SIAM J. DISCRETE MATH.
Vol. 11, No. 2, pp. 205–223, May 1998

003

ON PERFECT CODES AND TILINGS: PROBLEMS AND SOLUTIONS*

TUVI ETZION† AND ALEXANDER VARDY‡

Abstract. Although nontrivial perfect binary codes exist only for length $n = 2^m - 1$ with $m \geq 3$ and for length $n = 23$, many problems concerning these codes remain unsolved. Herein, we present solutions to some of these problems. In particular, we show that the smallest nonempty intersection of two perfect codes of length $2^m - 1$ consists of two codewords, for all $m \geq 3$. We also provide a complete solution to the intersection number problem for Hamming codes. Furthermore, we prove that a perfect code of length $2^{m-1} - 1$ is embedded in a perfect code $\mathbb{C}$ of length $2^m - 1$ if and only if $\mathbb{C}$ is not of full rank. This result implies the existence of distinct generalized Hamming weights for perfect codes, and we determine completely the generalized Hamming weights of all perfect codes that do not contain embedded full-rank perfect codes. We further explore the close ties between perfect codes and tilings: we prove that full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 14$ and show that the existence of full-rank tilings for other n is closely related to the existence of full-rank perfect codes with kernels of high dimension. We briefly survey the present state of knowledge on perfect binary codes and list several interesting and important open problems concerning perfect codes and tilings.

Key words. perfect codes, tilings, intersection, embedding, rank, kernel

AMS subject classifications. O5A18, O5B40, 20K01, 94B25, 94B60

PII. S0895480196309171

1. Introduction.

Let $\mathbb{F}_2^n$ be a vector space of dimension n over GF(2). A subset of $\mathbb{F}_2^n$ is a binary code of length n. Two codes $\mathbb{C}_1, \mathbb{C}_2 \subset \mathbb{F}_2^n$ are *isomorphic* if there exists a permutation π such that $\mathbb{C}_2 = \pi(\mathbb{C}_1) = \{\pi(c) : c \in \mathbb{C}_1\}$. They are *equivalent* if there exists a vector a and a permutation π such that $\mathbb{C}_2 = a + \pi(\mathbb{C}_1) = \{a + \pi(c) : c \in \mathbb{C}_1\}$. The Hamming *distance* between vectors $x, y \in \mathbb{F}_2^n$, denoted $d(x, y)$, is the number of coordinates in which x and y differ. The Hamming *weight* of x is given by $\mathrm{wt}(x) = d(x, \mathbf{0})$, where $\mathbf{0}$ is the all-zero vector. Without loss of generality, we shall assume (unless stated otherwise) that $\mathbf{0} \in \mathbb{C}$, throughout this paper. We let $\langle \mathbb{C} \rangle$ denote the linear span of a code $\mathbb{C} \subset \mathbb{F}_2^n$. The rank of $\mathbb{C}$, denoted $\mathsf{rank}(\mathbb{C})$, is the dimension of $\langle \mathbb{C} \rangle$. We say that $\mathbb{C}$ is of full-rank if $\mathsf{rank}(\mathbb{C}) = n$, or equivalently, if $\langle \mathbb{C} \rangle = \mathbb{F}_2^n$.

A binary code $\mathbb{C}$ of length n is *perfect* if, for some integer $r \geq 0$, every $x \in \mathbb{F}_2^n$ is within distance r from exactly one codeword of $\mathbb{C}$. The study of perfect codes has always been one of the most fascinating subjects in coding theory. It is shown in [32, 33, 38] that such codes exist only for $r = 0$, $r = n$, $r = (n-1)/2$ with n odd, $r = 1$ with $n = 2^m - 1$, and $r = 3$ with $n = 23$. The first three cases are trivial, while the last case corresponds to the well-known binary Golay code [20], which is known to be unique up to equivalence [7, 28, 29]. Thus the only parameters for which there

*Received by the editors September 10, 1996; accepted for publication (in revised form) May 8, 1997. This work was partially supported by grant 95-522 from the United States–Israel Binational Science Foundation.

http://www.siam.org/journals/sidma/11-2/30917.html

†Department of Computer Science, Technion–Israel Institute of Technology, Haifa 32000, Israel (etzion@cs.technion.ac.il). The research of this author was supported in part by the fund for promotion of sponsored research at the Technion.

‡Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 1308 W. Main Street, Urbana, IL 61801 (vardy@golay.csl.uiuc.edu). The research of this author was supported by the David and Lucile Packard Foundation, the National Science Foundation, and JSEP grant N00014–9610129.

exist inequivalent perfect binary codes are $r = 1$ and $n = 2^m - 1$, with $m \geq 4$, and we shall henceforth use the word "perfect" to refer specifically to codes of this type. The linear perfect codes are, again, unique up to equivalence — these are the well-known Hamming codes [20]. Nonlinear perfect codes were constructed and studied in [1, 5, 9, 12, 21, 23, 24, 26, 30, 35], among other works. Some of these constructions are outlined in the next section.

Although perfect binary codes have been the subject of much research, many interesting questions regarding these codes remain open. Herein, we provide answers to some of these questions. In section 3, we answer the question raised in [9] and show that, for each $m \geq 3$, there exist two perfect codes $\mathbb{C}_1, \mathbb{C}_2$ of length $n = 2^m - 1$ such that $|\mathbb{C}_1 \cap \mathbb{C}_2| = 2$. We also consider the more general problem of the *intersection numbers* of perfect codes and provide a complete solution to this problem for the linear (Hamming) perfect codes. In section 4, we consider the problem of embedding a perfect code $\mathbb{C}_1$ of length n_1 within a perfect code $\mathbb{C}_2$ of length $n_2 > n_1$. We prove that a perfect code of length $2^{m-1} - 1$ is embedded within a perfect code $\mathbb{C}$ of length $2^m - 1$ if and only if $\mathbb{C}$ is not of full rank. This result implies that perfect codes of the same length can have distinct generalized Hamming weights (cf. [36]) and distinct cardinality-length profiles (cf. [17]). We prove that the generalized Hamming weights of a perfect code $\mathbb{C}$ coincide with those of the Hamming code of the same length, provided there is no full-rank perfect code embedded in $\mathbb{C}$. In section 5, we investigate the connections between perfect codes and tilings, answering some of the questions that were left open in [5]. It was shown in [5] that full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 112$, and we prove in section 5 that, in fact, such tilings exist for all $n \geq 14$. Since full-rank tilings do not exist for $n \leq 7$ (cf. [5]), this leaves only six values of n unresolved. We show that the existence of full-rank tilings for these n is closely related to the existence of full-rank perfect codes with high-dimensional kernels. Finally, we conclude in section 6 with a list of open problems concerning perfect codes and tilings.

2. Constructions and properties of perfect codes. In this section, we briefly outline two constructions of perfect codes, termed Construction A and Construction B. These constructions will be used later in this paper. We also review some of the properties of these constructions, as well as certain properties of perfect codes in general, that are of relevance to our work.

We say that a code is *even* if all of its codewords have even weight. Given a code $\mathbb{C} \subset \mathbb{F}_2^n$ which is not even, we can extend it by an even parity coordinate to obtain an even code, called the *extended code* of $\mathbb{C}$. An even code $\mathbb{C}^*$ of length $n + 1 = 2^m$ is said to be *extended perfect* if it can be obtained by means of extending a perfect code of length n by an even parity coordinate. Notice that deleting any coordinate of an extended perfect code produces a perfect code. Also observe that Constructions A and B, described in what follows in the context of perfect codes, can be straightforwardly modified to produce extended perfect codes.

Let $\mathbb{E}_2^n$ denote the set of all the even-weight vectors in $\mathbb{F}_2^n$. For a code $\mathbb{C} \subset \mathbb{F}_2^n$ and a vector $a \in \mathbb{F}_2^n$, the code $a + \mathbb{C} = \{a + c : c \in \mathbb{C}\}$ is called a *translate* of $\mathbb{C}$. If $\mathbb{C}$ is linear, then a translate of $\mathbb{C}$ is also called a *coset*. Let e_i denote a vector of weight one with the nonzero entry in the ith position. It is easy to see that, for a perfect code $\mathbb{C} \subset \mathbb{F}_2^n$, the translates $\mathbb{C}, e_1 + \mathbb{C}, \ldots, e_n + \mathbb{C}$ form a partition of $\mathbb{F}_2^n$. Similarly, the set $\mathbb{E}_2^{n+1}$ can always be partitioned into even translates of an extended perfect code $\mathbb{C}^* \subset \mathbb{E}_2^{n+1}$. The following construction of perfect codes of length $2n + 1$ from perfect codes of length n is due to Phelps [23] and Solov'eva [30].

CONSTRUCTION A. *Let* $\mathbb{C}_0, \mathbb{C}_1, \ldots, \mathbb{C}_n$ *and* $\mathbb{C}_0^*, \mathbb{C}_1^*, \ldots, \mathbb{C}_n^*$ *be partitions of* $\mathbb{F}_2^n$ *and* $\mathbb{E}_2^{n+1}$*, into a perfect code and its translates, respectively, into an extended perfect code and its translates. Let* π *be a permutation on the set* $\{0, 1, \ldots, n\}$*. Then the code*

$$\mathbb{C}_{\mathrm{A}} \;=\; \{\, (x|\, y) \;:\; x \in \mathbb{C}_i, \quad y \in \mathbb{C}^*_{\pi(i)} \quad \text{for some } i = 0, 1, \ldots, n \,\},$$

where $(\cdot|\cdot)$ *denotes concatenation, is a perfect code of length* $2^{m+1} - 1$.

We say that a vector $a \in \mathbb{F}_2^n$ *covers* a subset $\mathcal{S}_a \subset \mathbb{F}_2^n$ if $\mathcal{S}_a = \{x : d(x, a) \le 1\}$. Similarly, we say that a code $\mathbb{C} \subset \mathbb{F}_2^n$ covers a subset $\mathcal{S}$ if

$$\mathcal{S} \;=\; \{\, x \;:\; \exists\, c \in \mathbb{C} \text{ such that } d(x, c) \le 1 \,\} \;=\; \cup_{c \in \mathbb{C}}\, \mathcal{S}_c.$$

We say that $\mathbb{C}$ *perfectly covers* $\mathcal{S}$ if $\mathbb{C}$ covers $\mathcal{S}$ and $d(\mathbb{C}) \stackrel{\text{def}}{=} \min_{x,y \in \mathbb{C}} d(x, y) = 3$. The following construction of perfect codes may be found in [9]; it can be viewed as a certain special case of the construction of Vasil'ev [35]. This construction leads to perfect codes with various useful properties, such as full-rank perfect codes or perfect codes with large intersections. First, we define the following codes:

$$\begin{aligned} \mathcal{A} &= \{\, (\, x \,|\, p(x) \,|\, x\,) \;:\; x \in \mathbb{F}_2^n \,\}, \\ \mathcal{B} &= \{\, (\, x \,|\, p(x)+1 \,|\, x\,) \;:\; x \in \mathbb{F}_2^n \,\}, \end{aligned} \tag{2.1}$$

where $p(x) = \mathrm{wt}(x) \bmod 2$ is the *parity* of x. The following lemma was established in Etzion and Vardy [9].

