AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **69(2)** (2017), Pages 215–221

Disjoint Hamiltonian cycles in minimum distance graphs of 1-perfect codes

Alexander M. Romanov*

Sobolev Institute of Mathematics
630090 Novosibirsk
Russia
rom@math.nsc.ru

Abstract

It is shown that for all admissible $n \geq 15$ there exists a nonlinear binary 1-perfect code of length n whose minimum distance graph contains at least $7(n+1)/16$ pairwise edge-disjoint Hamiltonian cycles. It is also shown that for all admissible $n \geq 15$ the minimum distance graph of the binary Hamming code of length n contains at least $7(n+1)/16$ pairwise edge-disjoint Hamiltonian cycles.

1 Introduction

Let $\mathbb{F}_2^n$ be a vector space of dimension n over the finite field $\mathbb{F}_2$. The *Hamming distance* between two vectors $\mathbf{x}$, $\mathbf{y} \in \mathbb{F}_2^n$ is the number of coordinates in which they differ, denoted by $d(\mathbf{x}, \mathbf{y})$. An arbitrary subset C of $\mathbb{F}_2^n$ is called a binary *perfect* 1-error correcting code (briefly 1-perfect code) of length n if for every vector $\mathbf{x} \in \mathbb{F}_2^n$ there exists a unique vector $\mathbf{c} \in C$ such that $d(\mathbf{x}, \mathbf{c}) \leq 1$. Non-trivial binary 1-perfect codes of length n exist only if $n = 2^m - 1$, where m is a natural number not less than two. The minimum distance of any 1-perfect code is 3. Two codes $C_1, C_2 \subseteq \mathbb{F}_2^n$ are said to be *equivalent* if there exists a vector $\mathbf{v} \in \mathbb{F}_2^n$ and a permutation π in the symmetric group S_n such that $C_2 = \{\mathbf{v} + \pi(\mathbf{c}) \mid \mathbf{c} \in C_1\}$ where $\pi(\mathbf{c}) = \pi(c_1, \ldots, c_n) := (c_{\pi^{-1}(1)}, \ldots, c_{\pi^{-1}(n)})$.

We assume that the all-zero vector $\mathbf{0}$ is in code. A code is called *linear* if it is a linear space over $\mathbb{F}_2$. A linear binary 1-perfect code of length n is unique up to equivalence and is called the binary *Hamming code*. We will denote the binary Hamming code of length n by H_n.

A *distance graph* of the code C is a graph whose vertex set is C and vertices $\mathbf{x}, \mathbf{y} \in C$ are adjacent if and only if $d(\mathbf{x}, \mathbf{y}) = d$, where d is a fixed natural number. If d is the minimum distance of the code C, then the distance graph is called the *minimum distance graph*, denoted by $G(C)$.

* The work is supported by RFFI (grant 17-01-00949).

Minimum distance graphs arise naturally from error-correcting codes. It was shown [3] that the minimum distance graphs of two binary 1-perfect codes are isomorphic if and only if the codes are equivalent. In [11], it was established that nonequivalent binary extended 1-perfect codes have non-isomorphic minimum distance graphs. In [6, 10], it was established that the minimum distance graphs of two extended Preparata codes are isomorphic if and only if the codes are equivalent. If C is a binary 1-perfect code of length n, then the minimum distance graph $G(C)$ is a $(n)(n-1)/6$-regular bipartite graph with 2^{n-m} vertices, $n = 2^m - 1, m \geq 2$.

Definition 1 *If G is a k-regular graph, then a Hamiltonian decomposition of G is a set of $\lfloor k/2 \rfloor$ pairwise edge-disjoint Hamiltonian cycles in G.*

It is known that a complete graph with more than two vertices is Hamiltonian decomposable [1, 4, 8]. The minimum distance graph of the vector space $\mathbb{F}_2^n$ is called *hypercube* of dimension n. The n-dimensional hypercube is an n-regular graph with 2^n vertices. The n-dimensional hypercube also has a Hamiltonian decomposition, i.e., $\lfloor n/2 \rfloor$ pairwise edge-disjoint Hamiltonian cycles [2].

