Hamiltonicity of minimum distance graphs of 1-perfect codes

Alexander M. Romanov[*]

Sobolev Institute of Mathematics
630090 Novosibirsk, Russia

rom@math.nsc.ru

Submitted: Jan 18, 2012; Accepted: Mar 18, 2012; Published: Mar 31, 2012
Mathematics Subject Classifications: 05C45, 94B25

Abstract

A 1-perfect code $\mathcal{C}_q^n$ is called *Hamiltonian* if its minimum distance graph $G(\mathcal{C}_q^n)$ contains a Hamiltonian cycle. In this paper, for all admissible lengths $n \geq 13$, we construct Hamiltonian nonlinear ternary 1-perfect codes, and for all admissible lengths $n \geq 21$, we construct Hamiltonian nonlinear quaternary 1-perfect codes. The existence of Hamiltonian nonlinear q-ary 1-perfect codes of length $N = qn + 1$ is reduced to the question of the existence of such codes of length n. Consequently, for $q = p^r$, where p is prime, $r \geq 1$ there exist Hamiltonian nonlinear q-ary 1-perfect codes of length $n = (q^m - 1)/(q - 1)$, $m \geq 2$. If $q = 2, 3, 4$, then $m \neq 2$. If $q = 2$, then $m \neq 3$.

1 Introduction

Let $\mathbf{F}_q^n$ be a vector space of dimension n over the Galois field $\mathbf{F}_q$. The Hamming distance between two vectors $\mathbf{x}$, $\mathbf{y} \in \mathbf{F}_q^n$ is the number of coordinates in which they differ and it is denote by $d(\mathbf{x}, \mathbf{y})$. An arbitrary subset $\mathcal{C}_q^n$ of $\mathbf{F}_q^n$ is called q-ary *1-perfect* code of length n, if for every vector $\mathbf{x} \in \mathbf{F}_q^n$ there exists a unique vector $\mathbf{c} \in \mathcal{C}_q^n$ such that $d(\mathbf{x}, \mathbf{c}) \leq 1$. It is known that q-ary 1-perfect codes of length n exist only if $n = (q^m - 1)/(q - 1)$, where m is a natural number not less than two. We shall assume that the all-zero vector $\mathbf{0}$ is in code. A code is called *linear* if it is a linear space over $\mathbf{F}_q$. The linear 1-perfect codes are called *Hamming* codes.

The sum of the vectors $\mathbf{x}, \mathbf{y} \in \mathbf{F}_q^n$ is denoted by $\mathbf{x} + \mathbf{y}$. Two codes $\mathcal{C}_q^n, \mathcal{D}_q^n \subseteq \mathbf{F}_q^n$ are said to be *isomorphic* if there exists a permutation π such that $\mathcal{D}_q^n = \{\pi(\mathbf{c}) : \mathbf{c} \in \mathcal{C}_q^n\}$. They are said to be *equivalent* if there exist a vector $\mathbf{u} \in \mathbf{F}_q^n$ and a permutation π such

[*]The work is supported by RFFI (grant 11-01-00997)

that $\mathcal{D}_q^n = \{\pi(\mathbf{c}) + \mathbf{u} : \mathbf{c} \in \mathcal{C}_q^n\}$. There exist at least $q^{q^{cn}}$ pairwise nonequivalent q-ary 1-perfect codes of length n where a constant $c = \frac{1}{q} - \varepsilon$. See [1, 2, 6, 7].

The *minimum distance* of a code $\mathcal{C}_q^n \subseteq \mathbf{F}_q^n$ is defined by $d(\mathcal{C}_q^n) = min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C}_q^n, \mathbf{x} \neq \mathbf{y}\}$. Let $\mathcal{C}_q^n$ be a 1-perfect code of length n. Then, $d(\mathcal{C}_q^n) = 3$ and the *minimum distance graph* of the code $\mathcal{C}_q^n$ is a graph $G(\mathcal{C}_q^n)$ whose vertex set is $\mathcal{C}_q^n$ and vertices $\mathbf{x}, \mathbf{y} \in \mathcal{C}_q^n$ are adjacent if and only if $d(\mathbf{x}, \mathbf{y}) = 3$. A *path* in a graph is a sequence of vertices such that two consecutive vertices in this path are connected by at least one edge. A finite path always has a first vertex, called its *start* vertex, and a last vertex, called its *end* vertex. A *cycle* is a path such that the start vertex and end vertex are the same. A cycle that contains each vertex of the graph exactly once is called *Hamiltonian* cycle. A 1-perfect code $\mathcal{C}_q^n$ is called *Hamiltonian* if its minimum distance graph $G(\mathcal{C}_q^n)$ contains a Hamiltonian cycle.