LEMMA 2.1. *The codes* $\mathcal{A}$ *and* $\mathcal{B}$ *perfectly cover the same subset of* $\mathbb{F}_2^{2n+1}$.

Lemma 2.1 will be used in the next section to construct perfect codes with small intersection.

CONSTRUCTION B. *Assume that* $\mathbb{C}_1$ *is a perfect code of the form* $\mathbb{C}_1 = \mathbb{C}' \cup (x + \mathcal{A})$*, where* $x = \mathbf{0}$ *or* $x \notin \mathcal{A}$*. Then the code* $\mathbb{C}_2 = \mathbb{C}' \cup (x + \mathcal{B})$ *is also a perfect code.*

Construction B follows immediately from Lemma 2.1. It is shown in [9] that the set $\mathcal{A}$ is a linear subcode of the Hamming code (in an appropriate permutation). Thus one can use Construction B to produce nonlinear perfect codes from the Hamming code. In [9], we have applied this construction m times to produce a *full-rank* perfect code of length $2^m - 1$ from the Hamming code of the same length, for all $m \ge 4$. A similar approach was subsequently used by Phelps and LeVan [26] to construct perfect codes with kernels of various dimensions, while generalizations to nonbinary perfect codes were developed in [8].

Another application of Construction B enables one to construct a large set of inequivalent perfect codes. Let $\mathcal{H}_m$ denote the Hamming code of length $n = 2^m - 1$, and let $c_1, c_2, \ldots, c_t$ be the coset representatives for $\mathcal{A}$ in $\mathcal{H}_m$, where $t = 2^{0.5(n+1)-m}$. By Lemma 2.1, the sets $c_i + \mathcal{A}$ and $c_i + \mathcal{B}$ perfectly cover the same subset of $\mathbb{F}_2^n$ for all i. Thus, we have the following.

THEOREM 2.2. *To each binary vector* $x = (x_1, x_2, \ldots, x_t)$*, there corresponds a perfect code*

$$\mathbb{C}_{\langle x \rangle} \;=\; \bigcup_{i=1}^{t} \big(c_i + x_i \mathcal{A} + \bar{x}_i \mathcal{B}\big),$$

where the notation $x_i\mathcal{A} + \bar{x}_i\mathcal{B}$ *stands for either* $\mathcal{A}$ *if* $x_i = 1$ *or* $\mathcal{B}$ *if* $x_i = 0$.

Theorem 2.2 produces a set of $2^t = 2^{2^{0.5(n+1)-\log(n+1)}}$ distinct perfect codes. It was shown in [9] that the number of inequivalent perfect codes in this set is close to $2^{2^{0.5n}}$ for large n.

The weight distribution of a perfect code is uniquely determined [20, p. 129] by its length n. An explicit closed-form expression for the weight distribution of perfect codes may be found in [9]. In particular, it is known that any perfect code $\mathbb{C}$ of length n that contains $\mathbf{0}$ also contains $\mathbf{1}$ — the unique binary vector of weight n. It follows that $\mathbf{1}$ belongs to $c+\mathbb{C}$ for all $c\in\mathbb{C}$. This, in turn, implies that if $c\in\mathbb{C}$, then also $\bar{c}\in\mathbb{C}$, where $\bar{c}=\mathbf{1}+c$ is the binary complement of c. Codes with this property are called *self-complementary*, and the foregoing observation shows that all perfect codes are self-complementary.

3. Intersections of perfect codes. Given two binary codes $\mathbb{C}_1,\mathbb{C}_2$ of the same length, the *intersection number* of $\mathbb{C}_1$ and $\mathbb{C}_2$ is defined as $\eta(\mathbb{C}_1,\mathbb{C}_2)\stackrel{\text{def}}{=}|\mathbb{C}_1\cap\mathbb{C}_2|$. In this section, we consider the following problem: what are the possible intersection numbers of perfect codes of a given length? The *largest* possible intersection number of perfect codes was determined in [9]. Specifically, it was shown in [9] that if $\mathbb{C}_1,\mathbb{C}_2$ are two distinct perfect codes of length $n=2^m-1$, then

$$\eta(\mathbb{C}_1,\mathbb{C}_2)\le 2^{2^m-m-1}-2^{2^{m-1}-1}$$

and this bound is tight; namely, for all $m\ge 3$ there exist perfect codes $\mathbb{C}_1,\mathbb{C}_2$ of length 2^m-1 such that $\eta(\mathbb{C}_1,\mathbb{C}_2)=2^{2^m-m-1}-2^{2^{m-1}-1}$.

A natural counterpart to this question is: what is the *smallest* possible (nonzero) intersection number of two perfect codes? It was shown [9] that for all $m\ge 3$ there exist two perfect codes $\mathbb{C}_1,\mathbb{C}_2$ of length 2^m-1 such that

$$\eta(\mathbb{C}_1,\mathbb{C}_2)=2^{2^{m-2}}.$$

However, the question of whether this intersection number is the smallest possible was left open in [9]. In fact, as will be shown in this section, it is not. Since all perfect codes are self-complementary, their intersection must have even cardinality. This implies that if $\mathbb{C}_1,\mathbb{C}_2$ are perfect codes and $\eta(\mathbb{C}_1,\mathbb{C}_2)\ne 0$, then $\eta(\mathbb{C}_1,\mathbb{C}_2)\ge 2$. In what follows, we prove that, for each $m\ge 3$, there exist two perfect codes $\mathbb{C}_1,\mathbb{C}_2$ of length 2^m-1 such that $\eta(\mathbb{C}_1,\mathbb{C}_2)=2$.

First, it is obvious that the intersection problem, in general, has the same answer for perfect codes and for extended perfect codes. We will use this simple fact later in the paper; we therefore state it formally as the following lemma.

LEMMA 3.1. *Perfect codes of length 2^m-1 with intersection number q exist if and only if there exist extended perfect codes of length 2^m with intersection number q.*

We now use a combination of Constructions A and B of the foregoing section to construct two extended perfect codes with intersection number 2. Let $\mathcal{H}_0$ be an extended Hamming code of length 2^m, and let $\mathcal{H}_1,\mathcal{H}_2,\ldots,\mathcal{H}_{2^m-1}$ be the even cosets of $\mathcal{H}_0$ in $\mathbb{E}_2^{2^m}$. Thus $\mathcal{H}_0,\mathcal{H}_1,\mathcal{H}_2,\ldots,\mathcal{H}_{2^m-1}$ is a partition of $\mathbb{E}_2^{2^m}$ into extended perfect codes. Hence, the code

$$\mathbb{C}\;=\;\{\,(x|\,y)\;:\;x,y\in\mathcal{H}_i\quad\text{for some } i=0,1,\ldots,2^m-1\,\} \tag{3.1}$$

is an extended perfect code of length 2^{m+1} obtained through Construction A, with π being the identity permutation. Furthermore, it can be easily verified that $\mathbb{C}$ is a linear code, and hence it must be an extended Hamming code of length 2^{m+1}. Without loss

of generality, we can assume that the parity-check matrix of $\mathbb{C}$ is given by

$$H_{m+1} \;=\; \begin{bmatrix} 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}. \tag{3.2}$$

That is, the columns of H_{m+1} are all of the $(m+1)$-tuples that end with a 1, ordered lexicographically. Indeed, it is easy to see that

$$H_{m+1} \;=\; \left[\begin{array}{c|c} 0 \cdots 0 & 1 \cdots 1 \\ \hline H_m & H_m \end{array}\right],$$

where H_m is a parity-check matrix for an extended Hamming code of length 2^m, which we take as $\mathcal{H}_0$. Thus the code defined by the parity-check matrix H_{m+1} is a Construction A perfect code consistent with (3.1). Notice that all the vectors in a given coset of $\mathcal{H}_0$ have the same syndrome with respect to H_m. That is, for all $i = 0, 1, \ldots, 2^m-1$, we have $s_i = H_m x^t$ for all $x \in \mathcal{H}_i$, and we say that s_i is the syndrome of $\mathcal{H}_i$.

We now use Construction B to modify the Hamming code $\mathbb{C}$ in (3.1) in an appropriate manner. Let

$$\mathcal{A}^* \;=\; \{\, (x|x) \;:\; x \in \mathcal{H}_i \quad \text{for some } i = 0, 1, \ldots, 2^m-1 \,\}. \tag{3.3}$$

Comparing (3.1) and (3.3), we see that $\mathcal{A}^*$ is a subcode of $\mathbb{C}$. Furthermore, since the codes $\mathcal{H}_0, \mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_{2^m-1}$ form a partition of $\mathbb{E}_2^{2^m}$, we can write

$$\mathcal{A}^* = \{\, (x|x) \;:\; x \in \mathbb{E}_2^{2^m} \,\},$$

which implies that $\mathcal{A}^*$ is just the extended code of $\mathcal{A}$ in (2.1). Pick a fixed integer j in the range $1 \le j \le 2^m$, and let $\mathcal{B}^* = (e_j|e_j) + \mathcal{A}^*$. Then $\mathcal{B}^*$ is the extended code of $\mathcal{B}$ in (2.1). This implies that the code

$$\mathbb{C}' \;=\; \big(\mathbb{C} \setminus \mathcal{A}^*\big) \cup \mathcal{B}^*$$

is an extended perfect code, obtained by Construction B. We note that $\mathbb{C}'$ does not contain the all-zero vector; however, the translate $\mathbb{C}_1 = (e_j|e_j) + \mathbb{C}'$ does. This translate is an extended perfect code, which can be written as $\mathbb{C}_1 = \mathcal{A}^* \cup \mathcal{D}$, where

$$\mathcal{D} \;=\; \{\, (x + e_j \,|\, y + e_j) \;:\; x, y \in \mathcal{H}_i \text{ and } x \ne y, \quad \text{for some } i = 0, 1, \ldots, 2^m-1 \,\}.$$

Now, let π be the permutation that fixes the last 2^m coordinates of $\mathbb{C}_1$ and effects the cyclic shift by one position on the first 2^m coordinates. Define $\mathbb{C}_2 = \pi(\mathbb{C}_1)$. Then obviously $\mathbb{C}_2$ is a perfect code, and we have the following.

