Rank and Kernel of binary Hadamard codes.

K.T. Phelps, J. Rifà *Senior Member IEEE,* M. Villanueva

***Abstract*— In this paper the rank and the dimension of the kernel for (binary) Hadamard codes of length a power of two are studied. In general, it is well-known (see [1]) that the rank of a Hadamard code of length $n = 2^t$ is a value in $\{t+1, \ldots, n/2\}$. In the present paper, the range of possible values for the dimension of the kernel is computed and a construction of Hadamard codes of length $n = 2^t$ for each one of these values is given. Lower and upper bounds for the rank and dimension of the kernel of a Hadamard code of length $n = 2^t$, are also established. Finally, we construct Hadamard codes for all possible ranks and dimension of kernels between these bounds.**

***Index Terms*— Hadamard matrices, Hadamard codes, extended perfect codes, rank, kernel.**

I. Introduction

Let $\mathbb{F}^n$ denote the set of all binary vectors of length n. The Hamming distance between two vectors $x, y \in \mathbb{F}^n$, denoted by $d(x, y)$, is the number of coordinates in which x and y differ. The Hamming weight of x is given by $wt(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the all-zero vector. The support of a vector $x \in \mathbb{F}^n$ is the set of nonzero coordinate positions of x and is denoted by $supp(x)$.

A *(binary)* (n, M, d)*-code* is a subset, C, of $\mathbb{F}^n$ such that $|C| = M$ and $d(c_1, c_2) \geq d$ for all pairs $c_1, c_2 \in C$. The elements of a code are called *codewords* and d is called *minimum distance*. A *1-perfect code* C of length n is a subset of $\mathbb{F}^n$, with distance $d = 3$, such that all the vectors in $\mathbb{F}^n$ are within distance one from a codeword. For any $t > 1$ there exists exactly one linear 1-perfect code of length $2^t - 1$, up to isomorphism, which is the well-known *Hamming code*. An *extended code* of the code C is a code resulting from adding an overall parity check digit to each codeword of C.

Two codes $C_1, C_2 \in \mathbb{F}^n$ are *equivalent* if there exists a vector $a \in \mathbb{F}^n$ and a permutation π such that $C_2 = \{a + \pi(c) \mid c \in C_1\}$. Two structural properties of non-linear codes are the rank and kernel. The *rank* of a binary code C, $r = rank(C)$, is simply the dimension of the linear span of C. By the binary orthogonal code of the non-linear code C, denoted by $C^\perp$, we mean the dual of the subspace spanned by C having dimension $n-r$. The *kernel* of a binary code C is defined as $K(C) = \{x \in \mathbb{F}^n \mid x + C = C\}$. If the zero word is in C, then $K(C)$ is a linear subspace of C. In general, C can be written as the union of cosets of $K(C)$ and $K(C)$ is the largest such linear code for which this is true (see [2]). We will denote the dimension of the kernel of C by $k = ker(C)$.

A *Hadamard matrix* H of order n is an $n \times n$ matrix of $+1$'s and -1's such that $HH^T = nI$, where I is the $n \times n$ identity matrix. In other words, the real inner product of any row with itself is n and distinct rows are orthogonal. Since $nH^{-1} = H^T$, we also have $H^T H = nI$, thus the columns have the same properties

Research partially supported by CICYT Grants TIC2003-08604-C04-01, TIC2003-02041 and by Catalan DURSI Grant 2001SGR 00219.

K.T. Phelps is with the Mathematics & Statistics Dept., Auburn University, Auburn, Al 36849-5307 (email: phelpkt@auburn.edu).

J. Rifà and M. Villanueva are with the Dept. d'Informàtica, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (email: {josep.rifa, merce.villanueva}@autonoma.edu).

and the transpose of any Hadamard matrix, H, is also a Hadamard matrix, which is not necessary equivalent to H. We know that if a Hadamard matrix H of order n exists, then n is 1, 2 or a multiple of 4 (see [5], [7]).

Two Hadamard matrices are *equivalent* if one can be obtained from the other by permuting rows and/or columns and multiplying rows and/or columns by -1. We can change the first row and column of H into $+1$'s and we obtain an equivalent Hadamard matrix which is called *normalized*.

From now on, we will use H' to denote a normalized Hadamard matrix of order n. If $+1$'s are replaced by 0's and -1's by 1's, H' is changed into a *(binary) Hadamard matrix* $c(H')$. Since the rows of H' are orthogonal, any two rows of $c(H')$ agree in $n/2$ places and differ in $n/2$ places, and so have Hamming distance $n/2$ apart. The binary $(n, 2n, n/2)$-code consisting of the rows of $c(H')$ and their complements is called a *(binary) Hadamard code* (see [7]) and we will use H to denote it.

