Quasi-Perfect Codes With Small Distance

Tuvi Etzion, *Fellow, IEEE,* and Beniamin Mounits

***Abstract*—The main purpose of this paper is to give bounds on the length of the shortest and longest binary quasi-perfect codes with a given Hamming distance, covering radius, and redundancy. We consider codes with Hamming distance 4 and 5 and covering radius 2 and 3, respectively. We discuss the blockwise direct sum (BDS) construction which has an important role in finding these bounds.**

***Index Terms*—Blockwise direct sum (BDS) construction, covering, density, packing, quasi-perfect codes.**

I. Introduction

LET $\mathcal{F}_2 = \{0, 1\}$ and let $\mathcal{F}_2^n$ denotes the set of all binary words of length n, $\mathcal{E}_2^n \subset \mathcal{F}_2^n$ denotes the set of all words with even weight, and $\mathcal{O}_2^n \subset \mathcal{F}_2^n$ denotes the set of all words with odd weight. For $x, y \in \mathcal{F}_2^n$, $d(x, y)$ denotes the Hamming distance between x and y. A code $\mathcal{C}$ is a nonempty subset of $\mathcal{F}_2^n$. For a code $\mathcal{C}$, we denote the minimum Hamming distance (or distance in short) of $\mathcal{C}$ by $d(\mathcal{C})$, i.e.,

$$d(\mathcal{C}) = \min_{c_1, c_2 \in \mathcal{C}, c_1 \neq c_2} d(c_1, c_2).$$

The packing radius $e(\mathcal{C})$ of the code is

$$e(\mathcal{C}) = \left\lfloor \frac{d(\mathcal{C}) - 1}{2} \right\rfloor$$

and the covering radius $R(\mathcal{C})$ of the code is

$$R(\mathcal{C}) = \max_{x \in \mathcal{F}_2^n} \min_{c \in \mathcal{C}} d(x, c).$$

An $(n, M, d)R$ code $\mathcal{C}$ is a binary code of length n, distance d, covering radius R, and M codewords. An (R, d) code $\mathcal{C}$ is a code with covering radius R and distance d. The *redundancy* r of an $(n, M, d)R$ code $\mathcal{C}$ is defined by $n - \log_2 M$. The *sphere* of radius t around a word $y \in \mathcal{F}_2^n$ is defined by

$$\{x : x \in \mathcal{F}_2^n, d(x, y) \leq t\}.$$

If the distance of an $(n, M, d)R$ code $\mathcal{C}$ is $d = 2R + 1$, then the spheres with radius R around the codewords are disjoint and they cover $\mathcal{F}_2^n$. Such codes are called *perfect*. The only binary perfect codes are

- $(n, 2^n, 1)0$ codes for each $n \geq 1$;
- $(2k + 1, 2, 2k + 1)k$ repetition codes for each $k \geq 1$;
- $(2^k - 1, 2^{2^k - k - 1}, 3)1$ codes for each $k \geq 2$;
- the $(23, 4096, 7)3$ Golay code.

A code is called *quasi-perfect* if its packing radius is e and its covering radius is $e + 1$, for some nonnegative integer e, i.e., the spheres with radius e around the codewords are disjoint, and the spheres with radius $e + 1$ cover $\mathcal{F}_2^n$. Clearly, the distance of such code is $2e + 1$ or $2e + 2$. Codes with covering radius 1 and distance 1 can be obtained easily, e.g., by adding any subset of distinct words to a $(2^k - 1, 2^{2^k - k - 1}, 3)1$ code. Codes with covering radius 1 and distance 2 can be also easily obtained. Any code with covering radius 1 is quasi-perfect. Therefore, quasi-perfect codes with covering radius 1 are not interesting in this context. Quasi-perfect codes with covering radius 2 were extensively studied [1], [3]–[6], [15]. Quasi-perfect codes with covering radius 3 were studied in [5], [7], [10], [15]–[17]. The only known quasi-perfect codes with covering radius greater than 3 are the extended Golay code with $d = 8$ and $R = 4$, and the repetition code of length $2t$, with $d = 2t$ and $R = t$.

There are a few interesting questions concerning quasi-perfect codes.

