypotheses of Proposition* 4.6.

Proof. The following argument is based on Cameron's outline proof of his Proposition 7.2 in [5]. The Prime Number Theorem [10, §1.8 and Ch. XXII] states that the number $\pi(x)$ of primes $n \leq x$ satisfies

$$\pi(x) \sim \frac{x}{\log x} \quad \text{as} \quad x \to +\infty.$$

We shall show that the set of primes of the form $n = (q^d - 1)/(q-1)$, where $q = p^e$ is a prime-power and $d \geq 2$, is significantly less dense than the set of all primes. (In fact, it is not known whether there are infinitely many primes of this form.)

First suppose that $d = 2$, so $n = q + 1$. If n is prime then q must be even, so $p = 2$ and $n = 2^e + 1$. If $n \leq x$ then $e < \log_2 x$, so the number of such primes $n \leq x$ is $O(\log x)$. (These are the Fermat primes, of which only five are known to exist.)

Now suppose that $d \geq 3$. Then $n > q^{d-1} \geq p^2$, so the number of primes p for which $n \leq x$ is

$$O(\pi(\sqrt{x})) = O\Big(\frac{\sqrt{x}}{\log \sqrt{x}}\Big) = O\Big(\frac{\sqrt{x}}{\log x}\Big).$$

For any such p, we have $(d-1)e < \log_p n = O(\log x)$, so the number of pairs d, e giving $n \leq x$ is $O((\log x)^2)$. (In fact, it is $O(\log x \cdot \log\log x)$, but the weaker estimate is sufficient here.) It follows that the number of integers $n \leq x$ of the form $(q^d - 1)/(q - 1)$ with $d \geq 3$ is

$$O\Big(\frac{\sqrt{x}}{\log x}\Big) \cdot O((\log x)^2) = O(\sqrt{x}\,\log x).$$

Taking the cases $d = 2$ and $d \geq 3$ together, we see that the number of primes $n \leq x$ of the form $(q^d - 1)/(q - 1)$ is $O(\sqrt{x}\,\log x)$. Since

$$\frac{\sqrt{x}\,\log x}{\pi(x)} \sim \frac{(\log x)^2}{\sqrt{x}} \to 0 \quad \text{as} \quad x \to +\infty,$$

'most' primes (and in particular, infinitely many) do not have the form $(q^d - 1)/(q - 1)$, so the result immediately follows. □

The smallest odd primes satisfying the hypotheses of Proposition 4.6 are $19, 29, 37, \ldots$

Theorem 4.8. *There are infinitely many pairs of integers (k, n) such that $1 \leq k \leq 2^n$ and k divides $2^n n!$, but there is no automorphic subset $X \subseteq Q_n$ with $|X| = k$.*

Proof. If there is an automorphic subset X where $|X| = k$ is odd, then by Corollary 4.2 there are subgroups $\tilde{H}_x \leq \tilde{H} \leq S_n$ with $|\tilde{H} : \tilde{H}_x| = k$. It is therefore sufficient to produce infinitely many pairs (k, n), satisfying the hypotheses of the theorem, for which k is odd and S_n has no pair of subgroups $S \geq T$ with $|S : T| = k$.

By Proposition 4.6 and Lemma 4.7, there are infinitely many odd primes n such that the only transitive groups of degree n are S_n, A_n and affine groups. Given such a prime n, choose an odd integer m such that $2 < m < (n-1)/2$ and m does not divide $n - 1$. For instance, we can take $m = (n-3)/2$ or $(n-5)/2$ as $n \equiv 1$ or 3 mod (4). We then define $k = mn$, so k is odd, $k \mid 2^n n!$ and $k \leq 2^n$.

Now suppose that $T \leq S \leq S_n$, with $|S : T| = k$, so that both m and n divide $|S|$. Since n is prime, S contains an n-cycle and is therefore a transitive group of degree n. It cannot be a subgroup of $AGL_1(n)$, since this has order $n(n-1)$ which is not divisible by m; thus $S = S_n$ or A_n, and $|T| = n!/k = (n-1)!/m$ or $n!/2k = (n-1)!/2m$ respectively.

