Extremal solutions of an inequality concerning supports of permutation groups and punctured Hadamard codes

András Pongrácz*

June 11, 2020

Abstract

If S is the degree of a permutation group and s is the maximum degree of its elements, then $S \leq 2s-2$. We show that this inequality is sharp for some permutation group if and only if s is a power of 2, and then there is exactly one such permutation group up to isomorphism. The unique example is an elementary Abelian 2-group that arises from a punctured Hadamard code. Then we discuss the solutions of $S = 2s-3$ and $S = 2s-4$.

2010 Mathematics Subject Classification: 94B05, 94B65, 20B10
Key words: code, anticode, support, maximum distance

1 Introduction

In this paper, a basic question is investigated: given a finite permutation group G, how large can the support of G be compared to the supports of the elements of G? The cardinality of the support of G is denoted by S, and the biggest set we obtain as a support of an element has size s.

The dual notion $\mu(G)$, the minimum degree of non-identity elements, is a central notion in permutation group theory. It was particularly

*This work is supported by the EFOP-3.6.2-16-2017-00015 project, which has been supported by the European Union, co-financed by the European Social Fund. The paper was also supported by the National Research, Development and Innovation Fund of Hungary, financed under the FK 124814 and PD 125160 funding schemes, the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, and by the ÚNKP-18-4 and ÚNKP-19-4 New National Excellence Programs of the Ministry of Human Capacities.

well-studied for primitive permutation groups, see [9] for a recent improvement on the lower bound. Often the results are phrased for the *fixity* $S - \mu(G)$ of G, i.e., the maximum number of fixed points of a non-identity element in G, see [11, 13, 14].

In a recent paper [1], an upper estimation for S in terms of s was applied to obtain a theoretical result about the asymptotic probability that a finite structure over a given finite relational language has an automorphism group isomorphic to some permutation group H, provided that the automorphism group contains a given permutation group G. Surprisingly, only finitely many H occurs with positive asymptotic probability, and the probability for any such H converges to a rational number. This recent result is an extension of the well-known theorem that, given a finite relational vocabulary, asymptotically almost all finite structures are rigid; see [6, 7, 5, 8] for further details. In order to compute the family of possible H corresponding to a given G, it is important to refine the upper bound of S in terms of s. The first result provides the sharpest estimation and classifies all permutation groups where equality holds.

Construction 1.1. *We define an action of $\mathbb{Z}_2^n$ on $2n$ elements, and refer to it as the natural action in the sequel. We partition the $2n$-element set into n pairs, and fix a one-to-one correspondence between the set of n coordinates of $\mathbb{Z}_2^n$ and the set of n pairs. A vector in $\mathbb{Z}_2^n$ switches the elements of each pair that corresponds to a coordinate where the entry of the vector is 1, and acts identically on the remaining pairs.*

Definition 1.2. *The punctured Hadamard code H_k for $k \geq 1$ is the binary linear code generated by the rows of the matrix obtained by writing the numbers from 1 to $2^k - 1$ in binary in columns in increasing order from left to right. We refer to the row vectors in this matrix as the standard basis $\{e_1, \cdots, e_k\}$ of H_k.*

Theorem 1.3. *Let G be a finite permutation group with support of size S and no singleton orbits. Let $\max_{g \in G} |\operatorname{supp}(g)| = s$. Then $S \leq 2s - 2$, and equality holds if and only if $s = 2^k$ for some $k \geq 1$, and G is isomorphic to the natural permutation group action of the punctured Hadamard code H_k with parameters $[2^k - 1, k, 2^{k-1}]_2$.*

The proof relies on the following classification of punctured Hadamard codes up to equivalence in terms of the maximum distance of the code. Following standard terminology [15], two binary linear codes are equivalent if one can be obtained from the other by permuting the coordinates. Throughout this paper, the distance of two codewords in a code is the Hamming distance, and the weight $w(c)$ of a codeword c is the distance of c from the all zero codeword. We only study linear codes, thus the maximum distance D equals to the maximum weight in the code.

Proposition 1.4. *Let $n \in \mathbb{N}$ and assume that a binary linear code C of length n has maximum distance $D \leq (n+1)/2$. Assume that all coordinates of the code are essential in the sense that some codeword is 1 in that position. Then $D = (n+1)/2 = 2^{k-1}$ for some $k \geq 1$, and C is equivalent to the punctured Hadamard code with parameters $[2^k - 1, k, 2^{k-1}]_2$.*

Furthermore, we discuss the situation when $S = 2s - \ell$ for some small values of ℓ.

Construction 1.5. *The group S_3 has an intransitive action of degree five. It can be obtained from the standard degree three action by adjoining a pair of new elements to the underlying set. The pair is point-wise fixed by elements of A_3 and switched by the other three elements.*

Proposition 1.6. *With the notation in Theorem 1.3, if $S = 2s - 3$, then G is isomorphic to the action of S_3 described in Construction 1.5, or the standard action of S_3 or A_3.*

In the following constructions, we make use of the idea of repeating a coordinate or a set of coordinates in a code C. Repeating the i-th coordinate means that we increase the length of the code by one by introducing a new coordinate, and for all codewords $c \in C$ the value of c in the new coordinate is the same as the value of c in the i-th coordinate. By executing this procedure simultaneously on several coordinates, we can also repeat a set of coordinates. For example, if we repeat all coordinates k times, then the distance of any pair of codewords is multiplied by k. This is a basic idea in the theory of error-correcting codes, as it is the simplest way to increase the error correcting number of a code [3]. If any two codewords $c, c' \in C$ has the same value in the i-th and j-th coordinates for some i, j, we say that the i-th and j-th coordinates are equivalent (with respect to C). Repeated coordinates are equivalent.

