# Partial permutation decoding for binary linear Hadamard codes ⋆

R. D. Barrolleta [1] and M. Villanueva [2]

*Departament d'Enginyeria de la Informació i de les Comunicacions*
*Universitat Autònoma de Barcelona*
*Cerdanyola del Vallès, Spain*

**Abstract**

Permutation decoding is a technique which involves finding a subset $S$, called PD-set, of the permutation automorphism group $\mathrm{PAut}(C)$ of a code $C$ in order to assist in decoding. A method to obtain $s$-PD-sets of size $s+1$ for partial permutation decoding for the binary linear Hadamard codes $H_m$ of length $2^m$, for all $m \geq 4$ and $1 < s \leq \lfloor (2^m - m - 1)/(1+m) \rfloor$, is described. Moreover, a recursive construction to obtain $s$-PD-sets of size $s+1$ for $H_{m+1}$ of length $2^{m+1}$, from a given $s$-PD-set of the same size for the Hadamard code of half length $H_m$ is also established.

*Keywords:* Permutation decoding, Hadamard codes, automorphism groups.

## 1 Introduction

Let $\mathbb{F}_2^n$ be the set of all binary vectors of length $n$. The *Hamming weight* $\mathrm{wt}(v)$ of a vector $v \in \mathbb{F}_2^n$ is the number of nonzero coordinates in $v$. The *Hamming*

⋆ Research partially supported by the Spanish MICINN under Grants TIN2010-17358 and TIN2013-40524-P, and by the Catalan AGAUR under Grant 2014SGR-691.

[1] Email: rolanddavid.barrolleta@uab.cat

[2] Email: merce.villanueva@uab.cat

*distance* $d(u,v)$ between two vectors $u, v \in \mathbb{F}_2^n$ is the number of coordinates in which $u$ and $v$ differ, that is, $d(u,v) = \mathrm{wt}(u+v)$. Let $\mathbf{0}$ and $\mathbf{1}$ denote the all-zero and all-one vectors, respectively.

A *binary code* $C$ of length $n$ is a subset of $\mathbb{F}_2^n$. The vectors of a code $C$ are called *codewords* and the *minimum (Hamming) distance*, denoted by $d$, is the smallest distance between any pair of different codewords in $C$. We said that a code $C$ is a $t$*-error-correcting code* if it corrects all error vectors of weight at most $t$ and does not correct at least one error vector of weight $t+1$, so $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ [7]. A binary code $C$ is *linear* if it is a $k$-dimensional subspace of $\mathbb{F}_2^n$. A *generator matrix* for a linear code $C$ of length $n$ and dimension $k$ is any $k \times n$ matrix $G$ whose rows forms a basis of $C$.

Let $C$ be a binary code of length $n$. For a vector $v \in \mathbb{F}_2^n$ and a set $I \subseteq \{1, \ldots, n\}$, we denote by $v_I$ the restriction of the vector $v$ to the coordinates in $I$ and by $C_I$ the set $\{v_I \mid v \in C\}$. For example, if $I = \{1, \ldots, k\}$ and $v = (v_1, \ldots, v_n)$, then $v_I = (v_1, \ldots, v_k)$. Suppose that $C$ has size $|C| = 2^k$. A set $I \subseteq \{1, \ldots, n\}$ of $k$ coordinate positions is an *information set* for $C$ if $|C_I| = 2^k$. For each information set $I \subseteq \{1, \ldots n\}$ of $k$ coordinates positions, the set $\{1, \ldots, n\} \backslash I$ of the remaining $n-k$ coordinate positions is a *check set* for $C$. If $C$ is linear, we can label the $i^{th}$ coordinate position by the $i^{th}$ column of a generator matrix of $C$, so we will consider any information set (or check set) not only as a set of coordinate positions, but also as the set of vectors representing these positions.

