Problems of Information Transmission, Vol. 40, No. 2, 2004, pp. 159–164. Translated from Problemy Peredachi Informatsii, No. 2, 2004, pp. 63–69.

CODING THEORY

On Components of Preparata Codes

N. N. Tokareva

Novosibirsk State University
tokareva@ccfit.nsu.ru

Received November 3, 2003; in final form, February 19, 2004

Abstract—The paper considers the interrelation between i-components of an arbitrary Preparata-like code P and i-components of a perfect code C containing P. It is shown that each i-component of P can uniquely be completed to an i-component of C by adding a certain number of special codewords of C. It is shown that the set of vertices of P in a characteristic graph of an arbitrary i-component of C forms a perfect code with distance 3.

1. INTRODUCTION

It is well known (see [1]) that there are only two nontrivial infinite families of codes that are both maximal and uniformly packed—these are the (closely related) families of perfect codes and Preparata codes.

The paper reveals one more property reflecting the relation between Preparata codes and perfect code containing them. The main subject of our study are components of Preparata codes and perfect codes; the main tool is the component switching method.

By a component of a code we mean a subset of codewords allowing special-type transformations, which change a code but preserve its parameters (code length, cardinality, and distance). Presently, the switching method (method of independent transformations of different components of a code) plays one of the main roles in studying the properties of perfect codes (see [2–4]); however, it should be noted that the method has never been applied to Preparata codes.

Each Preparata code is contained in a certain perfect code, which is unique (see [5]). The converse is not true in general. If, by switching of an arbitrary i-component (for the definition, see Section 2), we pass from a Preparata code P to a Preparata code P', what is the relation between perfect codes C and C' that contain P and P' respectively?

We show that any i-component of a Preparata code can uniquely be completed to an i-component of a perfect code, and a switch of an i-component in the Preparata code induces in the ambient perfect code a switch of the completed i-component only (Theorem 1). Thus, codes C and C' are obtained from each other by switching involving one coordinate i only. As a consequence, we obtain estimates for the cardinality of a minimal i-component of a Preparata code. We also show that the set of vertices of a Preparata code in a characteristic graph of an arbitrary i-component of the ambient perfect code forms a perfect code with distance 3 (Theorem 2).

2. NECESSARY DEFINITIONS AND STATEMENTS

Consider the n-dimensional vector space E^n over Galois field $GF(2)$ equipped with the *Hamming metric*: the distance $d(x, y)$ between vectors x and y (we will also call them vertices) is the number of positions in which they differ. The *weight* $w(x)$ of a vertex x is $d(x, \mathbf{0}^n)$, where $\mathbf{0}^n$ is the *zero* vertex, i.e., the vertex with all coordinates equal to zero. A set $C \subseteq E^n$ is called a *code* of

0032-9460/04/4002-0159

length n, dimension k, with code distance d if its cardinality is 2^k and the distance between any two codewords is not less than d.

A subset M of a code C with distance d is called an *i-component* of C if the set

$$C' = (C \setminus M) \cup (M \oplus e_i)$$

is also a code with distance d, where e_i is a vector with only one nonzero coordinate $i \in \{1, 2, \ldots, n\}$ (in other words, an i-component of a code is a component whose transformation is chosen to be inversion of an arbitrary coordinate i in each of the codewords, i.e., *switching* using coordinate i). The definition of a *minimal* (i.e., indecomposable into smaller components) i-component was introduced in [6]. According to this definition, an i-component of a code can be either minimal or composed of several i-components.

A code vertex u is called *i-close* to a code vertex v if it is at the minimum code distance from v and differs from v in the ith coordinate. We call a vector w in E^n the *i-direction* of a code vertex v if $v \oplus w$ is i-close to v. Thus, i-directions of any code vertex are vectors of weight d (not necessarily belonging to the code) with one in the ith position. For a code vertex v, the total number of its i-directions is referred to as the *i-degree* of the vertex.

Following [7], one can easily prove the fact below:

Proposition 1. *A subset M of a code C is an i-component of C if and only if together with any of its vertices it contains all vertices i-close to them.*

Proposition 1 immediately implies that, for an arbitrary coordinate i, any code can uniquely be represented as a union of disjoint minimal i-components. A code is called *distance-invariant* if the number of code vertices lying at a certain distance from a given code vertex does not depend on the choice of this vertex but depends only on the code length and this distance. Any maximal uniformly packed code is distance-invariant, see [1].