The *weight* of a vector $\mathbf{x} \in \mathbf{F}_q^n$ is the number of its nonzero coordinates. A vector of weight 3 of the Hamming code $\mathcal{H}_q^n$ is called *triple*. It is known that the set of all triples of the code $\mathcal{H}_q^n$ generates the code. Therefore, the Hamming codes are Hamiltonian, except $q = 2$, $m = 2$.

A mapping $\phi : \mathcal{C}_q^n \to \mathbf{F}_q^n$ is called an *isometry* from the code $\mathcal{C}_q^n$ to the code $\phi(\mathcal{C}_q^n)$ if $d(\mathbf{x}, \mathbf{y}) = d(\phi(\mathbf{x}), \phi(\mathbf{y}))$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{C}_q^n$. Obviously, two codes $\mathcal{C}_q^n$ and $\mathcal{D}_q^n$ are isometric if there are n permutations $\tau_1, \tau_2, \ldots, \tau_n$ of q elements in Galois field $\mathbf{F}_q$ and permutation σ of the n coordinates such that $\mathcal{D}_q^n = \{\sigma(\tau_1(c_1), \tau_2(c_2), \ldots, \tau_n(c_n)) : \mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathcal{C}_q^n\}$.

For $q \geq 5$ there are nonlinear q-ary 1-perfect codes that are isometric to the Hamming codes. Therefore, for $q \geq 5$ and for all admissible lengths there are nonlinear q-ary 1-perfect codes whose minimum distance graphs contain a Hamiltonian cycle.

The question of the existence of Hamiltonian nonlinear binary 1-perfect codes remained an open for a long time. The existence of Hamiltonian nonlinear binary codes for all admissible lengths $n \geq 15$ was constructively proved in [4].

In this paper, for all admissible lengths $n \geq 13$, we construct Hamiltonian nonlinear ternary 1-perfect codes, and for all admissible lengths $n \geq 21$, we construct Hamiltonian nonlinear quaternary 1-perfect codes. The existence of Hamiltonian nonlinear q-ary 1-perfect codes of length $N = qn+1$ is reduced to the question of the existence of such codes of length n. Consequently, for $q = p^r$, where p is prime, $r \geq 1$ there exist Hamiltonian nonlinear q-ary 1-perfect codes of length $n = (q^m - 1)/(q - 1)$, $m \geq 2$. If $q = 2, 3, 4$, then $m \neq 2$. If $q = 2$, then $m \neq 3$.

It remains an open question of the existence of a Hamiltonian cycle in the graph formed by the two middle levels of n-dimensional binary hypercube, where n is odd. Also, is not proved Lovász conjecture, which states that the every finite connected vertex-transitive graph contains a Hamiltonian path.

Let $\mathcal{H}_q^n$ be a q-ary Hamming code of length n. The parity-check matrix of Hamming code $\mathcal{H}_q^n$ of length $n = (q^m - 1)/(q - 1)$ consists of n pairwise linearly independent column vectors $\mathbf{h}_i$, where $\mathbf{h}_i^T \in \mathbf{F}_q^m$, $i \in \{1, \ldots, n\}$. The set $\mathbf{F}_q^m \setminus \{\mathbf{0}\}$ generates a projective space $PG_{m-1}(q)$ of dimension $(m-1)$ over the Galois field $\mathbf{F}_q$. In this space, points correspond to the column vectors of the parity-check matrix of the Hamming code $\mathcal{H}_q^n$ and the three points i, j, k lie on the same line if the corresponding column vectors $\mathbf{h_i}, \mathbf{h_j}, \mathbf{h_k}$ are linearly dependent.