Let $\mathrm{Sym}(n)$ be the symmetric group of permutations on the set $\{1, \ldots, n\}$ acting on $\mathbb{F}_2^n$ by permuting the coordinates of each vector. More specifically, for every vector $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ and permutation $\sigma \in \mathrm{Sym}(n)$, we define $\sigma(v_1, \ldots, v_n) = (v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(n)})$. Then, for any binary code $C$, we denote by $\mathrm{PAut}(C)$ the *permutation automorphism group* of $C$, that is, $\mathrm{PAut}(C) = \{\sigma \in \mathrm{Sym}(n) \mid \sigma(C) = C\}$.

Permutation decoding is a technique, introduced in [7] by MacWilliams, which involves finding a subset $S$, called PD-set, of the permutation automorphism group $\mathrm{PAut}(C)$ of a code $C$ in order to assist in decoding. The method works as follows: Given a $t$-error-correcting linear code $C \subseteq \mathbb{F}_2^n$ with fixed information set $I$, we denote by $y = x + e$ the received vector, where $x \in C$ and $e$ is the error vector. Suppose that at most $t$ errors occur, that is, $\mathrm{wt}(e) \leq t$. The aim of permutation decoding is to move all errors in a received vector out the information positions, that is, move the nonzero coordinates of $e$ out of $I$, by using an automorphism of the code.

Let $C$ be a $t$-error-correcting linear code with information set $I$. A subset $S \subseteq \mathrm{PAut}(C)$ is a *PD-set* for the code $C$ if every $t$-set of coordinate positions is moved out of the information set $I$ by at least one element of the set $S$. Equivalently, a subset $S \subseteq \mathrm{PAut}(C)$ is an *$s$-PD-set* if every $s$-set of coordinate positions is moved out of $I$ by at least one element of $S$, where $1 \leq s \leq t$.

Let $S_m$ be the binary simplex code of length $2^m - 1$, dimension $m$ and minimum distance $2^{m-1}$ with generator matrix $G_{S_m}$ containing as column vectors the $2^m - 1$ nonzero vectors from $\mathbb{F}_2^m$, with the basis elements $e_i^T$, $i \in \{1, \dots, m\}$, in the first $m$ positions. We take the set of standard basis elements of $\mathbb{F}_2^m$ to be the information set $I_m$ of this code, that is, $I_m = \{e_1, \dots, e_m\}$. Let $H_m$ be the binary linear Hadamard code of length $2^m$, that is, the extended code of the simplex code $S_m$ with generator matrix $G_{H_m}$ constructed from $G_{S_m}$ by adding an all-one row vector and an all-zero column vector as follows:

$$G_{H_m} = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{0} & G_{S_m} \end{pmatrix}. \qquad (1)$$

Now we consider as information set for $H_m$ the set $\mathcal{I}_m = \{w_1, \dots, w_{m+1}\} = \{(1, 0, \dots, 0), (1, 1, \dots, 0), \dots, (1, 0, \dots, 1)\}$ consisting of the first $m+1$ column vectors from the matrix $G_{H_m}$ considered as row vectors. The check set $\mathcal{C}_m$ for $H_m$ is the set containing the remaining column vectors from the matrix $G_{H_m}$ considered as row vectors and denoted by $\mathcal{C}_m = \{w_{m+2}, \dots, w_{2^m}\}$.

It is a well-know fact that $\mathrm{PAut}(S_m) = GL(m, 2)$, where $GL(m, 2)$ is the general linear group of degree $m$ over $\mathbb{F}_2$. It is also known that $\mathrm{PAut}(H_m) = AGL(m, 2)$ [8]. Recall that the affine group $AGL(m, 2)$ consists of all mappings $\alpha : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ of the form $\alpha(x^T) = Ax^T + b^T$ for $x \in \mathbb{F}_2^m$, where $A \in GL(m, 2)$ and $b \in \mathbb{F}_2^m$, together with the function composition as the group operation. The monomorphism $\varphi : AGL(m, 2) \rightarrow GL(m + 1, 2)$,

$$\varphi(b, A) = \begin{pmatrix} 1 & b \\ \mathbf{0} & A \end{pmatrix},$$

defines an isomorphism between $AGL(m, 2)$ and the subgroup of $GL(m+1, 2)$ consisting of all nonsingular matrices whose first column is $(1, 0, \dots, 0)$. From now on, we identify the $AGL(m, 2)$ with this subgroup.

