Full-rank Tilings of $\mathbb{F}_2^8$ Do Not Exist*

Ari Trachtenberg† Alexander Vardy‡

February 3, 2003

Abstract

We show that there are no full-rank tilings of $\mathbb{F}_2^8$, using a carefully designed exhaustive search. This solves an open problem posed in [5] and implies that a full-rank perfect binary code of length 15 with a kernel of dimension 7 does not exist.

A version of this paper will appear in the SIAM Journal on Discrete Mathematics 2003.

1. Introduction

Let $\mathbb{F}_2^n$ be a vector space of dimension n over GF(2). 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 $a \in A$. A tiling (V, A) of $\mathbb{F}_2^n$ is *trivial* if one of the sets V, A is $\mathbb{F}_2^n$ and the other is $\{\mathbf{0}\}$, where $\mathbf{0}$ denotes the all-zero vector in $\mathbb{F}_2^n$. It is of *full rank* if $\mathrm{rank}(V) = \mathrm{rank}(A) = n$ and $\mathbf{0} \in (V \cap A)$. The work of [3] 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. This reduces the classification of tilings of $\mathbb{F}_2^n$ to the study of full-rank tilings. Hence, the following question is of interest: for which values of n, does $\mathbb{F}_2^n$ admit a full-rank tiling?

It is established in [3, 4] that full-rank tilings of $\mathbb{F}_2^n$ exist for $n = 14$ and $n \geq 112$, and do not exist for $n \leq 7$. Theorem 16 of [5] shows that if $\mathbb{F}_2^{n_0}$ admits a full-rank tiling, then so does $\mathbb{F}_2^n$ for all $n \geq n_0$. Thus full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 14$.

There is also an interesting connection between full-rank tilings and full-rank perfect codes. A binary code $\mathbb{C}$ of length n is a subset of $\mathbb{F}_2^n$. A code $\mathbb{C} \subset \mathbb{F}_2^n$ is *perfect* if for some $r \geq 1$, the Hamming spheres of radius r about the codewords of $\mathbb{C}$ partition $\mathbb{F}_2^n$. A code $\mathbb{C} \subseteq \mathbb{F}_2^n$ is *full-rank* if $\mathbf{0} \in \mathbb{C}$ and $\mathrm{rank}(\mathbb{C}) = n$. It is known [4] that full-rank perfect codes exist if and only if $r = 1$ and $n = 2^m - 1$ for $m \geq 4$. The kernel of a code $\mathbb{C} \subseteq \mathbb{F}_2^n$, denoted $\ker\mathbb{C}$, is the set of all $x \in \mathbb{F}_2^n$ such that $x + \mathbb{C} = \mathbb{C}$. It is easy to see that $\ker\mathbb{C}$ is a linear subspace of $\mathbb{F}_2^n$. It is shown in [5] that there exists a full-rank perfect code of length $n = 2^m - 1$ with a kernel of dimension k if and only if there exists a full-rank tiling (V, A) of $\mathbb{F}_2^{n-k}$ with $|V| = 2^m$ and $\ker A = \{\mathbf{0}\}$. LeVan

*Part of this research was performed while both authors were with the University of Illinois.

†Department of Electrical and Computer Engineering, Boston University, 8 St. Mary's Street, Boston, MA 02215, U.S.A. (trachten@bu.edu).

‡Department of Electrical and Computer Engineering, Department of Computer Science and Engineering, University of California San Diego, 9500 Gilman Drive, La Jolla, CA 92093, U.S.A. (vardy@kilimanjaro.ucsd.edu).

and Phelps [8] found by computer search full-rank perfect codes of length 15 with kernels of dimension 2, 3, 4, and 5. This implies [5] that full-rank tilings of $\mathbb{F}_2^n$ exist for all $n \geq 10$.

Thus the only unresolved cases where it is not known whether $\mathbb{F}_2^n$ admits a full-rank tiling are $n = 8$ and $n = 9$. The following problem is posed in [5], we quote:

> 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.

The main objective of this note is to provide an answer to this problem for $n = 8$. We describe a carefully designed exhaustive search that proves the following theorem.