- Construction of such codes for all possible lengths for a given radius and distance.
- What is the sparse and the dense code for a given length, radius, and distance?
- For a given redundancy, radius, and distance, what is the longest and the shortest code?

Note that these questions are closely related. As we did not find any interesting quasi-perfect codes with noninteger redundancy, we consider only integer redundancies. In this paper, we mainly consider the last question, especially for $R = 2, R = 3$, and $d = 4, d = 5$, respectively. For this purpose, we need the following definitions. The length of the shortest code with covering radius R, distance d, and redundancy r, will be denoted by $l^*(R, d, r)$. The length of the longest code with covering radius R, distance d, and redundancy r, will be denoted by $n^*(R, d, r)$. The covering density of an $(n, M, d)R$ code $\mathcal{C}$ is defined by

$$\mu_c(\mathcal{C}) = \frac{M \sum_{i=0}^{R} \binom{n}{i}}{2^n}$$

and its packing density is defined by

$$\mu_p(\mathcal{C}) = \frac{M \sum_{i=0}^{e(\mathcal{C})} \binom{n}{i}}{2^n}.$$

For a family of $(n_i, M_i, d_i)R_i$ codes $\mathcal{C}_i$, $i = 1, 2, \ldots, n_{i+1} > n_i$, the covering (packing) density $\mu_c\{\mathcal{C}_i\}$ $(\mu_p\{\mathcal{C}_i\})$ of the family is defined by

$$\mu_c\{\mathcal{C}_i\} = \lim_{i \to \infty} \mu_c(\mathcal{C}_i) \quad (\mu_p\{\mathcal{C}_i\} = \lim_{i \to \infty} \mu_p(\mathcal{C}_i))$$

if the limit exists.

Manuscript received December 12, 2003; revised July 29, 2005. This work was supported in part by the Technion V.P.R. fund–Loewengart research fund. The material in this paper was presented in part in the IEEE International Symposium on Information Theory, Chicago, IL, June/July 2004.

T. Etzion is with the Department of Computer Science, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: etzion@cs.technion.ac.il).

B. Mounits is with the Department of Mathematics, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: mounitsb@tx.technion.ac.il.

Communicated by G. Zémor, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.856944

The rest of the paper is organized as follows. In Section II, we present the well-known *blockwise direct sum* (BDS) construction [8] which has a significant role in all our constructions. We present the Hamming and Preparata codes which are used in our constructions. These codes were used with the BDS construction in [5] and the method was developed in [15] to obtain new codes. In this paper, we further develop the technique by using new codes to obtain some new better quasi-perfect codes. In Section III, we discuss quasi-perfect codes with covering radius 2 and distance 4. In Section IV, we give new constructions for $R = 3$ and $d = 5$ and analyze the codes obtained by these constructions. In Section V, we conclude with a discussion and a list of open problems.

II. Preliminaries

A. The Blockwise Direct Sum (BDS) Construction

Definition 1: [2] A family of codes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_t\} \subseteq \mathcal{F}_2^n$ has *subnorm* S if

$$\min_{1 \le i \le t} d(x, \mathcal{C}_i) + \max_{1 \le i \le t} d(x, \mathcal{C}_i) \le S$$

holds for all $x \in \mathcal{F}_2^n$.

BDS Construction:
Suppose we are given four codes: an $(n_1, M_1, d_1)R_1$ code $\mathcal{C}_1$, an $(n_1, M_2 = bM_1, d_2)R_2$ code $\mathcal{C}_2$, an $(n_3, M_3, d_3)R_3$ code $\mathcal{C}_3$, and an $(n_3, M_4 = bM_3, d_4)R_4$ code $\mathcal{C}_4$ with the following properties:

- $\mathcal{C}_2$ is a union of b disjoint codes $\mathcal{C}_1^i$ with the parameters of $\mathcal{C}_1$

$$\mathcal{C}_2 = \bigcup_{i=1}^{b} \mathcal{C}_1^i;$$

- $\mathcal{C}_4$ is a union of b disjoint codes $\mathcal{C}_3^i$ with the parameters of $\mathcal{C}_3$

$$\mathcal{C}_4 = \bigcup_{i=1}^{b} \mathcal{C}_3^i;$$

- $\{\mathcal{C}_1^1, \mathcal{C}_1^2, \ldots, \mathcal{C}_1^b\}$ has subnorm S_1;
- $\{\mathcal{C}_3^1, \mathcal{C}_3^2, \ldots, \mathcal{C}_3^b\}$ has subnorm S_3.