In either case, n does not divide $|T|$, so T is intransitive. If T has an orbit of length $n-1$, then T is contained in $S \cap S_{n-1}$ $(= S_{n-1}$ or $A_{n-1})$ with index m; since $2 < m < n-1$, this is impossible by the simplicity of A_{n-1}. Hence $T \leq S \cap (S_r \times S_{n-r})$ for some $r = 2, 3, \ldots, n-2$, so $|S : T| \geq \binom{n}{r} \geq \binom{n}{2}$, which is impossible since $m < (n-1)/2$. □

The smallest value of n provided by the proof of Theorem 4.8 is $n = 19$: here one can take $m = 5$ or 7, so that Q_{19} contains no automorphic subsets of size $k = 95$ or 133.

5. Cwatsets and hypergraphs

Motivated by definitions introduced in [18], we now restrict our attention to automorphic subsets containing 0.

Sherman and Wattenberg [18] define a subset $C \subseteq V$ to be a *cwatset* (closed with a twist) if, for each $c \in C$, there exists $g \in S_n$ such that $C+c = C^g$. For example, any additive subgroup $C \leq V$ is a cwatset: take $g = e$ (the identity permutation) for each $c \in C$. Since each $g \in S_n$ fixes 0, and since $c+c = 0$ for each $c \in V$, it is clear that each nonempty cwatset contains 0.

Just as we defined the projection $\varphi : \mathcal{E}_n \to S_n$ by $\sigma = (g, f) \mapsto g$, we now define a projection $\pi : \mathcal{E}_n \to V$ by $\sigma = (g, f) \mapsto f$. Note that $0^\sigma = 0^g + f = f$, so we have $\pi(\sigma) = 0^\sigma$. Although φ is a homomorphism, π is not.

Proposition 5.1. *A nonempty subset $C \subseteq V$ is a cwatset if and only if it is the image $\pi(G)$ of some subgroup $G \leq \mathcal{E}_n$ under the projection $\pi : \mathcal{E}_n \to V$, $\sigma \mapsto 0^\sigma$.*

For the proof, which is elementary, see Proposition 6 of [18].

Theorem 5.2. *A nonempty subset $C \subseteq V$ is a cwatset if and only if C is an automorphic subset of V containing* 0.

Proof. We have to show that C is a cwatset if and only if it is the orbit of 0 under some subgroup $G \leq \mathcal{E}_n$. Since $\pi(\sigma) = 0^\sigma$ we have $\pi(G) = 0^G$ for each $G \leq \mathcal{E}_n$, so the result is just a restatement of Proposition 5.1. □

Corollary 5.3. *If C is a nonempty cwatset and $H = \mathrm{Stab}(C)$ then $|C| = |H : H_0| = |H|/|H_0|$.*

Proof. This is a direct application of the Orbit-Stabiliser Theorem. □

While the results proved earlier for automorphic subsets remain valid for cwatsets, we can use the special nature of cwatsets to deduce extra information. Recall from Section 3 that subsets X_1 and X_2 of V are similar if $X_1^\sigma = X_2$ for some $\sigma \in \mathcal{E}_n$. We regard the classification of cwatsets up to similarity as the main problem of the theory of cwatsets. As defined in Section 3, the invariant $b = b(C)$ of a cwatset C is just the number of subsets of V similar to C. Similarly, Theorem 5.2 implies that the invariant $r = r(C)$ defined in Section 3 is the number of cwatsets similar to C.

Proposition 5.4. (a) *Two cwatsets C_1 and C_2 are similar if and only if $C_1^g = C_2$ for some $g \in S_n$.*

(b) *The number r of cwatsets similar to a k-element cwatset C is given by*

$$r = \frac{bk}{2^n} = \frac{n!}{|H_0|}.$$

Proof. The proof of (a) follows easily from the definition of a cwatset, and then the Orbit-Stabiliser Theorem, applied to S_n, gives $r = n!/|H_0|$. Alternatively, one can deduce this formula from $r = bk/2^n$ (Proposition 3.1(5)), using $b = |\mathcal{E}_n : H|$ and $k = |H : H_0|$. □

The origins of cwatsets go back to statistics (see the references in [18] and especially [11]), where they are used for the construction of confidence intervals for the mean or median of certain random variables. Roughly speaking, statisticians need subsets X of $V = \mathcal{P}(\mathbf{N}_n)$ (sets of samples) which are 'smooth' in the sense that certain parameters of each element of X are equal. The existence of a subgroup of $\mathcal{E}_n$ acting transitively on X guarantees this. For technical reasons one also wants $\emptyset \in X$, so cwatsets satisfy the required conditions. This raises two intriguing questions. Although the concept of a cwatset is sufficient, is it also a necessary condition for this statistical smoothness? Secondly, although we have taken an essentially group-theoretic approach to cwatsets, can they be axiomatised purely combinatorially, thus leading to an alternative approach which might give additional insight into their properties and applications? For a discussion of such an approach, see Section 7 of [13].