Construction 1.7. *Let H_k be the punctured Hadamard code with parameters $[2^k - 1, k, 2^{k-1}]_2$, and let $m \leq k$. We define $H_{k \times m} := H_k \times H_m$, i.e., producing all concatenations of codewords in H_k and H_m. The code $H_{k|m}$ can be obtained from H_k by picking $2^m - 1$ coordinates such that the restriction of H_k to those is isomorphic to H_m, and repeating those coordinates simultaneously. It is easy to see that the first $2^m - 1$ coordinates is always a good choice if we represent the Hadamard code H_k as in Definition 1.2.*

Example 1.8. *The standard generating matrix of H_3 and H_2 according to Definition 1.2 are*

$$M_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

The restriction of H_3 to the firs $2^2 - 1 = 3$ coordinates yields H_2 (every codeword in H_2 occurs twice as a restricted codeword). Thus we obtain a generating matrix of $H_{3|2}$ from M_3 by copying the first three columns and add them to the right end of the matrix:

$$M_{3|2} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

We provide a generating matrix of $H_{3\times 2}$, as well:

$$M_{3\times 2} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Binary linear codes with maximum distance D and length n such that $D = \frac{n}{2} + 1$ appears to have a more complicated description than those with the property $D = \frac{n+1}{2}$, see Proposition 1.4. Clearly, $H_{k|m} \leq H_{k\times m}$, and any binary linear code C such that $H_{k|m} \leq C \leq H_{k\times m}$ has length $n = 2^k + 2^m - 2$ and maximum distance $D = 2^{k-1} + 2^{m-1} = \frac{n}{2} + 1$. However, this list is not exhaustive. For $m = k$, let C be a code generated as a vector space over $\mathbb{Z}_2$ by $H_{m|m}$ and any vector that is the characteristic vector of a subset of coordinates of H_m in the first copy and the characteristic vector of the complement of the subset in the second copy. Then C has the same length and maximum distance as $H_{m|m}$. Indeed, every codeword in $C \setminus H_{m|m}$ has weight $2^m - 1 = D - 1 < D$.

Interestingly, such lower bounds for the maximum distance of linear codes have not been studied yet. Few results are concerned with lower estimation of the maximum distance, see for example [2]. For an introduction to linear codes see [15, 3, 12].

We have the following partial results about codes with $D = \frac{n}{2} + 1$.

Proposition 1.9. *Let $C \leq (\mathbb{Z}_2, +)^n$ be a binary linear code all of whose coordinates are essential such that $n = 2$ or $4 \mid n$. Let D be the maximum weight of C, and assume that $D = \frac{n}{2} + 1$. Then $n = 2^k$ with $k \geq 1$, and C is one of the codes $H_{k\times 1}$, $H_{k|1}$ in Construction 1.7.*

Theorem 1.10. *Let $n \in \mathbb{N}$ and assume that a binary linear code C of length n has maximum distance $D = \frac{n}{2} + 1$. Assume that all coordinates of the code are essential in the sense that some codeword is 1 in that position. Then there exist $1 \leq m \leq k$ such that $n = 2^k + 2^m - 2$, $D = 2^{k-1} + 2^{m-1}$, and $H_{k|m}$ is a subcode of C.*

The full classification of codes with maximum distance $D = \frac{n}{2}+1$ is a challenging problem, see the follow-up paper [10]. Fortunately, the above partial results are sufficiently strong to classify permutation groups with $S = 2s - 4$.

Construction 1.11. *The group D_4 has an intransitive action with degree eight and maximum degree of elements six. It can be obtained from the standard degree four action on a square by adjoining two pairs of new elements to the underlying set. The pairs are point-wise fixed by elements in the center, and reflections to the diagonals switch both pairs. Both reflections to the perpendicular bisectors switch the first pair and act identically on the second, and the order four rotations switch the second pair and act identically on the first.*

The index two subgroup $G_{2,3,3} \leq S_3 \times S_3$ consists of all pairs of permutations of the same parity. It acts on the union of three orbits, one of which has size two and the others have size three. The action on the two 3-element orbits is the intransitive action of the direct product, and the pair is switched exactly by the permutations that are odd in both coordinates. The six element diagonal subgroup $D_{2,3,3} \leq G_{2,3,3}$ consists of those elements that act the same way on the two 3-element orbits. Then $D_{2,3,3}$ and $G_{2,3,3}$ both have degree eight and the maximum degree of elements is six.

For transitive groups of degree four we have $S = s = 4$. These are S_4, A_4, D_4, and the Cayley actions of the 4-element cyclic group and the Klein group.

Besides these particular permutation groups, there are two infinite families of examples. The first one consists of the natural actions of binary linear codes C with length n and maximum distance $D = \frac{n}{2} + 1$, see [10]. The other family of permutation groups consists of an action of H_k for all $k \geq 2$. This can be constructed by compressing the underlying set in the natural action of H_k, replacing three pairs of points by four new elements. We pick three coordinates so that the restriction of H_k to these is isomorphic to H_2, which is isomorphic to the Klein group as an abstract group. Now replace the action of H_2 on the restriction to the three pairs by the Cayley action of the Klein group. (The compressed action of H_2 is the Cayley action of the Klein group, which already appeared in the list above.) This permutation group has degree $2^{k+1} - 4$ and the maximum degree of elements is 2^k.