The simplest example of a Hadamard matrix is given by considering the binary dual code of an extended (binary) Hamming code. For example, the dual of the extended (binary) Hamming code of length 4, that is, the linear code with generator matrix $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ is a Hadamard code H. In this case,

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad c(H') = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \text{ and}$$

$$H' = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix}.$$

If we consider non-linear extended (binary) 1-perfect codes, then Hadamard matrices [6] can be constructed by using the codewords of the $\mathbb{Z}_4$-dual code corresponding to an extended 1-perfect $\mathbb{Z}_4$-linear code. A more general construction can be found in [3] where additive codes are used and not only $\mathbb{Z}_4$-linear ones. In all these cases, the Hadamard matrices have order a power of 2. In [8], [9] we computed the rank and the dimension of the kernel for additive Hadamard codes, using the fact that they are the additive dual of extended 1-perfect additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) codes. Moreover, for the admissible values r, k of these two parameters, the codes are unique up to equivalence.

In this paper we will focus on the rank and the kernel of binary Hadamard codes of length $n = 2^t$. The paper is arranged as follows. In section 2, we give some results on the rank and the kernel of Hadamard codes constructed using the Kronecker product. In section 3, we establish general lower and upper bounds on the dimension of the kernel as well as the rank. We establish that Hadamard codes of length $n = 2^t$ with a kernel of dimension k, exist if and only if $k \in \{1, 2, \ldots, t-1, t+1\}$. We also include an argument for the existence of Hadamard codes of length $n = 2^t$ for any possible rank, $r \in \{t+1, \ldots, n/2\}$. In section 4, we establish upper and lower bounds on the parameters r, k. Finally, in section 5, we construct Hadamard codes with parameters r, k for all possible values that satisfy the bounds of section 4.

II. Kronecker product construction

Apart from the Hadamard matrices obtained from additive dual codes of the corresponding additive extended 1-perfect codes, we can consider other Hadamard matrices constructed using a standard method, the *Kronecker product construction*. That is, if $H' = (h_{ij})$ is any

TABLE I

KRONECKER PRODUCT CONSTRUCTION

$$H' \otimes [B_1, B_2, \ldots, B_n] = \begin{pmatrix} h_{11}B_1 & h_{12}B_1 & \cdots & h_{1n}B_1 \\ h_{21}B_2 & h_{22}B_2 & \cdots & h_{2n}B_2 \\ \vdots & \vdots & \vdots & \vdots \\ h_{n1}B_n & h_{n2}B_n & \cdots & h_{nn}B_n \end{pmatrix}$$

$n \times n$ Hadamard matrix, and $B_1, B_2, \ldots, B_n$ are any $k \times k$ Hadamard matrices, then the matrix in Table I is a $nk \times nk$ Hadamard matrix.

If $B_1 = B_2 = \cdots = B_n = B$, we write $H' \otimes [B_1, B_2, \ldots, B_n] = H' \otimes B$ (see [1]).

Let S be the Hadamard matrix $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Starting from a Hadamard matrix S_0 we can recursively define S_t for $t \geq 1$, taking $S_t = S \otimes [S_{t-1}, S_{t-1}] = S \otimes S_{t-1}$. Taking $S_0 = (1)$, the corresponding succession S_1, S_2, S_3, ..., S_t, ... gives us Hadamard matrices of all orders which are powers of two. These are called *Sylvester* matrices. It is known that the binary codes of these Hadamard matrices, S_t, are the binary dual of the extended Hamming codes.

For length $n = 16$, we know that there exist exactly 5 non-equivalent Hadamard codes (see [1, p.266]). One of these is the linear Hadamard code with rank and dimension of the kernel equal to 5, and four more with each one of the parameters $(rank(H), ker(H)) \in \{(6,3),(7,2),(8,2),(8,1)\}$. In this case, all non-equivalent Hadamard codes can be completely classified using the rank and the dimension of the kernel.

Lemma 2.1: Let H'_1, H'_2 be two Hadamard matrices and H_1, H_2 the respective Hadamard codes. The kernel of the corresponding Hadamard code of $H'_1 \otimes H'_2$ has dimension $ker(H_1) + ker(H_2) - 1$ and the rank is $rank(H_1) + rank(H_2) - 1$.

Proof: The rank of the tensor or Kronecker product of real matrices is well-known to be the product of the ranks but this is not true of the Hadamard matrices derived from such a product. Let $\rho : \{1, -1\} \to \{0, 1\}$ be the mapping that converts a Hadamard matrix to a binary matrix. Let A', B' be Hadamard matrices with row vectors a_i, b_j respectively. Then the rows of $A' \otimes B'$ are $a_i \otimes b_j$ and

$$\rho(a_i \otimes b_j) = \rho(a_i \otimes \mathbf{1}) + \rho(\mathbf{1} \otimes b_j)$$

It is straight-forward to see that the binary rank of the product is $rank(A) + rank(B) - 1$. The dimension of the kernel of the corresponding code follows in similar fashion since the kernel is the Kronecker product of the matrices for the respective kernels. ∎

Corollary 2.2: Let H' be a Hadamard matrix and H its Hadamard code. The kernel dimension of the corresponding Hadamard code of $S \otimes H'$ is $ker(H) + 1$ and the rank is $rank(H) + 1$.