We will now consider the simplest class of cwatsets, namely the subgroups of V, called *group cwatsets*, or simply groups.

For any cwatset C, we define $d = d(C) = \min\{i \mid 1 \leq i \leq k \text{ and } k_i \neq 0\}$.

Proposition 5.5. (a) *If C is a group cwatset of order k then $k = 2^l$ for some $l = 0, 1, \ldots, n$.*
(b) *The number of group cwatsets of order 2^l in V is*

$$\begin{bmatrix} n \\ l \end{bmatrix}_2 = \frac{(2^n - 1)(2^{n-1} - 1)\ldots(2^{n-l+1} - 1)}{(2^l - 1)(2^{l-1} - 1)\ldots(2 - 1)}.$$

(c) *If C is a k-element group cwatset, then $k \leq 2^{n-d+1}$.*

Proof. Part (a) is an application of Lagrange's Theorem. In (b), the numerator counts all bases for such group cwatsets C (sets of l linearly independent vectors) in the n-dimensional vector space V, and the denominator counts those bases generating a particular C. In (c), the parameter d is simply the minimum size of any nonempty subset in $C \subseteq V = \mathcal{P}(\mathbf{N}_n)$; if A_1, A_2 are distinct subsets of $\mathbf{N}_{d-1}$ (and thus elements of V) then the cosets $C \triangle A_1$ and $C \triangle A_2$ of C in V are distinct, so $|\mathcal{P}(\mathbf{N}_{d-1})| \leq |V : C|$ giving $k \leq 2^n/2^{d-1} = 2^{n-d+1}$. □

For each prime-power q, the *Gaussian coefficient* $\left[\begin{smallmatrix} n \\ l \end{smallmatrix}\right]_q$ is the number of l-dimensional subspaces in an n-dimensional vector space over the field of order q; it is given by replacing each 2 with q in the formula in Proposition 5.5(b) (see [15], for instance). Taking the limit as $q \to 1$, we obtain the binomial coefficient $\binom{n}{l}$.

In coding theory, a *binary code* of length n is a nonempty subset of V, the vectors being regarded as codewords; a *binary linear code* is a subgroup of V, that is, a group cwatset. In this case, the parameter d is the *minimum distance* of C, and the bound in Proposition 5.5(c) is known as the *Singleton bound.* The codes attaining this bound form an interesting class, the simplest example of which is given in row 8 of Table 3.1: the vertex set of a tetrahedron contained in Q_3. Thus automorphic sets and cwatsets form a generalisation of linear codes, a theory where algebraic arguments have been successfully combined with purely combinatorial reasoning. We finish our remarks on codes with an example.

Example 5.1. If $n = 4$ then by Proposition 5.5(b) there are $15 \cdot 7/3 \cdot 1 = 35$ group cwatsets C of order $k = 4$. Now Proposition 5.5(c) gives $d(C) \leq 3$, but in fact this bound is not attained; this is shown by the description of the 35 cwatsets in following table. Each row represents the similarity class of some group cwatset C in $V = \mathcal{P}(\mathbf{N}_4)$. The numbers k_i can be interpreted as the coefficients of the weight enumerator polynomial of C.

#	C	k_1	k_2	k_3	k_4	r	d
1	$\{\emptyset, \{1\}, \{2\}, \{1,2\}\}$	2	1	0	0	6	1
2	$\{\emptyset, \{1\}, \{2,3\}, \{1,2,3\}\}$	1	1	1	0	12	1
3	$\{\emptyset, \{1\}, \{2,3,4\}, \{1,2,3,4\}\}$	1	0	1	1	4	1
4	$\{\emptyset, \{1,2\}, \{2,3\}, \{1,3\}\}$	0	3	0	0	3	2
5	$\{\emptyset, \{1,2\}, \{3,4\}, \{1,2,3,4\}\}$	0	2	0	1	4	2
6	$\{\emptyset, \{1,2\}, \{1,3,4\}, \{2,3,4\}\}$	0	1	2	0	6	2
						Total: 35	

