Siberian Mathematical Journal, *Vol.* 48, *No.* 2, *pp.* 327–333, 2007

ON DISTANCE NONREGULARITY OF PREPARATA CODES

F. I. Solov′eva and N. N. Tokareva UDC 519.725

Abstract: It is shown that among all Preparata codes only the code of length 16 is distance regular. An analogous result takes place for Preparata codes after puncturing any coordinate (only the code of length 15 is distance regular).

Keywords: Preparata codes, perfect codes, distance regular codes, automorphism groups of codes

1. Introduction

Let E^n denote the n-dimensional metric space of all binary vectors of length n with respect to the Hamming metric. The *Hamming distance* $d(x, y)$ between vectors x and y is the number of coordinate positions in which they differ. The *weight* $w(x)$ of a vector x is the distance between x and the zero vector $\mathbf{0}$. A subset of E^n having the cardinality M and the minimal distance d between its distinct elements is called a *binary* (n, M, d)*-code*. The elements of a code are called *codewords*.

For a (n, M, d)-code with odd code distance the operation of *extending* is defined by adding an overall parity check. It is the following map from E^n into E^{n+1} :

$$(x_1, \ldots, x_n) \longrightarrow \Big(x_1, \ldots, x_n, \sum_{i=1}^{n} x_i\Big),$$

where the sum is taken modulo 2. The image of the initial code under this mapping is called the *extended code*. It has parameters $(n + 1, M, d + 1)$. The inverse transformation is called *puncturing*. It consists of deleting one or more coordinate positions from each codeword. The code obtained in such a way from the initial code is called a *punctured* code. In general it depends essentially on the choice of coordinate positions to deletion. For details see the methods of constructing new codes from the given ones in the book [1].

A code is called *distance invariant* if the number of codewords at distance i from a given codeword x does not depend on the choice of x and depends only on i. A generalization of this property is the property of *strong distance invariance*. For the code satisfying this property the number of pairs of codewords x, y such that $d(x, y) = k$ and $d(x, z) = i$, $d(y, z) = j$ for any codeword z depends only on the integers i, j, k and does not depend on the choice of z. Even stronger property of a code is the property of *distance regularity*: for all codewords x, y and all numbers i, j, the number of codewords z such that $d(x, z) = i$, $d(y, z) = j$, does not depend on the choice of x, y and depends only on $d(x, y)$ and numbers i and j. It is not difficult to see that every distance regular code is strongly distance invariant (and, therefore, distance invariant).

Distance regularity, together with distance invariance and strong distance invariance, shows the specific structural code properties that are tightly connected with automorphism groups and groups of symmetries of codes, with an equivalence or isometries of codes. Distance regular codes can be helpful in investigating reconstruction of a code from some part (for instance, from given codewords in a sphere or face), to study and construct codes with large code distances. Study of distance regular codes is a natural

The first author was partially supported by the Royal Swedish Academy of Sciences, and the second author was supported by the Integration Project of the Siberian Branch of the Russian Academy of Sciences "A Tree-Like Catalog of Internet Mathematical Resources" (Grant No. 35).

Novosibirsk. Translated from *Sibirskiĭ Matematicheskiĭ Zhurnal*, Vol. 48, No. 2, pp. 408–416, March–April, 2007. Original article submitted December 20, 2005.

topic in coding theory. It was initiated by study of a significant class of distance regular graphs; see the books [2] and [3]. It should be mentioned that distance regular codes are also tightly connected with metric association schemes; see [2] and also [1, Chapter 21].

There are only few papers on the distance regularity of codes. It is known that the following binary codes are distance regular: an even weight code of any length, the infinite class of all Hadamard codes (see [4]); Kerdock codes (see [2]); the extended Golay code and once or twice shortened Golay codes (see [4]); the Golay code and punctured codes obtained from this code by deleting one or two coordinate positions (see [5]); and also three times shortened Golay code (see the paper of Topalova [5]). The distance regularity of q-ary codes, $q > 2$, is not enough investigated. It is only known that the ternary Golay code and shortened Golay code are distance regular (see [4]).