THEOREM 3.2. *The intersection number of* $\mathbb{C}_1$ *and* $\mathbb{C}_2$ *is* $\eta(\mathbb{C}_1, \mathbb{C}_2) = 2$.

Proof. Suppose $(x|\,y) \in \mathbb{C}_1$, for some $x, y \in \mathbb{F}_2^{2^m}$. Then clearly $\mathrm{wt}(x) \equiv \mathrm{wt}(y) \equiv 0$ modulo 2 if and only if $x = y$ and $(x|\,y) \in \mathcal{A}^*$, while $\mathrm{wt}(x) \equiv \mathrm{wt}(y) \equiv 1 \bmod 2$ if and only if $(x|\,y) \in \mathcal{D}$. Since the permutation π preserves the weight of x and y, we have

$$\mathbb{C}_1 \cap \mathbb{C}_2 \;=\; \big(\mathcal{A}^* \cap \pi(\mathcal{A}^*)\big) \;\cup\; \big(\mathcal{D} \cap \pi(\mathcal{D})\big). \tag{3.4}$$

A vector $x \in \mathbb{F}_2^{2^m}$ is equal to its own cyclic shift by one position if and only if $x \in \{\mathbf{0}, \mathbf{1}\}$. Hence $\mathcal{A}^* \cap \pi(\mathcal{A}^*) = \{\mathbf{0}, \mathbf{1}\}$. We now show that $\mathcal{D} \cap \pi(\mathcal{D}) = \varnothing$. First, notice that for each $(x|\, y) \in \mathcal{D}$, we have

$$H_m x^t \;=\; H_m y^t \;=\; s_i + H_m(e_j)^t \tag{3.5}$$

for some $i = 0, 1, \ldots, 2^m - 1$. On the other hand, it can be shown that if $(x|\, y) \in \pi(\mathcal{D})$, then $H_m x^t \neq H_m y^t$. Indeed, let $(x'|\, y') \in \mathcal{D}$ be the preimage of $(x|\, y)$ under π. That is, $y = y'$ and x is the cyclic shift of x' by one position. Then $H_m y^t = H_m(y')^t = H_m(x')^t$ by (3.5). Now, both x' and its cyclic shift x have odd weight, and therefore

$$(0101\cdots01)(x')^t \;\neq\; (0101\cdots01)\, x^t.$$

Since $(0101\cdots01)$ is a row of H_m, it follows that $H_m x^t \neq H_m(x')^t = H_m(y)^t$. Comparing this with (3.5), we conclude that $\mathcal{D} \cap \pi(\mathcal{D}) = \varnothing$. In conjunction with (3.4), this implies that $\mathbb{C}_1 \cap \mathbb{C}_2 = \mathcal{A}^* \cap \pi(\mathcal{A}^*) = \{\mathbf{0}, \mathbf{1}\}$, and therefore $\eta(\mathbb{C}_1, \mathbb{C}_2) = 2$. □

It follows from Theorem 3.2 and the results of [9] that the intersection number of any two distinct perfect codes $\mathbb{C}_1, \mathbb{C}_2$ of length $n = 2^m - 1$ is in the range

$$2 \;\leq\; \eta(\mathbb{C}_1, \mathbb{C}_2) \;\leq\; 2^{2^m - m - 1} - 2^{2^{m-1} - 1}, \tag{3.6}$$

and both bounds are achievable for all $m \geq 3$. Since perfect codes are self-complementary, their intersection numbers must be even. Thus a natural question is: which even integers in the range of (3.6) are intersection numbers of perfect codes of length $2^m - 1$? Using Theorem 2.2 of the previous section, we obtain intersection numbers of the form

$$k\, 2^{2^{m-1} - 1} \quad \text{for all} \quad k = 1, 2, \ldots, 2^{2^{m-1} - m} - 1.$$

These correspond to the intersection of $\mathbb{C}_{\langle \mathbf{0} \rangle}$ with $\mathbb{C}_{\langle x \rangle}$, where x is a binary vector of length $t = 2^{2^{m-1} - m}$ and weight $t - k$. Further, using modifications of Constructions A and B, along with the techniques developed in this section, we can obtain many more intersection numbers. In general, however, the problem of enumerating all possible intersection numbers of perfect codes remains open. By and large, this appears to be a difficult problem. For perfect codes of length 15, we have generated a large set of intersection numbers through a combination of known constructions and computer search. Even for this case, however, complete enumeration does not seem to be within easy reach.

A variant of the problem discussed in the previous paragraph asks for all possible intersection numbers of *linear* perfect codes, namely, the Hamming codes of length $2^m - 1$. In what follows, we provide a complete solution to this problem.

Let $\mathcal{H}_1, \mathcal{H}_2$ be two Hamming codes of length $n = 2^m - 1$. Since Hamming codes are unique, $\mathcal{H}_1$ and $\mathcal{H}_2$ are necessarily isomorphic. Since both codes are linear, their intersection number is necessarily a power of 2. For $m = 3$ and $n = 7$, it is easy to find specific permutations such that $\eta(\mathcal{H}_1, \mathcal{H}_2) = 2, 4$, or 8. For example, let $\mathcal{H}_1$ be a code defined by the parity-check matrix whose columns are ordered lexicographically, and let $\mathcal{H}_2$ be a code defined by the parity-check matrix

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \tag{3.7}$$

respectively. We will show that a similar situation occurs for all $m \geq 3$, namely, all the powers of 2 in the range $2^{n-2m}, 2^{n-2m+1}, \ldots, 2^{n-m-1}$ are attainable as intersection numbers of distinct Hamming codes of length $n = 2^m - 1$.

Let H_1, H_2 be parity-check matrices of the Hamming codes $\mathcal{H}_1$ and $\mathcal{H}_2$ of length $n = 2^m - 1$. Then $\mathbb{C} = \mathcal{H}_1 \cap \mathcal{H}_2$ is a linear code, whose parity-check matrix is given by

$$H \;=\; \left[\begin{array}{c} H_1 \\ \hline H_2 \end{array}\right]. \tag{3.8}$$

For the sake of brevity, we shall henceforth write $H = H_1 \| H_2$ to denote the structure of (3.8). It is obvious that $\mathsf{rank}(H) \le 2m$, since H_1 and H_2 each have m rows, and therefore,

$$\eta(\mathcal{H}_1, \mathcal{H}_2) \;=\; |\mathbb{C}| \;=\; 2^{n-\mathsf{rank}(H)} \;\ge\; 2^{n-2m}.$$

It is also obvious that $\eta(\mathcal{H}_1, \mathcal{H}_2) \le 2^{n-m-1}$ if the codes $\mathcal{H}_1$ and $\mathcal{H}_2$ are distinct.

LEMMA 3.3. *For each $m \ge 3$, there exist two Hamming codes $\mathcal{H}_1, \mathcal{H}_2$ of length $n = 2^m - 1$ such that $\eta(\mathcal{H}_1, \mathcal{H}_2) = 2^{n-2m}$.*

Proof. As $\eta(\mathcal{H}_1, \mathcal{H}_2) = 2^{n-\mathsf{rank}(H)}$, we need to construct parity-check matrices H_1 and H_2 for the codes $\mathcal{H}_1$ and $\mathcal{H}_2$ such that $\mathsf{rank}(H_1 \| H_2) = 2m$. We first show that there exists a $2m \times 2m$ binary matrix $A_m = A_1 \| A_2$, where A_1, A_2 are two $m \times 2m$ binary matrices whose columns are distinct and nonzero, such that $\mathsf{rank}(A_m) = 2m$. For $m = 3$, such a matrix is given by

$$A_3 \;=\; \left[\begin{array}{c} 1\,0\,0\,0\,1\,1 \\ 0\,1\,0\,1\,0\,1 \\ 0\,0\,1\,1\,1\,0 \\ \hline 1\,0\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1\,1 \\ 0\,0\,1\,0\,1\,1 \end{array}\right].$$

For $m \ge 4$, we can construct A_m recursively as follows. Suppose that $A_{m-1} = A'_1 \| A'_2$, and take

$$A_m \;=\; \left[\begin{array}{c} A_1 \\ \hline A_2 \end{array}\right] \;=\; \left[\begin{array}{c|c|c} 1 & 0\cdots0 & 0 \\ \hline \mathbf{0} & A'_1 & x \\ \hline \mathbf{1} & A'_2 & \mathbf{0} \\ \hline 1 & 0\cdots0 & 1 \end{array}\right], \tag{3.9}$$

where x is any nonzero $(m-1)$-tuple that does not appear as a column of A'_1. It is easy to see from (3.9) that if A_{m-1} is a nonsingular matrix of rank $2(m-1)$, then A_m is a nonsingular matrix of rank $2m$. Now, since the columns of A_1 and A_2 are nonzero and distinct, these matrices can be extended, in an arbitrary manner, to parity-check matrices H_1 and H_2 of two Hamming codes of length $2^m - 1$. By construction, we have $\mathsf{rank}(H_1 \| H_2) = \mathsf{rank}(A_1 \| A_2) = 2m$. □

THEOREM 3.4. *For each $m \ge 3$, there exist two Hamming codes $\mathcal{H}_1, \mathcal{H}_2$ of length $n = 2^m - 1$, such that*

$$\eta(\mathcal{H}_1, \mathcal{H}_2) \;=\; 2^{n-r} \quad \textit{for} \quad r = m{+}1, m{+}2, \ldots, 2m.$$

Proof. The proof is by induction on m. The induction basis for $m = 3$ is established in (3.7). Now assume that, for each $r = m, m{+}1, \ldots, 2(m{-}1)$, there exist parity-check matrices H'_1 and H'_2 of two Hamming codes of length $2^{m-1} - 1$, such that $\mathsf{rank}(H'_1 \| H'_2) = r$. Take

$$H_1 \;=\; \left[\begin{array}{c|c|c} 0\cdots0 & 1 & 1\cdots1 \\ \hline H'_1 & \mathbf{0} & H'_1 \end{array}\right], \qquad H_2 \;=\; \left[\begin{array}{c|c|c} 0\cdots0 & 1 & 1\cdots1 \\ \hline H'_2 & \mathbf{0} & H'_2 \end{array}\right].$$

It is easy to see that H_1, H_2 are parity-check matrices of isomorphic Hamming codes of length $2^m - 1$, and that

$$\mathsf{rank}(H_1 \| H_2) \;=\; \mathsf{rank}(H_1' \| H_2') + 1 \;=\; r + 1.$$

Thus, all ranks in the range $r + 1 = m+1, m+2, \ldots, 2m-1$ are attainable. Finally, the rank of $2m$ is also attainable by Lemma 3.3, which completes the induction step. □

4. Embeddings and generalized Hamming weights. Let $\mathbb{C}_1$ be a code of length n_1, and let $\mathbb{C}_2$ be a code of length $n_2 \geq n_1$. We say that $\mathbb{C}_1$ is *embedded* in $\mathbb{C}_2$, in the first n_1 positions, if the code $\mathbb{C}_2$ punctured in the last $n_2 - n_1$ positions contains $\mathbb{C}_1$ as a subcode, and furthermore all the codewords of $\mathbb{C}_2$ that correspond to this subcode agree in the last $n_2 - n_1$ positions. This definition extends in the obvious way to any set of n_1 positions. Thus we say that $\mathbb{C}_1$ is *embedded* in $\mathbb{C}_2$ if it is embedded in some n_1 positions of $\mathbb{C}_2$. We note that our definition of embedding is a natural generalization of the concept of *shortening* (cf. [20, p. 29]) to nonlinear codes.