Table 5.1: Group cwatsets in Q_4 with $k = 4$ elements

Here we introduce yet another notion which is suitable for studying cwatsets. A *hypergraph* is a pair $\mathcal{H} = (\Omega, E)$, where Ω is a (finite) set and E is a family of subsets of Ω. The set Ω, which we will identify with $\mathbf{N}_n$, is the set of *vertices* of $\mathcal{H}$, while elements of E are called *hyperedges*. Since Ω is fixed, $\mathcal{H}$ is uniquely determined by E, and we can write $\mathcal{H} = \mathcal{H}(E)$; if no misunderstanding can arise, we will use the same notation for $\mathcal{H}$ and E, regarding $\mathcal{H}$ as a set of subsets of $\mathbf{N}_n$. In particular, each cwatset determines a hypergraph: according to the notation introduced in Section 3, it has k_i hyperedges of size i, where $i = 0, \ldots, n$, and $\sum_{i=0}^{n} k_i = k$. (See Table 5.1 for some examples.)

Two hypergraphs $\mathcal{H}_1 = \mathcal{H}(E_1)$ and $\mathcal{H}_2 = \mathcal{H}(E_2)$ on $\Omega = \mathbf{N}_n$ are *isomorphic* if there is some $g \in S_n$ such that $A \in E_1$ if and only if $A^g \in E_2$. It follows from Proposition 5.4(a) that two cwatsets C_1 and C_2 are similar if and only if the corresponding hypergraphs $\mathcal{H}(C_1)$ and $\mathcal{H}(C_2)$ are isomorphic. Thus the classification of cwatsets up to similarity is equivalent to the classification of hypergraphs up to isomorphism.

As mentioned in the Introduction, we aim to answer two questions posed in [18]. We have (in effect) already answered the second question: if $k \leq 2^n$ and k divides $2^n n!$, does Q_n necessarily contain cwatsets of order k ? The results in Section 4 give a negative answer, both for this and for the more general question about the existence of automorphic subsets. The first question posed in [18] involves further concepts, which we will discuss in the next section.

6. Cyclic cwatsets

In addition to group cwatsets, Sherman and Wattenberg [18] defined another simple class of cwatsets as follows: take any $g \in S_n$ and $f \in V$, and let $C = C(g,f) = \{f_1, f_2, \ldots\} \subseteq V$, where $f_1 = f$ and $f_l = (f_{l-1})^g + f$ for $l \geq 2$. They proved that C is a cwatset, called a *cyclic cwatset.*

Example 6.1. We repeat their example for $n = 3$: taking $g = (1,2,3) \in S_3$ and $f = 100 \in V$, we have $C((1,2,3),100) = \{100, 110, 111, 011, 001, 000\}$.

The following result is the analogue of Theorem 5.2 for the special case of cyclic cwatsets.

Proposition 6.1. *A subset $C \subseteq V$ is a cyclic cwatset if and only if there is a cyclic subgroup $S \leq \mathcal{E}_n$ such that $C = 0^S$.*

Proof. Given a cyclic cwatset $C = C(g,f) = \{f_1, f_2, \ldots\}$, let S be the cyclic subgroup $\langle\sigma\rangle$ of $\mathcal{E}_n$ generated by $\sigma = (g,f)$. Then $f_1 = f = 0^\sigma$, and $f_l = f_{l-1}^\sigma$ for all $l \geq 2$, so C is the orbit of S containing 0. Conversely, if $S = \langle\sigma\rangle$ for some $\sigma = (g,f) \in \mathcal{E}_n$, then 0^S is the cyclic cwatset $C(g,f)$. □

For instance, the cyclic cwatset $C(g,f)$ considered in Example 6.1 is the orbit of the cyclic subgroup $S \leq \mathcal{E}_3$ generated by the element $\sigma = (g,f)$, where $g = (1,2,3)$ and $f = 100$.