Proof: Follows directly from the previous lemma. Specifically, assume C is the Hadamard code of $S \otimes H'$. Code C consists of all vectors (y, y), $(y, \bar{y})$, $(\bar{y}, y)$, $(\bar{y}, \bar{y})$, where $y \in H'$ and $\bar{y}$ means the complementary vector of y, so $rank(C) = rank(H) + 1$.
It is easy to see that the kernel of C is $K(C) = \{(x, x), (x, \bar{x}), (\bar{x}, x), (\bar{x}, \bar{x}) \mid x \in K(H)\}$, so $ker(C) = ker(H) + 1$. ∎

The next result is well-known and could be reformu-

lated in the following way:

Lemma 2.3: [1] Let H_1' ,H_2' be two Hadamard matrices and H_1, H_2 theirs Hadamard codes. The rank of the corresponding Hadamard code of $S \otimes [H_1', H_2']$ is $rank(H_1) + rank(H_2) + 1 - dim(<H_1> \cap <H_2>)$ or, equivalently, $dim(<H_1 \cup H_2>) + 1$.

Note that this last result coincides with Corollary 2.2 when $H_1' = H_2'$.

Lemma 2.4: Let H_1', H_2' be two Hadamard matrices. Let H_1, H_2 be their Hadamard codes and $K(H_1)$, $K(H_2)$ their kernels. If for all v, $H_1 \neq v + H_2$, then the kernel K of the corresponding Hadamard code of $S \otimes [H_1', H_2']$ is $K = \{(x, x) \mid x \in K(H_1) \cap K(H_2)\}$.

Proof: It is clear that $\{(x, x) \mid x \in K(H_1) \cap K(H_2)\} \subseteq K$. If $(x, y) \in K$, then for all $h \in H_1$ we have $(x+h, y+h) \in (H_1, H_1)$ or $(x + h, y + h) \in (H_2, \bar{H_2})$, so either $x = y$ or $x = \bar{y}$, where $\bar{y}$ means the complementary vector of y and $\bar{H} = \{\bar{y} \,|\, y \in H\}$.

Assume $x = y$. Then for all $h \in H_1$ we will always have $(x + h, y + h) \in (H_1, H_1)$ and for all $h \in H_2$, $(x + h, y + \bar{h}) \in (H_2, \bar{H_2})$, so $x \in K(H_1) \cap K(H_2)$.

Assume now that $x = \bar{y}$. Then for all $h \in H_1$ we will always have $(x + h, y + h) \in (H_2, \bar{H_2})$ and for all $h \in H_2$, $(x + h, y + \bar{h}) \in (H_1, H_1)$. But this contradicts the condition, $H_1 \neq v + H_2$, hence our assumption, $x = \bar{y}$ is not possible and lemma follows. ∎

It is an open problem to decide if it is always true that $S_t \subseteq <H>$ for any Hadamard code H of length 2^t, where S_t means the linear Hadamard code of length 2^t. As usual, we can assume S_t is generated by the binary vectors $\mathbf{1}, v_1, v_2, \ldots, v_t$ of length 2^t, where the j-th coordinate of v_i is 1 if and only if 2^{t-j} occurs in the binary expansion of $n - i$. For example,

$$v_1 = (\underbrace{1, 1, ..., 1}_{n/2}, \underbrace{0, 0, ..., 0}_{n/2}),$$

$$v_2 = (\underbrace{1, 1, ..., 1}_{n/4}, \underbrace{0, 0, ..., 0}_{n/4}, \underbrace{1, 1, ..., 1}_{n/4}, \underbrace{0, 0, ..., 0}_{n/4}), \quad (1)$$

etc.

Note, however, that if a Hadamard code H has $ker(H) = k$, we can always assume that the kernel is generated by k independent vectors from S_t.

III. Dimension of the kernel and rank of Hadamard codes

The next propositions give us general lower and upper bounds for the dimension of the kernel and for the rank, separately. We will prove that the bounds on each of these parameters are tight and that it is possible to construct Hadamard codes for every rank and codes for every dimension of the kernel between these bounds, using the previous results about the Kronecker product construction.

Proposition 3.1: If a Hadamard code of length $n = 2^t$, $t \geq 4$, has a kernel of dimension k, then $k \in \{1, 2, \ldots, t-1, t+1\}$.

Proof: In a Hadamard code, H, the kernel has dimension at least 1, since the complement of any codeword is in the code. It is clear that the maximum is $t+1$, when the Hadamard code is a linear code. There can not exist any Hadamard code with $ker(H) = t$ since, in that case, the code would be linear. ∎

Proposition 3.2: For all $t \geq 4$, there exists a Hadamard code of length $n = 2^t$ with kernel of dimension k if and only if $k \in \{1, 2, \ldots, t-1, t+1\}$.

Proof: By Proposition 3.1, any Hadamard code of length $n = 2^t$, $t \geq 4$, has kernel of dimension $k \in \{1, 2, \ldots, t-1, t+1\}$.

We know that the result is true for $n = 16$. Suppose it is true for $n = 2^t$, so there exists a Hadamard code H_i with kernel of dimension i for all $i \in \{1, \ldots, t-1\}$. We want to construct Hadamard codes of length 2^{t+1} with kernels of dimensions $\{1, 2, \ldots, t\}$. By Corollary 2.2, the corresponding Hadamard code of $S \otimes H_i'$ has a kernel of dimension $i+1$. By Lemma 2.4, the corresponding Hadamard code of $S \otimes [H_1', H_j']$ for any $j \neq 1$ has a kernel of dimension 1. ∎

Lemma 3.3: Let H' be a Hadamard matrix of order $n \geq 8$ and H its Hadamard code. The minimum weight in the linear span $<H>$ is greater or equal to four.