It is known that $G(H_7)$ is Hamiltonian decomposable [12]. We conjecture that the minimum distance graph $G(H_n)$ of the binary Hamming code H_n of length n is Hamiltonian decomposable for all $n = 2^m - 1$, $m \geq 3$.

In [12], Pike has shown that the minimum distance graph $G(H_n)$ has at least $\lfloor (n-m)/2 \rfloor$ edge-disjoint Hamiltonian cycles, $n = 2^m - 1$, $m \geq 3$. In this paper, we prove that for all admissible $n \geq 15$ the minimum distance graph $G(H_n)$ has at least $7(n+1)/16$ edge-disjoint Hamiltonian cycles. This is better than the Pike bound for $n = 15, 31$.

In [13], it was shown that for all admissible $n \geq 15$ there exists a nonlinear binary 1-perfect code of length n whose minimum distance graph has Hamiltonian cycles. In [14], it was shown that for all $n = (q^m - 1)/(q-1), m \geq 2$ (except $q = 2, 3, 4, m = 2$, and $q = 2, m = 3$) there exists a nonlinear q-ary 1-perfect code of length n whose minimum distance graph has Hamiltonian cycles. In this paper, we prove that for all admissible $n \geq 15$ there exists a nonlinear binary 1-perfect code of length n whose minimum distance graph contains at least $7(n+1)/16$ pairwise edge-disjoint Hamiltonian cycles.

It has been shown [15] that there exist at least $2^{2^{cn}}$ nonequivalent binary 1-perfect codes of length n, where $c = \frac{1}{2} - \epsilon$.

2 Main results

In this section, we construct a nonlinear binary 1-perfect code T_n and we prove that the minimum distance graph $G(T_n)$ of the code T_n contains a certain special subgraph.

The parity-check matrix $H = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n]$ of the binary Hamming code H_n of length $n = 2^m - 1$ consists of n pairwise linearly independent column vectors $\mathbf{h}_i$, $i \in \{1, \ldots, n\}$. The transposed column vector $\mathbf{h}_i^T$ belongs to $\mathbb{F}_2^m \setminus \{\mathbf{0}\}$, $i \in \{1, \ldots, n\}$. We assume that the columns of the parity-check matrix H are arranged in some fixed order. Set $\mathbb{F}_2^m \setminus \{\mathbf{0}\}$ generates a projective geometry $\mathrm{PG}(m-1,2)$ of geometric dimension $m-1$ over the finite field $\mathbb{F}_2$. In this geometry, the points correspond to the columns of H and the points i, j, k lie on the same line if the corresponding columns $\mathbf{h}_i, \mathbf{h}_j, \mathbf{h}_k$ are linearly dependent, i.e., their sum is all-zero column.

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, then the *support* of the vector $\mathbf{x}$ is the set

$$supp(\mathbf{x}) = \{i \mid x_i \neq 0\}.$$

A vector of weight 3 of the binary Hamming code H_n is called *triple*. Let $i \in \{1, \ldots, n\}$, then we denote a subspace spanned by the set of all triples of the code H_n having 1 in the ith coordinate by R_i. By definition, the minimum distance of the code R_i is 3.