Proposition 6.2. *If $S = \langle\sigma\rangle \leq \mathcal{E}_n$ and $\varphi(\sigma) = g \in S_n$, then $|S| = m$ or $2m$ where m is the order of g.*

Proof. The epimorphism $\varphi : \mathcal{E}_n \to S_n$, $(g,f) \mapsto g$ restricts to an epimorphism $\varphi|_S : S \to \tilde{S}$, where $\tilde{S} = \langle g\rangle$ has order m. Now $\ker(\varphi|_S) = S \cap V$ is a cyclic subgroup of V, so it has order $\varepsilon = 1$ or 2, and hence $|S| = \varepsilon|\tilde{S}| = m$ or $2m$. □

Corollary 6.3. (Sherman and Wattenberg [18]) *Let C be a cyclic cwatset $C(g,f)$, and let $k = |C|$. Then k divides $2m$, where m is the order of g.*

Proof. The proof of Proposition 6.1 implies that C is an orbit of $S = \langle\sigma\rangle$, where $\sigma = (g,f)$. The result now follows from Corollary 5.3 and Proposition 6.2. □

Example 6.2. We look for the smallest dimension of a noncyclic cwatset. One can check that all cwatsets of dimension $n \leq 3$ are cyclic. Now let $n = 4$ and

$$C = \{0000, 0010, 0011, 0100, 0110, 0111, 1000, 1001, 1011, 1100, 1101, 1111\}.$$

The graph $\Gamma_1 = \Gamma_1(C)$ generated by C is shown in Figure 6.1.

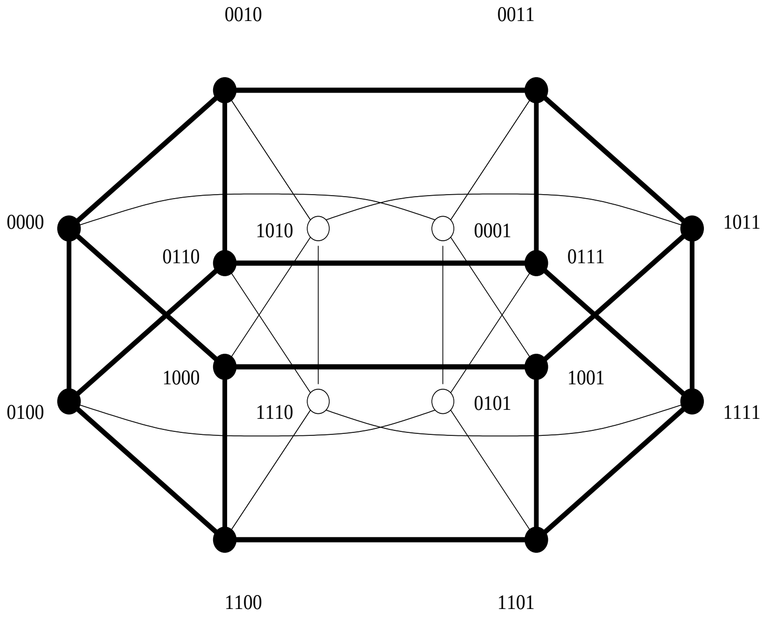

Figure 6.1

We note the following properties:

- Γ_1 is a hexagonal prism, so $\mathrm{Aut}(\Gamma_1) \cong D_6 \times S_2$ where D_6 denotes the dihedral group of order 12, the symmetry group of a hexagon; in fact $\mathrm{Aut}(\Gamma_1) \leq \mathrm{Aut}(\Gamma_i)$ for $i = 2, 3, 4$, so if $\Gamma = \Gamma(C)$ then $G = \mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \cong D_6 \times S_2$, a group of order 24.

- The group $H = \mathrm{Stab}(C)$ contains an automorphism $\sigma = (e, 0100)$ with no fixed points.

- The 'upper' and 'lower' subgraphs of Γ_1, lying in the hyperplanes $v_2 = 0$ and $v_2 = 1$ of Q_4, are two hexagons transposed by σ.

- The six vertices of each hexagon form an automorphic subset of its hyperplane Q_3, isomorphic to the subset in line 9 of Table 3.1 (see also Example 6.1)

- $H \cong \overline{H} \cong G \cong D_6 \times S_2$.

Thus C is the orbit of H on V containing 0000, so it is a cwatset. However, $D_6 \times S_2$ has no cyclic subgroups of order 12 (its elements have orders $1, 2, 3$ and 6), so C is not the orbit of any cyclic subgroup of $\mathcal{E}_4$, and is therefore not a cyclic cwatset.

This cwatset C was found by J. Kerr [14], using a computer. Our input is the proof that C is a non-cyclic cwatset, and the visual interpretation. We will return to this example later.

Example 6.3. Here we consider another example from [14]. Again let $n = 4$, but now let

$$C = \{0000, 0011, 0110, 1111, 1100, 1001\}.$$

To illustrate various techniques presented in this paper, we will treat this example in two different ways. In particular, we will show that C is cyclic.