Proof: The minimum weight in $H^\perp$ is at least 3, since H does not contain equal columns. As $H \subset H^\perp$, we have that $<H> \subset H^\perp$ and the weight of the vectors in H is even. So, the the minimum weight in $<H>$ is greater or equal to four. ∎

Proposition 3.4: For all $t \geq 4$, there exists a Hadamard code of length $n = 2^t$ with $rank(H) = r$ if and only if $r \in \{t+1, \ldots, n/2\}$.

Proof: In [1], it is shown that $r \leq n/2$ and $r \geq t+1$. Now, we will see that we can construct a Hadamard code for each possible rank between these bounds.

Let K' be a Hadamard matrix of order n and K its Hadamard code with $rank(K) = r$ and such that the (last) r column vectors of K are the independent ones. We will see how to construct Hadamard matrices of order $2n$ with different ranks.

First, the rank of the corresponding Hadamard code of $S \otimes K'$ is $r+1$, by Corollary 2.2. Now, consider $L_1' = \pi_{0,1}(K')$ the matrix formed by switching columns n and $n-1$ in K', (i.e. $\pi_{0,1} = (n-1, n)$) and let L_1 be its Hadamard code. The independent vectors in $< K \cup L_1 >$ include those in K as well as, the vector $u_{r-1,r} = (0, \ldots, 0, 1, 1) = (x, 01) + (x, 10)$ for some $(x, 01) \in K$ and $(x, 10) \in L_1$. By Lemma 3.3, $u_{r-1,r}$ is independent from $<K>$. Hence the rank of the corresponding Hadamard code of $S \otimes [K', L_1']$ is $dim(<K \cup L_1>) + 1 = r + 2$.

We can continue in this way taking $L_2' = \pi_{0,2}(L_1')$ the matrix formed by switching columns n and $n-2$ in L_1', $\pi_{0,2} = (n-2, n)$ or, equivalently, by a cyclic shift $L_2' = (n, n-1, n-2)K'$. The independent vectors in $<K \cup L_2>$ include those in K and, moreover, vectors $u_{r-1,r} = (0 \ldots, 0, 1, 1)$ and $u_{r-2,r} = (0 \ldots, 0, 1, 0, 1)$ which are independent from $< K >$ by Lemma 3.3. There exist some vectors in $<K>$ with different values in the last three coordinates (e.g. $(x, 001), (x, 010), (x, 100)$), such that adding pairwise these vectors to the corresponding vectors in L_2 we find vectors $u_{r-1,r}$ and $u_{r-2,r}$. So, the rank of the corresponding Hadamard code of $S \otimes [K', L_2']$ is $dim(<K \cup L_2>) + 1 = r + 3$.

In the same way, we can form matrices $L_i' = \pi_{0,i}(L_{i-1}')$ or equivalently by taking cyclic shifts $L_i' = (n, n-1, \ldots, n-i)K'$, of $i+1 \leq r$ independent columns in K'. Hence if you assume we have a Hadamard code of length $n/2 = 2^{t-1}$ and rank $r \in \{t, t+1, \cdots, n/4\}$ we can construct new Hadamard codes of twice the length $n = 2^t$ and rank from $r+1$ to $2r$ which, in general, gives us Hadamard codes of rank from $t+1$ to $n/2$.

We know that for length $n = 16$ there exist non-equivalent Hadamard codes H of all possible ranks, so $rank(H) = r \in \{5, 6, 7, 8\}$. Hence, starting from one of these Hadamard codes and using the above arguments we can construct Hadamard codes of length 32 and rank from 6 to 16, and recursively for any length $n = 2^t$ ($t > 4$). ∎

IV. Bounds on the rank and the dimension of the kernel

In this section we will give an upper and lower bound on the rank, in terms of the dimension of the kernel.

Proposition 4.1: A non-linear Hadamard code of length $n = 2^t$ ($t \geq 4$) with rank r and a kernel of dimension k satisfies

$$r \leq \begin{cases} 2^{t+1-k} + k - 1 & \text{if} \quad 3 \leq k \leq t-1 \\ 2^{t-1} & \text{if} \quad 1 \leq k \leq 2 \end{cases}$$

Proof: Let H be a Hadamard code of length $n = 2^t$ with rank r and a kernel of dimension k. We know that $K(H)$ is the largest linear subspace in H such that H can be written as the union of cosets of $K(H)$ and that the cosets of $K(H)$ form a partition of H. There are 2^{t+1-k} cosets in H. When each coset has an independent vector, the rank is maximum, so $r \leq 2^{t+1-k} + k - 1$. This same argument was used in [10] for 1-perfect codes. For $k = 1$ and $k = 2$, $2^{t+1-k} + k - 1 > 2^{t-1}$, but by Proposition 3.4 we know that $r \leq n/2 = 2^{t-1}$, so in these two cases the upper bound is 2^{t-1}. ∎

Lemma 4.2: There exist Hadamard codes of length $n = 2^t$ ($t \geq 4$), rank $t+2$ having a kernel of dimension 3.