Proposition 2 *The minimum distance graph $G(R_i)$ and the hypercube of dimension $(n-1)/2$ are isomorphic.*

Proof. Let $\mathbf{u} \in H_n$ be a triple having 1 in the ith coordinate. Then the $supp(\mathbf{u})$ can be considered as a line in the projective geometry $\mathrm{PG}(m-1,2)$. The number of lines passing through a fixed point in $\mathrm{PG}(m-1,2)$ is equal to $(n-1)/2$, $n = 2^m - 1$, $m \geq 3$. By definition of the binary Hamming code H_n and the parity-check matrix H of code H_n, it follows that all triples of the code H_n having 1 in the ith coordinate are linearly independent. Therefore the dimension of R_i is $(n-1)/2$. Since all triples have weight 3, the minimum distance graph $G(R_i)$ and the hypercube of dimension $(n-1)/2$ are isomorphic. $\square$

Consider a vector $\mathbf{x} \in \mathbb{F}_2^n$ such that its $supp(\mathbf{x})$ is a hyperplane of geometric dimension $m-2$. Let $C \subseteq \mathbb{F}_2^k$, $k = (n-1)/2$, α be a bijective map from $supp(\mathbf{x})$ to $\{1, 2, \ldots, k\}$, and $C^{\mathbf{x}} \subseteq \mathbb{F}_2^n$. Then a vector $\mathbf{c}' = (c'_1, c'_2, \ldots, c'_n)$ belongs to the code $C^{\mathbf{x}}$ if and only if there exists $\mathbf{c} = (c_1, c_2, \ldots, c_k) \in C$ such that

$$c'_i = \begin{cases} c_{\alpha(i)} & \text{if } i \in supp(\mathbf{x}), \\ 0 & \text{if } i \notin supp(\mathbf{x}), \end{cases}$$

for all $i \in \{1, 2, \ldots, n\}$. The code $C^{\mathbf{x}}$ can be viewed as embedding the code C in a large dimensional space.

Now we construct a nonlinear binary 1-perfect code T_{15} of length 15 by switching construction [5, 15]. For given $i \in \{1, 2, \ldots, 15\}$, $R_i \subset H_{15}$, and $\mathbf{c} \in (H_{15} \setminus R_i)$, we set

$$T_{15} = (H_{15} \setminus (R_i + \mathbf{c})) \cup (R_i + \mathbf{c} + \mathbf{e}_i),$$

where $\mathbf{e}_i$ is a binary vector of length 15, in which the ith component is equal to 1 and all other components are 0.

The binary Hamming code H_n of length n is unique linear code with 2-transitive automorphism group [9]. Hence the nonlinear binary 1-perfect code T_{15} is unique.

Next, we present a recursive construction of a code T_n of length $n = 2^m - 1$, $m \geq 5$. Let us assume that we have already constructed the code T_k of length

$k = (n-1)/2$. Then for given $\mathbf{x} \in \mathbb{F}_2^n$ such that its $supp(\mathbf{x})$ is an $m-2$ dimensional hyperplane, $i \in \{1, 2, \ldots, n\}$, $i \notin supp(\mathbf{x})$, $R_i \subset H_n$, we set

$$T_n = \bigcup_{\mathbf{u} \in T_k^{\mathbf{x}}} (R_i + \mathbf{u}).$$

Lemma 3 *Let $\mathbf{x} \in \mathbb{F}_2^n$ be such that its $supp(\mathbf{x})$ is an $m-2$ dimensional hyperplane, $i \in \{1, 2, \ldots, n\}$, $i \notin supp(\mathbf{x})$, the code $R_i \subset H_n$, $k = (n-1)/2$, $n = 2^m - 1$, $m \geq 5$. Then the following statement holds:*

$$T_k^{\mathbf{x}} \cap R_i = \{\mathbf{0}\}.$$

Proof. By definition, $\mathbf{0} \in T_k^{\mathbf{x}}$ and $\mathbf{0} \in R_i$. Therefore $\mathbf{0} \in T_k^{\mathbf{x}} \cap R_i$.