In [6] it is established that all perfect binary codes with code distance 3 are not distance regular with the exception of the Hamming codes of lengths 3 and 7. In a similar manner it is proved that all extended perfect binary codes are not distance regular with the exception of the extended Hamming codes of lengths 4 and 8 (see [7]). It should be noted that according to the papers of Vasil′eva [8, 9] all perfect binary codes and Preparata codes are strongly distance invariant. Several punctured and shortened binary extended Golay codes are not distance regular. Moreover there exist two nonequivalent shortened Golay codes of length 18 such that one of them is distance regular whereas the other lacks this property (see [5]).

In this paper we show that all Preparata codes with the exception of the code of length 16 are not distance regular. Any punctured Preparata code of length more than 15 is not distance regular. Every punctured Preparata code of length 15 is distance regular.

2. Distance Regularity and Preparata Codes

Without loss of generality we will consider the only *reduced codes*, that is, the codes containing the zero vector. To prove the distance regularity of the Preparata code of length 16 we need some connection of the automorphism group and the group of symmetries of an arbitrary code with the distance regularity property of this code.

The *automorphism group* $\mathrm{Aut}(C)$ of a binary code C of length n consists of all isometries of E^n (compositions of permutations of n coordinate positions and translations by vectors of the space E^n) that transform the code into itself; i.e.,

$$\mathrm{Aut}(C) = \{(\pi, v) \,|\, \pi \in S_n, v \in E^n, v + \pi(C) = C\},$$

where S_n is the symmetric group of permutations of length n.

The *group of symmetries* $\mathrm{Sym}(C)$ of a code C is isomorphic to the subgroup of $\mathrm{Aut}(C)$ corresponding to all permutations of coordinates; i.e.,

$$\mathrm{Sym}(C) = \{\pi \mid \pi \in S_n, \pi(C) = C\}.$$

A code is said to be *transitive* if its automorphism group acts on all its codewords transitively. Two codes of length n are *equivalent* if there exists an isometry of E^n mapping one code into the other.

Lemma 1. *If the group of symmetries* $\mathrm{Sym}(C)$ *of a transitive code* C *acts transitively on every set of all codewords of a fixed weight then* C *is distance regular.*

Proof. Fix the numbers i, j, k in $\{0, 1, 2, \ldots, n\}$. Consider a pair of codewords x and y at distance $d(x, y) = k$. Show that the number of codewords z such that $d(x, z) = i$, $d(y, z) = j$ does not depend on the choice of x and y. Without loss of generality we can put $x = \mathbf{0}$ on using the transitivity of the code. Since the group $\mathrm{Sym}(C)$ acts transitively on the set of all codewords of weight k and every permutation of n coordinate positions is an isometry, the number of weight i codewords z at distance j from some codeword y of weight k does not depend on the choice of y. □

A maximal binary code P of length $n = 2^m$, $m \geq 4$ is even, with code distance 6 is called a *Preparata code*. The size of the code is $2^n/n^2$. The first construction of such codes of any admissible length n was proposed by Preparata in 1968 (see [10]). Using special automorphisms of the Galois field $GF(n/2)$, the series of pairwise nonequivalent Preparata codes of any admissible length n was constructed by Dumer [11] and later by Baker, van Lint, and Wilson [12]. Preparata codes are exceptional in some prominent properties. It is shown by Semakov, Zinoviev, and Zaitsev [13] that after puncturing by deleting any coordinate position each such code is uniformly packed (in the narrow sense) in the space E^{n-1} and can uniquely be completed to some perfect code with distance 3 (see [14]), and in some sense is close packed in the perfect code (see [14] and also [15]). Recall that a *perfect binary code* with distance 3 is a code such that the balls of radius 1 centered at all codewords make the partition of the whole space.

Sometimes in coding theory a maximal binary code of length $n-1$ with code distance 5 is called the Preparata code. It is easy to see that every such code P' can be obtained by puncturing some Preparata code P of length n with code distance 6 by deleting one coordinate position. It should be noted that an extension of a code by adding an overall parity check is not in general the inverse operation of a puncturing. However in the case of perfect codes and Preparata codes these operations are always in one-to-one correspondence as follows easily from [13]. Therefore, the above definitions of Preparata codes with code distance 6 are equivalent.