Proposition 2. *Let C be an arbitrary maximal uniformly packed code containing the zero vertex $\mathbf{0}^n$ and the all-one vertex $\mathbf{1}^n$. Then $\mathbf{0}^n$ and $\mathbf{1}^n$ belong to the same minimal i-component of C.*

Let us prove this fact, which is a direct generalization of a statement proved in [8] for the case where C is a perfect code. Assume that $\mathbf{0}^n$ and $\mathbf{1}^n$ belong to different minimal i-components of C. Consider the code C' obtained from C by switching only the i-component that contains $\mathbf{1}^n$. Codes C and C' must have the same weight distribution with respect to the zero vertex. However, this distance-invariance property is violated since $\mathbf{1}^n$ belongs to C but does not belong to C'. $\triangle$

Any code can be represented as a union of two disjoint sets: i-even and i-odd vertices. A code vertex is called *i-even* (*i-odd*) if its projection with respect to the coordinate i is of even (odd) weight. Each of these sets is an i-component of the code if the code distance is odd. This partition is called the *trivial* partition of a code into i-components. Indeed, if the code distance is odd, then, for an arbitrary vertex, all vertices i-close to it have the same i-parity as this vertex and hence belong to the same set in the partition.

Consider a distance-invariant code C with odd code distance such that all of its vertices have the same i-degree for some coordinate i. Let this i-degree be different from the number of all code vertices lying at the minimum distance from an arbitrary vertex of the code. Then we have the following statement.

Proposition 3. *The code C defined above is partitioned with respect to the coordinate i into two i-components of equal size.*

Proof. It suffices to show that, in such a code, the sets C_0 and C_1 (of i-even and i-odd vertices respectively) are of the same cardinality; in this case, the required partition is the trivial one. Consider a bipartite graph on the set of code vertices in which edges connect vertices of different

i-parity that are at the minimum distance from each other. For any code vertex v, the set of all codewords that lie at the minimum distance from it consists of a set of vertices of the same i-parity (these are vertices i-close to v) and a set of vertices of i-parity different from that of v. By the conditions imposed on the code, cardinalities of both sets are independent of the choice of a vertex v. The considered graph is regular; hence, its parts C_0 and C_1 must be of equal cardinality. $\triangle$

Now let us proceed to codes of our interest.

A code C of length n with distance 3 is *perfect* if disjoint balls of radius 1 centered in the code vertices cover the whole space E^n. Perfect binary codes with distance 3 exist only if $n = 2^m - 1$, $m = 2, 3, \ldots$. They are of dimension $k = n - \log_2(n+1)$.

A code P of length $n = 2^{2m} - 1$, $m = 2, 3, \ldots$, is called a Preparata-like code (referred to as a *Preparata code* in the sequel) if it has code distance 5 and dimension $k = n - 2\log_2(n+1) + 1$.

Perfect and Preparata codes are maximal and uniformly packed and obey the antipodality property: vertices v and $v \oplus \mathbf{1}^n$ either both belong to the code or both do not. The following fact is known.

Proposition 4 (see [5]). *Any Preparata code is contained in some perfect code, which is unique.*

Denote by $C(P)$ the perfect code containing a Preparata code P. Recall that the *rank* of a set of vectors is the dimension of its linear span.

Proposition 5 (see [9]). *The rank of a Preparata code is equal to the rank of its ambient perfect code.*

Any weight-k vector of E^n can be represented as a collection $(i_1, \ldots i_k)$ of its nonzero coordinates (we will use this representation as well as the vector representation; by $\oplus$ we denote addition modulo 2 for the corresponding vectors). A subset T of the set of weight-k vectors in E^n is called a t-(n, k, λ)-*design* if any t-subset of the set $\{1, 2, \ldots, n\}$ is contained among nonzero coordinates of exactly λ vectors from T. Minimum-weight codewords in a reduced (i.e., containing the zero vertex) perfect code or Preparata code form, respectively, a 2-$(n, 3, 1)$-design or a 2-$(n, 5, (n-3)/3)$-design (see [1]). This means that, in each of these codes, with respect to any coordinate i, all vertices have the same i-degree. Therefore, Proposition 3 implies the following fact.

Proposition 6. *A minimal i-component in a perfect code or Preparata code by any coordinate i is at most half of the code.*

It should be noted that in the case of a perfect code this bound is tight. Sharp upper and lower bounds on the cardinality of a minimal i-component of a perfect code are given in [7, 8] (see also [10]).

Take any coordinate i in the set $\{1, 2, \ldots, n\}$, where $n = 2^{2m} - 1$, $m = 2, 3, \ldots$. Denote by $N^P(v)$ and $D^P(v)$, respectively, the set of i-close code vertices and the set of i-directions of a vertex v of a Preparata code P. Introduce the similar notations, $N^C(u)$ and $D^C(u)$, for a vertex u of a perfect code C.