Next we prove that $(T_k^{\mathbf{x}} \cap R_i) \setminus \{\mathbf{0}\} = \varnothing$. For every two distinct points, there is exactly one line that contains both points. Let l be a line which passes through the point i. Since $i \notin supp(\mathbf{x})$, the intersection of the hyperplane $supp(\mathbf{x})$ with the line l contains exactly one point. Otherwise, all points on the line l must belong to the hyperplane $supp(\mathbf{x})$. Let $\mathbf{u}, \mathbf{u}'$ be triples of the code H_n having 1 in the ith coordinate and let $supp(\mathbf{u}) = \{i, j, k\})$, $supp(\mathbf{u}') = \{i, j', k'\})$. Since $\{i, j, k\}$ and $\{i, j', k'\}$ are lines of the projective geometry PG$(m-1, 2)$, $j = j'$ if and only if $k = k'$. Therefore

$$supp(\mathbf{c}) \nsubseteq supp(\mathbf{x}) \text{ for all } \mathbf{c} \in R_i,\ \mathbf{c} \neq \mathbf{0}. \tag{1}$$

Further we define a set $\mathbb{F}^{\mathbf{x}}$. Let

$$\mathbb{F}^{\mathbf{x}} = \left\{\mathbf{c} \in \mathbb{F}_2^n \mid supp(\mathbf{c}) \subseteq supp(\mathbf{x})\right\}.$$

From (1) it follows that $(\mathbb{F}^{\mathbf{x}} \cap R_i) \setminus \{\mathbf{0}\} = \varnothing$. By definition, $T_k^{\mathbf{x}} \subseteq \mathbb{F}^{\mathbf{x}}$. Hence, we proved that $(T_k^{\mathbf{x}} \cap R_i) \setminus \{\mathbf{0}\} = \varnothing$. □

Lemma 4 *The code T_n is a nonlinear binary 1-perfect code of length $n = 2^m - 1$, $m \geq 4$.*

Proof. We will prove the theorem by induction on m. By definition, the code T_{15} is a nonlinear binary 1-perfect code of length 15, see [5, 15]. By induction hypothesis, the code T_k is a nonlinear binary 1-perfect code of length $k = (n-1)/2$. Next we prove that the code

$$T_n = \bigcup_{\mathbf{u} \in T_k^{\mathbf{x}}} (R_i + \mathbf{u})$$

is a nonlinear binary 1-perfect code of length $n = 2^m - 1$, $m \geq 5$.

We need to prove that the number of codewords in the code T_n is correct and that the minimum distance of T_n is equal to 3. From Proposition 2 it follows that the code $R_i \subseteq H_n$ contains $2^{\frac{n-1}{2}}$ codewords. By induction hypothesis, the code T_k contains $2^{\frac{n-1}{2}-m+1}$ codewords. Hence, taking into account Lemma 3, we have that the code T_n contains 2^{n-m} codewords.

Now we show that the minimum distance of T_n is equal to 3. Suppose that the first $k+1$ components of the vector $\mathbf{x}$ are equal to 0, and the remaining components of this vector are equal to 1. Then any codeword in T_n can be represented in the form

$$(\mathbf{v}|\mathbf{w}) + (\mathbf{0}|\mathbf{u}),$$

where $(\cdot|\cdot)$ denotes concatenation, $(\mathbf{v}|\mathbf{w}) \in R_i$, $supp(\mathbf{v}) \cap supp(\mathbf{x}) = \varnothing$, $supp(\mathbf{w}) \subseteq supp(\mathbf{x})$, and $\mathbf{u} \in T_k^{\mathbf{x}}$. Since $i \notin supp(\mathbf{x})$, then from the definition of the code R_i, it follows that $d(\mathbf{v}, \mathbf{v}') \geq 2$ for all $(\mathbf{v}|\mathbf{w}), (\mathbf{v}'|\mathbf{w}') \in R_i$ and $(\mathbf{v}|\mathbf{w}) \neq (\mathbf{v}'|\mathbf{w}')$. For $d(\mathbf{v}, \mathbf{v}') \geq 3$ taking into account Lemma 3, we have that the minimum distance of the code T_n is 3.