Let $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$. Then, the *support* of vector $\mathbf{x}$ is the set $supp(\mathbf{x}) = \{i : x_i \neq 0\}$. Consider the vector $\mathbf{x} \in \mathbf{F}_q^n$ such that its $supp(\mathbf{x})$ is $m-2$ dimensional hyperplane. Denote by $\mathcal{H}_q^n(\mathbf{x})$ the set of all vectors $\mathbf{v} \in \mathcal{H}_q^n$ such that $supp(\mathbf{v}) \subseteq supp(\mathbf{x})$. The set $\mathcal{H}_q^n(\mathbf{x})$ forms in $\mathcal{H}_q^n$ subcode previous dimension.

Let $N = qn + 1 = (q^{m+1} - 1)/(q - 1)$. In the projective space $PG_m(q)$ of dimension m, we consider the pencil of lines through a point i, where $i \in \{1, 2, \ldots, N\}$. It is known that the pencil of lines contains n lines which will be denoted by $l_1, l_2, \ldots, l_n$. Denote by $\mathcal{H}_q^N(l_p)$ the subcode of the code $\mathcal{H}_q^N$ defined by the line l_p, $p \in \{1, 2, \ldots, n\}$. Let

$$R_i^N = \mathcal{H}_q^N(l_1) + \mathcal{H}_q^N(l_2) + \cdots + \mathcal{H}_q^N(l_n).$$

All cosets $R_i^N + \mathbf{v}$ (where $\mathbf{v} \in \mathcal{H}_q^N$) form the set of *i-components* of the Hamming code $\mathcal{H}_q^N$. Since the dimension of $\mathcal{H}_q^N(l_p)$ is $q-1$, it follows that the dimension of R_i^N is $(q-1)n = q^m - 1$. See [3, 5].

A triple belongs to the line if the support of this triple belongs to the line. Consider the subspace R_i^n of the Hamming code $\mathcal{H}_q^n$ of length n. In the projective space $PG_{m-1}(q)$, each line contains $q+1$ points. Therefore, each line contains $q-1$ linearly independent triples with nonzero ith coordinate which form the basis of the subspace $\mathcal{H}_q^n(l_p)$, where $p \in \{1,\ l, 2, \ldots, (n-1)/q\}$. Thus the subspace R_i^n is generated by all triples with nonzero ith coordinate. The dimension of R_i^n is $q^{m-1} - 1$. Let $\mathbf{e}_i$ denote the vector of length n in which ith component is 1 and other components are equal to 0. Let $\lambda \in \mathbf{F}_q$. It is known [3], the set

$$\mathcal{C}_q^n = \left(\mathcal{H}_q^n \setminus\ (R_i^n + \mathbf{u})\right) \cup (R_i^n + \mathbf{u} + \lambda \cdot \mathbf{e}_i)$$

is a 1-perfect code of length n. It is said that the code $\mathcal{C}_q^n$ is obtained from the code $\mathcal{H}_q^n$ by switching or translation of the i-component $(R_i^n + \mathbf{u})$ of the code $\mathcal{H}_q^n$.

2 Main results

Consider the vector $\mathbf{x} \in \mathbf{F}_q^n$ such that its $supp(\mathbf{x})$ is $m-2$ dimensional hyperplane. Denote by $\mathbf{F}_q^n(\mathbf{x})$ the set of all vectors $\mathbf{v} \in \mathbf{F}_q^n$ such that $supp(\mathbf{v}) \subseteq supp(\mathbf{x})$.

Lemma 1. *Let $i \notin supp(\mathbf{x})$ and $\mathbf{u} \in \mathbf{F}_q^n(\mathbf{x})$. Then, the intersection*

$$(R_i^n + \mathbf{u}) \cap \mathbf{F}_q^n(\mathbf{x})$$

contains only one vector.

Proof. Let l_p be an arbitrary line through the point i. Since $i \notin supp(\mathbf{x})$, it follows that any line passing through the point i intersects with the hyperplane $supp(\mathbf{x})$ only at one point. Hence the intersection of $\mathcal{H}_q^n(l_p) \cap \mathbf{F}_q^n(\mathbf{x})$ can contain only vectors of weight 0 or 1. It is obvious that $\mathbf{0} \in \mathcal{H}_q^n(l_p) \cap \mathbf{F}_q^n(\mathbf{x})$. Since the minimum weight of the nonzero vectors in $\mathcal{H}_q^n(l_p)$ is equal to 3, it follows that $\mathcal{H}_q^n(l_p) \cap \mathcal{R}_q^n(\mathbf{x}) = \{\mathbf{0}\}$. Since the line l_p was chosen arbitrarily and set R_i^n is a subspace, we have $R_i^n \cap \mathcal{R}_q^n(\mathbf{x}) = \{\mathbf{0}\}$. The lemma is proved.