Theorem 1. *A full-rank tiling of $\mathbb{F}_2^8$ does not exist.*

Theorem 1, along with Proposition 24 of [5], also implies that there is no full-rank perfect binary code of length 15 with a kernel of dimension 7. For more details on the rank and kernel-dimension of perfect binary codes, we refer the reader to [1, 2, 5, 9].

2. Nonexistence of full-rank tilings in eight dimensions

Let (V, A) be a full-rank tiling of $\mathbb{F}_2^8$. Since every $x \in \mathbb{F}_2^8$ can be represented uniquely as $x = v + a$ with $v \in V$ and $a \in A$, we have $|V||A| = 28$. By definition $\mathbf{0} \in V$ and $\mathbf{0} \in A$. Since $\mathrm{rank}(V) = \mathrm{rank}(A) = 8$, we must have $|V| \geq 9$ and $|A| \geq 9$, implying that $|V| = |A| = 16$.

Lemma 1. *Let (V, A) be a full-rank tiling of $\mathbb{F}_2^n$, let M be an invertible $n \times n$ binary matrix, and let $\varphi_M(x) = xM$. Then $(\varphi_M(V), \varphi_M(A))$ is a full-rank tiling of $\mathbb{F}_2^n$.*

Proof. Since M is invertible, we have $\varphi_M(x) = \varphi_M(v) + \varphi_M(a)$ if and only if $x = v + a$. It is clear that the mapping φ_M is one-to-one and preserves the rank. ∎

Let $\{e_1, e_2, \ldots, e_8\}$ denote the set of vectors of weight one in $\mathbb{F}_2^8$. Using Lemma 1, we can transform a full-rank tiling (V, A) of $\mathbb{F}_2^8$ into a full-rank tiling $(\varphi_M(V), \varphi_M(A))$ with the property that $\{e_1, e_2, \ldots, e_8\} \subset \varphi_M(V)$. Thus we will henceforth assume without loss of generality that $\{e_1, e_2, \ldots, e_8\} \subset V$. Together with $\mathbf{0} \in V$, this determines 9 out of the 16 vectors of V.

Lemma 2. *Let (V, A) be a full-rank tiling of $\mathbb{F}_2^8$. Then $d(a_1, a_2) \geq 3$ for any distinct vectors $a_1, a_2 \in A$, where $d(\cdot, \cdot)$ denotes the Hamming distance.*

Proof. Assume to the contrary that $\mathrm{wt}(a_1 + a_2) \leq 2$. Since $\{\mathbf{0}, e_1, \ldots, e_8\} \subset V$ by assumption, it follows that there exist distinct $v_1, v_2 \in V$ such that $v_1 + v_2 = a_1 + a_2$. But this implies that $a_1 + v_1 = a_2 + v_2$, which violates the unique representation property of a tiling. ∎

If (V, A) is a full-rank tiling of $\mathbb{F}_2^8$ and π is any permutation of the 8 positions, then $(\pi V, \pi A)$ is also a full-rank tiling of $\mathbb{F}_2^8$. Since the set $\{\mathbf{0}, e_1, \ldots, e_8\}$ is preserved under all permutations $\pi \in S_8$, we have $\{\mathbf{0}, e_1, \ldots, e_8\} \subset \pi V$ and Lemma 2 holds with A replaced by πA. Hence, as potential candidates for A, it suffices to consider the nonisomorphic $(8, 16, 3)$ codes of full rank containing the vector $\mathbf{0}$.