Now, we describe how to identify a permutation $\sigma \in \mathrm{PAut}(H_m) \subseteq \mathrm{Sym}(2^m)$ with a matrix $B \in AGL(m, 2)$. Recall that each coordinate position can be labelled by the corresponding column of the generator matrix $G_{H_m}$ given in (1). The first $m + 1$ coordinate positions are labelled by the vectors of the information set $\mathcal{I}_m$ and the remaining coordinate positions are represented by the vectors of the check set $\mathcal{C}_m$. The vector $w_i$ represents the $i^{th}$ position, for all $i \in \{1, \ldots, 2^m\}$. Note that an index $i \in \{1, \ldots, m+1\}$ represents a position in $\mathcal{I}_m$ and an index $i \in \{m+2, \ldots, 2^m\}$ a position in $\mathcal{C}_m$. Thus, $w_i B = w_j$ will denote that the $i^{th}$ position of a codeword moves to the $j^{th}$ position of that codeword. Therefore, any matrix $B \in AGL(m,2)$ can be seen as an element of $\mathrm{PAut}(H_m) \subseteq \mathrm{Sym}(2^m)$. Along the paper, we will represent PD-sets for $H_m$ as subsets of matrices of the affine group $AGL(m,2)$.

In [3], it is shown how to find $s$-PD-sets of size $s+1$ that satisfy the Gordon-Schönheim bound for partial permutation decoding for the binary simplex code $S_m$, for all $m \geq 4$ and $1 < s \leq \left\lfloor \frac{2^m-m-1}{m} \right\rfloor$. In this paper, we establish similar results for the binary linear Hadamard code $H_m$, for all $m \geq 4$ and $1 < s \leq \left\lfloor \frac{2^m-m-1}{1+m} \right\rfloor$, following the same techniques as the ones described in [3]. In [9], a 2-PD-set of size 5 and 4-PD-sets of size $\binom{m+1}{2} + 2$ are found for binary linear Hadamard codes $H_m$, for all $m > 4$. As a consequence, 3-PD-sets of size $\binom{m+1}{2} + 2$ are also found for these codes. Small PD-sets that satisfy the Gordon-Schönheim bound have been found for binary Golay codes [4,10] and for the binary simplex code $S_4$ [5,6].

This work is organized as follows. In Section 2, we adapt the so-called Gordon-Schönheim bound for $H_m$ and we define a bound that allow us to obtain $s$-PD-sets of size $s+1$ for $H_m$. In Section 3, we provide a criterion on subsets of matrices of $AGL(m,2)$ to be an $s$-PD-set of size $s+1$. In Section 4, we define a recursive construction to obtain $s$-PD-sets of size $s+1$ for $H_{m+1}$ from a given $s$-PD-set of the same size for $H_m$. Finally, in Section 5, we show the conclusions and a further research on this topic.

## 2 Bound on the minimum size of $s$-PD-sets for $H_m$

There is a well-known bound on the minimum size of PD-sets for linear codes based on the length, the dimension and the minimum distance of such codes.

**Proposition 2.1** *[4] Let $C$ be a $t$-error correcting linear code of length $n$, dimension $k$ and minimum distance $d$. Let $r = n - k$ be the redundancy of $C$. If $S$ is a PD-set for $C$, then*

$$|S| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

The above inequality is often called the *Gordon-Schönheim bound*. Recall that a linear code with minimum distance $d$ can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors, so for the binary linear Hadamard code $H_m$, we have that its error-correcting capability, denoted by $t_m$, is $t_m = 2^{m-2} - 1$. We do not take into account the case $m = 3$ in our results since $t_3 = 1$. The Gordon-Schönheim bound can be adapted to $s$-PD-sets for all $s$ up to the error correcting capability of the code. We compute the function $g_m(s)$ defined by the right side of this bound given in Proposition 2.1 in the particular case of the binary linear Hadamard code $H_m$, for all $1 \leq s \leq t_m$. The minimum value of $g_m(s)$ is also computed.

