Discrete Mathematics 81 (1990) 103–109
North-Holland

COMMUNICATION

PERFECT CODES WITH DISTINCT PROTECTIVE RADII

J.M. van den AKKER, J.H. KOOLEN and R.J.M. VAESSENS

Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Communicated by J.H. van Lint
Received 5 December 1989

We consider codes C for which the decoding regions for codewords $\boldsymbol{c}$ are balls $B_\rho(\boldsymbol{c})$, where $\rho = r_1$ or $\rho = r_2$. These are called (r_1, r_2)-error-correcting codes. If these balls are not only disjoint but also partition the space of all words, then C is called perfect. We are especially interested in codes with the property that centers of balls with the same radius r_i are at least $2r_i + 2$ apart $(i = 1, 2)$. These are called bipartite codes. Our main theorem states that a bipartite perfect $(r, 1)$-error-correcting code with $r \geqslant 2$ must have $r = 2$ and in fact is obtained from a code with the parameters of a Preparata code.

1. Introduction

We shall use standard terminology. A code C of length n over an alphabet Q with q symbols is a subset of Q^n. We denote the cardinality $|C|$ of the code by M; d is the minimum (Hamming-)distance of the code. A *ball* $B_r(\boldsymbol{c})$ with center $\boldsymbol{c}$ and radius r is defined by

$$B_r(\boldsymbol{c}) := \{\boldsymbol{x} \in Q^n \mid d(\boldsymbol{x}, \boldsymbol{c}) \leqslant r\}. \tag{1.1}$$

Suppose that C is the union of two disjoint subcodes C_1 and C_2 such that the following holds. There are integers r_1 and r_2 such that the balls $B_r(\boldsymbol{c})$, where $r = r_i$ if $\boldsymbol{c} \in C_i$ $(i = 1, 2)$ are disjoint. We then call C, with the specified subcodes C_1 and C_2, a (r_1, r_2)-error-correcting code. Let $M_i := |C_i|$ and let d_i be the minimum distance of C_i. Then $d_i \geqslant 2r_i + 1$ $(i = 1, 2)$. If we also define

$$d_{1,2} := \min\{d(\boldsymbol{c}_1, \boldsymbol{c}_2) \mid \boldsymbol{c}_1 \in C_1, \boldsymbol{c}_2 \in C_2\},$$

then it is also clear that

$$d_{1,2} \geqslant r_1 + r_2 + 1. \tag{1.2}$$

Define $r(\boldsymbol{c}) = r_i$ if $\boldsymbol{c} \in C_i$. If $\boldsymbol{c}$ and $\boldsymbol{c}'$ are codewords with

$$d(\boldsymbol{c}, \boldsymbol{c}') = r(\boldsymbol{c}) + r(\boldsymbol{c}') + 1,$$

then $\boldsymbol{c}$ and $\boldsymbol{c}'$ will be called *adjacent*. In this way a graph is defined on the vertex set consisting of codewords of C. The code C is called *bipartite* if the two sets C_1 and C_2 are independent sets in this graph.

If

$$Q^n = \bigcup_{c \in C_1} B_{r_1}(c) \cup \bigcup_{c \in C_2} B_{r_2}(c), \tag{1.3}$$

then C is called a *perfect* (r_1, r_2)-error-correcting code.

Let $V(n, r)$ denote the volume of a ball of radius r in Q^n, i.e.

$$V(n, r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i. \tag{1.4}$$

Then obviously

$$V(n, r) = V(n, r-1) + \binom{n}{r} (q-1)^r, \tag{1.5}$$

and from well-known relations for binomial coefficients we find

$$qV(n, r) = \binom{n}{r} (q-1)^{r+1} + V(n+1, r). \tag{1.6}$$

If C is a perfect (r_1, r_2)-error-correcting code in Q^n, then by (1.3) we have

$$M_1 \cdot V(n, r_1) + M_2 \cdot V(n, r_2) = q^n. \tag{1.7}$$

Perfect codes with distinct protective radii were studied by M. Gundlach [4] (see also [2, 3]). He found a number of examples that we mention below (all of which were also recently found independently by the present authors, before Prof. J.H. van Lint called Gundlach's work to their attention; no new examples were found). The aim of the present paper is to prove a non-existence result that does not occur in [4]. This theorem states that Example 4 (below) is unique (in a certain sense).