Theorem 1.12. *With the notation in Theorem 1.3, if $S = 2s - 4$, then G is isomorphic to a permutation group in Construction 1.11.*

2 Binary linear codes and the extremal permutation groups

Lemma 2.1. *Let G be a finite permutation group with no singleton orbits. Denote $\max_{g \in G} |\operatorname{supp}(g)| = s$ and $|\operatorname{supp}(G)| = S$. Let n_i denote the number of orbits of size i. Then*

1. $S \leq 2s - 1 - \sum_{i=3}^{\infty} (i-2)n_i$,
2. *and if $S = 2s - \ell$ for some $\ell \in \mathbb{N}$, then $n_i = 0$ for all $i > \ell$.*
3. *In particular, $S \leq 2s - 2$.*

Proof. Double counting yields $\sum_{i=2}^{\infty} i n_i = S$. As G is a finite permutation group with no singleton orbits, the average number of fixed points of its elements is $\sum_{i=2}^{\infty} n_i$ by Burnside's lemma. The identity element has S fixed points, and all other group elements have at least $S - s$ fixed points. Thus

$$\sum_{i=2}^{\infty} n_i \geq \frac{1}{|G|}(S + (|G| - 1)(S - s)) = S - \left(1 - \frac{1}{|G|}\right) s$$
$$\sum_{i=2}^{\infty} 2n_i \geq 2S - 2s + \frac{2}{|G|} s$$

Subtracting both sides from $\sum_{i=2}^{\infty} i n_i = S$ yields the first item as follows:

$$\sum_{i=3}^{\infty} (i-2)n_i \leq -S + 2s - \frac{2}{|G|} s$$
$$S \leq 2s - \frac{2}{|G|} s - \sum_{i=3}^{\infty} (i-2)n_i < 2s - \sum_{i=3}^{\infty} (i-2)n_i$$
$$S \leq 2s - 1 - \sum_{i=3}^{\infty} (i-2)n_i$$

Putting $\ell = 2s - S$ we have $\ell \in \mathbb{N}$. Thus if there exists an $i \geq \ell + 2$ such that $n_i \neq 0$, then $S < 2s - \ell$. Note that as $S = 2s - \ell$, we have $S \equiv \ell \pmod 2$.

Assume that ℓ is odd, or equivalently, S is odd. Then it is impossible that all orbits have size 2 or $(\ell+1)$. Thus there must be an orbit of size $2 < k \leq \ell$. In particular, $\ell \neq 1$, and we obtain the third item of the lemma. Moreover, $\ell \geq 3$, thus the first item yields $\ell \geq 1 + \sum_{i=3}^{\infty}(i-2)n_i = 1 + (\ell-1)n_{\ell+1} + \sum_{i=3}^{\ell}(i-2)n_i$, where $\sum_{i=3}^{\ell}(i-2)n_i \geq 1$ as we observed. Hence, $\ell - 2 \geq (\ell-1)n_{\ell+1}$, and thus $n_{\ell+1} = 0$.

Finally, assume that ℓ is even, or equivalently, S is even. If all orbits have size 2 or $(\ell+1)$, then there must be an even number of the latter. Hence, if $n_{\ell+1} \neq 0$, then $n_{\ell+1} \geq 2$. The formula in the first item yields $\ell \geq 1+\sum_{i=3}^{\infty}(i-2)n_i = 1+(\ell-1)n_{\ell+1}+\sum_{i=3}^{\ell}(i-2)n_i \geq 1+2(\ell-1) = 2\ell-1$, and consequently, $\ell \leq 1$, a contradiction. Hence, if $n_{\ell+1} \neq 0$, then there must be some $2 < k \leq \ell$ such that $n_k \neq 0$, in which case we proceed as before: $\ell \geq 1+\sum_{i=3}^{\infty}(i-2)n_i = 1+(\ell-1)n_{\ell+1}+\sum_{i=3}^{\ell}(i-2)n_i \geq 2+(\ell-1)n_{\ell+1}$, and $\ell - 2 \geq (\ell-1)n_{\ell+1}$ yields $n_{\ell+1} = 0$. □

Proof of Proposition 1.4. Because every coordinate is essential in C, the average weight of codewords in C is $\frac{n}{2}$. Since in any nontrivial linear code the average weight is strictly smaller than the maximum weight, we have $\frac{n}{2} < D \leq \frac{n+1}{2}$, and consequently $D = \frac{n+1}{2}$.

We prove the assertion by induction on n. Clearly, the only code with one essential coordinate is H_1, so assume that $n \geq 2$ and the statement holds for smaller values of the length. Puncture the code by omitting the coordinates in the support of a maximum weight codeword c. Let C' be the code obtained and $\varrho : C \to C'$ the restriction homomorphism. Clearly, every codeword $c' \in C$ has at most as many ones outside the support of c as inside, as otherwise $w(c+c') > D$. Thus C' has length $n' = n - D = \frac{n-1}{2}$ and maximum weight at most $\frac{D}{2} = \frac{n+1}{4} = \frac{n'+1}{2}$, and all coordinates of C' are essential. Hence, by the induction hypothesis $C' \cong H_{k-1}$ for some $k \geq 2$. In particular, the dimension of C' is $k-1$ and the length is $2^{k-1}-1 = \frac{n-1}{2}$, which yields $n = 2^k - 1$, and then $D = \frac{n+1}{2} = 2^{k-1}$.

Let C_0 be the code generated by the ϱ-preimage of a basis of C' and c. Then C_0 has the same properties as those of C in the proposition. Moreover, the kernel of $\varrho \restriction_{C_0}$ is $\{0, c\}$, thus the dimension of C_0 is k.

Hence, the total weight of codewords in C_0 is $\frac{n}{2} \cdot 2^k = n2^{k-1}$, which yields $n2^{k-1} \leq (2^k-1)D = n2^{k-1}$, where the inequality is obtained by estimating the weight of all nonzero codewords in C_0 by D. Thus all nonzero codewords in C_0 have weight D.

Pick a basis $c_1, \ldots, c_k \in C_0$. The fact that every nonempty subsum

of $c_1 + \cdots + c_i$ has weight D for any given $i \leq k$ uniquely determines the weight of the intersection of the supports of any given subset $c_{i_1}, \ldots, c_{i_j}$ to be 2^{k-j}. Thus we can inductively rearrange the coordinates of C_0 so that the mapping $c_j \mapsto e_j$ for $j \leq i$ induces an isomorphism of the codes $\langle c_1, \ldots, c_i \rangle$ and the standard basis $\langle e_1, \ldots, e_i \rangle$ (see Definition 1.2), and then $C_0 \cong H_k$.