For a perfect code, one can easily deduce the following statement.

Proposition 7. *The set $D^C(u)$, which consists of vectors of weight 3, defines a partition of the set $\{1, 2, \ldots, n\} \setminus \{i\}$ into pairs $\{j, k\}$ such that each triple (i, j, k) belongs to $D^C(u)$. We have*

$$|D^C(u)| = (n-1)/2.$$

Proposition 8 (see [1, 5]). *The set $D^P(v)$, which consists of vectors of weight 5, for any coordinate $j \in \{1, 2, \ldots, n\}$, $j \neq i$, defines a partition of the set $\{1, 2, \ldots, n\} \setminus \{i, j, k\}$ into subsets $\{\ell, m, r\}$ such that any quintuple (i, j, ℓ, m, r) belongs to $D^P(v)$, where (i, j, k) is a triple from $D^{C(P)}(v)$. We have*

$$|D^P(v)| = (n-1)(n-3)/12.$$

By [1], each vertex w of the code $C(P) \setminus P$ is at distance 3 from the maximum number $n/3$ of vertices of P; therefore, we have the following proposition.

Proposition 9 (see [1, 5]). *For any vertex w of the code $C(P) \setminus P$, the set $\{1, 2, \ldots, n\}$ is partitioned into subsets $\{q, s, t\}$ such that $w \oplus (q, s, t) \in P$.*

3. RELATIONS BETWEEN COMPONENTS OF PREPARATA CODES AND PERFECT CODES

Consider an arbitrary reduced Preparata code P and an ambient perfect code $C = C(P)$. Let a set M be a minimal i-component of P for an arbitrary coordinate i. We denote by P' the Preparata code obtained from P by switching of the i-component M with respect to the coordinate i. Denote by C' the code $C(P')$.

Let us define a one-to-one function f acting from P to P' according to the following rule:

$$f(v) = \begin{cases} v \oplus e_i & \text{if } v \in M, \\ v & \text{if } v \in P \setminus M. \end{cases}$$

Lemma 1. *Let P, P', C, and C' be the codes defined above. For any vector v in P, we have*

$$D^P(v) = D^{P'}(f(v)), \tag{1}$$

$$D^C(v) = D^{C'}(f(v)). \tag{2}$$

Proof. Let v be a vector from P. Equality (1) obviously follows from Proposition 1 taking into account the way in which P' is obtained from P. Let us prove the equality of $D^C(v)$ and $D^{C'}(f(v))$. Let (i, j, k) be a triple from $D^C(v)$. Assume that (i, j, k) does not belong to $D^{C'}(f(v))$; then, by Proposition 7, the set $D^{C'}(f(v))$ contains a triple (i, j, ℓ) with $\ell \neq k$. According to Proposition 8, the set $D^P(v)$ contains a quintuple (i, j, ℓ, m, r) for any coordinate ℓ, $\ell \neq k$, with some $m, r \in \{1, 2, \ldots, n\} \setminus \{i, j, k\}$. Equality (1) implies that (i, j, ℓ, m, r) belongs also to $D^{P'}(f(v))$. Hence, $d(f(v) \oplus (i, j, \ell, m, r), f(v) \oplus (i, j, \ell))$ equals 2, which is less than the code distance of the perfect code C', a contradiction. Thus, the triple (i, j, k) belongs to $D^{C'}(f(v))$; i.e., $D^C(v) \subseteq D^{C'}(f(v))$. Similarly, one can demonstrate that $D^{C'}(f(v)) \subseteq D^C(v)$. $\triangle$

Theorem 1. *Let a set M be a minimal i-component of a Preparata code P. Then the set $R = M \cup N^C(M)$ is an i-component of the perfect code C, where $N^C(M) = \bigcup\limits_{v \in M} N^C(v)$.*

Proof. Let us show that, for any vector v in R, the set $N^C(v)$ is contained in R. If $v \in M$, then $N^C(v)$ is contained in R by the definition of $N^C(M)$. Let $v \in N^C(M)$; then a vector $u \in M$ exists such that v belongs to $N^C(u)$. The vector u is contained in $N^C(v)$ and belongs to R. Proposition 9 implies that u is the only vector in the set $N^C(v)$ that belongs to P, and other vectors $N^C(v) \setminus \{u\}$ belong to $C \setminus P$. Let us show that they are also contained in R. Take an arbitrary vector v_1 in $N^C(v) \setminus \{u\}$. Again by Proposition 9, there exists exactly one vector $u_1 \in P$ such that v_1 belongs to $N^C(u_1)$. If we show that u_1 is contained in M, we will prove that v_1 belongs to $N^C(M)$ and hence to R. Assume that $u_1 \in P \setminus M$. Consider the code P'. The vertex u belongs to M; therefore, under the action of f it is taken to the vertex $u \oplus e_i$. By Lemma 1 we have $D^C(u) = D^{C'}(u \oplus e_i)$; hence, $v \oplus e_i$ belongs to C'. By the assumption, we have $f(u_1) = u_1$; hence, v_1 belongs to C'. Then $d(v \oplus e_i, v_1) = 2$, which is less than the code distance of the perfect code C'. Thus, u_1 belongs to M, and $N^C(v)$ is contained in R. $\triangle$