It is well known that any Hamming code of length $n = 2^m - 1$ contains a Hamming code of length $\nu = 2^{m-1}$–1 as a shortened subcode. Under which conditions is a similar assertion true for nonlinear perfect codes? Namely, when does a perfect code $\mathbb{C}$ of length $n = 2^m - 1$ contain a perfect code of length $\nu = 2^{m-1} - 1$ embedded in it? In what follows, we will prove that this happens if and only if $\mathbb{C}$ is not of full rank.

For a code $\mathbb{C} \subset \mathbb{F}_2^n$, we denote by $\mathbb{C}^\perp$ the subspace of $\mathbb{F}_2^n$ consisting of those vectors that are orthogonal to all the codewords of $\mathbb{C}$. It is obvious that $\dim \mathbb{C}^\perp + \dim \langle \mathbb{C} \rangle = n$, and therefore $\mathbb{C}$ is full rank if and only if $\mathbb{C}^\perp = \{\mathbf{0}\}$. The following observation, established in [9], will be key to our results in this section: for a perfect code $\mathbb{C}$ of length $n = 2^m - 1$, all the nonzero codewords in $\mathbb{C}^\perp$ have weight 2^{m-1}.

PROPOSITION 4.1. *If $\mathbb{C}$ is a perfect code of length $n = 2^m - 1$ and $\mathsf{rank}(\mathbb{C}) < n$, then there exists a perfect code of length $\nu = 2^{m-1} - 1$ embedded in $\mathbb{C}$.*

Proof. Let v be a codeword of $\mathbb{C}^\perp$ of weight 2^{m-1}. Without loss of generality, we can assume that $v = (\mathbf{1}|\mathbf{0})$ so that every codeword of $\mathbb{C}$ has even weight in the first 2^{m-1} positions. For $x \in \mathbb{E}_2^{\nu+1}$, define $\mathbb{C}_x = \{y : (x|\, y) \in \mathbb{C}\}$. Then either $\mathbb{C}_x = \varnothing$ or $\mathbb{C}_x$ is a code of length $\nu = 2^{m-1} - 1$ embedded in $\mathbb{C}$. We will show that, in fact, $\mathbb{C}_x$ is a perfect code for all x. Indeed, if $\mathbb{C}_x \neq \varnothing$, then $d(\mathbb{C}_x) \geq 3$ and therefore $|\mathbb{C}_x| \leq 2^{2^{m-1}-m}$. Hence,

$$2^{2^m - m - 1} \;=\; |\mathbb{C}| \;=\; \sum_x |\mathbb{C}_x| \;\leq\; 2^{2^{m-1}-m} \left|\mathbb{E}_2^{2^{m-1}}\right| \;=\; 2^{2^m - m - 1}. \tag{4.1}$$

Since (4.1) must hold with equality, for all $x \in \mathbb{E}_2^{2^{m-1}}$ we have $|\mathbb{C}_x| = 2^{2^{m-1}-m}$, and $\mathbb{C}_x$ is a perfect code of length ν embedded in $\mathbb{C}$. □

PROPOSITION 4.2. *If $\mathbb{C}$ is a perfect code of length $n = 2^m - 1$ and $\mathsf{rank}(\mathbb{C}) = n$, there is no perfect code of length $\nu = 2^{m-1} - 1$ embedded in $\mathbb{C}$.*

Proof. Assume to the contrary that $\mathbb{C}_1$ is a perfect code of length ν embedded in the last ν positions of $\mathbb{C}$. Then $\mathbb{C}$ contains $|\mathbb{C}_1| = 2^{\nu-(m-1)}$ codewords of the form $(a|c)$, where $a = (a_1, a_2, \ldots, a_{\nu+1})$ is a fixed $(\nu+1)$-tuple. Now let M be a $|\mathbb{C}| \times (\nu+1)$ matrix whose rows are the codewords of $\mathbb{C}$ truncated to the first $\nu + 1$ positions. For $x \in \mathbb{F}_2^\nu$, let $\omega_0(x)$, respectively, $\omega_1(x)$, denote the number of times $(x|0)$, respectively, $(x|1)$, appears as a row of M. Since $\mathbb{C}$ is an orthogonal array of strength ν (cf. [20, p. 139]), it is obvious that $\omega_0(x) + \omega_1(x) = |\mathbb{C}|/2^\nu = 2^{\nu-(m-1)}$ for

all x. Furthermore, it is shown in Proposition 4.2 of [9] that

$$\omega_0(x) = \begin{cases} \omega_0(\mathbf{0}) & \text{if } \mathrm{wt}(x) \equiv 0 \mod 2, \\ \omega_1(\mathbf{0}) & \text{if } \mathrm{wt}(x) \equiv 1 \mod 2. \end{cases} \tag{4.2}$$

Observe that since $\mathbb{C}$ contains the all-zero codeword $\mathbf{0}$, we have $\omega_0(\mathbf{0}) \neq 0$. Now consider $x = (a_1, a_2, \ldots, a_\nu)$; it is clear that either $\omega_0(x) = 2^{\nu-(m-1)}$ if $a_{\nu+1} = 0$, or $\omega_1(x) = 2^{\nu-(m-1)}$ if $a_{\nu+1} = 1$. In either case, this implies that $\omega_0(\mathbf{0}) = 2^{\nu-(m-1)}$ in view of (4.2) and the fact that $\omega_0(\mathbf{0}) \neq 0$. We can now count the number of even-weight rows of M, given by

$$\sum_{\substack{x \in \mathbb{F}_2^\nu \\ \mathrm{wt}(x) \equiv 0}} \omega_0(x) + \sum_{\substack{x \in \mathbb{F}_2^\nu \\ \mathrm{wt}(x) \equiv 1}} \omega_1(x) = 2^{\nu-1}\omega_0(\mathbf{0}) + 2^{\nu-1}\omega_0(\mathbf{0}) = 2^\nu \cdot 2^{\nu-(m-1)} = |\mathbb{C}|.$$

Thus *all* the codewords of $\mathbb{C}$ have even weight in the first $\nu+1$ positions, which implies that the vector $(\mathbf{1}|\mathbf{0})$ of weight $\nu+1$ is orthogonal to $\mathbb{C}$. Hence $\mathbb{C}^\perp \neq \{\mathbf{0}\}$, which contradicts the fact that $\mathbb{C}$ is of full rank. □

Propositions 4.1 and 4.2 show that those sets of positions, where a perfect code of length $\nu = 2^{m-1}-1$ is embedded in a perfect code $\mathbb{C}$ of length $n = 2^m - 1$, are in one-to-one correspondence with nonzero codewords of $\mathbb{C}^\perp$. In particular, we have the following corollary.

COROLLARY 4.3. *Let $\mathbb{C}$ be a perfect code of length $2^m - 1$. A perfect code of length $2^{m-1}-1$ is embedded in $\mathbb{C}$ if and only if $\mathbb{C}$ is not of full rank.*

The embedding problem considered above leads to another interesting question about perfect codes and generalized Hamming weights. The generalized Hamming weights were introduced by Wei [36] for linear codes and were studied by several authors; see [4, 10, 11, 13, 37], among others. We now review the definition of generalized Hamming weights in [36] and extend it to nonlinear codes.

The *support* of a code $\mathbb{C}$ of length n, denoted $\chi(\mathbb{C})$, is the set of positions i, such that there exist codewords $(c_1, c_2, \ldots, c_n)$, $(c'_1, c'_2, \ldots, c'_n) \in \mathbb{C}$ with $c_i \neq c'_i$. Notice that this definition of $\chi(\cdot)$, introduced in [17], applies to both linear and nonlinear codes; it coincides with the usual notion of support as the set of nonzero positions for linear codes. Now let $\mathbb{C}$ be a linear code of length n and dimension k. Then the ith generalized Hamming weight of $\mathbb{C}$ is defined [36] as

$$d_i(\mathbb{C}) \stackrel{\text{def}}{=} \min_D |\chi(D)| \quad \text{for} \quad i = 1, 2, \ldots, k, \tag{4.3}$$

where the minimum is taken over all linear subcodes $D \subset \mathbb{C}$ such that $\dim D = i$. The sequence $d_1(\mathbb{C}), d_2(\mathbb{C}), \ldots, d_k(\mathbb{C})$ is called the *generalized Hamming weight hierarchy* (GHW) of $\mathbb{C}$. This sequence plays an important role in many applications, ranging from the wire-tap channel [22] to trellis decoding [11]. For some of these applications, an equivalent sequence $\kappa_1(\mathbb{C}), \kappa_2(\mathbb{C}), \ldots, \kappa_n(\mathbb{C})$, called the *dimension-length profile* (DLP) of $\mathbb{C}$, is more convenient to deal with. This sequence, introduced in [34] and later studied in [11, 16, 17] and other works, is defined as follows:

$$\kappa_i(\mathbb{C}) \stackrel{\text{def}}{=} \max_D \dim D \quad \text{for} \quad i = 1, 2, \ldots, n, \tag{4.4}$$

where the maximum is taken over all linear subcodes $D \subset \mathbb{C}$ such that $|\chi(D)| = i$. The DLP and GHW are equivalent sequences, in the sense that either sequence can

be obtained from the other, as follows:

$$d_i(\mathbb{C}) = \min\{\, j \;:\; \kappa_j(\mathbb{C}) \geq i \,\} \quad \text{for} \quad i = 1, 2, \ldots, k, \tag{4.5}$$

$$\kappa_i(\mathbb{C}) = \max\{\, j \;:\; d_j(\mathbb{C}) \leq i \,\} \quad \text{for} \quad i = 1, 2, \ldots, n. \tag{4.6}$$

A natural generalization of DLP and GHW to nonlinear codes is through the notion of *cardinality-length profile* (CLP), defined as follows. For any code $\mathbb{C} \subset \mathbb{F}_2^n$, we let

$$\kappa_i(\mathbb{C}) \stackrel{\text{def}}{=} \max_D \log_2 |D| \quad \text{for} \quad i = 1, 2, \ldots, n, \tag{4.7}$$

where the maximum is taken over all subcodes $D \subset \mathbb{C}$ such that $|\chi(D)| = i$. Thus $\kappa_i(\mathbb{C})$ is the log cardinality of the largest code of length i embedded in $\mathbb{C}$. The GHW of a nonlinear code $\mathbb{C}$ may be now defined[1] by (4.5), with $\lfloor \log_2 |\mathbb{C}| \rfloor$ replacing k.