**Lemma 2.2** *Let $m$ be an integer, $m \geq 4$. Let $H_m$ be the binary linear Hadamard code. For $1 \leq s \leq t_m$,*

$$g_m(s) = \left\lceil \frac{2^m}{2^m - m - 1} \left\lceil \frac{2^m - 1}{2^m - m - 2} \left\lceil \dots \left\lceil \frac{2^m - s + 1}{2^m - m - s} \right\rceil \right\rceil \dots \right\rceil \right\rceil \geq s + 1,$$

*where $t_m = 2^{m-2} - 1$ is the error-correcting capability of $H_m$.*

The smaller the size of the PD-set is, the more efficient permutation decoding becomes. Because of this, we will focus on the case when we have that $g_m(s) = s + 1$. Let $m$ be an integer, $m \geq 4$. For the binary linear Hadamard code $H_m$, we define $f_{H_m} = \max\{s \mid 2 \leq s,\ g_m(s) = s + 1\}$. For each $H_m$, the integer $f_{H_m}$ represents the greater $s$ in which we can find $s$-PD-sets of size $s + 1$. The following result characterize this parameter from the value of $m$.

**Lemma 2.3** *For $m \geq 4$, $f_{H_m} = \left\lfloor \frac{2^m - m - 1}{1 + m} \right\rfloor$.*

## 3 Finding $s$-PD-sets of size $s + 1$ for $H_m$

Let $M$ be a matrix of $GL(m, 2)$. We can regard the rows of $M$ as row vectors and consider the set $V = \{v_1, \dots, v_m\}$ consisting of such row vectors. We define $M^*$ as the matrix with rows given by $V^* = \{v_1, v_1 + v_2, \dots, v_1 + v_m\}$. We denote by $Id_m$ the $m \times m$ identity matrix.

An $s$-PD-set of size $s+1$ meets the Gordon-Schönheim bound for correction of $s$ errors if $s \leq f_{H_m}$. The following proposition provides us a condition on sets of matrices of $AGL(m, 2)$ in order to be $s$-PD-sets of size $s + 1$.

**Proposition 3.1** *Let $H_m$ be the binary linear Hadamard code of length $n = 2^m$, with $m \geq 4$. Let $P_s = \{M_i \mid 0 \leq i \leq s\}$ be a set of $s + 1$ matrices in $AGL(m, 2)$. Then, $P_s$ is an $s$-PD-set of size $s + 1$ for $H_m$ if and only if no two matrices $(M_i^{-1})^*$ and $(M_j^{-1})^*$ for $i \neq j$ have a row in common. Moreover, any subset $P_k \subseteq P_s$ of size $k + 1$ is a $k$-PD-set for $k \in \{1, \dots, s\}$.*

**Example 3.2** The set of matrices $P_2 = \{Id_5, M_1, M_2\}$, where

$$M_1 = \begin{pmatrix} 1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,1 \\ 0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,1 \\ 0\,0\,1\,1\,0 \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 1\,1\,1\,1\,1 \\ 0\,1\,0\,0\,1 \\ 0\,0\,1\,1\,0 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1 \end{pmatrix},$$

is a 2-PD-set for the binary linear Hadamard code $H_4$ of length 16. Note that $P_2 \subset AGL(4,2) \subset GL(5,2)$. It is straightforward to check that $Id_5^*$,