Remark. The constructed i-component R is the smallest (in cardinality) i-component of the perfect code C containing the given i-component M of the Preparata code P. Obviously, any other i-component of C containing M must also contain the set $N^C(M)$ and hence the set R.

Consider the characteristic graph $G^{\tilde{R}} = (\widetilde{R}, E)$ of an arbitrary i-component $\widetilde{R}$ of the perfect code C, where $E = \{(u, v) \mid u \in N^C(v)\}$. The graph $G^{\tilde{R}}$ is a regular graph of degree $(n-1)/2$.

Theorem 1 implies the following facts.

Corollary 1. *We have* $|R| = (n+1)|M|/2$.

Proof. In the graph G^R, let us find the number of edges joining the sets M and $N^C(M)$. On the one hand, this number equals $(n-1)|M|/2$; on the other hand, it equals $|N^C(M)|$. Using the relation $|R| = |M| + |N^C(M)|$, we get the desired equality. $\triangle$

Corollary 2. *We have* $2^{\frac{n+1}{2} - \log_2(n+1)} \le |M| \le 2^{n - 2\log_2(n+1)}$.

Proof. The lower bound is directly obtained from the known sharp lower bound on the cardinality of a minimal i-component of a perfect code (see [8, 10]):

$$2^{\frac{n-1}{2}} \le |R|.$$

The upper bound follows from Proposition 6. $\triangle$

According to Proposition 4, the code C' is uniquely defined by the code P', and we have $C' = (C \setminus R) \cup (R \oplus e_i)$. This implies the following fact.

Corollary 3. *Switching of an arbitrary i-component M in a Preparata code induces in the ambient perfect code a switching of the smallest i-component R containing M.*

Corollary 4. *The rank of an arbitrary i-component M of a Preparata code equals the rank of the smallest i-component R of the ambient perfect code such that $M \subset R$.*

The proof directly follows the proof of Proposition 5 given in [9]. Without loss of generality, we may assume (since the Preparata code is distance-invariant) that the i-component M contains the zero vertex $\mathbf{0}^n$ and hence, by Proposition 2, the vertex $\mathbf{1}^n$. Denote by $r(M)$ and $r(R)$ the ranks of the i-components M and R respectively. The set M is contained in R; therefore, we have $r(M) \le r(R)$. Let us show that $r(M) \ge r(R)$, i.e., any vector v in R is a linear combination of vectors from M. Let v belong to $R \setminus M$; then, by the definition of R, there is a vertex u in M such that $v = u \oplus (i, j, k)$, where $(i, j, k) \in D^C(u)$. By Proposition 8, the set $D^P(u)$ contains precisely $(n-3)/3$ vectors which contain ones in the positions i and j and are nonintersecting in the other positions; denote the corresponding vectors of $N^P(u)$ by $u_1, \ldots, u_{\frac{n-3}{3}}$. Then, since $(n-3)/3$ is even, we have the equality $(i, j, k) = u_1 \oplus \ldots \oplus u_{\frac{n-3}{3}} \oplus \mathbf{1}^n$, whose right-hand side is a linear combination of vectors from M. $\triangle$

Consider the characteristic graph as a metric space with the natural metric: the distance between two vertices is the length of the shortest path joining them.