Example 1. Let C_1 be any r-error-correcting code and let C consist of the words of C_1 and all words in Q^n with distance $>r$ to C_1. Then C is a trivial example of a perfect code with distinct protective radii, namely an $(r, 0)$-error-correcting code.

Example 2. Let C be the binary repetition code of length n, and $C_1 = \{\mathbf{0}\}$. If $r_1 + r_2 + 1 = n$ then this is a perfect (r_1, r_2)-error-correcting code.

Example 3. Let C be a perfect e-error-correcting code of length n. Let C' be the code of length $n-1$ obtained from C by puncturing (on the last position). We define C_1', respectively C_2', to be the subcodes of C' obtained from the words of C ending in a 0, respectively not ending in a 0. Then C' is a perfect $(e, e-1)$-error-correcting code (since we have $|C_1'| = q^{-1}|C|$). Examples can be made using the known perfect codes.

Example 4. Let $\mathscr{P}$ be a code with the parameters of a Preparata code of length $n = 2^{2t} - 1$. Let $\mathscr{H}$ be the union of $\mathscr{P}$ and all the words in $\mathbb{F}_2^n$ that have distance 3

to $\mathscr{P}$. In [7] it is proved that $\mathscr{H}$ is a perfect 1-error-correcting code. Now take the extended codes $C := \mathscr{H}$ and $C_1 := \bar{\mathscr{P}}$. Then C is a perfect $(2, 1)$-error-correcting code. Note that if $\mathscr{P}$ is the Preparata code, then $\mathscr{H}$ is the Hamming code (cf. [1]).

We can now state our main theorem.

Theorem 1. *If C is a bipartite perfect $(r, 1)$-error-correcting code with $r \geq 2$, then $r = 2$ and C belongs to the family of codes mentioned in Example 4.*

2. Perfect codes

We shall prove several elementary results on (bipartite) perfect codes. In many cases the roles of C_1 and C_2 can be interchanged. From now on we usually assume that $r_1 \geq r_2$. Of course, $r_1 = r_2$ does not yield anything new, and in view of Example 1 the case $r_2 = 0$ is not of much interest. Therefore, our main interest will be in codes with $r_1 > r_2 > 0$. Nevertheless, most of the results hold without this restriction.

Lemma 1. *Let C be a perfect (r_1, r_2)-error-correcting code. If $d_1 \geq 2r_1 + 2$, then each word in C_1 is adjacent to some word in C_2; consequently*

$$d_{1,2} = r_1 + r_2 + 1. \tag{2.1}$$

Proof. Let $\boldsymbol{c} \in C_1$. Let $\boldsymbol{x} \in Q^n$ be a word with $d(\boldsymbol{x}, \boldsymbol{c}) = r_1 + 1$. There is a codeword $\boldsymbol{c}'$ such that $d(\boldsymbol{x}, \boldsymbol{c}') \leq r(\boldsymbol{c}')$. This implies that $\boldsymbol{c}$ and $\boldsymbol{c}'$ are adjacent, and hence $\boldsymbol{c}' \in C_2$. By (1.2) we are done. □

Remark. It is not difficult to show that (2.1) holds for any perfect (r_1, r_2)-error-correcting code (but we do not need that result in the following).

The next lemma shows that nontrivial bipartite perfect codes are binary.

Lemma 2. *Let $q \geq 3$ and let C be a perfect q-ary (r_1, r_2)-error-correcting code. Then $d_1 = 2r_1 + 1$ or $d_2 = 2r_2 + 1$.*

Proof. Assume that $d_1 > 2r_1 + 1$. Consider a word $\boldsymbol{c} \in C_1$; without loss of generality we assume that this word is $\mathbf{0}$. Let $\boldsymbol{x} = (11 \cdots 100 \cdots 0)$ be a word of weight $r_1 + 1$. By Lemma 1 there is a codeword $\boldsymbol{c}' \in C_2$ such that $d(\boldsymbol{x}, \boldsymbol{c}') = r_2$, and again we may assume without loss of generality that $\boldsymbol{c}' = (11 \cdots 1** \cdots * 00 \cdots 0)$, where the first $r_1 + 1$ coordinates are 1, the next r_2 are nonzero, and the remaining coordinates are 0. Now define $\boldsymbol{y} := (a11 \cdots 100 \cdots 0)$, a words of weight $r_1 + 1$ with $a \notin \{0, 1\}$. By the same argument as above, there is a codeword

c'' of weight $r_1 + r_2 + 1$ with $d(y, c'') = r_2$. The words c' and c'' are both in C_2, distinct, and their distance is clearly at most $2r_2 + 1$. Therefore their distance equals $2r_2 + 1$ and we are done. □

The following lemma is of interest, but we do not need it for our main result.