Let $d(\mathbf{v}, \mathbf{v}') = 2$, then it follows from the definition of R_i that

$$1 \leq d(\mathbf{w}, \mathbf{w}') \leq 2.$$

From the definition of the 1-perfect code it follows that the 1-perfect code $T_k^{\mathbf{x}}$ of length k and vectors $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_k$ form a partition of the space $\mathbb{F}_2^k$. Then since $1 \leq d(\mathbf{w}, \mathbf{w}') \leq 2$, then taking into account Lemma 3, we get that

$$d(\mathbf{w} + \mathbf{u}, \mathbf{w}' + \mathbf{u}') \geq 1 \text{ for all } \mathbf{u}, \mathbf{u}' \in T_k^{\mathbf{x}}.$$

Hence we have that the minimum distance of the code T_n is 3.

By induction hypothesis, the code T_k is nonlinear, therefore the code T_n is also nonlinear. □

We will use the notation $G_1 \square G_2$ for the Cartesian product of graphs. Further we consider a special subgraph $G(R_i) \square G(T_k)$.

Lemma 5 *The minimum distance graph $G(T_n)$ of the code T_n contains the spanning subgraph $G(R_i) \square G(T_k)$ where $\mathbf{x} \in \mathbb{F}_2^n$, $supp(\mathbf{x})$ is an $m-2$ dimensional hyperplane, $R_i \subset H_n$, $i \notin supp(\mathbf{x})$, $k = (n-1)/2$, $n = 2^m - 1$, $m \geq 5$.*

Proof. By definition, the minimum distance graph $G(T_k^{\mathbf{x}})$ and the minimum distance graph $G(T_k)$ are isomorphic. Hence from Lemma 3, it follows that the minimum distance graph $G(T_n)$ of the code T_n contains the spanning subgraph $G(R_i) \square G(T_k)$. □

Theorem 6 *The minimum distance graph $G(T_n)$ of the nonlinear binary 1-perfect code T_n contains at least $7(n+1)/16$ pairwise edge-disjoint Hamiltonian cycles, $n = 2^m - 1$, $m \geq 4$.*

Proof. We will prove the theorem by induction on m. It is not difficult to check by computer that the minimum distance graph $G(T_{15})$ contains at least 7 pairwise edge-disjoint Hamiltonian cycles. By induction hypothesis, the minimum distance graph $G(T_k)$ contains at least $7(n+1)/32$ pairwise edge-disjoint Hamiltonian cycles, $k = (n-1)/2$, $n = 2^m - 1$, $m \geq 5$. By Proposition 2 as well as observations made in [2], it follows that the minimum distance graph $G(R_i)$ of the code $R_i \subset H_n$

contains $(n-3)/4$ pairwise edge-disjoint Hamiltonian cycles. It is well known that Cartesian product of any two cycles can be decomposed into two Hamiltonian cycles [7]. Therefore, by Lemma 5, it follows that the minimum distance graph $G(T_n)$ of the nonlinear binary 1-perfect code T_n contains at least $7(n+1)/16$ pairwise edge-disjoint Hamiltonian cycles, $n = 2^m - 1$, $m \geq 4$. □

Lemma 7 *The minimum distance graph $G(H_n)$ of the binary Hamming code H_n contains the spanning subgraph $G(R_i) \square G(H_k)$ where H_k is the binary Hamming code of length $k = (n-1)/2$, $n = 2^m - 1$, $m \geq 3$, $i \in \{1, 2, \ldots, n\}$.*

Proof. Let $\mathbf{x} \in \mathbb{F}_2^n$ be such that its $supp(\mathbf{x})$ is an $m-2$ dimensional hyperplane. Let

$$H_k^{\mathbf{x}} = \{\mathbf{u} \in H_n \mid supp(\mathbf{u}) \subseteq supp(\mathbf{x})\},$$

where $k = (n-1)/2$. If $i \notin supp(\mathbf{x})$ then $H_k^{\mathbf{x}} \cap R_i = \{\mathbf{0}\}$ and

$$H_n = \bigcup_{\mathbf{u} \in H_k^{\mathbf{x}}} (R_i + \mathbf{u}).$$

Therefore the minimum distance graph $G(H_n)$ of the binary Hamming code H_n contains the spanning subgraph $G(R_i) \square G(H_k)$. □