The Preparata code with parameters $(16, 256, 6)$ called the *Nordstrom–Robinson code* is unique up to an equivalence (see [1, Chapter 2]). It is well known (see [16]) that the Nordstrom–Robinson code is $\mathbb{Z}_4$-linear and, therefore, transitive. It is proved in the paper [17] that every set of fixed weight codewords of the Nordstrom–Robinson code forms the unique orbit under an action of its group of symmetries. Using Lemma 1, we can then prove

Proposition 1. *The Preparata code of length* 16 *is distance regular.*

REMARK. The distance regularity property of an extended perfect binary code of length 8 can be shown by Lemma 1 so far as the code satisfies the conditions of this lemma (also see [6]).

To prove that any Preparata code of length $n > 16$ is not distance regular we analyze the weight spectrum of the code (see the definition below). More precisely we will show that it is sufficient to investigate the set of codewords of weight at most 8. We now give the needed notations and two lemmas.

Let A_i denote the number of all weight i codewords of a Preparata code of length n. The set of numbers $\{A_0, A_1, \ldots, A_n\}$ is called the *weight spectrum* of the code. Using the fact that each Preparata code contains the zero vector and has code distance 6, we immediately get the following equalities:

$$A_0 = 1, \quad A_2 = 0, \quad A_4 = 0. \tag{1}$$

By [13, Theorem 5] for odd numbers k such that $3 \leq k \leq n-3$ the weight spectrum of every Preparata code satisfies the equation

$$b_k A_{k+3} + c_k A_{k+1} + c_{n-k} A_{k-1} + b_{n-k} A_{k-3} = 2(n-1)\binom{n}{k},$$

where

$$b_\ell = (\ell+1)(\ell+2)(\ell+3),$$
$$c_\ell = (\ell+1)(3\ell(n-\ell-1) + 2(n-1)).$$

Here $\binom{n}{k}$ is a binomial coefficient. Using this equation for k equal to 3 or 5 and also (1), we infer

$$A_6 = \frac{n(n-1)(n-2)(n-4)}{360}, \tag{2}$$

$$A_8 = \frac{n(n-1)(n-2)(n-4)(n^2-21n+95)}{8 \cdot 7 \cdot 360}. \tag{3}$$

In [13, a Corollary to Theorem 7] it is established that the set of weight 6 codewords of each Preparata code of length n defines $3-(n,6,(n-4)/3)$-design, i.e. for every three different coordinate positions a,b,c there exist exactly $(n-4)/3$ weight 6 codewords of the Preparata code with 1 in these coordinate positions. For the sake of brevity, denote the triple of these coordinate positions by (a,b,c) and say that the triple *enters* into $(n-4)/3$ codewords of weight 6.

Lemma 2. *Let some weight* 6 *codeword of a Preparata code of length* n *have nonzero coordinate positions* p,q,a,b,c,e. *Then the number of weight* 6 *codewords with* 1 *in the coordinate positions* p,q *and* 0 *in the coordinate positions* a,b,c,e *equals*

$$\frac{n^2-22n+108}{12}.$$

Proof. We prove first that the number of weight 6 codewords with nonzero coordinate positions p,q equals $(n-2)(n-4)/12$. In fact the number of different triples chosen from n integers and containing p and q is equal to $n-2$. Every such triple enters into exactly $(n-4)/3$ weight 6 codewords. The number of all such occurrences of the triples into weight 6 codewords equals $(n-2)(n-4)/3$. Considering that each codeword of weight 6 with nonzero coordinate positions p,q contains exactly 4 different triples including p and q, we get the required number of codewords.

Let us find the number of weight 6 codewords having 1 in the coordinate positions p,q and 0 in the coordinate positions a,b,c,e. Each of the triples (p,q,a), (p,q,b), (p,q,c), and (p,q,e) enters into exactly $(n-4)/3$ weight 6 codewords with 1 in the coordinate positions p,q. Moreover, there exists the unique weight 6 codeword containing more than one of these four triples (in fact it contains all these four triples). Therefore the required number of weight 6 codewords having 1 in the coordinate positions p,q and 0 in the coordinate positions a,b,c,e is equal to

$$\frac{(n-2)(n-4)}{12}-\left(4\cdot\frac{(n-7)}{3}+1\right)=\frac{n^2-22n+108}{12}.$$

□

According to [6] denote by $S_{ij}^k(C)$ (abbreviated in what follows to S_{ij}^k) the number of the ordered pairs (x,y) of codewords of length n code C such that $w(x)=i$, $w(y)=j$, and $d(x,y)=k$.