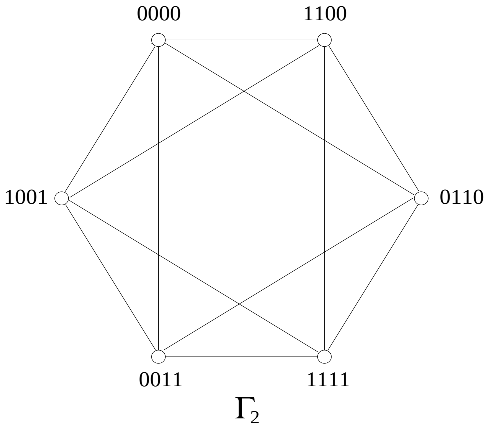

Figure 6.2

First we consider the hypergraph $\mathcal{H}(C) = \{\emptyset, \{3,4\}, \{2,3\}, \{1,2,3,4\}, \{1,2\}, \{1,4\}\}$. The vertices of weight 2 generate a quadrilateral, with automorphism group $H_0 \cong D_4$ of order 8. It follows that

$$k = 6, \quad r = \frac{n!}{|H_0|} = 3, \quad b = \frac{2^n r}{k} = 8 \quad \text{and} \quad |H| = \frac{2^n n!}{b} = 48.$$

Figure 6.2 shows the graph $\Gamma_2 = \Gamma_2(C)$, and we see from this that $|G| = 48$. Note that $|\overline{H}_0| = 8$, and hence $|\overline{H}| = 48$.

Secondly, we consider the subset $X = \{0101, 0110, 0011, 1010, 1001, 1100\}$ in Example 3.2. If $f = 0101 \in V$ then the automorphism $\sigma = (e, f)$ of Q_4 satisfies $X^\sigma = X + f = C$, so X and C are similar and have the same group-theoretic properties. In particular, H is the symmetry group $S_4 \times S_2$ of an octahedron. This has a cyclic subgroup $C_3 \times S_2 \cong C_6$ which permutes the six vertices regularly, so C is a cyclic cwatset (correcting the claim in [14]). In fact, $C = C(g, f')$ where $g = (1,3,2)(4) \in S_4$ and $f' = 0011 \in V$.

So far, we have met two classes of cwatsets: group cwatsets and cyclic cwatsets. Further examples can be constructed using the direct sum operation $\oplus$. First, we give a simple illustration.

Example 6.4. Let $C_1 = \{0000, 0100\}$ and $C_2 = \{0000, 0010, 0011, 1011, 1001, 1000\}$. Clearly these are both 4-dimensional cwatsets, contained in the subspaces $v_1 = v_3 = v_4 = 0$ and $v_2 = 0$ of V. If C is the cwatset in Example 6.2, then every $c \in C$ has a unique representation of the form $c = c_1 + c_2$, where $c_i \in C_i$. We therefore write $C = C_1 \oplus C_2$, the direct sum of C_1 and C_2.

We now give the general definition of a direct sum of cwatsets. If I is any d-element subset of $\mathbf{N}_n$, then by choosing a bijection $\mathbf{N}_d \to I$ one can embed Q_d in Q_n; its vertices form the subspace $\mathcal{P}(I)$ of V $(= \mathcal{P}(\mathbf{N}_n))$ defined by the equations $v_i = 0$ for all $i \notin I$. In particular, any d-dimensional cwatset $C \subseteq Q_d$ can be embedded in Q_n in this way.

More generally, if $\mathbf{N}_n = I_1 \dot\cup \cdots \dot\cup I_m$ is a partition of $\mathbf{N}_n$ into nonempty disjoint subsets I_i with d_i elements, then we have a decomposition

$$V = \mathcal{P}(I_1) \oplus \cdots \oplus \mathcal{P}(I_m)$$

of V as a direct sum of d_i-dimensional subspaces $\mathcal{P}(I_i)$, each defined by setting coordinates from $\mathbf{N}_n \setminus I_i$ equal to 0. If C_i is a d_i-dimensional cwatset for each $i = 1, \ldots, m$, we can regard it as a subset of $\mathcal{P}(I_i)$, and we can form the *direct sum*

$$C = C_1 \oplus \cdots \oplus C_m \subseteq V,$$

consisting of the elements $c = c_1 + \cdots + c_m$ where $c_i \in C_i$; this representation of c is unique, so $|C| = |C_1| \ldots |C_m|$. For instance, the decomposition $C = C_1 \oplus C_2$ in Example 6.4 arises from using the partition $\mathbf{N}_4 = \{2\} \dot\cup \{1,3,4\}$ to embed Q_1 and Q_3 in Q_4.