Proof: Let S_t denote the linear Hadamard code of length $n = 2^t$ generated by words $\mathbf{1}, v_1, v_2, \ldots, v_t$. Consider the sub-code $K = <\mathbf{1}, v_1, v_2>$ of S_t. Define $H = (S_t \setminus (K + w)) \cup (K + v_1v_2 + w)$ for $w \in S_t \setminus K$. Then H is a Hadamard code of rank $t+2$ having kernel K of dimension 3. To prove that the minimum distance between codewords is 2^{t-1} it suffices to show that this is the minimum weight for the words of type $v_1v_2 + y$ for any $y \in S_t \setminus K$. Assume $v_1v_2 = (\underbrace{11\ldots1}, 00\ldots0)$, where the ones cover the first $n/4$ coordinates and $y = (\underbrace{y_1}, y_0) \in S_t \setminus K$. Then $y + v_1v_2 = (\underbrace{y_1 + 11\ldots1}, y_0)$ and $yv_1v_2 = (\underbrace{y_1}, 00\ldots0)$, so the weight of y_1 is 2^{t-3}. Thus $y_1 + 11\ldots1$ also has weight 2^{t-3} and $y + v_1v_2$ has weight 2^{t-1}. ∎

Lemma 4.3: There exist Hadamard codes of length $n = 2^t$ ($t > 4$), rank $t+3$ having a kernel of dimension 1.

Proof: Let S_t denote the linear Hadamard code of length $n = 2^t$ generated by words $\mathbf{1}, v_1, v_2, \ldots, v_t$ ($t \geq 5$). Consider the sub-codes $K_{12} = <\mathbf{1}, v_1, v_2>$ and $K_{34} = <\mathbf{1}, v_3, v_4>$ of S_t. Define $H_{12} = (S_t \setminus (K_{12} + v_5)) \cup (K_{12} + v_1v_2 + v_5)$. Then from Lemma 4.2 H_{12} is a Hadamard code of rank $t+2$ having kernel K_{12} of dimension 3. Now define $H = (H_{12} \setminus (K_{34} + v_1)) \cup (K_{34} + v_3v_4 + v_1)$.

The claim is that H is a Hadamard code of rank $t+3$ with a kernel of dimension 1 (the intersection of K_{12} and K_{34}). To prove that the minimum distance between codewords is 2^{t-1} it suffices to show that this is the minimum weight for the words of type $v_1v_2 + v_3v_4 + y$ for any $y \in S_t \setminus <\mathbf{1}, v_1, v_2, v_3, v_4>$, but the proof is straightforward using arguments similar to those in the previous Lemma 4.2. ∎

Next lemma is a generalization to non-linear Hadamard codes of a Perseval equation (see [7, Corollary 3, page 416]) for the linear case.

Lemma 4.4: Let H be a Hadamard code of length $n = 2^t$, $\mathbf{0} \neq s \in \mathbb{Z}_2^n$ and $S = supp(s)$. Then $|S|^2 - 2^t|S| + 2\sum_h x_h^2 = 0$, where the sum is extended to all the vectors $h \in H$ of weight 2^{t-1} and x_h is such that $|supp(s) \cap supp(h)| = |S|/2 \pm x_h$.

Proof: Consider a vector $s \in \mathbb{Z}_2^n$ and compute $\sum_h |supp(s) \cap supp(h)|^2$ extended to all the vectors $h \in H$ of weight 2^{t-1}.

We will use $\chi_h(a)$ which is either one or zero depending on whether a belongs or it does not belong to $supp(h)$.

Let $a, b \in S$ and $h \in H$ of weight 2^{t-1}. Then:

$$\sum_h |supp(s) \cap supp(h)|^2 =$$

$$= \sum_h \Big(\sum_{a \in S} \chi_h(a)\Big)^2 = \sum_{a \in S}\sum_{b \in S}\sum_h \chi_h(a)\chi_h(b) = \quad (2)$$

$$= |S|(2^t - 1) + |S|\,(|S| - 1)(2^{t-1} - 1)$$

In the right hand side the result comes from the (2^t-1) words in H which contain $a \in S$ and the $(2^{t-1}-1)$ through a pair $a, b \in S$.

In the left hand side the value of $|supp(s) \cap supp(h)|$ is exactly $|S|/2$ or, in general, $|supp(s) \cap supp(h)| = (|S|/2 + x_h)$ for $x_h \leq |S|/2$ and $|supp(s) \cap supp(\bar{h})| = (|S|/2 - x_h)$, where $\bar{h}$ means the complementary vector of h. So we can write $\sum_h |supp(s) \cap supp(h)|^2 = (|S|/2)^2(2^{t+1}-2) + \sum_h x_h^2$, where the sum $\sum_h$ is extended to all the vectors $h \in H$ of weight 2^{t-1}.

Finally, doing some operations, equation (2) could be seen as:

$$|S|^2 - 2^t|S| + 2\sum_h x_h^2 = 0 \qquad (3)$$

∎

Lemma 4.5: There do not exist Hadamard codes of length $n = 2^t$ ($t \geq 4$), rank $t+2$ having a kernel of dimension less than 3.