Assume that there is a maximum weight codeword $c \in C \setminus C_0$. Then the same argument yields that the intersection of the supports of $c, c_1, \ldots, c_k$ has weight $2^{k-(k+1)} = \frac{1}{2}$, a contradiction. Thus every codeword $c \in C \setminus C_0$ has weight at most $\frac{n-1}{2}$, making the average weight in C less than $\frac{n}{2}$, a contradiction. Hence, $C = C_0 \cong H_k$.

□

We mention an alternative way to end the proof. Once it is shown that all non-zero codewords of C_0 have the same weight D, i.e., C_0 is a so-called 1-weight code, we can refer to A. Bonisoli's famous theorem [4], which provides a classification to such codes. In particular, binary linear 1-weight codes are precisely those equivalent to the r-fold repetition of a punctured Hadamard code H_k for some $k, r \in \mathbb{N}$. By comparing the weight D and the length n of C_0, we have $r = 1$. We note that in the follow-up paper [10], the codes with $D = \frac{n}{2} + 1$ are described, and most of them are 2-weight codes or 3-weight codes.

Proof of Theorem 1.3. According to Lemma 2.1, we have $S \leq 2s - 2$ by item 3, and if equality holds, then all orbits are pairs by item 2. In such a permutation group, every element either switches a pair of elements in an orbit or fixes them both. Consider the natural action of $\mathbb{Z}_2^{s-1}$ on the $S/2 = s - 1$ pairs. We define a mapping $\varphi : G \to \mathbb{Z}_2^{s-1}$. Given a $g \in G$, let the i-th coordinate of $\varphi(g)$ be 1 iff the i-th pair is switched by g, and 0 otherwise. Then φ is an injective permutation group homomorphism. So we may identify G by a subgroup of $\mathbb{Z}_2^{s-1}$, i.e., G is a binary linear code with length $n = s - 1$.

Every codeword in G has weight at most $\frac{s}{2} = \frac{n+1}{2}$. Clearly, every coordinate is essential in the code, as every pair of points that forms an orbit of G is in the support of G, thus some group element switches them. Hence, the assertion follows from Proposition 1.4. □

3 Near-extremal permutation groups

Relaxing the inequality constraint of Theorem 1.3 does not necessarily lead to more examples. The condition $S = 2s - 3$ turns out to be more restrictive than $S = 2s - 2$.

Proof of Proposition 1.6. By Lemma 2.1 item 2, all orbits have size 2 or 3. Item 1 of Lemma 2.1 yields $n_3 \leq 2$. As S is odd, we have $n_3 = 1$. Hence, there is exactly one orbit X of size 3, and all other orbits are pairs. If there are no such pairs, then G acts transitively on X, and it is isomorphic to the Cayley action of the 3-element group or the standard action of S_3.

We may assume that the set of pairs is nonempty. Then the number of pairs is $\frac{S-3}{2} = s - 3$.

Let H be the restriction of G to the union of pairs. Note that H is a homomorphic image of G as an abstract group. The degree of H is $S' := S - 3 = 2s - 6$.

There exists a group element g that acts as a 3-cycle on X. By replacing g with g^2 if necessary, we may assume that g acts trivially on the pairs. Thus every $h \in H$ has a support of size at most $s' := s - 2$, as otherwise the element $h' \in G$ whose restriction is h or the element $h'g \in G$ has a support of size greater than s, since the restriction of both of these elements to X cannot be identical. But then H is a permutation group with $S \geq 2s' - 2$. Hence, by Theorem 1.3, the restriction is the natural action of H_k for some $k \geq 1$, and $s' = s - 2 = 2^k$

Let $\varphi : G \to S_3$ be the group homomorphism obtained by restricting permutations to X, and let N be the preimage of A_3. Given a permutation in N, it can be multiplied by a power of g so that the restriction to X is a 3-cycle, and it is unaltered on the pairs. Thus all such group elements can move at most $s-3$ points in the union of pairs, which is less than s'. Thus the restriction of any permutation in N to the union of pairs is the trivial element of the Hadamard code, and then $N \cong A_3$ with the standard action on X and the trivial one on the pairs. In particular, φ is injective. It is also surjective, otherwise every element of G would act trivially on the pairs. Hence, G is isomorphic to S_3 as an abstract group. As $H \cong H_k$ is also a homomorphic image of G, we have $k = 1$, so there is exactly one pair among the orbits. The action of $A_3 \leq S_3 \cong G$ was already described, and it is consistent with Construction 1.5. As some permutation in G has to switch the elements of the unique pair, it must be an element outside A_3. But then all of them have to act as a transposition on the pair as they can be obtained from each other by multiplication with a power of g, and then the permutation action is as described in Construction 1.5. □

Before solving $S = 2s - 4$, we note that the number 3 is special in Proposition 1.6, in the sense that there is a finite number of permutation groups with $S = 2s - 3$. Given a group G as in Theorem 1.3, the intransitive action of the direct product G^m on the union of m copies of the underlying set satisfies $S = 2s - 2m$. Similarly, the intransitive

action of $G^m \times S_3$ satisfies $S = 2s - 2m - 3$. Thus for any integer $\ell \geq 2$ and $\ell \neq 3$ there are infinitely many non-isomorphic permutation groups such that $S = 2s - \ell$.

Lemma 3.1. *Let $C \leq (\mathbb{Z}_2, +)^n$ be a binary linear code all of whose coordinates are essential such that $2 \mid n$. Let D be the maximum weight of C, and assume that $D = \frac{n}{2} + 1$. Assume that there is a coordinate such that every codeword with maximum weight is 1 in that coordinate. Then $n = 2^k$, and C is one of the codes $H_{k\times 1}$, $H_{k|1}$ in Construction 1.7.*

Proof. Let H be the code obtained by puncturing a coordinate of C where all maximum weight codewords are 1. Then $H \cong H_k$ for some Hadamard code H_k by Proposition 1.4. There are two possibilities: the kernel K of the homomorphism $\varphi : C \to H$ defined by the above restriction is either trivial or a 2-element subgroup.