A more restricted definition of the direct sum of cwatsets was introduced by Sherman and Wattenberg in [18], taking $I_1, \ldots, I_m$ to be consecutive subintervals of $\mathbf{N}_n$; by permuting coordinates, they then obtain the decompositions considered above.

Proposition 6.4. *Any direct sum of cwatsets is a cwatset.*

Proof. Let $C = C_1 \oplus \cdots \oplus C_m \subseteq V$, as above. Since each C_i is a cwatset it contains the zero element of Q_{d_i}, so C contains their sum, the zero vector of V. The embeddings of $Q_{d_1}, \ldots, Q_{d_m}$ in Q_n embed $\mathcal{E}_{d_1}, \ldots, \mathcal{E}_{d_m}$ as subgroups which generate their direct product in $\mathcal{E}_n$. Let $H_i = \mathrm{Stab}(C_i) \leq \mathcal{E}_{d_i}$, and let $H = H_1 \times \cdots \times H_m \leq \mathcal{E}_n$. Since each C_i is an orbit of H_i, it follows that C is an orbit of H, so it is an automorphic subset and hence a cwatset by Theorem 5.2. □

In Examples 6.2 and 6.4 we considered a cwatset which is neither a group nor cyclic, though it is a direct sum of two cyclic cwatsets (one of which is also a group). Since any direct sum of group cwatsets is another group cwatset, the most general direct sum of group and cyclic cwatsets has the form

$$C = A \oplus C_1 \oplus \cdots \oplus C_m,$$

where A is a group and each C_i is a cyclic cwatset. Sherman and Wattenberg [18, p. 113], ask whether every cwatset has this form. To the best of our knowledge, this question is still open. We will give a negative answer, showing that there are infinitely many cwatsets which are not direct sums of groups and cyclic cwatsets.

Theorem 6.5. *Suppose that w and n are integers such that $0 < w < n$, and there are distinct odd primes p and q dividing $\binom{n}{w}$ with $p + q > n$. Then there exists a cwatset $C \subseteq Q_n$ with $\binom{n}{w}$ elements, which is not a direct sum of groups and cyclic cwatsets.*

Proof. Let B be the set of all vectors of weight w in Q_n, where w and n satisfy the hypotheses of the theorem, and let $C = B + b$ for some $b \in B$. Since B is an orbit of S_n (the stabiliser of 0 in $\mathcal{E}_n$), C is an orbit of a conjugate of S_n (the stabiliser of b), so C is an automorphic subset; since C contains $b+b=0$, it is a cwatset by Theorem 5.2. We have $|C|=|B|=\binom{n}{w}$, divisible by p and q.

Now suppose that C has a direct sum decomposition $C=A\oplus C_1\oplus\cdots\oplus C_m$, where A is a group and each C_i is a cyclic cwatset. Then $|C|=|A|\cdot\prod_i|C_i|$, with $|A|$ a power of 2, so there must exist i and j such that p divides $|C_i|$ and q divides $|C_j|$. If $i=j$ then since C_i is cyclic, $\mathcal{E}_n$ contains an element of order divisible by pq, and hence its epimorphic image S_n contains commuting elements g and h of orders p and q. If $i\neq j$ then the definition of the direct sum implies that C_i and C_j are isomorphic to cwatsets in Q_d and Q_e where $d+e\leq n$; since C_i and C_j are cyclic, S_d and S_e contain elements of orders p and q, so S_n (which contains $S_d\times S_e$) again contains commuting elements g and h of orders p and q. In either of these two cases, g must have a cycle of length p on either the fixed-points or the q-cycles of h in $\mathbf{N}_n$, giving $p+q\leq n$ or $pq\leq n$ respectively. Both of these contradict our hypothesis that $p+q>n$, so C does not have a decomposition of the given form. □

Example 6.5. The integers $n=6$ and $w=2$ satisfy the conditions of Theorem 6.5, with $p=3$ and $q=5$, so there is a 6-dimensional counterexample with $|C|=\binom{6}{2}=15$; similarly one can take $n=7$ and $w=2$, with $p=3$, $q=7$ and $|C|=21$.