$$(M_1^{-1})^* = \begin{pmatrix} 1\,0\,0\,1\,1 \\ 1\,1\,0\,0\,1 \\ 1\,0\,1\,1\,1 \\ 1\,0\,1\,1\,0 \\ 1\,1\,0\,1\,1 \end{pmatrix} \quad \text{and} \quad (M_2^{-1})^* = \begin{pmatrix} 1\,1\,1\,0\,0 \\ 1\,0\,1\,0\,1 \\ 1\,1\,1\,1\,0 \\ 1\,1\,0\,1\,0 \\ 1\,1\,1\,0\,1 \end{pmatrix}$$

have no rows in common. In addition, note that $f_{H_4} = 2$, so no $s$-PD-set of size $s+1$ can be found for $s \geq 3$. We can also observe that $f_{H_4} = 2 < 3 = t_4$, where $t_4$ is the error-correcting capability of $H_4$. In fact, the value of the bound $f_{H_m}$ is always smaller than $t_m$, for all $m \geq 4$. Finally, $P_2$ can be regarded as a subset of Sym(16). In this case, we obtain the 2-PD-set $\{id, \sigma_1, \sigma_2\}$ where $\sigma_1 = (1,14,11,9,6,10,13,3,15,5,16,2,12,8)(4,7)$ and $\sigma_2 = (1,14,11,2,7,9,5,12,3,16,13,6)(4,15,8,10)$.

Let $S$ be an $s$-PD-set of size $s+1$. The set $S$ is a *nested* $s$-PD-set if there is an ordering of the elements of $S$, $S = \{\sigma_0, \ldots, \sigma_s\}$, such that $S_i = \{\sigma_0, \ldots, \sigma_i\} \subseteq S$ is an $i$-PD-set of size $i+1$, for all $i \in \{0, \ldots, s\}$. Note that $S_i \subset S_j$ if $0 \leq i < j \leq s$ and $S_s = S$. From Proposition 3.1, we have two important consequences. The first one is related to how to obtain nested $s$-PD-sets and the second one provides another proof of Lemma 2.3.

**Corollary 3.3** *Let $m$ be an integer, $m \geq 4$. If $P_s$ is an $s$-PD-set of size $s+1$ for the binary linear Hadamard code $H_m$, then any ordering of the elements of $P_s$ gives nested $k$-PD-sets for $k \in \{1, \ldots, s\}$.*

**Corollary 3.4** *Let $m$ be an integer, $m \geq 4$. Let $P_s$ be an $s$-PD-set of size $s+1$ for the binary linear Hadamard code $H_m$. Then, $s \leq \left\lfloor \frac{2^m-m-1}{1+m} \right\rfloor$.*

## 4 Recursive construction of $s$-PD-sets of size $s+1$

Given an $s$-PD-set of size $s+1$ for the binary linear Hadamard code $H_m$ of length $2^m$, where $0 \leq s \leq f_{H_m}$, we can construct recursively an $s$-PD-set of the same size for $H_{m'}$ of length $2^{m'}$, for all $m' > m$.

Let $M \in AGL(m,2)$ and $v = (0, v_2 \dots, v_{m+1})$ be the last row of the matrix $M$. We define the matrix $M(v) \in AGL(m+1,2)$ as

$$M(v) = \left( \begin{array}{c|ccc} 1 & & & \\ 0 & & M & \\ \vdots & & & \\ \hline 0 & 1 \; v_2 & \dots & v_{m+1} \end{array} \right). \quad (2)$$

Since the first column of $M(v)$ is $e_1 = (1,0,\dots,0)$, we can guarantee that the first column of $M(v)^{-1}$ is $e_1$ as well. Thus, $M(v)$, $M(v)^{-1} \in AGL(m+1,2)$. Also note that $v \in \mathbb{F}_2^{m+1}$ depends on each $M \in AGL(m,2)$.