Lemma 3. *For every Preparata code of length* n *it is true that*

$$S_{68}^6=\frac{n(n-1)(n-2)(n-4)(n^2-22n+108)}{8\cdot 36}.$$

Proof. Fix a codeword x of weight 6. We at first find the number of codewords y of weight 6 such that $d(x,y)=8$. Such a codeword y has exactly two nonzero coordinate positions common with the codeword x. A pair of coordinate positions p,q among the six nonzero coordinate positions of the codeword x can be chosen in $\binom{6}{2}$ different ways. Then from Lemma 2 it follows that the number of codewords y we are looking for (denote it by γ) equals

$$\binom{6}{2}\cdot\frac{n^2-22n+108}{12}=\frac{5\cdot(n^2-22n+108)}{4}.$$

Note that the number γ does not depend on the choice of the code and the codeword x of weight 6. It follows easily that γ equals the number of weight 8 codewords z such that $d(x,z)=6$. Multiplying γ by A_6 and using (2), we obtain S_{68}^6. □

Theorem 1. *Any Preparata code of length $n = 2^m$, for even m, is not distance regular for $n \geq 64$.*

Proof. Suppose that some Preparata code is distance regular. From the definition of distance regularity of a code it follows that all numbers S_{ij}^k/A_i and S_{ij}^k/A_j are integers. Show that the number δ, equal to S_{68}^6/A_8, is an integer only for $n = 16$. Using Lemma 3 and substituting (3) for A_8 we obtain

$$\delta = 70 \cdot \frac{n^2 - 22n + 108}{n^2 - 21n + 95}. \tag{4}$$

According to Lemma 1 the Preparata code is distance regular for $n = 16$. For $n = 64$ we get the irreducible fraction $\delta = 65240/(13 \cdot 73)$. Assume further that $n \geq 256$. Let us remark that for all $n \geq 16$ the fraction in (4) is less than one, and so for such n we have

$$0 < \delta < 70. \tag{5}$$

Transforming (4), we obtain a homogeneous equation of the argument n with the constant term equal to $(70 \cdot 108 - 95\delta)$. It is obvious that the term should be divisible by n. This yields that for some integer r we have

$$70 \cdot 108 - 95\delta = nr. \tag{6}$$

Dividing both sides of (6) by 8 and applying $n = 2^m$, $n \geq 256$, we derive

$$35 \cdot 27 - \frac{95\delta}{8} = 32\ell, \tag{7}$$

where ℓ is an integer. As far as the first item in the equality is odd, the second should be odd too and so δ equals $8(2t + 1)$ for some integer t. Inserting this expression for δ into (7), we see that

$$(85 - 19t) \text{ is divisible by } 16. \tag{8}$$

By (5), the possible values of t are $0, 1, 2$, or 3. But for each of these values the condition (8) is not satisfied. Thus, for $n \geq 64$ any Preparata code is not distance regular. □

3. Punctured Preparata Codes

A group of symmetries of a code is *t-transitive* if for any two t-element subsets of coordinates there is an automorphism (a permutation) transforming one subset into another one.