Then the BDS of $\mathcal{C}_2$ and $\mathcal{C}_4$ is the following code $\mathcal{C}$:

$$\mathcal{C} = \bigcup_{i=1}^{b} \mathcal{C}_1^i \times \mathcal{C}_3^i.$$

The given construction is a combination of the constructions given in [2], [8], [9], [13].

Theorem 1: [2], [9], [13] The $(n, M, d)R$ code $\mathcal{C}$ of the BDS construction has the following parameters:

$$n = n_1 + n_3, \quad M = bM_1M_3,$$
$$d \ge \min\{d_1, d_3, d_2 + d_4\}, \quad R \le (S_1 + S_3)/2.$$

B. The Hamming and the Preparata Codes

Several families of codes will be used in the BDS construction. Four families will be used more often.

1) Hamming Codes
The Hamming code of order $m, \mathcal{H}_0'(m)$, is a $(2^m - 1, 2^{2^m-1-m}, 3)1$ code. $\{\mathcal{H}_i'(m) : 0 \le i \le 2^m - 1\}$ is the family of codes which contains the Hamming code and its $2^m - 1$ cosets. The subnorm of this family is 1. Any family which is a nonempty proper subset of this family has subnorm 2.

2) Extended Hamming Codes
The extended Hamming code of order $m, \mathcal{H}_0(m)$, is a $(2^m, 2^{2^m-1-m}, 4)2$ code, obtained by adding an even parity bit to $\mathcal{H}_0'(m)$.

$$\{\mathcal{H}_i(m) : 0 \le i \le 2^{m+1} - 1\}$$

is the family of codes which contains the extended Hamming code and its $2^{m+1} - 1$ cosets. The subnorm of this family is 2.

$$\{\mathcal{H}_i^e(m) : 0 \le i \le 2^m - 1\}$$

is the family of codes which contains $\mathcal{H}_0(m) = \mathcal{H}_0^e(m)$ and its $2^m - 1$ cosets with even weight. The subnorm of this family is also 2.

3) Preparata Codes
The Preparata code of order $m, \mathcal{P}_0(m), m$ is an even integer, $m \ge 4$, is a $(2^m, 2^{2^m-2m}, 6)4$ code. It is well known [17] that there exist 2^{m-1} translates of $\mathcal{P}_0(m)$ whose union is $\mathcal{H}_0(m)$. Let $\{\mathcal{P}_i(m) : 0 \le i \le 2^{m-1} - 1\}$ be the family which consists of these 2^{m-1} translates. It is proved in [2, p. 111] that the subnorm of this family is 4. Let $\{\mathcal{P}_i(m) : 0 \le i \le 2^{2m-1} - 1\}$ be the family which consists of the 2^{2m-1} translates whose union is $\mathcal{E}_2^{2^m}$, and

$$\mathcal{H}_j^e(m) = \bigcup_{i=j2^{m-1}}^{(j+1)2^{m-1}-1} \mathcal{P}_i(m)$$

for each $j, 0 \le j \le 2^m - 1$.

Lemma 1: If x, z are two different even-weight vectors of length 2^m such that $x + z \notin \mathcal{H}_0(m)$ then there exist 2^{m-1} words in $z + \mathcal{H}_0(m)$ at distance 2 from x.

Proof: Each even coset of $\mathcal{H}_0(m)$, and in particular, $x + z + \mathcal{H}_0(m)$, has 2^{m-1} words of weight 2. Hence, there are 2^{m-1} words in $\mathcal{H}_0(m)$ at distance 2 from $x + z$. Therefore, there exist 2^{m-1} words in $z + \mathcal{H}_0(m)$ at distance 2 from x. □

Corollary 1: If $\{z_j\}_{j=1}^k$ are k different even-weight vectors of length 2^m such that $z_i + z_j \notin \mathcal{H}_0(m), i \ne j, 1 \le i, j \le k$, then the family of codes

$$\{z_j + \mathcal{P}_i(m) : 1 \le j \le k, 0 \le i \le 2^{m-1} - 1\}$$

has subnorm equal to 4.