Obvious that the minimum distance between two distinct vectors in R_i^n is equal to 3. Denote by $G(R_i^n)$ the minimum distance graph of the set R_i^n.

Lemma 2. *Let $m \geq 3$, $n = (q^m - 1)/(q - 1)$. Then, graph $G(R_i^n)$ contains a Hamiltonian cycle.*

Proof. Consider a cyclic q-ary Gray code of dimension $q^{m-1} - 1$. The Gray code defines a linear combinations of the basis vectors of the subspace R_i^n. Since the subspace R_i^n is generated by all triples with non-zero ith coordinate, it follows that all basis vectors of the subspace R_i^n have weight equal to the 3. Hamming distance between two consecutive vectors in the Gray code is one. Therefore, the distance between two consecutive vectors (the consecutive vectors in the subspace R_i^n defined by the consecutive vectors of the Gray code) in the subspace R_i^n is 3. Thus a cyclic q-ary Gray code of dimension $q^{m-1} - 1$ determines a Hamiltonian cycle in the graph $G(R_i^n)$. The lemma is proved.

Now we turn to a proof of the main theorem.

Theorem 1. *Assume that there exists a nonlinear q-ary 1-perfect code $\mathcal{C}_q^n$ of length $n = (q^{m-1} - 1)/(q - 1)$, $m \geq 3$ such that the minimum distance graph of the code $\mathcal{C}_q^n$ contains a Hamiltonian cycle. Then, there exists a nonlinear q-ary 1-perfect code $\mathcal{D}_q^N$ of length $N = qn + 1$ such that the minimum distance graph of the code $\mathcal{D}_q^N$ also contains a Hamiltonian cycle.*

Proof. Consider the construction of nonlinear q-ary 1-perfect codes proposed in [2, 6]. This construction is a generalization of the construction from [7]. We assume that the columns of parity-check matrix of the Hamming code $\mathcal{H}_q^N$ are ordered lexicographically. The vectors of the space $\mathbf{F}_q^N$ will also be considered as words of length N over an alphabet $\{0, 1, \ldots, q - 1\}$. Let

$$\mathcal{D}_q^N = \bigcup_{\mathbf{c} \in \mathcal{C}_q^n} \left(R_i^N + (\mathbf{c} \mid \mathbf{0}) \right), \tag{1}$$

where the vector $\mathbf{0} \in \mathbf{F}_q^{(qn-n+1)}$, $i \geq n + 1$ and the vertical bar (|) denotes concatenation. Formula (1) is a certain modification of the construction from [2, 6]. Lemma 1 implies that the set $\mathcal{D}_q^N$ is a q-ary 1-perfect code of length $N = qn + 1$. The nonlinearity of the code $\mathcal{D}_q^N$ follows from (1) and the nonlinearity of the code $\mathcal{C}_q^n$. It is known that the graph that is a Cartesian product of two Hamiltonian cycles always contains a Hamiltonian cycle. Consequently, hamiltonicity of code $\mathcal{D}_q^N$ follows from Lemma 2, formula (1) and hamiltonicity of the code $\mathcal{C}_q^n$. The theorem is proved.

Statement 1. *Let $i \notin supp(\mathbf{x})$ and $\mathbf{u} \in \mathcal{H}_q^n$. Then, the intersection*

$$(R_i^n + \mathbf{u}) \cap \mathcal{H}_q^n(\mathbf{x})$$

contains only one vector.