Lemma 2. *Let M and R be the above-defined i-components of the Preparata code P and the perfect code C respectively. The set M is a perfect code with distance 3 in the characteristic graph G^R.*

Proof. Let v be a vector from R. A ball of radius 1 centered at the vertex v in the graph G^R is the set $\{v\} \cup N^C(v)$; its cardinality is $(n+1)/2$. By Corollary 1, the set M meets the sphere-packing bound for the graph G^R packed by balls of radius 1 centered at vertices from M. It remains to show that no two of these balls intersect. Indeed, if for some vertices v_1 and v_2 from M the corresponding balls intersect, then the distance $d(v_1, v_2)$ is less than 5, which is not true since M is a subset of a Preparata code. $\triangle$

Theorem 2. *Let P be a Preparata code, and let $\widetilde{R}$ be an arbitrary i-component of the perfect code $C(P)$. Then the set $P \cap \widetilde{R}$ is a perfect code with distance 3 in the characteristic graph $G^{\widetilde{R}}$.*

Proof. The Preparata code P is partitioned with respect to the coordinate i into several minimal i-components. Each of them is uniquely completed to an i-component of $C(P)$ in the way described

in Theorem 1. Thus, a partition of P into minimal i-components defines a partition of $C(P)$ into i-components, not necessarily minimal. In other words, the characteristic graph of any completed i-component can have several connected components. It follows from Lemma 2 that vertices of the Preparata code form perfect codes in these components. Therefore, in each connected component of $G^{C(P)}$, the intersection with the Preparata code P is a perfect code. The theorem follows from the fact that any i-component $\widetilde{R}$ of the code $C(P)$ is a union of minimal i-components, and $G^{\tilde{R}}$ is, respectively, a union of connected components of the graph $G^{C(P)}$. $\triangle$

Theorem 2 has something in common with a remark in [5] that a Preparata code P can be considered to be uniformly and closely packed in the perfect code $C(P)$ (in this case, as an i-component $\widetilde{R}$, it suffices to take the whole code $C(P)$).

It remains to note that a Preparata code P is in a sense a "frame" for constructing the ambient perfect code $C(P)$ (see Propositions 4 and 5). Now we can say more: each i-component of a Preparata code P is a "frame" for some i-component of the perfect code $C(P)$.

The author would like to express his deep gratitude to participants of the seminar *Coding Theory* of the S.L. Sobolev Institute of Mathematics, Siberian Branch of the Russian Acad. Sci., for their valuable remarks and suggestions.

REFERENCES

1. Semakov, N.V., Zinoviev, V.A., and Zaitsev, G.V., Uniformly Packed Codes, *Probl. Peredachi Inf.*, 1971, vol. 7, no. 1, pp. 38–50 [*Probl. Inf. Trans.* (Engl. Transl.), 1971, vol. 7, no. 1, pp. 30–39].
2. Avgustinovich, S.V. and Solov'eva, F.I., New Constructions and Properties of Perfect Codes, *Trudy konferentsii po diskretnomu analizu i issledovaniyu operatsii* (Proc. Conf. on Discrete Analysis and Operations Research), Novosibirsk, 2000, pp. 5–10.
3. Vasil'ev, Yu.L., On Nongroup Closely Packed Codes, *Probl. Kibern.*, 1962, vol. 8, pp. 337–339.
4. Etzion, T. and Vardy, A., Perfect Binary Codes: Constructions, Properties, and Enumeration, *IEEE Trans. Inf. Theory*, 1994, vol. 40, no. 3, pp. 754–763.
5. Semakov, N.V., Zinoviev, V.A., and Zaitsev, G.V., Interrelation of Preparata and Hamming Codes and Extension of Hamming Codes to New Double-Error-Correcting Codes, *Proc. 2nd Int. Symp. on Information Theory, Tsahkadsor, Armenia, USSR, 1971*, Petrov, P.N. and Csaki, F., Eds., Budapest: Akad. Kiado, 1973, pp. 257–263.
6. Avgustinovich, S.V. and Solov'eva, F.I., Construction of Perfect Binary Codes by the Sequential Translations of the i-Components, in *Proc. 5th Int. Workshop on Algebr. Comb. Coding Theory*, Sozopol, Bulgary, 1996, pp. 9–13.
7. Solov'eva, F.I., On Factorization of Code-Generating DNFs, *Metody diskretnogo analiza v issledovanii funktsional'nykh sistem* (Methods of Discrete Analysis in Studying Functional Systems), Novosibirsk: Inst. Mat. Sib. Otd. Akad. Nauk SSSR, 1988, vol. 47, pp. 66–88.
8. Solov'eva, F.I., Sharp Bounds for the Connectivity of Code-Generating DNFs, *Preprint of Inst. Mat. Sib. Otd. Akad. Nauk SSSR*, Novosibirsk, 1990, no. 10.
9. Borges, J., Phelps, K.T., Rifà, J., and Zinoviev, V.A., On Z_4-Linear Preparata-Like and Kerdock-Like Codes, *IEEE Trans. Inf. Theory*, 2003, vol. 49, no. 11, pp. 2834–2843.
10. Solov'eva, F.I., Structure of i-Components of Perfect Binary Codes, *Discr. Appl. Math.*, 2001, vol. 111, pp. 189–197.