Proof: Let $s \in <H>$ is a vector of minimum weight $s \notin H$ and let $S = supp(s)$. As above let $|supp(s) \cap supp(h)| = |S|/2 \pm x_h$, for $h \in H$, $wt(h) = 2^{t-1}$. It follows that $wt(h+s) = 2^{t-1} \pm 2x_h$. Since by (3), we can not have all $x_h = 0$, we have that $|S| < 2^{t-1}$. It follows immediately from this that in fact there have to be at least two words $s, s' \in <H>$ having weight less than 2^{t-1}.

The rank of H is $t+2$, and the minimum distance is 2^{t-1}, so $H+s$ is disjoint from H and we can write $<H> = H \cup (H+s)$. This is true in fact for any word s' of weight less than 2^{t-1} in $<H>$. It follows that $H+s = H+s'$ or $H = H+s+s'$. Thus $s+s'$ is in the kernel of H. Let K be the linear sub-code of the kernel of H such that the words of weight less than 2^{t-1} in $<H>$ are in $K+s$.

It follows from the above argument that $dim(K) \geq 1$. Moreover, if $dim(K) = 1$, we would have only two vectors (the vector and its complement) such that $x_h \neq 0$ and $x_h \leq |S|/2$. Then, from equation (3):

$0 = |S|^2 - 2^t|S| + 2\sum_h x_h^2 \leq |S|^2 - 2^t|S| + 4(|S|/2)^2$, so $2^t|S| \leq 2|S|^2$ and $2^{t-1} \leq |S|$, which contradicts the assumption about s.

Hence, finally, K has at least two independent vectors and with the all-one vector the dimension of the kernel is greater or equal to three. ∎

Proposition 4.6: A non-linear Hadamard code of length $n = 2^t$ ($t > 4$) with rank r and a kernel of dimension k fulfills

$$r \geq \begin{cases} t+2 & \text{if} \quad 3 \leq k \leq t-1 \\ t+3 & \text{if} \quad 1 \leq k \leq 2 \end{cases}$$

Proof: It is straightforward from the previous lemmas. ∎

V. Hadamard codes with a given pair of parameters (r, k)

The bounds for r, k, the rank and the dimension of the kernel, given in section IV, are tight for $n = 16$ (see [1, p.266] and Table II). Next we will construct Hadamard codes of length $n = 2^t$ ($t > 4$) with ranks between the bounds established in Propositions 4.1 and 4.6, having kernels of dimension k.

TABLE II

Dimension of the kernels and ranks of Hadamard codes of length $n = 16$.

	$rank(C)$			
$ker(C)$	5	6	7	8
5	*			
3		*		
2			*	*
1				*

Lemma 5.1: Given a non-linear Hadamard code H of length $n = 2^t$ ($t \geq 4$) with rank r and kernel

of dimension k, there exist Hadamard codes of length $n = 2^{t+1}$ with rank $r + 1 + \delta$ and kernel of dimension $k + 1 - \delta \ \ \forall \delta \in \{0, \ldots, k\}$.

Proof: By Corollary 2.2 the corresponding Hadamard code of $S \otimes H'$ has rank $r+1$ and kernel of dimension $k+1$. By the same argument as in the proof of Proposition 3.4, for each $\delta \in \{1, \ldots, k\}$ there exists a permutation π_δ such that the corresponding Hadamard code of $C = S \otimes [H', \pi_\delta(H')]$ has rank $r+1+\delta$. These permutations represent a cyclic shift of $\delta + 1$ independent columns in H'. We can choose these columns in the following way. If $\delta = 1$, π_1 is a transposition that fixes $K(H)$ and in this case, by Lemma 2.4, the Hadamard code of C has kernel of dimension $k = k + 1 - 1$. If $\delta \in \{2, \ldots, k\}$, π_δ effects $\delta - 1$ vectors in $K(H)$, so C has kernel of dimension $k - (\delta - 1) = k + 1 - \delta$. ∎

Lemma 5.2: There exist Hadamard codes of length $n = 2^t$ ($t \geq 4$) with kernel of dimension 1 and rank $r, \ \forall r \in \{2t, \ldots, n/2\}$.

Proof: For $t = 4$ it is true. Let H be a Hadamard code of length 2^{t-1}, rank $2(t-1)$ and kernel of dimension 1. By Lemma 5.1 there exists a Hadamard code of length $n = 2^t$, rank $2(t-1)+2 = 2t$ and kernel of dimension 1. The result follows using Lemma 2.4 and the same argument as in the proof of Proposition 3.4. ∎

Lemma 5.3: There exist Hadamard codes of length $n = 2^t$ ($t \geq 4$) with kernel of dimension 2 and rank $r, \ \forall r \in \{2^{t-2} + 3, \ldots, n/2\}$.

Proof: The Hadamard codes considered in Lemma 5.2 have a kernel of dimension 1 and were constructed using the Kronecker product. After a normalization we can always assume there exists a column c with all the coordinates one and, so another column c' with half the coordinates equal to one and the other half equal to zero. If we take the transposed matrix, we obtain a new Hadamard code with dimension of the kernel at least two (the two independent vectors in the kernel are the rows c^T and c'^T).