If the kernel is trivial, then the φ-image of the codewords in C that are 0 in the punctured coordinate is an index 2 subgroup in $H \cong H_k$, thus it is generated by $k - 1$ independent codewords. There is exactly one coordinate such that all those $k - 1$ codewords in that coordinate is 0. Hence, in this case, the repetition of that coordinate in H yields C, so $C \cong H_{k|1}$.

If $|K| = 2$, then the nontrivial element in K is a codeword with only one nonzero coordinate, and $C \cong H \times K \cong H_{k\times 1}$. □

Proof of Proposition 1.9. If $n = 2$, then there are only two codes up to isomorphism with all coordinates essential, namely $H_{1|1}$ and $H_{1\times 1}$. Hence, assume that $4 \mid n$. Let $c \in C$ be a codeword of maximum weight $D = \frac{n}{2} + 1$. Given any other codeword $c' \in C$, there are at most as many ones in c' outside the support of c as inside, otherwise $w(c + c') > D$. Hence, there are at most $\frac{n}{4}$ ones in c' outside the support of c. Thus if we puncture the code by omitting the essential coordinates of c, then we obtain a code with length $n' := \frac{n}{2} - 1$ and maximum distance at most $\frac{n}{4} = \frac{n'+1}{2}$. The conditions of Theorem 1.3 apply to the punctured code, and consequently, it is isomorphic to H_k for some $k \geq 1$. In particular, all nonzero codewords in the punctured code has weight $\frac{n}{4}$, and then $w(c') \geq \frac{n}{2}$. Thus $w(c')$ is either $\frac{n}{2}$ or $\frac{n}{2} + 1$. If the support of some nonzero codeword in C is a subset of the support of any maximum weight codeword, then we are done by Lemma 3.1. Assuming that this is not the case, the weight of every nonzero codeword is either $\frac{n}{2}$ or $\frac{n}{2} + 1$. The parity homomorphism that maps every codeword to its weight (mod 2) is surjective, hence exactly half of the codewords have weight $\frac{n}{2} + 1$. The kernel of the parity homomorphism is a subgroup which consists of elements of weight 0 and $\frac{n}{2}$. In particular, not all coordinates are essential in this subgroup, as the average weight is less than half

the length. Pick a coordinate where all codewords of even weight is zero. As exactly half of the elements in C is one in that coordinate, the maximum weight codewords must be one there, and then we are done by Lemma 3.1. □

Proof of Theorem 1.10. Clearly, the length n must be even. We use induction on n, ranging through the even positive integers. By Proposition 1.9, we may assume that $n \equiv 2 \pmod 4$, and the statement holds for $n = 2$.

Now assume that $n \geq 6$, $n \equiv 2 \pmod 4$, and the assertion holds for all smaller even numbers. Let c be a maximum weight codeword. Puncture the code by omitting the essential coordinates of c. Let C' be the code obtained and $\varrho : C \to C'$ the restriction homomorphism. Then C' has length $n' = n - D = \frac{n}{2} - 1$, which is an even number less than n, and maximum weight D'. If D' were bigger than $\frac{n'}{2} + 1 = \frac{n+2}{4}$, then a codeword $c' \in C$ with maximum weight D' in the punctured code would have at most $\frac{n}{2}+1-D'$ essential coordinates in common with c, otherwise $w(c') > D$. Then $w(c + c') \geq 2 \cdot D' > 2 \cdot \frac{n+2}{4} = D$, a contradiction. As n' is even and the maximum distance in the punctured code is bigger than $\frac{n'}{2}$, we have $D' \geq \frac{n'}{2} + 1$. Hence, $D' = \frac{n'}{2} + 1$. By the induction hypothesis, $H_{k'|m'} \leq C'$ with some $1 \leq m' \leq k'$. Thus $n' = 2^{k'} + 2^{m'} - 2$, $D' = 2^{k'-1} + 2^{m'-1}$, and consequently, putting $k = k' + 1$ and $m = m' + 1$ we have $n = 2^k + 2^m - 2$ and $D = 2^{k-1} + 2^{m-1}$. Furthermore, the above calculation shows that any maximum weight codeword in C' is the restriction of some maximum weight codeword in C. In particular, every coordinate is covered by a maximum weight codeword in C.

Hence, by omitting all codewords from C whose restriction in the punctured code is not in $H_{k'|m'}$, the code obtained has the same length and maximum distance as C, and every coordinate is covered by a maximum weight codeword in the new code as well. Iterating this process for all maximum weight codewords, we obtain a new code C_0 that has the same properties, and whose restriction to the complement of any maximum weight codeword is a code isomorphic to $H_{k'|m'}$. We may also assume that the kernel of ϱ with any maximum weight codeword c is $\{0, c\}$, as the code generated by c and the ϱ-preimage of a basis of C' also has the above properties.

In particular, there exist pairs of equivalent coordinates in C_0, i.e., two coordinates such that every codeword has the same value in them. There cannot be triples of equivalent coordinates. Indeed, if every maximum weight codeword intersects such a given triple, then we obtain a contradiction by Lemma 3.1, as n is not a power of 2. If there is a maximum weight codeword that is all zero in the triple, then choosing

it as c and puncturing the code leads to $H_{k'|m'}$ with three equivalent coordinates, again a contradiction. Thus there are p pairs of equivalent coordinates in C_0 with $p \geq 1$, and some coordinates that are singleton equivalence classes, which we are going to refer to as singleton coordinates. As every coordinate is covered by a maximum weight codeword in C_0, the pairs of equivalent coordinates cannot coincide with those in any punctured code obtained by omitting coordinates of a maximum weight codeword in C_0. In particular, $p \geq 2^{m'}$.