4) Punctured Preparata Codes
The punctured Preparata code of order m, $\mathcal{P}_0'(m), m$ is an even integer, $m \ge 4$, is a $(2^m - 1, 2^{2^m-2m}, 5)3$ code obtained from $\mathcal{P}_0(m)$ by deleting the last coordinate (by deleting another coordinate we obtain an equivalent code). Let

$$\{\mathcal{P}_i'(m) : 0 \le i \le 2^{m-1} - 1\}$$

be the family of 2^{m-1} translates of $\mathcal{P}_0'(m)$ whose union is $\mathcal{H}_0'(m)$. It is proved in [2, p. 111] that the subnorm of this family is 3. Furthermore, let $\mathcal{P}_i'(m), 0 \le i \le 2^{2m-1} - 1$, be

the code obtained from $\mathcal{P}_i(m)$ by deleting the last coordinate, i.e., for each $j, 0 \le j \le 2^m - 1$

$$\mathcal{H}'_j(m) = \bigcup_{i=j2^{m-1}}^{(j+1)2^{m-1}-1} \mathcal{P}'_i(m). \tag{1}$$

The reader interested in properties of the partitions of the Hamming and the extended Hamming codes into translates of the punctured Preparata and Preparata codes, respectively, is referred to [5, Lemma 1], [17, Theorems 1, 2, and Corollary 1].

III. Codes With Covering Radius $R = 2$

If $R = 2$ and $d = 4$ then $n^*(2, 4, r) = 2^{r-1}$. These values are attained by the extended Hamming codes. Next, we give upper bounds on $l^*(2, 4, r)$. The first two cases are of known codes.

Case A: If $r \equiv 0 \pmod 4, r = 2m, m$ is even, $m \ge 4$, then $l^*(2, 4, 2m) \le 3 \cdot 2^{m-1} - 1$. The codes which attain this bound are obtained by the BDS construction [15, Construction 4.22, Remark 4.23], where

$$\mathcal{C}_1 = \mathcal{P}'_0(m), \quad \mathcal{C}_2 = \bigcup_{i=0}^{2^{m-1}-1} \mathcal{P}'_i(m) = \mathcal{H}'_0(m)$$

$$\mathcal{C}_3 = \mathcal{H}^e_0(m-1), \quad \mathcal{C}_4 = \bigcup_{i=0}^{2^{m-1}-1} \mathcal{H}^e_i(m-1) = \mathcal{E}_2^{2^{m-1}}.$$

The obtained codes will be denoted by $\Psi(m)$; $\Psi(m)$ is a

$$(3 \cdot 2^{m-1} - 1, 2^{3 \cdot 2^{m-1}-1-2m}, 4)2$$

code with $\mu_c\{\Psi(m)\} = \frac{9}{8}$.

Case B: If $r \equiv 2 \pmod 4, r = 2m+2, m$ is even, $m \ge 4$, then $l^*(2, 4, 2m + 2) \le 15 \cdot 2^{m-2} - 3$. The codes which attain this bound are linear $(15 \cdot 2^{m-2} - 3, 2^{15 \cdot 2^{m-2}-5-2m}, 4)2$ codes which were constructed in [6]. The covering density of this family is $\frac{225}{128}$.

In the next two cases the known upper bounds on $l^*(2, 4, r)$ are improved.

Case C: If $r \equiv 1 \pmod 4, r = 2m + 1, m$ is even, $m \ge 4$, then $l^*(2, 4, 2m + 1) \le 5 \cdot 2^{m-1} - 1$. The codes which attain this bound are a variation of codes given in [5]. Let

$$\Psi_j(m) = \bigcup_{i=0}^{2^{m-1}-1} \mathcal{P}'_i(m) \times \mathcal{H}^e_{i+j}(m-1)$$

$$\Psi_{2^{m-1}+j}(m) = 10^{3 \cdot 2^{m-1}-3}1 + \Psi_j(m)$$

$0 \le j \le 2^{m-1} - 1$, where the subscript $i + j$ is taken modulo 2^{m-1} and a^k denotes a sequence of k a's. Note that $\Psi_0(m)$ is the code designed in Case A. It is easy to verify that $\bigcup_{i=0}^{2^m-1} \Psi_i(m)$ is a $(3 \cdot 2^{m-1} - 1, 2^{3 \cdot 2^{m-1}-1-m}, 2)1$ code and the family $\{\Psi_i(m) : 0 \le i \le 2^m - 1\}$ has subnorm 3. The codes which attain the bound are obtained by the BDS construction, where