Lemma 6.6. *There are infinitely many pairs of integers w and n which satisfy the hypotheses of Theorem* 6.5.

Proof. There are infinitely many primes p. By Bertrand's Postulate (a theorem of Chebyshev, see [10, §22.3 and notes for Ch. XXII]), if $p>3$ there is a prime q such that $p<q<2p-2$. Thus there exist infinitely many pairs of primes p and q such that $2<p<q<2p-1$. Taking $w=p-1$ and $n=q$ we then have $p+q>n$. Since $\max(w,n-w)=\max(p-1,q-p+1)<p<q\leq n$ we have $pq\mid\binom{n}{w}$, so w and n satisfy the required hypotheses. □

This, together with Theorem 6.5, yields infinitely many cwatsets C giving negative answers to Sherman and Wattenberg's question. For instance, one can take $p=5$ and $q=7$, giving $w=4$ and $n=7$, so that $|C|=35$.

Acknowledgements. Our interest in cwatsets originated in the discussion of this notion by the second and third authors in 1994 in Newark, when M. Klin visited the Department of Mathematical Sciences, University of Delaware. This paper was begun in January 1997, when G. A. Jones and F. Lazebnik were guests of the Department of Mathematics and Computer Science, Ben-Gurion University of the Negev. The kind hospitality of both universities is gratefully acknowledged. We thank G. Sherman for sending us a copy of Kerr's report [14], and for his continued and stimulating interest in our work, M. Muzychuk for showing us a proof of Lemma 4.4, and I. J. Leary for some helpful discussions concerning group cohomology.

References

[1] Atkins, J. E.; Sherman, G. J.: *Sets of typical subsamples.* Statistics and Probability Letters **14** (1992), 115–117.

[2] Brown, K. S.: *Cohomology of Groups.* Springer-Verlag, New York 1982.

[3] Burnside, W.: *On some properties of groups of finite order.* Proc. London Math. Soc. **33** (1900), 162–185.

[4] Burnside, W.: *Theory of Groups of Finite Order.* Second edition, Cambridge University Press, Cambridge 1911.

[5] Cameron, P. J.: *Permutation groups and finite simple groups.* Bull. London Math. Soc. **13** (1981), 1–22.

[6] Dixon, J. D.; Mortimer, B.: *Permutation Groups.* Springer, Berlin 1996.

[7] Dress, A. W. M.; Klin, M. H.; Muzichuk, M. E.: *On p-configurations with few slopes in the affine plane over F_p and a theorem of W. Burnside's.* Bayreuther Math. Schr. **40** (1992), 7–19.

[8] Harary, F.: *Exponentiation of permutation groups.* Amer. Math. Monthly **66** (1959), 572–575.

[9] Harary, F.: *Graph Theory.* Addison-Wesley, Reading 1969.

[10] Hardy, G. H.; Wright, E. M.: *Introduction to the Theory of Numbers.* Fifth edition, Oxford University Press, Oxford 1979.

[11] Hartigan, J. A.: *Using subsample values as typical values.* Amer. Stat. Assoc. J. **64** (1969), 1303–1317.

[12] Huppert, B.: *Endliche Gruppen I.* Springer-Verlag, Berlin 1967.

[13] Jones, G. A.; Klin, M.; Lazebnik, F.: *Introduction to the theory of automorphic subsets of the n-dimensional cube.* Preprint No. 309, Faculty of Mathematical Studies, University of Southampton 1998.

[14] Kerr, J.: *Hypergraph Representations and Orders of Cwatsets.* Rose-Hulman Institute of Technology, Technical Report 93-02, 1993.

[15] Lint, J. H. van; Wilson, R. M.: *Course in Combinatorics.* Cambridge University Press, Cambridge 1992.

[16] Rotman, J. J.: *Introduction to the Theory of Groups.* Fourth edition, Springer-Verlag, Berlin 1995.

[17] Sherman, G. J.: *Confidence intervals from groups.* Math. Mag. **65** (1992), 118–122.

[18] Sherman, G. J.; Wattenberg, M.: *Introducing … cwatsets!* Math. Mag. **67** (1994), 109–117.

[19] Wielandt, H. W.: *Finite permutation groups.* Academic Press, New York 1964.

[20] Wielandt, H. W.: *Mathematische Werke – Mathematical Works I: Group Theory.* (Eds. B. Huppert and H. Schneider), de Gruyter, Berlin 1994.

Received October 20, 1998