Given any non-singleton coordinate, there is a maximum weight codeword $c \in C_0$ that is zero in that coordinate, as otherwise Lemma 3.1 leads to a contradiction. Hence, if a non-maximum weight codeword $c' \in C_0$ is one in any of the non-singleton coordinates, then $\varrho(c')$ is a maximum weight codeword in C', and then c' must have maximum weight in C_0, a contradiction. Thus non-maximum weight codewords $c' \in C_0$ are all zeros in the non-singleton coordinates. Let K be the restriction of C_0 to a set of coordinates X with $|X| = p$ that contains exactly one element from each of the p pairs of equivalent coordinates. Then K consists of the zero vector and all restrictions of maximum weight codewords in C_0. There are at least $2^{m'} + 1$ such restrictions: fixing a maximum weight codeword $c \in C_0$, $2^{m'}$ is obtained by the zero vector and maximum weight codewords different from c whose restriction to the complement of the support of c has maximum weight in $H_{k'|m'}$, and at least one further element is obtained as the restriction of c. As K is a 2-group, we have $|K| \geq 2^{m'+1}$. Clearly, every coordinate of K is essential, thus the average weight of codewords in K is $\frac{p}{2}$. As the punctured code corresponding to every maximum weight $c \in C_0$ is isomorphic to $H_{k'|m'}$, a code with exactly $2^{m'} - 1$ equivalent pairs of coordinates, we have that every maximum weight $c \in C_0$ intersects exactly $p - 2^{m'} + 1$ of the p equivalent pairs of coordinates of C_0. Thus the average weight of codewords in K is $\frac{|K|-1}{|K|}(p - 2^{m'} + 1) = \frac{p}{2}$. Rearranging the equality yields $|K| = 2 + \frac{2^{m'+1}-2}{p-2^{m'+1}+2}$. In particular, $p \geq 2^{m'+1} - 1$. The expression $2 + \frac{2^{m'+1}-2}{p-2^{m'+1}+2}$ is strictly monotone decreasing as a function of p for $p \geq 2^{m'+1} - 1$, thus its maximum is $2^{m'+1}$, the value attained at $p = 2^{m'+1} - 1$. Summarizing the estimations, we have $2^{m'+1} \leq |K| = 2 + \frac{2^{m'+1}-2}{p-2^{m'+1}} \leq 2^{m'+1}$, and consequently $p = 2^{m'+1} - 1 = 2^m - 1$ and $|K| = 2^{m'+1} = 2^m$. In particular, every maximum weight codeword in C_0 intersects exactly $p - 2^{m'} + 1 = 2^{m-1}$ of the p equivalent pairs of coordinates of C_0. Hence, the maximum weight in the code K is 2^{m-1}, and the length of K is $2^m - 1$. By Proposition 1.4, $K \cong H_m$.

If $m = k$, then $n = 2^{m+1} - 2 = 2p$. Thus C_0 is obtained from K by simultaneously repeating all coordinates, and then $C_0 \cong H_{m|m}$. Hence, we may assume that $k > m$. Then the number of singleton coordinates is $n - 2p = 2^k - 2^m > 0$. Note that $m \geq 2$ as n is not a power of 2.

Let $N \subseteq C_0$ be the set of non-maximum weight codewords. As these are exactly those elements of C_0 whose support is in the set of singleton coordinates Y, we have $N \leq C_0$.

We show that given any coordinate $y \in Y$, the number of equivalent coordinates in Y with respect to the code N is 2^m. By Lemma 3.1, there is a maximum weight codeword $c \in C_0$ such that y is not in the support of c. Then y is among the singleton coordinates of $C' = \varrho(C_0) \cong H_{k'|m'}$ corresponding to c. Let c' be the ϱ-preimage of a maximum weight codeword in C' whose support does not contain y. Such a codeword exists, as y is a singleton coordinate in $C' \cong H_{k'|m'}$. Let $Y_1 = Y \setminus (\mathrm{supp}(c) \cup \mathrm{supp}(c'))$, $Y_2 = Y \cap (\mathrm{supp}(c') \setminus \mathrm{supp}(c))$, $Y_3 = Y \cap (\mathrm{supp}(c) \cap \mathrm{supp}(c'))$ and $Y_4 = Y \cap (\mathrm{supp}(c) \setminus \mathrm{supp}(c'))$. The non-maximum weight codewords in $H_{k'|m'}$ form a subcode with equivalence classes of size $2^{m'} = 2^{m-1}$ on the singleton coordinates of $H_{k'|m'}$ (see the penultimate paragraph of the proof of Proposition 1.4). If we adjoin a maximum weight codeword, then these equivalence classes are cut in half, i.e., we obtain classes of size 2^{m-2}. Using this argument in the code obtained from C_0 by omitting the support of c and $\varrho(c')$ shows that there are exactly 2^{m-2} N-equivalent coordinates in Y_1 and in Y_2, as well. Switching the roles of c and c' yields the same for Y_1 and Y_4. Finally, by replacing c' in the above argument by $c+c'$, we obtain the same result for Y_1 and Y_3. Thus there are exactly 2^{m-2} coordinates N-equivalent to y in Y_1, Y_2, Y_3 and Y_4, which is a total of 2^m N-equivalent coordinates in Y.

Consequently, the weight of any non-maximum weight codeword is divisible by 2^m, and by definition, it is less than $D = 2^{k-1} + 2^{m-1}$. Hence, such a weight is at most 2^{k-1}. As maximum weight codewords in C_0 have exactly 2^{k-1} ones in $X \cup Y$, the restriction of C_0 to $X \cup Y$ has maximum weight exactly 2^{k-1}. Since $|X \cup Y| = 2^k - 1$, the conditions of Proposition 1.4 apply to the restriction, and then it is isomorphic to H_k. The code C_0 is obtained from its restriction to $X \cup Y$ by repeating the coordinates in X, where the restriction is isomorphic to H_m. Hence, $C_0 \cong H_{k|m}$. □

Proof of Theorem 1.12. By Lemma 2.1 item 2, all orbits have size 2, 3 or 4. Item 1 of Lemma 2.1 yields $3 \geq n_3 + 2n_4$. As S is even, n_3 is even, thus we have three possibilities in terms of the values of n_3 and n_4.