From Proposition 4.1 we know there does not exist any Hadamard code with dimension of the kernel greater than two and rank greater or equal to $2^{t-2} + 3$. Hence, when the rank has these values we conclude that the dimension of the kernel is 2. ∎

Apart from the linear Hadamard code, by Lemmas 5.1, 5.2 and 5.3, we can construct any Hadamard code of length $n = 2^t$ ($t > 4$) with kernel of dimension k and rank r such that

$$2t + 1 - k \leq r$$

$$r \leq \begin{cases} 2^{t+1-k} + k - 1 & \text{if} \quad 3 \leq k \leq t-1 \\ 2^{t-1} & \text{if} \quad 1 \leq k \leq 2 \end{cases} \tag{4}$$

except for the cases when the rank is $r = 2^{t+1-k} + k - 1$ for each $3 \leq k \leq t-2$ and the dimension of the kernel is k or $k-1$. For example, in Tables III and IV, for $t = 5$ and $t = 6$ respectively, the constructed codes are denoted by $\star$ and the exceptions by $\circ$.

The next lemmas and propositions settle the remaining cases needed to establish the existence of a Hadamard code for all the admissible pairs (r, k), where r is the rank and k the dimension of the kernel.

Proposition 5.4: There exists a Hadamard code of length $n = 2^t$ ($t > 4$) with kernel of dimension k and rank r for all r such that

$$\left.\begin{array}{lll} \text{if} & 3 \leq k \leq t-1 & t+2 \\ \text{if} & 1 \leq k \leq 2 & t+3 \end{array}\right\} \leq r \leq 2t + 1 - k \tag{5}$$

Proof: By Lemma 4.2 there exists a Hadamard code with kernel of dimension 3 and rank $t + 2$ and by Lemma 4.3 one with kernel of dimension 1 and rank $t + 3$. Let H_1, H_2 be Hadamard codes of length 16 with $r = 7$, $k = 2$ and $r = 8$, $r = 1$ respectively, such that $S_4 \subseteq < H_1 >$ and $S_4 \subseteq < H_2 >$ (see [1]).

TABLE III

DIMENSION OF THE KERNELS AND RANKS OF HADAMARD CODES OF LENGTH $n = 32$.

	$rank(C)$										
$ker(C)$	6	7	8	9	10	11	12	13	14	15	16
6	*										
4		$\star$									
3		$\bullet$	$\star$	$\star$	$\circ$						
2			$\bullet$	$\star$	$\circ$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$
1			$\bullet$	$\bullet$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$	$\star$

TABLE IV

DIMENSION OF THE KERNELS AND RANKS OF HADAMARD CODES OF LENGTH $n = 64$.

	$rank(C)$													
$ker(C)$	7	8	9	10	11	12	13	...	17	18	19	20	...	32
7	*													
5		$\star$												
4		$\bullet$	$\star$	$\star$	$\circ$									
3		$\bullet$	$\bullet$	$\star$	$\circ$	$\star$	$\star$	...	$\star$	$\circ$				
2			$\bullet$	$\bullet$	$\star$	$\star$	$\star$	...	$\star$	$\circ$	$\star$	$\star$	...	$\star$
1			$\bullet$	$\bullet$	$\bullet$	$\star$	$\star$	...	$\star$	$\star$	$\star$	$\star$	...	$\star$

Then, for $n = 32$ the corresponding Hadamard codes of $S \otimes [S'_4, H'_1]$ and $S \otimes [S'_4, H'_2]$ have $r = 8$, $k = 2$ and $r = 9$, $k = 1$ respectively, by Lemmas 2.3 and 2.4. Finally, by using induction and Lemma 5.1 it is easy to prove the statement. ∎

For example, in Tables III and IV, for $t = 5$ and $t = 6$ respectively, these codes are denoted by $\bullet$. This last proposition also shows that, once the dimension of the kernel is fixed, the lower bound for the rank given by Proposition 4.6 is tight.

Note that so far, we know how to construct a Hadamard code of length $n = 2^t$ ($t \geq 4$) with a kernel of dimension k, for any admissible rank except for the cases when the rank is $r = 2^{t+1-k} + k - 1$ for each $3 \leq k \leq t - 2$ and the dimension of the kernel is k or $k - 1$.

Also note that it is not necessary to construct Hadamard codes for all these cases. Using the above lemmas recursively, we only need to consider the cases when the dimension of the kernel is $k = 3$ and 2 and the rank is $r = 2^{t-2} + 2$ which we will do in the next proposition.

Proposition 5.5: There exist Hadamard codes of length $n = 2^t$ ($t > 4$) with rank $r = 2^{t-2} + 2$ and dimension of the kernel $k = 3$ and $k = 2$.

Proof: By Lemma 5.3 we know there exists a Hadamard code H of length $n = 2^{t-1}$ ($t > 5$) with rank 2^{t-2} and dimension of the kernel 2. For $t = 5$ there also exists a Hadamard code of length $n = 16$ with rank 8 and dimension of the kernel 2. Using Lemma 5.1 we get a Hadamard code of length $n = 2^t$ with rank $2^{t-2} + 2$ and dimension of the kernel $k = 2$.