Theorem 8 *The minimum distance graph $G(H_n)$ of the binary Hamming code H_n contains at least $7(n+1)/16$ pairwise edge-disjoint Hamiltonian cycles, $n = 2^m - 1$, $m \geq 4$.*

Proof. This proof is similar to the proof of Theorem 6. It is not difficult to check by computer that the minimum distance graph $G(H_{15})$ of the binary Hamming code H_{15} of length $n = 15$ contains at least 7 pairwise edge-disjoint Hamiltonian cycles. Therefore, by Lemma 7, it follows that the minimum distance graph $G(H_n)$ of the binary Hamming code H_n contains at least $7(n+1)/16$ pairwise edge-disjoint Hamiltonian cycles, $n = 2^m - 1$, $m \geq 4$. □

Acknowledgments

The author would like to thank the anonymous referees for their helpful comments and suggestions, which greatly improved the final manuscript.

References

[1] B. Alspach, The Wonderful Walecki Construction, *Bull. Inst. Combin. Appl.* **52** (2008), 7–20.

[2] B. Alspach, J.-C. Bermond and D. Sotteau, Decomposition into cycles I: Hamilton decompositions, Proc. 1987 *Cycles and Rays* Colloquium, Montréal, NATO Adv. Sci. Inst. Ser. C 301, Kluwer Acad. Publ., Dordrecht, 1990, 9–18.

[3] S. V. Avgustinonvich, Perfect binary (n,3) codes: the structure of graphs, *Discrete Appl. Math.* **114** (2001), 9–11.

[4] D. E. Bryant, Cycle Decompositions of Complete Graphs, *Surveys in Combinatorics 2007* (Eds. A. J. W. Hilton and J. M. Talbot) London Math. Soc. Lec. Note Ser. 346, Cambridge, England: Cambridge University Press, 2007, 67–98.

[5] T. Etzion and A. Vardy, Perfect binary codes: Constructions, properties, and enumeration, *IEEE Trans. Inf. Theory* **40 (3)** (1994), 754–763.

[6] C. Fernández-Córdoba and K. T. Phelps, On the minimum distance graph of an extended Preparata code, *Des. Codes Crypto.* **57 (2)** (2010), 161–168.

[7] A. Kotzig, Every Cartesian product of two circuits is decomposable into two Hamiltonian circuits, Rapport 233, Le Centre de Recherches Mathématiques, Montréal, 1973.

[8] É. Lucas, *Récréations Mathématiques*, tome II. Paris, 1892.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland Publishing Co., 1977.

[10] I. Y. Mogilnykh, On weak isometries of Preparata codes, *Prob. Inform. Transmis.* **45** (2009), 145–150.

[11] I. Y. Mogilnykh, P. R. J Östergård, O. Pottonen and F. I. Solov'eva, Reconstructing extended perfect binary one-error-correcting codes from their minimum distance graphs, *IEEE Trans. Inform. Theory* **55 (6)** (2009), 2622–2625.

[12] D. A. Pike, *Hamilton Decompositions of Graphs*, Ph.D. Dissertation, Auburn University, 1996.

[13] A. M. Romanov, On combinatorial Gray codes with distance 3, *Discr. Math. Appl.* **19** (2009), 383–388.

[14] A. M. Romanov, Hamiltonicity of minimum distance graphs of 1-perfect codes, *Electron. J. Combin.* **19** (2012), #P65.

[15] Yu. L. Vasil'ev, On nongroup close-packed codes, *Probl. Kybern.* **8** (1962), 337–339.

(Received 11 Dec 2016; revised 19 Apr 2017, 19 July 2017)