To efficiently reject isomorphisms, we convert the set isomorphism problem to a graph isomorphism problem, as in [7]. Specifically, given a set $\mathcal{S} = \{a_1, \ldots, a_s\} \subset \mathbb{F}_2^8$, we define the bipartite graph $G(\mathcal{S})$ as follows: there are s left-hand vertices $\alpha_1, \ldots, \alpha_s$ and 8 right-hand vertices $\beta_1, \ldots, \beta_8$, with (α_i, β_j) being in the edge set of $G(\mathcal{S})$ if and only if the j-th position of a_i is nonzero. Then two sets $\mathcal{S}_1, \mathcal{S}_2 \subset \mathbb{F}_2^8$ are isomorphic if and only if the corresponding graphs $G(\mathcal{S}_1)$ and $G(\mathcal{S}_2)$ are isomorphic (cf. [7]). We check for graph isomorphism using the well-tested program NAUTY of [6]. Due to memory constraints, we have limited isomorphism rejection to a subset of A consisting of 7 linearly independent vectors. Finally, we have also made use of the following lemma, which implies that any one vector in either A or V can be computed as the sum of the other vectors in this set.

Lemma 3. *Let (V, A) be a full-rank tiling of $\mathbb{F}_2^8$, let $V = \{\mathbf{0}, v_1, v_2, \ldots, v_{15}\}$, and let $A = \{\mathbf{0}, a_1, a_2, \ldots, a_{15}\}$. Then $v_1 + v_2 + \cdots + v_{15} = a_1 + a_2 + \cdots + a_{15} = \mathbf{0}$.*

Proof. Let $H(V)$ be the 8×15 matrix having $v_1, v_2, \ldots, v_{15}$ as its columns, and consider the code $\mathbb{C} = \{\, x \in \mathbb{F}_2^{15} : H(V)x^t \in A \,\}$. It follows from [5, Propositions 18-20] that $\mathbb{C}$ is a full-rank perfect code with a kernel of dimension $7 + \dim(\ker A)$. It is furthermore shown in [3, Proposition 8.3] that $v_1 + v_2 + \cdots + v_{15} \in \ker A$. Thus if $v_1 + v_2 + \cdots + v_{15} \neq \mathbf{0}$, then $\ker\mathbb{C}$ has dimension at least 8. In view of Proposition 21 of [5] this, in turn, implies the existence of a full-rank tiling of $\mathbb{F}_2^n$ for $n \leq 7$. But it was established in [3, Corollary 7.3] that such a tiling does not exist. The fact that $a_1 + a_2 + \cdots + a_{15} = \mathbf{0}$ follows by symmetry. ∎

Exhaustive search based on the foregoing results did not produce a full-rank tiling of $\mathbb{F}_2^8$, thereby proving Theorem 1. The source code of our search program is available at `http://people.bu.edu/trachten/`. The search takes about a week on a contemporary PC workstation.

Acknowledgement. We are grateful to the MEDICIS Project at the École Polytechnique, Palaiseau, France, for the generous use of their computational resources.

References

[1] S.V. AVGUSTINOVICH, O. HEDEN, AND F.I. SOLOV'EVA, *On ranks and kernels of perfect codes*, preprint, October 2002.

[2] S.V. AVGUSTINOVICH, F.I. SOLOV'EVA, AND O. HEDEN, *On ranks and kernels problem of perfect codes*, in Proceedings Eighth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-VIII), St. Petersburg, Russia, September 2002.

[3] G.D. COHEN, S. LITSYN, A. VARDY, AND G. ZÉMOR, *Tilings of binary spaces*, SIAM J. Discrete Math., 9 (1996), pp. 393–412.

[4] T. ETZION AND A. VARDY, *Perfect codes: Constructions, properties and enumeration*, IEEE Trans. Inform. Theory, 40 (1994), pp. 754–763.

[5] T. ETZION AND A. VARDY, *On perfect codes and tilings: problems and solutions*, SIAM J. Discrete Math., 11 (1998), pp. 205–233.

[6] B.D. MCKAY, *Nauty User Guide*, Technical Report TR–CS–94–10, Computer Science Department, Australian National University, 1994.

[7] P.R.J. Östergård, T. Baicheva, and E. Kolev, *Optimal binary one-error-correcting codes of length* 10 *have* 72 *codewords*, IEEE Trans. Inform. Theory, 45 (1999), pp. 1229–1231.

[8] K.T. Phelps, private communication, 1996.

[9] K.T. Phelps and M. LeVan, *Kernels of nonlinear Hamming codes*, Designs, Codes, Crypto., 6 (1995), pp. 247–257.