The construction of the other code is not so straightforward. Start with a Hadamard code H (which exists by Lemma 5.1) of length $n = 2^t$ ($t > 4$) with rank $2^{t-2}+1$ and dimension of the kernel 3. Assume (after a coordinate permutation if it is needed) the basis vectors for the kernel $K(H)$ are $\mathbf{1}, v_1, v_2$, as they are defined in equation (1). Let L be a code whose codewords are those in K and $x+v_1v_2$ for all $x \in H \setminus K$. Following the same argument as in Lemma 4.2 it is easy to prove that L is a Hadamard code. The kernel of this code L is K and $rank(L) = rank(H) + 1$ because $<L>=<H, v_1v_2>$. Hence, code L is a Hadamard code of length $n = 2^t$ ($t > 4$) with rank $2^{t-2} + 2$ and dimension of the kernel $k = 3$. ∎

Finally, we have established the next theorem which summarizes all the results in this section.

Theorem 5.6: There exist Hadamard codes of length $n = 2^t$ ($t > 4$) with kernel of dimension k and rank r for all r such that

$$\begin{cases} t+2 \leq r \leq 2^{t+1-k} + k - 1 & \text{if} \quad 3 \leq k \leq t-1 \\ t+3 \leq r \leq 2^{t-1} & \text{if} \quad 1 \leq k \leq 2 \end{cases} \tag{6}$$

VI. Conclusions

The p-ranks of Hadamard matrices (or equivalently, of Hadamard designs), that is the ranks over a field of characteristic p, have been widely studied (see, for instance, [1]). These parameters have been sometimes used to distinguish between non-equivalent Hadamard matrices, since equivalent ones have the same p-ranks.

In the present paper, for Hadamard matrices of order a power of two, we studied another parameter, the dimension of the kernel of its corresponding binary Hadamard code, together with the 2-rank. We proved the existence of Hadamard codes of length $n = 2^t$ for any possible dimension of the kernel and any possible 2-rank.

Actually, apart from the linear Hadamard code, by the results in Section V, we can construct any Hadamard code of length $n = 2^t$ ($t > 4$), kernel of dimension k and 2-rank r as long as

$$\begin{cases} t+2 \leq r \leq 2^{t+1-k} + k - 1 & \text{if} \quad 3 \leq k \leq t-1 \\ t+3 \leq r \leq 2^{t-1} & \text{if} \quad 1 \leq k \leq 2 \end{cases} \tag{7}$$

This means that we can get any Hadamard code of length $n = 2^t$ with any possible rank between the lower and upper bounds, given the dimension of the kernel. These bounds are given by Propositions 4.6 and 4.1.

In [1], it was mentioned that the linear span of all Hadamard codes of length 2^t investigated by the authors contained as a sub-code the linear Hadamard code. This was found to be true of the examples investigated as part of the present research. It would be interesting to establish whether this was always true. Such a result would simplify a number of the arguments in this paper.

Other possible lines for future research, on Hadamard codes, could be to further analyze the relationship between the dimension of the kernel and the p-ranks in order to obtain the possible p-ranks for a given kernel.

Acknowledgment

The authors want to thank the anonymous referees for their work in reviewing this manuscript. Their comments have enabled us to improve the presentation of this paper.

References

[1] E. F. Assmus Jr. and J. D. Key, *Designs and their codes*, Cambridge University Press, Great Britain (1992).

[2] H. Bauer, B. Ganter, F. Hergert, *Algebraic techniques for nonlinear codes*, Combinatorica, Vol. 3 (1983) pp. 21-33.

[3] J. Borges, K. T. Phelps and J. Rifà, *The rank and kernel of extended 1-perfect $\mathbb{Z}_4$-linear codes and additive non-$\mathbb{Z}_4$-linear codes*, IEEE Transactions on Information Theory, Vol. 49, No. 8 (2003) pp. 2028-2034.

[4] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam (1997).

[5] J. Hadamard, *Résolution d'une question relative aux déterminants*, Bulletin des Sciences Mathématiques, 17 (1893) pp. 240-246.

[6] D. S. Krotov, $\mathbb{Z}_4$*-linear Hadamard and extended perfect codes*, Procs. of the International Workshop on Coding and Cryptography, Paris (France), Jan. 8-12 (2001) pp. 329-334.

[7] F. I. MacWilliams and N. J. Sloane, *The theory of Error-Correcting codes*, North-Holland, New York (1977).

[8] K. T. Phelps, J. Rifà and M. Villanueva, *Rank and Kernel of additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes*, Proceedings of ACCT'04 conference. Kranevo, Bulgary, June 2004.

[9] K. T. Phelps, J. Rifà and M. Villanueva, *On the additive ($\mathbb{Z}_4$-linear and non-$\mathbb{Z}_4$-linear) Hadamard codes. Rank and Kernel*, submitted to IEEE Transactions on Information Theory.

[10] K. T. Phelps and M. Villanueva, *On Perfect Codes: Rank and Kernel*, Designs, Codes and Cryptography, Vol. 27 (2002) pp. 183-194.