$$\mathcal{C}_1 = \Psi_0(m), \quad \mathcal{C}_2 = \bigcup_{i=0}^{2^m-1} \Psi_i(m)$$

$$\mathcal{C}_3 = \mathcal{H}_0(m), \quad \mathcal{C}_4 = \bigcup_{i=0}^{2^m-1} \mathcal{H}^e_i(m) = \mathcal{E}_2^{2^m}.$$

The obtained codes will be denoted by $\Upsilon(m)$; $\Upsilon(m)$ is a $(5 \cdot 2^{m-1} - 1, 2^{5 \cdot 2^{m-1}-2-2m}, 4)2$ code with

$$\mu_c\{\Upsilon(m)\} = \frac{25}{16}.$$

The previous bound was attained by family of linear codes whose covering density is $\frac{529}{256}$ [6].

For the last case we need the following lemma.

Lemma 2: If S_1 is partitioned into k subsets $A_0, A_1, \ldots, A_{k-1}$ and S_2 is partitioned into t subsets $B_0, B_1, \ldots, B_{t-1}$ then

$$S_1 \times S_2 = \bigcup_{j=0}^{t-1} \bigcup_{i=0}^{k-1} A_i \times B_{i+j}$$

where $i + j$ is taken modulo t, and

$$\left(\bigcup_{i=0}^{k-1} A_i \times B_{i+j_1}\right) \bigcap \left(\bigcup_{i=0}^{k-1} A_i \times B_{i+j_2}\right) = \varnothing$$

iff $j_1 \ne j_2$.

Definition 2: An $(n, M, d)R$ code $\mathcal{C}$ has the *space property* if there exist disjoint $(n, M, d)R$ codes (one of which is $\mathcal{C}$) whose union is $\mathcal{F}_2^n$.

Lemma 3: $\Upsilon(m)$ has the space property.

Proof: By Lemma 2 and properties of code families from Case C

$$\bigcup_{i=0}^{2^m-1} \Psi_i(m) \times \mathcal{E}_2^{2^m}$$

can be partitioned into codes with parameters of $\Upsilon(m)$, where

$$S_1 = \bigcup_{i=0}^{2^m-1} \Psi_i(m)$$

and

$$S_2 = \mathcal{E}_2^{2^m} = \bigcup_{i=0}^{2^m-1} \mathcal{H}^e_i(m)$$

in Lemma 2. Since

$$\bigcup_{i=0}^{2^m-1} \Psi_i(m) = \mathcal{H}'_0(m) \times \mathcal{E}_2^{2^{m-1}} \bigcup \mathcal{H}'_j(m) \times \mathcal{O}_2^{2^{m-1}}$$

for some $j \ne 0$, it is easy to verify that $\mathcal{F}_2^{5 \cdot 2^{m-1}-1}$ can be partitioned into codes with the parameters of $\bigcup_{i=0}^{2^m-1} \Psi_i(m) \times \mathcal{E}_2^{2^m}$. Hence, $\Upsilon(m)$ has the space property. □

Case D: $r \equiv 3 \pmod 4, r = t \cdot 2^k - 1, t$ odd, and $k \ge 2$. Let $l(t, k), t$ odd, $k \ge 1, (t, k) \ne (1, 1)$, be the length of the shortest $(2, 4)$ code $\mathcal{C}$ with redundancy $t \cdot 2^k - 1$ which has the space property. We claim that for $k \ge 2$

$$l(t, k) \le \sum_{i=0}^{k-1} 2^{t \cdot 2^i} - k + \lfloor 2^{t-2} \rfloor.$$

The codes which attain this bound are obtained by using modification and developing the ideas of [15, Construction 4.24]. We use the BDS construction, where

$$\mathcal{C}_1 = \mathcal{P}'_0(t \cdot 2^{k-1}), \mathcal{C}_2 = \bigcup_{i=0}^{2^{t \cdot 2^{k-1}-1}-1} \mathcal{P}'_i(t \cdot 2^{k-1}) = \mathcal{H}'_0(t \cdot 2^{k-1})$$