The generalized Hamming weights of the Hamming codes were determined by Wei in [36]. Wei [36] showed that if $\mathcal{H}_m$ is a Hamming code of length $n = 2^m - 1$, then its GHW is given by $\{d_1(\mathbb{C}), d_2(\mathbb{C}), \ldots, d_k(\mathbb{C})\} = \{1, 2, \ldots, n\} \setminus \{1, 2, 2^2, \ldots, 2^{m-1}\}$. From this, it is easy to deduce that

$$\kappa_i(\mathcal{H}_m) \;=\; i - \lfloor \log_2 i \rfloor - 1 \quad \text{for} \quad i = 1, 2, \ldots, n.$$

In what follows, we show that certain nonlinear perfect codes, in particular the full-rank perfect codes, have a different cardinality-length profile. We also prove that the cardinality-length profile $\kappa_i(\mathbb{C})$ of any perfect code $\mathbb{C}$ of length $2^m - 1$ coincides with that of $\mathcal{H}_m$ for $i \geq 2^{m-1}$, and provide bounds on $\kappa_i(\mathbb{C})$ for other values of i. These bounds will enable us to conclude that the GHW of "most" perfect codes coincides with the GHW of the Hamming codes.

THEOREM 4.4. *Let $\mathbb{C}$ be a perfect code of length $n = 2^m - 1$. Then*

$$\kappa_i(\mathbb{C}) \;=\; i - m \quad \textit{for} \quad i = 2^{m-1}, 2^{m-1}+1, \ldots, 2^m - 1.$$

Proof. For these values of i, we have $n - i \leq 2^{m-1} - 1$. Since $\mathbb{C}$ is an orthogonal array of strength $2^{m-1} - 1$ (cf. [20, p. 139]), it follows that every set of $n-i$ positions of $\mathbb{C}$ contain each binary $(n-i)$-tuple exactly $|\mathbb{C}|/2^{n-i} = 2^{i-m}$ times. □

For $i = 2^{m-1}-1$, however, the CLP is *not* the same for all perfect codes. Specifically, if $\mathbb{C}$ is not of full rank, then $\kappa_{2^{m-1}-1}(\mathbb{C}) = 2^{m-1} - m$ by Proposition 4.1. If $\mathbb{C}$ is a full-rank perfect code, then $\kappa_{2^{m-1}-1}(\mathbb{C}) < 2^{m-1} - m$ by Proposition 4.2, since if a code D of length $2^{m-1} - 1$ and cardinality $2^{m-1} - m$ is embedded in $\mathbb{C}$, it must be a perfect code.

PROPOSITION 4.5. *If $\mathbb{C}$ is a full-rank perfect code of length $n = 2^m - 1$, then*

$$2^{m-1} - m - 1 \;<\; \kappa_{2^{m-1}-1}(\mathbb{C}) \;<\; 2^{m-1} - m.$$

Proof. The upper bound is Proposition 4.2. The lower bound may be proved as follows. For a vector $v \in \mathbb{F}_2^n$, let $\xi(v)$ be the number of codewords of $\mathbb{C}$ whose support is disjoint with the support of v. Further, let $\chi_v(\mathbb{C}) = \sum_{c \in \mathbb{C}} (-1)^{<v,c>}$ be the corresponding character of $\mathbb{C}$ (cf. [20, p. 134]). Now suppose that $\mathrm{wt}(v) = 2^{m-1}$. Then it follows from (4.2) that $\chi_v(\mathbb{C}) = 2^{2^{m-1}} \xi(v) - 2^{n-m}$. Since all perfect codes have the same weight distribution, the MacWilliams identities for nonlinear codes [6, 20] imply

$$\frac{1}{2^{n-m}} \sum_{\mathrm{wt}(v) = 2^{m-1}} \chi_v(\mathbb{C}) \;=\; \sum_{\mathrm{wt}(v) = 2^{m-1}} \left(\frac{\xi(v)}{2^{2^{m-1}-m-1}} - 1 \right) \;=\; 2^m - 1.$$

[1] The CLP was first introduced in [17]. For an alternative way to extend the definition of generalized Hamming weight hierarchy to nonlinear codes, see [4].

Hence, there exists at least one v of weight 2^{m-1} such that $\xi(v) > 2^{2^{m-1}-m-1}$. Now, it is obvious that $\kappa_{2^{m-1}-1}(\mathbb{C}) \geq \max_{\mathrm{wt}(v)=2^{m-1}} \log_2 \xi(v)$, and the lower bound follows. □

Establishing nontrivial bounds on the cardinality-length profile $\kappa_i(\mathbb{C})$ of full-rank perfect codes for $i \leq 2^{m-1}-1$ appears to be a difficult problem. On the other hand, we have the following.

THEOREM 4.6. *If a perfect code $\mathbb{C}$ of length $n = 2^m - 1$ has no full-rank perfect codes (of any length $\leq n$) embedded in it, then*

$$\begin{aligned} \kappa_i(\mathbb{C}) &\geq i - \lfloor \log_2 i \rfloor - 1 \quad \textit{for} \quad i = 1, 2, \ldots, 2^{m-1}-5, \\ \kappa_i(\mathbb{C}) &= i - \lfloor \log_2 i \rfloor - 1 \quad \textit{for} \quad i = 2^{m-1}-4, 2^{m-1}-3, \ldots, 2^m-1. \end{aligned}$$

Proof. Without loss of generality, assume that the dual code $\mathbb{C}^\perp$ contains the vector $(\mathbf{1}|\mathbf{0})$ of weight 2^{m-1}, and let $\mathbf{0}^i$ denote the all-zero i-tuple. It follows from the proof of Proposition 4.1 that $\mathbb{C}_1 = \{x : (\mathbf{0}^{2^{m-1}} | \, x) \in \mathbb{C}\}$ is a perfect code of length $2^{m-1}-1$. As such, it is an orthogonal array of strength $2^{m-2}-1$. Therefore, for each $i = 1, 2, \ldots, 2^{m-2}-1$, the set

$$D = \left\{ x : \left(\mathbf{0}^{2^{m-1}} | \, \mathbf{0}^i | \, x\right) \in \mathbb{C} \right\}$$

is a code of cardinality $|D| = |\mathbb{C}_1|/2^i = 2^{2^{m-1}-m-i}$ embedded in $\mathbb{C}$. Furthermore, the code $\mathbb{C}_1$ is not of full rank, by assumption. Hence, we can assume w.l.o.g. that $\mathbb{C}_1^\perp$ contains the vector $(\mathbf{1}|\mathbf{0})$ of weight 2^{m-2}. It follows, again by Proposition 4.1, that

$$\mathbb{C}_2 = \left\{ x : \left(\mathbf{0}^{2^{m-1}} | \, \mathbf{0}^{2^{m-2}} | \, x\right) \in \mathbb{C} \right\}$$

is a perfect code of length $2^{m-2}-1$ embedded in both $\mathbb{C}_1$ and $\mathbb{C}$. This code is again an orthogonal array and is not of full rank by assumption. Therefore, its dual code contains a vector of weight 2^{m-3}, and so on. Continuing in this manner until the length of $\mathbb{C}$ is exhausted, we obtain

$$\kappa_i(\mathbb{C}) \geq i - \lfloor \log_2 i \rfloor - 1 \quad \text{for} \quad i = 1, 2, \ldots, n. \tag{4.8}$$

The equality in (4.8) for $i \geq 2^{m-1}-1$ follows from Theorem 4.4 and Proposition 4.1. The equality for $i = 2^{m-1}-4, 2^{m-1}-3, 2^{m-1}-2$ follows from the fact, established in [2], that triply shortened perfect codes are optimal. □

We conjecture that, in fact, equality always holds in (4.8). That is, the CLP of a perfect code $\mathbb{C}$ coincides with that of a Hamming code, provided there are no full-rank perfect codes embedded in $\mathbb{C}$. This is certainly true for perfect codes of length 15.

COROLLARY 4.7. *Let $\mathbb{C}$ be a perfect code of length 15. Then*

$$\kappa_i(\mathbb{C}) = i - \lfloor \log_2 i \rfloor - 1 \quad \textit{for} \quad i = 1, 2, \ldots, 15$$

if and only if $\mathbb{C}$ is not of full rank.

Proof. This follows from Proposition 4.5 and Theorem 4.6, along with the following observations: a perfect code of length 7 is necessarily a $(7, 4, 3)$ Hamming code; shortening the $(7, 4, 3)$ code any number of times produces optimal codes. □

Returning from the cardinality-length profiles to the generalized Hamming weights, Theorem 4.6 implies the following strong result.

THEOREM 4.8. *Let $\mathbb{C}$ be a perfect code of length $n = 2^m - 1$. Then*

$$\{d_1(\mathbb{C}), d_2(\mathbb{C}), \ldots, d_{n-m}(\mathbb{C})\} = \{1, 2, \ldots, n\} \setminus \{1, 2, 2^2, \ldots, 2^{m-1}\}, \tag{4.9}$$

provided there are no full-rank perfect codes embedded in $\mathbb{C}$.

Proof. Recall that the GHW of $\mathbb{C}$ is defined by (4.5). Thus, the theorem follows immediately from Theorem 4.6, along with the observation that $\kappa_i(\mathbb{C}) < i - \lfloor \log_2 i \rfloor$ for all i. The latter statement follows from the fact that an $(n, M, 3)$ code with $M \geq 2^{n-\lfloor \log_2 n \rfloor}$ does not exist by the sphere-packing bound [20, p. 19]. □

Finally, we observe that the generalized Hamming weight hierarchy of a full-rank perfect code is not given by (4.9), in view of Proposition 4.5.