**Proposition 4.1** *Let $m$ be an integer, $m \geq 4$, and $P_s = \{Id_{m+1}, M_1, \dots, M_s\}$ be an $s$-PD-set of size $s+1$ for the binary linear Hadamard code $H_m$. Let $N_i = M_i^{-1}$, for all $i \in \{1,\dots,s\}$. Then, $Q_s = \{Id_{m+2}, (N_1(v))^{-1}, \dots, (N_s(v))^{-1}\}$ is an $s$-PD-set of size $s+1$ for the binary linear Hadamard code $H_{m+1}$.*

**Example 4.2** Considering the matrices from the 2-PD-set $P_2 = \{Id_5, M_1, M_2\}$ for $H_4$ of length 16, given in Example 3.2, matrices $N_1(v) = (M_1^{-1})(v)$ and $N_2(v) = (M_2^{-1})(v)$ are

$$N_1(v) = \left( \begin{array}{c|ccccc} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 1 & 1 & 0 & 0 & 0 \end{array} \right) \quad \text{and} \quad N_2(v) = \left( \begin{array}{c|ccccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 \end{array} \right).$$

Note that the last row of $N_1$ is $v = (0, 1, 0, 0, 0)$, and the last row of $N_2$ is $v = (0, 0, 0, 0, 1)$. Since matrices $Id_6^*$, $(N_1(v))^*$ and $(N_1(v))^*$ have no rows in common, the set $\{Id_{m+2}, (N_1(v))^{-1}, (N_2(v))^{-1}\}$ is a 2-PD-set for $H_5$.

**Note 1** *Proposition 4.1 is also true if we define the matrix $M(v)$ taking as vector $v$ any of the last $m$ rows of $M$ instead of the last one as in (2).*

**Note 2** *The bound $f_{H_{m+1}}$ for $H_{m+1}$ cannot be achieve recursively from an s-PD-set for $H_m$. The recursive construction only works when fixing the number $s$ of errors we want to correct and increasing the length of the Hadamard code.*

## 5 Conclusions and further research

In this work, we studied how to find $s$-PD-sets for partial permutation decoding for binary linear Hadamard codes. An alternative permutation decoding algorithm for $\mathbb{Z}_2\mathbb{Z}_4$-linear codes [2] is described in [1]. In particular, it can be applied to Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes. Nevertheless, this method assumes that we know an appropriate PD-set for such codes. Further work will be study how to find $s$-PD-sets for Hadamard $\mathbb{Z}_2\mathbb{Z}_4$-linear codes (not necessarily binary linear Hadamard codes) and establish the size of these $s$-PD-sets.

## References


[1] Bernal, J. J., J. Borges, C. Fernández-Córboda, and M. Villanueva, *Permutation decoding of $\mathbb{Z}_2\mathbb{Z}_4$-linear codes*, Des. Codes Cryptogr. (2014), DOI 10.1007/s10623-014-9946-4.

[2] Borges, J., C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, *$\mathbb{Z}_2\mathbb{Z}_4$-linear codes: generator matrices and duality*, Des. Codes and Cryptogr. **54** (2010), 167-179.

[3] Fish, W., J. D. Key, and E. Mwambene, *Partial permutation decoding for simplex codes*, Advances in Mathematics of Comunications **6** (2012), 505-516.

[4] Gordon, D. M., *Minimal permutation sets for decoding the binary Golay codes*, IEEE Trans. Inform. Theory **28** (1982), 541-543.

[5] Kroll, H.-J., and R. Vicenti, *PD-sets related to the codes of some classical varieties*, Discrete Math. **301** (2005), 89-105.

[6] Kroll, H.-J., and R. Vicenti, *PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of PG(5,2)*, Discrete Math. **308** (2008), 408-414.

[7] MacWilliams, F. J., *Permutation decoding of systematics codes*, Bell System Tech. J. **43** (1964), 485-505.

[8] MacWilliams F. J., and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland Publishing Company, Amsterdam, 1977.

[9] Seneviratne, P., *Partial permutation decoding for the first-order Reed-Muller codes*, Discrete Math. **309** (2009), 1967–1970.

[10] Wolfmann, J., *A permutation decoding of the (24, 12, 9) Golay code*, IEEE Trans. Inform. Theory **29** (1983), 748-750.