Case 1: $n_3 = n_4 = 0$. Then every orbit is a pair, and the permutation group is the natural action of a binary linear code. The length is $n = \frac{S}{2} = s - 2$, and the maximum weight is $D = \frac{s}{2} = \frac{n}{2} + 1$.

Case 2: $n_3 = 0, n_4 = 1$. If $n_2 = 0$, then G is a transitive group of degree 4. So we may assume that $n_2 \geq 1$.

First suppose that there exists a group element g_3 that acts as a 3-cycle on the 4-element orbit X. We may assume that g_3 is a 3-cycle by taking the square of it if necessary. Then $S = 2n_2 + 4$, $s = n_2 + 4$. There cannot be an $h \in G$ moving more than $n_2 + 2$ elements in the union of pairs, otherwise h or hg_3 would move more than $n_2 + 4$ elements. First assume that the maximum number of elements moved in the union of pairs is $n_2 + 2$.

As the restriction of G to X contains a 3-cycle and is transitive, it is either A_4 or S_4. In particular, all eight 3-cycles are represented. Using the square-trick, all eight permutations that act as a 3-cycle on X and identically on the union of pairs are in G. Any element of S_4 can be multiplied by (at most two) 3-cycles such that the product be a degree four permutation. Thus every $g \in G$ moves at most n_2 points within the n_2 pairs. This is a contradiction, as the average degree of the restriction to the pairs is n_2.

We conclude that the restriction of G to X does not contain a 3-cycle. Thus it is a degree four transitive permutation group in a Sylow 2-subgroup of S_4. Then the four points of X can be arranged as vertices of a square, and the restriction is in the dihedral group D_4, namely it is either D_4, the four element cyclic group generated by the rotation with a right angle, or a Klein group that is generated by the two reflections whose axes are the perpendicular bisectors of the sides of the square.

First assume that the restriction is the Klein group. Then we replace X by three new pairs of elements $\{1, 2\}, \{3, 4\}, \{5, 6\}$, and define the action of G on this new underlying set as follows. Assign to every nontrivial element of the Klein group one of the permutations $(1\ 2)(3\ 4), (1\ 2)(5\ 6), (3\ 4)(5\ 6)$. Every permutation $h \in G$ acts on the union of original pairs as before. On the new pairs, h acts identically iff it acted identically on X. Finally, if h acted as a nontrivial element of the Klein group, then replace this part of the action by the assigned permutation on the new pairs. Note that the degree of every element is the same as before. This way we obtain a new permutation group all of whose orbits are pairs with support of size $S'' = 2n_2 + 6$ and maximum degree $s'' = s = n_2 + 4$. Hence, $S'' = 2s'' - 2$, and the conditions of Theorem 1.3 apply. Thus the redefined action is the natural action of a punctured Hadamard code, and then G is a compressed punctured Hadamard code.

Now assume that the restriction of the action of G to X is either D_4 or the set of rotations in D_4. Note that every permutation on the pairs and in D_4 moves an even number of elements. In particular, s is even, and then $n_2 = s - 4$ is also even. Pick an element $g_4 \in G$ such that g_4

acts as a rotation by a right angle on the square X, and let $g_{2,2} = g_4^2$. Then $g_{2,2} \in G$ is the permutation that transposes the endpoints of both diagonals in the square X and acts identically on the union of pairs. Given any $h \in G$ that moves the most points in the union of pairs, h or $hg_{2,2}$ moves at least two points in X. Thus the maximum number of points moved in the union of pairs by any permutation in G is at most $n_2 + 2$. Then it must be exactly $n_2 + 2$, as it is bigger than n_2, and the maximum and n_2 are both even numbers. Hence, the restriction H of G to the union of pairs contains $H_{k|m}$ for some $1 \leq m \leq k$ by Theorem 1.10.

Maximum degree elements of H must pair up with degree two elements of D_4 on X. Thus the restriction of G to X is D_4, as the group of rotations does not contain elements of degree two. Moreover, a maximum degree element of H must pair up with both degree two elements in D_4, as multiplying such a permutation in G by $g_{2,2}$ maps the transposition of the elements of each diagonal to that of the other. Hence, $m = 1$, as otherwise there exist two maximum weight codewords in $H_{k|m}$ whose sum also has maximum weight, and pairing up these with the two different elements of degree two in D_4 would yield a pair of permutations in G whose product has degree $n_2 + 6$. Thus $n_2 = 2^k$.

In D_4, exactly a quarter of elements have degree two, and hence a quarter of elements in G has such a restriction to X. In particular, at most a quarter of elements in H has maximum weight. As $n_2 = 2^k$, we have that H is isomorphic to $H_{k|1}$ or $H_{k\times 1}$ by Proposition 1.9. The ratio of maximum weight elements in these codes are $1 - \frac{1}{2^k}$ and $\frac{1}{2}(1 - \frac{1}{2^k})$, respectively, hence it is at most $\frac{1}{4}$ iff the code is $H_{1\times 1}$, in which case it is exactly $\frac{1}{4}$.

Consequently, $k = 1$, $n_2 = 2$, $S = 8$, $s = 6$. Let $\psi : G \to H$ be the restriction homomorphism to the union of pairs. Then $|\psi^{-1}[(1, 1)]| \leq 2$, thus $|G| \leq 8$. Hence, $G \cong D_4$, as the restriction homomorphism to X must be an isomorphism. In particular, $|\psi^{-1}[(1, 1)]| = 2$, thus $\psi^{-1}[(1, 1)]$ consists of the two reflections to the diagonals. As $g_{2,2}$ is the square of some element in G, we have $\psi^{-1}[(0, 0)] = \{\mathrm{id}, g_{2,2}\}$. Each reflection to the perpendicular bisector of a side can be obtained from the other by multiplication with $g_{2,2}$, thus these are in the ψ-preimage of the same element. Without loss of generality, we may assume that this element is $(1, 0)$. Hence, through the process of elimination, the order four rotations are the ψ-preimages of $(0, 1)$, and we obtain that G is the intransitive action of D_4 described in Construction 1.11.