5. Full-rank tilings and kernels of perfect codes. A *tiling* of $\mathbb{F}_2^n$ is a pair (V, A) of subsets of $\mathbb{F}_2^n$ such that every $x \in \mathbb{F}_2^n$ has a unique representation of the form $x = v + a$, with $v \in V$ and $a \in A$. Thus (V, A) is a tiling if and only if

$$V + A = \mathbb{F}_2^n \text{ and } (V + V) \cap (A + A) = \{\mathbf{0}\}.$$

Without loss of generality, we can always assume that $\mathbf{0} \in (V \cap A)$. A tiling (V, A) of $\mathbb{F}_2^n$ is *trivial* if one of the sets V, A is $\{\mathbf{0}\}$ and the other is $\mathbb{F}_2^n$. It is of *full rank* if $\langle V \rangle = \langle A \rangle$ or, equivalently, $\mathsf{rank}(V) = \mathsf{rank}(A) = n$. The study of [5] shows that any tiling of $\mathbb{F}_2^n$ can be uniquely decomposed into, or constructed from, smaller tilings that are either trivial or have full rank. Hence, the following question is of interest: for which values of n does $\mathbb{F}_2^n$ admit a full-rank tiling?

It is shown in [9, 5] that full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 112$. In this section we show that, in fact, full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 14$. Two alternative constructions of such tilings are presented: an iterative "lifting" from a full-rank tiling of $\mathbb{F}_2^{14}$ exhibited in [5] and a direct reduction from a full-rank perfect code of length 1023. Since full-rank tilings of $\mathbb{F}_2^n$ do not exist for $n \leq 7$, as established in [5], these constructions leave only the six values $n = 8, 9, \ldots, 13$ unresolved. We will show that the existence of full-rank tilings for these values of n is closely related to the existence of full-rank perfect codes with kernels of high dimension. We start with the following iterative construction of tilings.

CONSTRUCTION C. *Let (V, A) be a tiling of $\mathbb{F}_2^n$ and let a^* be a nonzero element of A. Consider the sets*

$$V' = \{\, (v|0) : v \in V \,\} \cup \{\, (v|1) : v \in V \,\}, \tag{5.1}$$

$$A' = \{\, (a|0) : a \in A^* \,\} \cup \{\, (a^*|1) \,\}, \tag{5.2}$$

where $A^* = A \backslash \{a^*\}$. Then (V', A') is a tiling of $\mathbb{F}_2^{n+1}$.

Indeed, suppose that $x \in (V' + V') \cap (A' + A')$. Since $(V + V) \cap (A + A) = \{\mathbf{0}\}$, it follows that $x = (\mathbf{0}|0)$ or $x = (\mathbf{0}|1)$. But $(\mathbf{0}|1) \notin A' + A'$, which implies that $x = \mathbf{0}$. Furthermore, since $|V'| = 2|V|$ and $|A'| = |A|$, we have $|V'||A'| = 2^{n+1}$. Hence (V', A') is a tiling, as claimed.

PROPOSITION 5.1. *If (V, A) is a full-rank tiling of $\mathbb{F}_2^n$ and $\mathsf{rank}(A^*) = n$, then the tiling (V', A') obtained by* Construction C *is a full-rank tiling of $\mathbb{F}_2^{n+1}$.*

Proof. It is obvious from (5.1) that $\langle V \rangle = \mathbb{F}_2^n$ implies $\langle V' \rangle = \mathbb{F}_2^{n+1}$. Since $\mathsf{rank}(A^*) = n$, it follows that any vector of the form $(x|0)$, including $(a^*|0)$, belongs to $\langle A' \rangle$. Hence $(\mathbf{0}|1) = (a^*|0) + (a^*|1)$ also belongs to $\langle A' \rangle$, and therefore $\langle A' \rangle = \mathbb{F}_2^{n+1}$. □

A full-rank tiling (V, A) of $\mathbb{F}_2^{14}$ with $|V| = 2^{10}$ and $|A| = 2^4$ was constructed in [5]. We will call this the *seed tiling*. Starting with the seed tiling, and iteratively applying Construction C, establishes the following.

THEOREM 5.2. *For all $n \geq 14$, there exists a full-rank tiling of $\mathbb{F}_2^n$.*

Since we are interested here in the connections between tilings and perfect codes, we will now present an alternative proof of Theorem 5.2 which employs such connections. As a by-product, we will obtain certain bounds relating the rank of a perfect

code and the dimension of its kernel. The following theorem, established in [3, 5], is based on the matrix construction of covering of Blokhuis and Lam [3].

THEOREM 5.3. *Let (V, A) be a tiling of $\mathbb{F}_2^n$ and let $\nu = |V| - 1$. Further, let $H(V)$ be an $n \times \nu$ matrix having the nonzero elements of V as its columns. Define*

$$\mathbb{C} \;=\; \{\, x \in \mathbb{F}_2^{\nu} \;:\; H(V)x^t \in A \,\}.$$

Then $\mathbb{C}$ is a perfect code of length ν.

We shall say that $\mathbb{C}$ is the perfect code *associated* with the tiling (V, A). The following relation between the ranks of V, A, and $\mathbb{C}$ was established in [5].

PROPOSITION 5.4. *If $\mathbb{C}$ is the perfect code of length ν associated with a tiling (V, A), then*

$$\mathsf{rank}(\mathbb{C}) \;=\; \nu - \mathsf{rank}(V) + \mathsf{rank}(A_{\langle V\rangle}),$$

where $A_{\langle V\rangle} = A \cap \langle V\rangle$. In particular, if $\langle V\rangle = \mathbb{F}_2^n$, then

$$\mathsf{rank}(\mathbb{C}) \;=\; \nu - n + \mathsf{rank}(A).$$

It follows from Proposition 5.4 that if $\langle V\rangle = \langle A\rangle = \mathbb{F}_2^n$, then $\mathsf{rank}(\mathbb{C}) = \nu$. Thus if (V, A) is a full-rank tiling, then the associated perfect code $\mathbb{C}$ is also of full rank.

Given a code $\mathbb{C} \subset \mathbb{F}_2^n$, the *kernel* of $\mathbb{C}$ is the set of all $x \in \mathbb{F}_2^n$ that leave $\mathbb{C}$ invariant under translation. Assuming that $\mathbf{0} \in \mathbb{C}$, the kernel of $\mathbb{C}$ can be defined (cf. [1, 26]) as follows:

$$\mathsf{ker}\,\mathbb{C} \;\stackrel{\text{def}}{=}\; \{\, x \in \mathbb{C} \;:\; x + \mathbb{C} = \mathbb{C} \,\}.$$

It is easy to see that $\mathsf{ker}\,\mathbb{C}$ is a linear subcode of $\mathbb{C}$, and $\mathsf{ker}\,\mathbb{C} = \mathbb{C}$ if and only if $\mathbb{C}$ itself is linear. The kernel of $\mathbb{C}$ is sometimes called the set of stabilizers of $\mathbb{C}$ (cf. [14]) or the set of periodic points of $\mathbb{C}$ (cf. [5]).

Now let $\mathbb{C}$ be the perfect code associated with a tiling (V, A). Then it is easy to see that

$$\mathsf{ker}\,\mathbb{C} \;=\; \{\, x \in \mathbb{C} \;:\; H(V)x^t \in \mathsf{ker}\,A \,\}.$$

Along with Proposition 5.4, this immediately implies the following.

PROPOSITION 5.5. *If $\mathbb{C}$ is the perfect code of length ν associated with a tiling (V, A), then*

$$\dim(\mathsf{ker}\,\mathbb{C}) \;=\; \nu - \mathsf{rank}(V) + \dim(\mathsf{ker}\,A_{\langle V\rangle}),$$

where $A_{\langle V\rangle} = A \cap \langle V\rangle$. In particular, if $\langle V\rangle = \mathbb{F}_2^n$, then

$$\dim(\mathsf{ker}\,\mathbb{C}) \;=\; \nu - n + \dim(\mathsf{ker}\,A).$$

Kernels play an important role in the construction of tilings introduced in [5]. We now briefly describe this construction.

Let A_0 be a subspace of $\mathbb{F}_2^n$ of dimension k. For any $V \subset \mathbb{F}_2^n$, we define V/A_0 as follows. Fix a basis $a_1, a_2, \ldots, a_k$ for A_0 and complete this to a basis $a_1, a_2, \ldots, a_k$, $b_1, b_2, \ldots, b_{n-k}$ for $\mathbb{F}_2^n$. Then each vector $v = \sum_{i=1}^{k} \alpha_i a_i + \sum_{i=1}^{n-k} \beta_i b_i$ in V is mapped onto the vector $v' = \sum_{i=1}^{n-k} \beta_i b_i$ in V/A_0. Thus V/A_0 is just the projection of V onto $\mathbb{F}_2^n/A_0$. Note that $\mathbb{F}_2^n/A_0$ may be regarded as $\mathbb{F}_2^{n-k}$ under an appropriate change of

basis (cf. [5]), namely, under the linear transformation that takes $b_1, b_2, \ldots, b_{n-k}$ into unit vectors. Thus we will identify $\mathbb{F}_2^n/A_0$ with $\mathbb{F}_2^{n-k}$ and think of V/A_0 as a subset of $\mathbb{F}_2^{n-k}$.

CONSTRUCTION D. *Let (V, A) be a tiling of $\mathbb{F}_2^n$. Further, let A_0 be a k-dimensional subspace of $\ker A$. Then $(V/A_0, A/A_0)$ is a tiling of $\mathbb{F}_2^{n-k}$.*

It is shown in [5] that if (V, A) is a full-rank tiling, then so is $(V/A_0, A/A_0)$. This implies the following.

PROPOSITION 5.6. *If there exists a full-rank tiling (V, A) of $\mathbb{F}_2^n$ with $\dim(\ker A) = r$, then there exist full-rank tilings of $\mathbb{F}_2^{n-k}$ for all $k = 1, 2, \ldots, r$.*

Propositions 5.4–5.6 and Theorem 5.3 provide an alternative proof for Theorem 5.2 as follows. Consider again the seed full-rank tiling (V, A) of $\mathbb{F}_2^{14}$ exhibited in [5]. Recall that for this tiling $|V| = 2^{10}$, $|A| = 2^4$, and $\ker V = \ker A = \{\mathbf{0}\}$. By Theorem 5.3 and Proposition 5.4, the associated perfect code $\mathbb{C}$ is a full-rank code of length $2^{10} - 1 = 1023$. By Proposition 5.5, we have

$$\dim(\ker \mathbb{C}) \;=\; 1023 - \mathsf{rank}(V) + \dim(\ker A) \;=\; 1023 - 14 \;=\; 1009.$$

Now let $\mathcal{V}_n$ denote the Hamming sphere of radius 1 in $\mathbb{F}_2^n$. Then $(\mathcal{V}_{1023}, \mathbb{C})$ is obviously a full-rank tiling of $\mathbb{F}_2^{1023}$. Applying to this tiling Construction D and Proposition 5.6, we obtain full-rank tiling of $\mathbb{F}_2^n$ for all $n = 14, 15, \ldots, 1022$. On the other hand, it was already shown in [5] that full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 112$.