TABLE I

length	redundancy	reference	linear
$\mathbf{2^m-2}$, $m\geq 4$, m is even	$2m$	Red. Goppa[10]	Yes
$\mathbf{2^m-1}$	$2m$	BCH[7]	Yes
$\mathbf{2^m-1}$, $m\geq 4$, m is even	$2m-1$	Punctured Preparata[9]	No
$\mathbf{2^m-1}$, $m\geq 5$, m is odd	$3(m-1)$	Etzion and Greenberg[5]	No
$\mathbf{2^m}$, m is odd	$2m$	Irred. Goppa[11]	Yes
$\mathbf{2^m+1}$, $m\geq 4$, m is even	$2m$	Zetterberg[11]	Yes
$\mathbf{2^m+2^{m-1}-2}$, $m\geq 4$, m is even	$3m-2$	Struik[15]	No
$\mathbf{2^{2m}+2^m-1}$, m is even	$4m$	Zaitsev et al.[17]	No

$\mathcal{C}_3$ is a code with the space property which attains $l(t,k-1)$ and $\mathcal{C}_4=\mathcal{F}_2^{l(t,k-1)}$. By Lemma 2, we can partition $\mathcal{H}_0'(t\cdot 2^{k-1})\times \mathcal{F}_2^{l(t,k-1)}$ into codes with the parameters of the obtained code. Hence, the code obtained by the BDS construction has redundancy $t\cdot 2^k-1$ and the space property. Therefore, for $k\geq 2$ we obtain

$$l(t,k)\leq 2^{t\cdot 2^{k-1}}-1+l(t,k-1)$$

with the initial conditions $l(1,2)=4$ (which is attained by the extended Hamming code of length 4) and $l(t,1)=5\cdot 2^{t-2}-1$ for $t\geq 3$ (by Case C, Lemma 3, and since $l(3,1)=9$ [1] which is attained by linear code, which obviously has the space property).

It is now easy to verify that

$$l(t,k)\leq \sum_{i=0}^{k-1}2^{t\cdot 2^i}-k+\lfloor 2^{t-2}\rfloor$$

and hence,

$$l^*(2,4,t\cdot 2^k-1)\leq l(t,k)\leq \sum_{i=0}^{k-1}2^{t\cdot 2^i}-k+\lfloor 2^{t-2}\rfloor$$

where t is odd and $k\geq 2$. Hence, this is a

$$\left(\sum_{i=0}^{k-1}2^{t\cdot 2^i}-k+\lfloor 2^{t-2}\rfloor, 2^{\sum_{i=0}^{k-1}2^{t\cdot 2^i}-k+\lfloor 2^{t-2}\rfloor-t\cdot 2^k+1},4\right)2$$

code. The density of this family of codes is 1, i.e., these codes are asymptotically perfect. The first family of asymptotically perfect $(2,4)$ codes was obtained by Struik [15, Construction 4.24]. For $r=7,11$ the parameters of our codes are the same as those of Struik. For $r\geq 15$, our codes are shorter than the codes of Struik. For $r=15$ our construction gives the code of length 274 whereas the code obtained in [15, Construction 4.24] has length 276, and for $r\geq 19, r=t\cdot 2^k-1, t$ odd, $k\geq 2$, the code of Struik has the following parameters:

$$\left(2^{t\cdot 2^{k-1}}+\frac{23}{16}2^{t\cdot 2^{k-2}}-4, 2^{2^{t\cdot 2^{k-1}}+\frac{23}{16}2^{t\cdot 2^{k-2}}-3-t\cdot 2^k},4\right)2.$$

IV. Codes With Covering Radius $R=3$

Table I describes parameters of the known infinite families of $(3,5)$ codes. If there exist a few families with the same parameters, we mention only one of them.

For small redundancies there are codes obtained by Wagner [16] via computer search, and codes constructed in [17].