Proof. Let l_p be an arbitrary line through the point i. Since $i \notin supp(\mathbf{x})$, it follows that any line passing through the point i intersects with the hyperplane $supp(\mathbf{x})$ only at one point. Hence, the intersection of $R_i^n \cap \mathcal{H}_q^n(\mathbf{x})$ can contain only vectors of weight 0 or 1. It is obvious that $\mathbf{0} \in \mathcal{H}_q^n(l_p) \cap \mathcal{H}_q^n(\mathbf{x})$. Since the minimum weight of nonzero vectors that belong to the subcode $\mathcal{H}_q^n(l_p)$ is 3, it follows that $\mathcal{H}_q^n(l_p) \cap \mathcal{H}_q^n(\mathbf{x}) = \{\mathbf{0}\}$. Since the line l_p was chosen arbitrarily and set R_i^n is a subspace, we have $R_i^n \cap \mathcal{H}_q^n(\mathbf{x}) = \{\mathbf{0}\}$. Next, we show that the number of cosets formed subspace R_i^n equals the number code vectors belonging to the subcode $\mathcal{H}_q^n(\mathbf{x})$. The dimension of the code $\mathcal{H}_q^n$ is equal to $n-m$, and the dimension of R_i^n is $q^{m-1}-1$. Hence, the number of cosets formed subspace R_i^n is equal to $q^{\frac{n-1}{q}-m+1}$. Number of codewords in the subcode $\mathcal{H}_q^n(\mathbf{x})$ is equal to $q^{\frac{n-1}{q}-m+1}$. Thus we have the equality $\mid (R_i^n + \mathbf{u}) \cap \mathcal{H}_q^n(\mathbf{x}) \mid = 1$. The statement is proved.

Statement 2. *Let $N = qn + 1 = (q^{m+1}-1)/(q-1)$. Then, the graph $G(\mathcal{H}_q^N)$ contains a spanning subgraph which is a Cartesian product of a Hamiltonian cycle of the graph $G(\mathcal{H}_q^n)$ and a Hamiltonian cycle of the graph $G(R_i^N)$.*

Proof. Let $i \notin \{1, 2, \ldots, n\}$. Then, by Statement 1 for the Hamming code $\mathcal{H}_q^N$ we have

$$\mathcal{H}_q^N = \bigcup_{\mathbf{c} \in \mathcal{H}_q^n} \Big(R_i^N + (\mathbf{c} \mid \mathbf{0}) \Big).$$

Hence, the graph $G(\mathcal{H}_q^N)$ contains a spanning subgraph which is a Cartesian product of a Hamiltonian cycle of the graph $G(\mathcal{H}_q^n)$ and a Hamiltonian cycle of the graph $G(R_i^N)$. The statement is proved.

Next, let $q = 3$. For $m = 2$ all ternary 1-perfect codes of length $n = 4$ are equivalent to the ternary Hamming code $\mathcal{H}_3^4$. A minimum distance graph of the ternary Hamming code $\mathcal{H}_3^4$ is a complete graph on nine vertices.

Theorem 2. *For $q = 3$ and $q = 4$, $m \geq 3$ there exist nonlinear q-ary 1-perfect codes of length $n = (q^{m-1}-1)/(q-1)$ whose minimum distance graphs contain a Hamiltonian cycle.*

Proof. We can construct the nonlinear ternary 1-perfect codes of length $n = 13$ by switching of i-components of the ternary Hamming code $\mathcal{H}_3^{13}$ and inspect by computer that the minimum distance graphs of these codes contain a Hamiltonian cycle. If we use Statement 2, then the construction of Hamiltonian nonlinear ternary 1-perfect codes of length $n = 13$ will be simple. Similarly we can construct the Hamiltonian nonlinear quaternary 1-perfect codes of length $n = 21$. The theorem is proved.

References

[1] T. Etzion *Nonequivalent q-ary Perfect Codes.* SIAM J. Disc. Math. 9 (1996) 413–423.

[2] B. Lindström *On group and nongroup perfect codes in q symbols.* Math. Scand. 25 (1969) 149–158.

[3] K. T. Phelps, M. Villanueva *Ranks of q-ary 1-perfect codes.* Des. Codes Cryptogr. 27 (2002) 139–144.

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

[5] A. M. Romanov *On partitions of q-ary Hamming codes into disjoint components.* Diskretn. Anal. Issled. Oper. Ser. 1, 11, (2004) 80–87.

[6] J. Schönheim *On linear and nonlinear single-error-correcting q-nary perfect codes.* Inform. and Control 12 (1968) 23–26.

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