Kernels of perfect binary codes were studied by Phelps and LeVan in [26]. It is shown in [26] that given $m \geq 4$ and $n = 2^m - 1$, there exists a nonlinear perfect code $\mathbb{C}$ of length n with kernel of dimension k, if and only if $k = 1, 2, \ldots, n-m-2$. However, if we also impose constraints on the rank of $\mathbb{C}$, for example require that $\mathbb{C}$ is of full rank, much less is known about the possible dimensions of its kernel. Propositions 5.4–5.6 shed some light on this problem. For example, starting with the full-rank tiling $(\mathcal{V}_{1023}, \mathbb{C})$ of $\mathbb{F}_2^{1023}$ discussed in the foregoing paragraph, and applying Construction D, yields associated full-rank perfect codes of length $n = 2^m - 1$ with kernels of dimension $\geq n - m - 10$ for $m = 4, 5, \ldots, 1022$. Furthermore, the code $\mathbb{C}$ itself, associated with the seed tiling, has kernel of dimension $n - m - 4$ for $m = 10$. The following theorem shows that this is the highest possible kernel dimension for a full-rank perfect code.

THEOREM 5.7. *If $\mathbb{C}$ is a full-rank perfect code length $n = 2^m - 1$, then*

$$\dim(\ker \mathbb{C}) \;\leq\; n - m - 4. \tag{5.3}$$

Furthermore, this bound is tight for $m = 10$ and $m = 11$.

Proof. Let $A_0 = \ker \mathbb{C}$, and assume to the contrary that $\dim A_0 \geq n - m - 3$. Obviously $(\mathcal{V}_n, \mathbb{C})$ is a full-rank tiling. Applying to this tiling Construction D, we obtain another full-rank tiling $(V, A) = (\mathbb{C}/A_0, \mathcal{V}_n/A_0)$ with

$$|V| \;=\; |\mathbb{C}/A_0| \;=\; \frac{|\mathbb{C}|}{|A_0|} \;\leq\; \frac{2^{n-m}}{2^{n-m-3}} \;=\; 8.$$

By Theorem 5.3 and Proposition 5.4, the perfect code associated with (V, A) must be a full-rank perfect code of length $|V| - 1 \leq 7$. But such a code obviously does not exist. The tightness of (5.3) for $m = 11$ follows by considering the perfect code associated with the tiling $(\mathbb{C}, \mathcal{V}_{15})$, where $\mathbb{C}$ is a full-rank perfect code of length 15. □

More generally, one could ask: What is the largest possible dimension $\alpha(m)$ of the kernel of a full-rank perfect code of length $n = 2^m - 1$? The following theorem provides a complete answer to this question for all $m \geq 10$.

THEOREM 5.8. *Let δ be the unique integer such that $2^{\delta-1} - (\delta-1) \leq m < 2^\delta - \delta$. Then*

$$\alpha(m) \;=\; 2^m - m - \delta - 1 \quad \textit{for} \quad m = 10, 11, \ldots. \tag{5.4}$$

Proof. We first show that $\alpha(m) \leq 2^m - m - \delta - 1 = n - (m+\delta)$, where $n = 2^m - 1$. Assume to the contrary that there exists a full-rank perfect code $\mathbb{C}$ of length n such that $\dim(\ker\mathbb{C}) = 2^m - m - \delta$. Observe that $\mathbb{C}$ is the union of $|\mathbb{C}|/|\ker\mathbb{C}|$ cosets of $\ker\mathbb{C}$. Hence, the total number of linearly independent vectors in $\mathbb{C}$ is at most

$$\dim(\ker\mathbb{C}) \;+\; \left(\frac{|\mathbb{C}|}{|\ker\mathbb{C}|} - 1\right) \;\geq\; n, \tag{5.5}$$

where the inequality follows from the assumption that $\mathbb{C}$ is of full rank. Substituting $\dim(\ker\mathbb{C}) = 2^m - m - \delta$ and $|\mathbb{C}| = 2^{n-m}$ into (5.5), we obtain $m \leq 2^{\delta-1} - \delta$, which contradicts the definition of δ. In conjunction with the result of Theorem 5.7, this proves (5.4) for $m = 10$ and $m = 11$.

Next, we show how to construct a full-rank perfect code $\mathbb{C}_{12}$ of length $n = 2^{12} - 1$, such that $\dim(\ker\mathbb{C}) = n - 17 = (2^m - 1) - m - \delta$, for $m = 12$. Start with the full-rank tiling $(V, A) = (\mathcal{V}_{15}, \mathbb{C})$ of $\mathbb{F}_2^{15}$, where $\mathbb{C}$ is a full-rank perfect code of length 15. Then apply Construction C to obtain a full-rank tiling (V', A') of $\mathbb{F}_2^{16}$ with $|V'| = 2^5$ and $|A'| = 2^{11}$. Now, apply Construction C again, with the roles of V' and A' interchanged. This produces a full-rank tiling (V_{12}, A_{12}) of $\mathbb{F}_2^{17}$ with $|V_{12}| = 2^{12}$ and $|A_{12}| = 2^5$. The full-rank perfect code $\mathbb{C}_{12}$ associated with this tiling has length $n = |V_{12}| - 1 = 2^{12} - 1$. Furthermore, by Proposition 5.5 we have

$$\dim(\ker\mathbb{C}_{12}) \;\geq\; n - \mathsf{rank}(V_{12}) \;=\; n - 17.$$

In view of the upper bound on $\alpha(m)$ that we have already proved, the above expression holds with equality. Thus, we have established (5.4) for $m = 12$. Now, iteratively applying Construction C to (V_{12}, A_{12}), we obtain full-rank tilings (V_m, A_m) of $\mathbb{F}_2^{m+5}$ with associated full-rank perfect codes of length $n = 2^m - 1$ and kernel of dimension $n - (m+5)$. Since in all of these tilings $|A_m| = |A_{12}| = 2^5$, we can keep iterating Construction C in this way as long as $m + 5 \leq 2^5 - 1$ or, equivalently, $m < 2^5 - 5 = 27$. This proves (5.4) for all $m = 12, 13, \ldots, 26$. For $m = 27, 28, \ldots, 57$, we start with the full-rank tiling $(\mathcal{V}_{31}, \mathbb{C})$, where $\mathbb{C}$ is a full-rank perfect code of length 31, and proceed as before. Continuing in this manner establishes (5.4) for all $m \geq 10$. □

Note that Theorem 5.7 is not a special case of Theorem 5.8, since it holds also for $m < 10$. For example, for $m = 4$ it follows from Theorem 5.7 that the possible dimensions of the kernel of a full-rank perfect code of length 15 are $1, 2, \ldots, 7$. The problem of determining which of these kernel dimensions are attainable is closely related to the problem of existence of full-rank tilings of $\mathbb{F}_2^n$ for $n = 8, 9, \ldots, 13$. Indeed, a full-rank perfect code of length 15 and kernel of dimension k implies by Proposition 5.6 the existence of a full-rank tilings of $\mathbb{F}_2^n$ for all $n \geq 15 - k$. Furthermore, we have the following result.

PROPOSITION 5.9. *A full-rank perfect code of length* 15 *with kernel of dimension* 7 *exists if and only if a full-rank tiling of $\mathbb{F}_2^8$ exists.*

Proof. Suppose that (V, A) is a full-rank tiling of $\mathbb{F}_2^8$. Then clearly $|V| = |A| = 16$. Hence, by Propositions 5.4 and 5.6, the associated perfect code has length 15, is of full rank, and has kernel of dimension $15 - \mathsf{rank}(V) = 7$. □

The linear code $\mathcal{A}$ defined in (2.1) plays a prominent role in the construction of full-rank perfect codes in [9] and has dimension 7 for $n = 15$. A generator matrix for $\mathcal{A}$ is given by

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0\,1\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix}.$$

However, we now show that $\mathcal{A}$ cannot be the kernel of a full-rank perfect code $\mathbb{C}$ of length 15. Indeed, assume to the contrary that this is so. Then $(\mathcal{V}_{15}/\mathcal{A}, \mathbb{C}/\mathcal{A})$ is a full-rank tiling of $\mathbb{F}_2^8$ by Proposition 5.6. Since both $\mathcal{V}_{15}$ and $\mathcal{A}$ are known, we can compute $\mathcal{V}_{15}/\mathcal{A}$ explicitly to obtain

$$\mathcal{V}_{15}/\mathcal{A} = \left\{ \begin{array}{llll} 0\,0\,0\,0\,0\,0\,0\,0, & 0\,0\,0\,1\,0\,0\,0\,1, & 1\,0\,0\,0\,0\,0\,0\,0, & 0\,0\,0\,0\,1\,0\,0\,0 \\ 1\,0\,0\,0\,0\,0\,0\,1, & 0\,0\,0\,0\,1\,0\,0\,1, & 0\,1\,0\,0\,0\,0\,0\,0, & 0\,0\,0\,0\,0\,1\,0\,0 \\ 0\,1\,0\,0\,0\,0\,0\,1, & 0\,0\,0\,0\,0\,1\,0\,1, & 0\,0\,1\,0\,0\,0\,0\,0, & 0\,0\,0\,0\,0\,0\,1\,0 \\ 0\,0\,1\,0\,0\,0\,0\,1, & 0\,0\,0\,0\,0\,0\,1\,1, & 0\,0\,0\,1\,0\,0\,0\,0, & 0\,0\,0\,0\,0\,0\,0\,1 \end{array} \right\}.$$

We now observe that $\mathsf{ker}(\mathcal{V}_{15}/\mathcal{A}) = \{(00000000), (00000001)\}$ has dimension 1. In view of Proposition 5.6, this implies the existence of a full-rank tiling of $\mathbb{F}_2^7$. But such a tiling does not exist, as shown in [5].

Remark. LeVan and Phelps [25] have recently found full-rank perfect codes of length 15 with kernels of dimension 2, 3, 4, and 5. This, along with the results of this section, implies that full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 10$.

6. Open problems. We have considered herein three topics concerning perfect codes and tilings: the intersection number problem; embeddings and generalized Hamming weights; and full-rank tilings and kernels of full-rank perfect codes. Solutions to some of these problems are provided in the foregoing three sections. Nevertheless, it is fair to say that we know much less than we would like to, and many problems concerning perfect codes remain open. We conclude this paper with a list of ten open problems on perfect binary codes which, at least in our opinion, seem to be the most interesting.

Intersection numbers. For a given m, what are the possible intersection numbers of distinct perfect codes of length $n = 2^m - 1$? For more details on this problem, see section 3.