Lemma 3. *Let C be a perfect (r_1, r_2)-error-correcting code with $d_1 > 2r_1 + 1$. Then the covering radius $\rho(C_2)$ of C_2 satisfies*

$$\rho(C_2) = d_{1,2} = r_1 + r_2 + 1. \tag{2.2}$$

Proof. To prove the lemma, we consider a perfect (r_1, r_2)-error-correcting code C with $\rho(C_2) = \rho > r_1 + r_2 + 1$. We consider words x, c with $c \in C_2$ and $d(x, c) = d(x, C_2) = \rho$. Without loss of generality $c = 0$ and $x = (x_1 \cdots x_\rho 00 \cdots 0)$. We define

$$y_1 := (x_1 \cdots x_{r_2+1} 00 \cdots 0).$$

Clearly $d(y_1, C_2) = r_2 + 1$. There must be a codeword $u \in C_1$ such that $d(y_1, u) \leq r_1$, hence $u = (x_1 \cdots x_{r_2+1} ** \cdots *)$, a word of weight $r_1 + r_2 + 1$. This implies that there is a j with $r_2 + 1 < j \leq \rho$ such that $u_j = 0$, and we assume that the numbering of coordinates is such that $j = r_2 + 2$. We define

$$y_2 := (x_1 \cdots x_{r_2+2} 00 \cdots 0).$$

Now we have $d(y_2, u) = r_1 + 1$ and $d(y_2, C_2) = r_2 + 2$. So, there is a codeword $u' \neq u$ in C_1 such that $d(y_2, u') \leq r_1$. Hence $d_1 \leq d(u, u') \leq 2r_1 + 1$. □

Lemma 4. *Let C be a perfect (r_1, r_2)-error-correcting code. Then we have:*

(1) *If $d_1 \geq 2r_1 + 2$, then*

$$(q-1)^{r_1+1}\binom{n-1}{r_1} M_1 \leq (q-1)^{r_2}\binom{n-1}{r_2} M_2; \tag{2.3}$$

(2) *If $d_2 \geq 2r_2 + 2$, then*

$$(q-1)^{r_1}\binom{n-1}{r_1} M_1 \geq (q-1)^{r_2+1}\binom{n-1}{r_2} M_2. \tag{2.4}$$

Proof. It is sufficient to prove the first assertion. So, assume that $d_1 \geq 2r_1 + 2$. From (2.1) it follows that the punctured code C' (delete the last symbol) is an $(r_1, r_2 - 1)$-error-correcting code. So, not only does (1.7) hold, but we also have

$$M_1 \cdot V(n-1, r_1) + M_2 \cdot V(n-1, r_2 - 1) \leq q^{n-1}. \tag{2.5}$$

If we multiply both sides of (2.5) by q, subtract from (1.7), and apply (1.5) and (1.6), the result follows. □

Remark. Since (2.3) and (2.4) cannot hold simultaneously unless $q = 2$, we have a second proof of Lemma 2.

Lemma 5. *If C ia a (binary) bipartite perfect (r_1, r_2)-error-correcting code, then*

$$\binom{n-1}{r_1} M_1 = \binom{n-1}{r_2} M_2, \tag{2.6}$$

$$d_i = 2r_i + 2 \quad (i = 1, 2) \quad \text{if } d_{1,2} < n. \tag{2.7}$$

Proof. The first assertion is a direct consequence of Lemma 4. To prove the second assertion, assume for example that $d_1 \geqslant 2r_1 + 3$, $d_2 \geqslant 2r_2 + 2$. Now C is also an $(r_1 + 1, r_2 - 1)$-error-correcting code. So we have

$$M_1 \cdot V(n, r_1 + 1) + M_2 \cdot V(n, r_2 - 1) \leqslant 2^n. \tag{2.8}$$

From (2.8), (1.5) and (1.7) we find

$$M_1 \binom{n}{r_1 + 1} \leqslant M_2 \binom{n}{r_2}. \tag{2.9}$$

Combining (2.6) and (2.9) we find $n \leqslant r_1 + r_2 + 1 = d_{1,2}$. □

Lemma 6. *If C is a (binary) bipartite perfect (r_1, r_2)-error-correcting code, then the punctured code $C' = C_1' \cup C_2'$ is a perfect $(r_1, r_2 - 1)$-error-correcting code and also a perfect $(r_1 - 1, r_2)$-error-correcting code.*

Proof. If (2.3) and (2.4) both hold, i.e. (2.6) holds, then we must have equality in (2.5), showing that C' is perfect for $(r_1, r_2 - 1)$. The second assertion follows in the same way. □

There is a partial converse to Lemma 6. We state it, although we shall not need it later.