Case 3: $n_3 = 2, n_4 = 0$. If $n_2 = 0$, then G is a permutation group of degree 6 with maximum degree 5 acting on two 3-element orbits. It is easy to see that no such permutation group exists. So we may assume

that $n_2 \geq 1$.

Hence, $S = 2n_2 + 6$ and $s = n_2 + 5$. We show that there is an element $g_{3,3} \in G$ that acts as a 3-cycle on both 3-element orbits X_1, X_2 and identically on the pairs. First observe that there is an element that acts as a 3-cycle on X_1. By taking the square, we may assume that it acts identically on the pairs. If the element obtained this way permutes X_2 in a 3-cycle, then we have found $g_{3,3} \in G$. If not, then the same argument can be applied with switching the roles of X_1 and X_2. Then there are two 3-cycles in G, one with support X_1 and the other with X_2, and then their product is a good choice for $g_{3,3} \in G$.

Assume that there is an $h \in G$ which moves at least $n_2 + 2$ points in the union of pairs. Then such a permutation can move at most three points in $X_1 \cup X_2$. Hence, those points must belong to the same orbit. Then $hg_{3,3}$ or $hg_{3,3}^2$ moves at least two points in that orbit and three in the other X_i. So one of these permutations move at least $n_2 + 2 + 5 = n_2 + 7$ points, a contradiction.

Hence, the restriction H of G to the union of pairs satisfies the conditions of Theorem 1.3, and thus $H \cong H_k$ for some $k \geq 1$. An element $h \in G$ with nontrivial restriction to the pairs must move exactly four elements in $X_1 \cup X_2$: indeed, repeating the above argument shows that h cannot move at most three elements, otherwise $hg_{3,3}$ or $hg_{3,3}^2$ moves at least $n_2 + 1 + 5 = n_2 + 6$ points, and h cannot move more than four elements in $X_1 \cup X_2$, because in that case h has degree at least $n_2 + 6$. Moving four elements in $X_1 \cup X_2$ is only possible by moving two elements in both X_1 and X_2, thus the restriction of h to any of the 3-element orbits is odd. In particular, the homomorphism φ from G to the Klein group that maps every element to $\{0,1\}^2$ based on the parity of the restriction to X_1 and X_2 has in its image $(0,0)$ and $(1,1)$. The proportion of elements with image $(1,1)$ is thus at most $\frac{1}{2}$. In particular, the proportion $1 - \frac{1}{2^k}$ of maximum weight codewords in H_k is at most $\frac{1}{2}$. Hence $k = 1$, and then $n_2 = 1$, $S = 8$ and $s = 6$, the above ratio is exactly $\frac{1}{2}$, and the image of φ is exactly $\{(0,0),(1,1)\}$. The homomorphism φ must be injective, otherwise the product of the nontrivial element in the kernel and $g_{3,3}$ would move all 8 elements. Thus G is a subgroup of $G_{2,3,3}$ in Construction 1.11. As we have seen, all $h \in G$ with $\varphi(h) = (1,1)$ must switch the pair, otherwise we would have less than half of the elements switching the pair. The permutations $g_{3,3}$ and such an h generate $D_{2,3,3}$, an index 3 subgroup in $G_{2,3,3}$, hence maximal. Thus G is either $D_{2,3,3}$ or $G_{2,3,3}$. □

References

[1] Ahlman, O., and Koponen, V. Limit laws and automorphism groups of random nonrigid structures. *Journal of Logic and Analysis 7*, 2 (2015), 1–53.

[2] Ball, S. M., and Blokhuis, A. A bound for the maximum weight of a linear code. *SIAM Journal on Discrete Mathematics 27*, 1 (2013), 575–583.

[3] Betten, A., Braun, M., Fripertinger, H., Kerber, A., Kohnert, A., and Wassermann, A. *Error-Correcting Linear Codes: Classification by Isometry and Applications (Algorithms and Computation in Mathematics)*. Springer-Verlag, Berlin, Heidelberg, 2006.

[4] Bonisoli, A. Every equidistant linear code is a sequence of dual Hamming codes. *Ars Combinatoria 18* (1983), 181–186.

[5] Cameron, P. J. On graphs with given automorphism group. *European Journal of Combinatorics 1* (1980), 91–96.

[6] Erdős, P., and Rényi, A. Asymmetric graphs. *Acta Mathematica Hungarica 14* (1963), 295–315.

[7] Fagin, R. The number of finite relational structures. *Discrete Mathematics 19* (1977), 17–21.

[8] Koponen, V. Typical automorphism groups of finite nonrigid structures. *Archive for Mathematical Logic 54*, 5-6 (2015), 571–586.

[9] Liebeck, M. W., and Shalev, A. On fixed points of elements in primitive permutation groups. *Journal of Algebra 421* (2015), 438–459.

[10] Pongrácz, A. Binary linear codes with near-extremal maximum distance. submitted.

[11] Ronse, C. On permutation groups of prime power order. *Mathematische Zeitschrift 173*, 3 (1980), 211–215.

[12] Roth, R. *Introduction to Coding Theory*. Cambridge University Press, New York, NY, USA, 2006.

[13] Saxl, J., and Shalev, A. The fixity of permutation groups. *Journal of Algebra 174*, 3 (1995), 1122–1140.

[14] Shalev, A. On the fixity of linear groups. *Proceedings of the London Mathematical Society 68*, 3 (1994), 265–293.

[15] Xing, C., and Ling, S. *Coding Theory: A First Course*. Cambridge University Press, New York, NY, USA, 2003.