GHW and CLP. Give a complete characterization of the generalized Hamming weights and/or the cardinality length profiles for perfect codes. Compare the generalized Hamming weight hierarchies for full-rank and not full-rank perfect codes, derived from different constructions. For more details on this problem, see section 4.

Full-rank tilings. Construct full-rank tilings of $\mathbb{F}_2^n$ for $n = 8$ and $n = 9$, or prove that such tilings do not exist. This problem appears to be quite challenging despite the small size of the sets involved. For more details on this, see section 5 and [5].

Rank and kernel. Given a perfect code $\mathbb{C}$ of length $n = 2^m - 1$, its rank r is in the range $n-m, \ldots, n$, while the dimension k of its kernel is in the range $1, \ldots, n-m-2$ or $n-m$. Furthermore, as shown in [9] and [26], each value of r or k in the corresponding range is attainable. We ask: which pairs (r, k) are attainable as the rank and kernel dimension of a perfect code of length $2^m - 1$? For bounds, and more details, see section 5.

Systematicity. A binary code $\mathbb{C}$ with 2^k codewords is called systematic if there exists a set of k positions in which every binary k-tuple appears (exactly once) among

the codewords of $\mathbb{C}$. Thus $\mathbb{C}$ is systematic if there exist some k positions that can be used as information positions for the code. All *known* perfect codes are systematic, and a longstanding conjecture says that *all* perfect codes are systematic. This conjecture is related to certain results on systems of t-resilient functions [18]. The systematicity problem was posed as open in an earlier version of this paper. It has been recently solved by Solov'eva and Avgustinovich [31] who showed that the systematicity conjecture is false: they proved that for each $n = 2^m - 1$ with $m \geq 6$, there exists a nonsystematic perfect code. Phelps and LeVan [27] have extended this result to all $m \geq 4$.

Enumeration. Classification of inequivalent perfect codes was first posed as a research problem in [20, p. 180]. However, it soon became apparent [23] that an exact classification is intractable. On the other hand, asymptotic bounds on the *number* of inequivalent perfect codes of length $n = 2^m - 1$ are known. A lower bound of $2^{2^{0.5n}}$ for sufficiently large n is given in [9, 24], while an upper bound of $2^{2^{n-m}}$ can be easily derived. The gap is very large and any improvement on these bounds would be an important result.

Optimality of shortening. It is established in [2] that triply shortened perfect codes of length $2^m - 1$ are optimal. That is, the number of codewords in these codes achieves the value of $A(n, 3)$ for $n = 2^m - 2, 2^m - 3, 2^m - 4$. Referring to the table of best known codes [19] suggests that shortening a perfect code of length $2^m - 1$ up to $2^{m-2} - 1$ times is likely to produce optimal codes for $m \leq 9$. However, the result of Kabatiansky and Panchenko [15] shows that this is not true in general for large m. Thus we ask: What is the largest integer s_m such that shortening a perfect code of length $2^m - 1$ up to s_m times produces optimal codes?

Uniqueness of shortening. Shortening a perfect code of length $2^m - 1$ once, that is, taking all the codewords that coincide in a fixed coordinate, produces a code of length $n = 2^m - 2$, with 2^{n-m} codewords and minimum Hamming distance 3. Now, we ask the reverse question: Given a code $\mathbb{C}$ of length $n = 2^m - 2$ with $|\mathbb{C}| = 2^{n-m}$ and minimum Hamming distance 3, is it always possible to extend $\mathbb{C}$ to a perfect code of length $2^m - 1$? The same question can be asked for shortening by more than one coordinate.

Uniqueness of STS. It is known that the codewords of weight 3 in a perfect code of length $n = 2^m - 1$ form a Steiner triple system (STS) of order n. Again we ask the reverse question: Can any Steiner triple system of order $n = 2^m - 1$ be extended to a perfect code of length n? A solution even for the fist case $n = 15$, would be very interesting. This problem was considered by Phelps in [23].

Space partitions. Finally, we suggest the following question. Given a perfect code $\mathbb{C}$ of length $n = 2^m - 1$, we know that there always exist $n+1$ translates of $\mathbb{C}$, say $\mathbb{C}_0, \mathbb{C}_1, \mathbb{C}_2, \ldots, \mathbb{C}_n$ with $\mathbb{C}_0 = \mathbb{C}$, that form a partition of $\mathbb{F}_2^n$. Under which conditions is there another, different, partition of $\mathbb{F}_2^n$ into perfect codes $D_0, D_1, D_2, \ldots, D_n$ with $D_0 = \mathbb{C}$? Can such partitions be classified for a given perfect code $\mathbb{C}$?

Acknowledgments. We wish to thank Simon Litsyn for the preprint of [19]. We are grateful to Noga Alon, Kevin Phelps, and Faina Solov'eva for stimulating discussions.

REFERENCES

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

[2] M.R. Best and A.E. Brouwer, *The triply shortened binary Hamming code is optimal*, Discrete Math., 17 (1977), pp. 235–245.
[3] A. Blokhuis and C.W.H. Lam, *More coverings by rook domains*, J. Combin. Theory Ser. A, 36 (1984), pp. 240–244.
[4] G.D. Cohen, S. Litsyn, and G. Zémor, *Upper bounds on generalized distances*, IEEE Trans. Inform. Theory, 40 (1994), pp. 2090–2092.
[5] G.D. Cohen, S. Litsyn, A. Vardy, and G. Zémor, *Tilings of binary spaces*, SIAM J. Discrete Math., 9 (1996), pp. 393–412.
[6] Ph. Delsarte, *Four fundamental parameters of a code and their combinatorial significance*, Inform. Control, 23 (1973), pp. 407–438.
[7] Ph. Delsarte and J.-M. Goethals, *Unrestricted codes with the Golay parameters are unique*, Discrete Math., 12 (1975), pp. 211–224.
[8] T. Etzion, *Nonequivalent q-ary perfect codes*, SIAM J. Discrete Math., 9 (1996), pp. 413–423.
[9] T. Etzion and A. Vardy, *Perfect codes: Constructions, properties and enumeration*, IEEE Trans. Inform. Theory, 40 (1994), pp. 754–763.
[10] G.-L. Feng, K.K. Tzeng, and V.K. Wei, *On the generalized Hamming weights of several classes of cyclic codes*, IEEE Trans. Inform. Theory, 38 (1992), pp. 133–1140.
[11] G.D. Forney, Jr., *Dimension/length profiles and trellis complexity of linear block codes*, IEEE Trans. Inform. Theory, 40 (1994), pp. 1741–1752.
[12] O. Heden, *A binary perfect code of length* 15 *and codimension* 0, Des. Codes Cryptogr., 4 (1994), pp. 213–220.
[13] T. Helleseth, T. Kløve, and Ø. Ytrehus, *Generalized Hamming weights of linear codes*, IEEE Trans. Inform. Theory, 38 (1992), pp. 1412–1418.
[14] T.W. Hungerford, *Algebra*, Holt, Rinehart and Winston, New York, 1974.
[15] G. Kabatiansky and V. Panchenko, *Packings and coverings of the Hamming space by spheres of radius one*, Probl. Peredachi Inform., 24 (1988), pp. 3–16.
[16] A.B. Kiely, S. Dolinar, R.J. McEliece, L. Ekroot, and W. Lin, *Trellis decoding complexity of linear block codes*, IEEE Trans. Inform. Theory, 42 (1996), pp. 1687–1697.
[17] A. Lafourcade and A. Vardy, *Lower bounds on trellis complexity of block codes*, IEEE Trans. Inform. Theory, 41 (1995), pp. 1938–1954.
[18] V.I. Levenshtein, *private communication*, 1994.
[19] S. Litsyn, *An updated table of best known binary codes*, preprint, December 1995.
[20] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.
[21] M. Mollard, *A generalized parity function and its use in the construction of perfect codes*, SIAM J. Alg. Disc. Meth., 7 (1986), pp. 113–115.
[22] L.H. Ozarow and A.D. Wyner, *Wire-tap-channel II*, Bell Labs Tech. J., 63 (1984), pp. 2135–2157.
[23] K.T. Phelps, *A combinatorial construction of perfect codes*, SIAM J. Alg. Disc. Meth., 4 (1983), pp. 398–403.
[24] K.T. Phelps, *A general product construction for error-correcting codes*, SIAM J. Alg. Disc. Meth., 5 (1984), pp. 224–228.
[25] K.T. Phelps, *private communication*, Auburn University, Auburn, AL, 1996.
[26] K.T. Phelps and M. LeVan, *Kernels of nonlinear Hamming codes*, Des. Codes Cryptogr., 6 (1995), pp. 247–257.
[27] K.T. Phelps and M. LeVan, *Non-systematic perfect codes*, preprint, 1996.
[28] V. Pless, *On the uniqueness of the Golay codes*, J. Combin. Theory, 5 (1968), pp. 215–228.
[29] S.L. Snover, *The Uniqueness of the Nordstrom-Robinson and the Golay Binary Codes*, Ph.D. Thesis, Dept. of Mathematics, Michigan State Univ., East Lansing, MI, 1973.
[30] F.I. Solov'eva, *On binary nongroup codes*, Metody Diskret. Anal., 37 (1981), pp. 65–76 (in Russian).
[31] F.I. Solov'eva and S.V. Avgustinovich, *Existence of nonsystematic perfect binary codes*, in Proc. Fifth Intl. Workshop on Algebraic and Combinatorial Coding Theory, Cosopol, Bulgaria, June 1996, pp. 15–19.
[32] A. Tietäväinen, *On the nonexistence of perfect codes over finite fields*, SIAM J. Appl. Math., 24 (1973), pp. 88–96.
[33] J.H. vanLint, *Nonexistence theorems for perfect error-correcting-codes*, in Computers in Algebra and Number Theory, vol. IV, SIAM–AMS Proceedings, SIAM, Philadelphia, 1971.
[34] A. Vardy and Y. Be'ery, *Maximum-likelihood soft decision decoding of BCH codes*, IEEE Trans. Inform. Theory, 40 (1994), pp. 546–554.
[35] J.L. Vasil'ev, *On nongroup close-packed codes*, Probl. Kibernet., 8 (1962), pp. 375–378 (in Russian).

[36] V.K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory, 37 (1991), pp. 1412–1418.
[37] V.K. Wei and K. Yang, *On the generalized Hamming weights of product codes*, IEEE Trans. Inform. Theory, 39 (1993), pp. 1709–1713.
[38] V.A. Zinov'ev and V.K. Leont'ev, *The nonexistence of perfect codes over Galois fields*, Probl. Control and Inform. Theory, 2 (1973), pp. 123–132 (in Russian).