Lemma 7. *If $C = C_1 \cup C_2$ is a binary perfect $(r_1, r_2 - 1)$-error-correcting code and also a perfect $(r_1 - 1, r_2)$-error-correcting code, with $d_{1,2} < n$, then if $d_{1,2}$ is odd the extended code $\bar{C} = \bar{C}_1 \cup \bar{C}_2$ is a perfect bipartite (r_1, r_2)-error-correcting code.*

Proof. For the distances, $\overline{d_1}$, $\overline{d_2}$, $\overline{d_{1,2}}$ of $\bar{C}$ we find $\overline{d_1} \geqslant 2r_1 + 2$, $\overline{d_2} \geqslant 2r_2 + 2$, $\overline{d_{1,2}} \geqslant d_{1,2} + 1 = r_1 + r_2 + 1$ (by Lemma 1). So, $\bar{C}$ is certainly an (r_1, r_2)-error-correcting code. That $\bar{C}$ is perfect now again easily follows by using (1.7) three times. □

3. Proof of Theorem 1

We remind the reader of the *Johnson bound* for binary codes (cf. [6]). If C is a binary e-error-correcting code of length n, then

$$|C|\left\{V(n,e)+\binom{n}{e}\frac{\left(\frac{n-e}{e+1}\right)-\left\lfloor\frac{n-e}{e+1}\right\rfloor}{\left\lfloor\frac{n}{e+1}\right\rfloor}\right\}\leqslant 2^n. \tag{3.1}$$

If equality holds in (3.1), then either $e+1$ divides $n+1$ in which case C is a perfect code, or otherwise C is called *nearly perfect*. Note that if the fraction on the left-hand side of (3.1) is not 0, then it is at least $(1/n)\binom{n}{e}$. Therefore

$$|C|\left\{V(n,e)+\frac{1}{n}\binom{n}{e}\right\}=2^n \tag{3.2}$$

implies that $e+1$ divides n and that C is a nearly perfect code.

Now assume that C is a bipartite perfect $(r, 1)$-error-correcting code with $r\geqslant 2$. Apply Lemma 5 and Lemma 6. We find that C' is a perfect $(r, 0)$-error-correcting code and that

$$M_2=\frac{1}{n-1}\binom{n-1}{r}M_1.$$

It follows that C_1' is an r-error-correcting code with equality in (3.2). Therefore C_1' is nearly perfect. It is well-known (cf. [5]) that (since $r\geqslant 2$) this implies that C_1' has the parameters of a Preparata code. This completes the proof, (since it is not known whether the Preparata codes are unique for length >16, we cannot claim that C is actually obtained from a Preparata code). □

Acknowledgement

The authors express their gratitude towards Prof. J.H. van Lint for his help in preparing this paper.

References

[1] R.D. Baker, J.H. van Lint and R.M. Wilson, On the Preparata and Goethals codes, IEEE Trans. Inform. Theory IT-29 (May 1983) 342–345.

[2] M. Gundlach, On codes with distinct protective radii, Atti Sem. Mat. Fis. Univ. Modena 32 (1983) 379–396.

[3] M. Gundlach, On strongly tactical codes, Proc. AAECC-3, Lecture Notes in Computer Science 229 (Springer Verlag, 1986).

[4] M. Gundlach, Fehlerkorrigierende Codes, bei denen die Codewörter durch Hamming-Kugeln mit verschiedenen Radien gesichert sind, Ph.D. thesis, University of Mainz (1986).

[5] K. Lindström, The nonexistence of unknown nearly perfect binary codes, Ann. Univ. Turku, Ser. AI 169 (1975).

[6] J.H. van Lint, Introduction to Coding Theory (Springer Verlag, 1982).

[7] G.V. Zaitsev, V.A. Zinovjev and N.V. Semakov, Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes, in B.N. Petrov and F. Csáki, Eds., 2nd International Symposium on Information Theory (Akadémiai Kiadó, Budapest, 1973) 257–263.