Lemma 4. *Let the group* $\mathrm{Sym}(C)$ *of a transitive reduced code C of length n be* 1*-transitive. Then the punctured code C' obtained from C by deleting any coordinate is transitive.*

Proof. Let the code C' be obtained from the code C by deleting a coordinate a. It is convenient to use for all coordinate positions of the code C' the previous enumeration with the exception of a. Let us give an equivalent definition of transitivity for a reduced code. A code C is transitive if and only if for every codeword x there exists a permutation $\pi \in S_n$ such that $x + \pi(C) = C$. Suppose that $\pi(b) = a$ for some coordinate b. Since the group $\mathrm{Sym}(C)$ is 1-transitive, there exists a permutation $\tau \in \mathrm{Sym}(C)$ such that $\tau(a) = b$. For the permutation $\sigma = \pi \circ \tau$ the following holds:

$$x + \sigma(C) = x + \pi(\tau(C)) = x + \pi(C) = C; \tag{9}$$

and, furthermore, $\sigma(a) = a$. Let the codeword x turn to the codeword $x' \in C'$ after the puncturing the coordinate a. We have

$$x' = (x_1, \ldots, x_{a-1}, x_{a+1}, \ldots, x_n).$$

Define the permutation $\pi' \in S_{n-1}$ as follows:

$$\pi' = (\sigma(1), \ldots, \sigma(a-1), \sigma(a+1), \ldots, \sigma(n)).$$

Then from the equalities (9) and $\sigma(a) = a$ it follows that $x' + \pi'(C') = C'$ for the code C'. Since we choose the codeword x (and hence the codeword x') arbitrarily, the code C' is transitive. □

As it was noticed above, the Nordstrom–Robinson code of length 16 is transitive. In [18] it is proved that the group of symmetries of this code is three times transitive. Therefore by Lemma 4 the code of length 15 obtained from the Nordstrom–Robinson code by a puncturing any coordinate is transitive. For the reduced $(15, 256, 5)$-code we checked by an exhaustive search that for a codeword x of weight i the number of codewords y of weight j such that $d(x, y) = k$ does not depend on the choice of x for any admissible values i, j, k. Since the code is transitive and unique up to equivalence (see [1, Chapter 2]), this is sufficient for the code to be distance regular. Thus, we have

Proposition 2. *Every $(15, 256, 5)$-code is distance regular.*

REMARK. It is interesting to mention that if we add to this code all vectors of the space E^{15} at distance 3 from the code, we obtain the linear perfect $(15, 256 \cdot 8, 3)$-code (see [14]) which, in turn, is not distance regular (see [6]).

By the same arguments as for Preparata codes of length n we can prove the following fact (in this case we address the codewords of weight at most 6).

Theorem 2. *An arbitrary $(n-1, 2^n/n^2, 5)$-code obtained from some $(n, 2^n/n^2, 6)$-Preparata code by puncturing any coordinate is not distance regular for $n - 1 \geq 63$.*

Let us sketch a proof. In [13] it is shown that the set of all weight 5 codewords of a punctured Preparata code of length $n-1$ forms a 2–$(n-1, 5, (n-4)/3)$-design. Hence we can compute the quantities

$$A_5 = \frac{(n-1)(n-2)(n-4)}{60}, \tag{10}$$

$$A_6 = \frac{(n-1)(n-2)(n-4)(n-6)}{360}. \tag{11}$$

Lemma 5. *For every punctured Preparata code of length $n-1$ we have*

$$S_{56}^5 = \frac{(n-1)(n-2)(n-4)(n-7)}{18}.$$

PROOF. Take a codeword x of weight 5 with nonzero coordinate positions p, q, a, b, c. It is not difficult to show that the number of weight 5 codewords with 1 in the coordinate positions p, q and 0 in the coordinate positions a, b, c is equal to $(n-7)/3$. Multiplying it by $\binom{5}{2}$ we get the number of weight 5 codewords y such that $d(x, y) = 6$. The so-obtained number does not depend on the choice of the code and the codeword x and hence it equals the number of weight 6 codewords z such that $d(x, z) = 5$. Multiplying this number by A_5 and applying (10), we derive S_{56}^5. □

Suppose that a punctured Preparata code of length $n-1$ is distance regular. In this case all numbers S_{ij}^k/A_i and S_{ij}^k/A_j should be integers. It can easily be checked by Lemma 5 and (11) that the number

$$\frac{S_{56}^5}{A_6} = 20 \cdot \frac{n-7}{n-6}$$

is an integer only for $n - 1 = 15$. This implies that punctured Preparata codes of length $n - 1 > 15$ are not distance regular.

REMARK. It should be noted that Theorems 1 and 2 address the codewords of weights at most 8 and 6 respectively. Moreover, these weights of codewords are the least for which the property of distance regularity becomes violated. To put it informally for the codewords of less weight, all Preparata codes and codes obtained from them by deleting any coordinate are locally distance regular in a sense.

The results of this paper were partially announced in [19].

References

1. *MacWilliams F. J. and Sloane N. J. A.,* The Theory of Error—Correcting Codes, North-Holland, Amsterdam (1977).
2. *Delsarte P.,* An Algebraic Approach to the Association Schemes of Coding Theory, Philips Research Reports Supplements 10, Historical Jrl., Ann Arbor (1973).
3. *Brouwer A. E., Cohen A. M., and Neumaier A.*, Distance-Regular Graphs, Springer-Verlag, Berlin (1989).
4. *Levenshtein V. I.*, "Universal bounds for codes and designs," in: Handbook of Coding Theory, V. S. Pless and W. C. Huffman (eds.), Elsevier, Amsterdam, **1**, 1998, pp. 499–648.
5. *Topalova S.*, "Distance regularity of some linear codes," in: Abstracts of the Annual Workshop on Algebraic and Combinatorial Coding Theory, St. Zagora, Bulgaria, **18**, 2000.
6. *Avgustinovich S. V. and Solov′eva F. I.*, "On distance regularity of perfect binary codes," Problems Inform. Transmission, **34**, No. 3, 247–249 (1998).
7. *Avgustinovich S. V. and Solov′eva F. I.*, "New constructions and properties of perfect codes," in: Proc. Intern. Workshop "Discrete Analysis and Operation Research" [in Russian], Novosibirsk, 2000, pp. 5–10.
8. *Vasil′eva A. Yu.*, "Strong distance invariance of perfect binary codes," Diskret. Anal. Issled. Oper. Ser. 1, **9**, No. 4, 33–40 (2002).
9. *Vasil′eva A. Yu.*, "Local and interweight spectra of completely regular codes and perfect colourings," in: Proc. Tenth Int. Workshop "Algebraic and Combinatorial Coding Theory," Zvenigorod, Russia, 2006, pp. 273–276.
10. *Preparata F. P.*, "A class of optimum nonlinear double-error-correcting codes," Inform. and Control, **13**, No. 5, 378–400 (1968).
11. *Dumer I. I.*, "Some new uniformly packed codes," in: Trudy MFTI Ser. "Radiotekhnika i Elektronika" [in Russian], MFTI, Moscow, 1976, pp. 72–78.
12. *Baker R. D., van Lint J. H., and Wilson R. M.*, "On the Preparata and Goethals codes," IEEE Trans. Inform. Theory, **29**, No. 3, 342–345 (1983).
13. *Semakov N. V., Zinoviev V. A., and Zaitsev G. V.*, "Uniformly packed codes," Problems Inform. Transmission, **7**, No. 1, 30–39 (1971).
14. *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," in: Proc. 2nd Int. Sympos. Information Theory, Tsakhadsor, Armenia (1971). Akademia Kiado, Budapest, 1973, pp. 257–263.
15. *Tokareva N. N.*, "On components of Preparata codes," Problems Inform. Transmission, **40**, No. 2, 159–164 (2004).
16. *Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., and Solé P.*, "The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes," IEEE Trans. Inform. Theory, **40**, No. 2, 301–319 (1994).
17. *Conway J. H. and Sloane N. J. A.*, "Orbit and coset analysis of the Golay and related codes," IEEE Trans. Inform. Theory, **36**, No. 5, 1038–1050 (1990).
18. *Berlekamp E. R.*, "Coding theory and the Mathieu groups," Inform. and Control, **18**, No. 1, 40–64 (1971).
19. *Solov′eva F. I. and Tokareva N. N.*, "On the property of distance regularity of Kerdock and Preparata codes," in: Proc. Tenth Int. Workshop "Algebraic and Combinatorial Coding Theory," Zvenigorod, Russia, 2006, pp. 248–251.

F. I. Solov′eva
Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail address: sol@math.nsc.ru

N. N. Tokareva
Novosibirsk State University, Novosibirsk, Russia
E-mail address: toknn@ngs.ru