A. Constructions of New Codes

Construction A: Let $m,k\geq 4$ be even integers such that $k\leq m\leq 2k$. Define

$$\mathcal{A}(m,k)=\bigcup_{i=0}^{2^{m-1}-1}\mathcal{P}_i'(m)\times\mathcal{P}_i(k).$$

Note that by definition

$$\mathcal{H}_j^e(k)=\bigcup_{i=j2^{k-1}}^{(j+1)2^{k-1}-1}\mathcal{P}_i(k)$$

for each $0\leq j\leq 2^k-1$. By Lemma 1, Corollary 1, and Theorem 1 we have the following.

Theorem 2: $\mathcal{A}(m,k)$ is a

$$(2^m+2^k-1, 2^{2^m+2^k-1-(m+2k)},5)3$$

code, where m,k are even integers greater than 3 and $k\leq m\leq 2k$.

The code $\mathcal{A}(m,m)$ coincides with the code $\mathcal{D}(m)$ defined in [5]. We have $\mu_c\{\mathcal{A}(m,m)\}=4/3$ which is the smallest covering density for known family of codes with covering radius 3. The code $\mathcal{A}(2k,k)$ coincides with the code of Zaitsev *et al.* [17], which was also constructed in [13]; $\mu_p\{\mathcal{A}(2k,k)\}=1/2$. The code $\mathcal{A}(2k,k)$ is the longest known code with distance 5 and redundancy $4k$. The punctured Preparata codes are the only ones known to have better packing density for family of codes with minimum distance 5.

The only known infinite family of $(3,5)$ codes with odd redundancy is the punctured Preparata codes. In the next construction we obtain more infinite families of such codes.

For the next construction we need the following lemma.

Lemma 4: For any integer $t\geq 3$, let $\{\mathcal{C}_i: 0\leq i\leq 2^t-1\}$ be a family of codes, where $\mathcal{C}_i$ is an $(n_0,2^{n_0-r},5)R$ code for each $i, 0\leq i\leq 2^t-1$. If

$$\mathcal{C}=\bigcup_{i=0}^{2^t-1}\mathcal{C}_i$$

is an $(n_0,2^{n_0-(r-t)},d)1$ code, then $n_0\leq 2^{t+1}-1$ and $r\leq 2t+1$.

Proof: Since the covering radius of $\mathcal{C}$ is 1, it follows by the sphere-covering bound that

$$|\mathcal{C}|\geq\frac{2^{n_0}}{1+n_0}$$

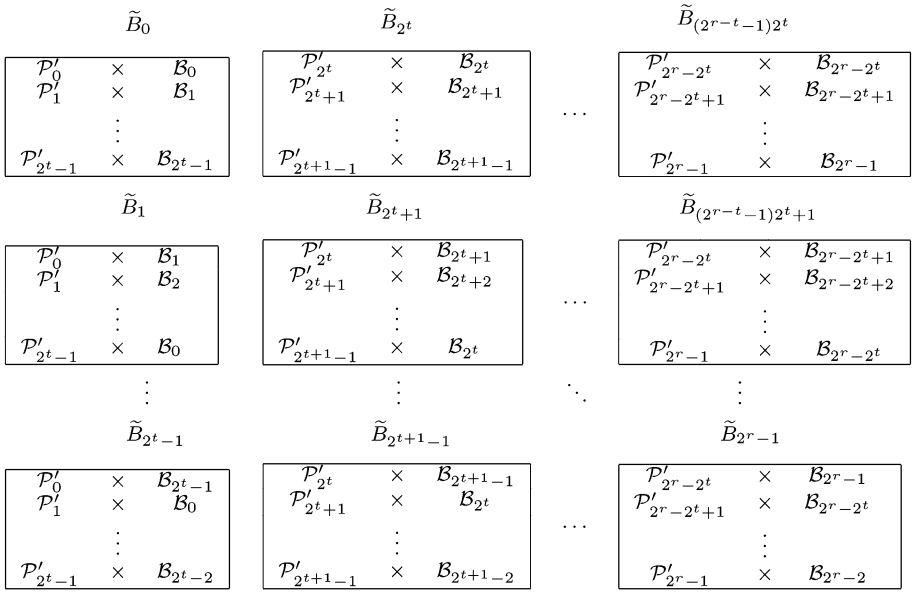

Fig. 1.

i.e.,

$$|\mathcal{C}_i| = \frac{|\mathcal{C}|}{2^t} \geq \frac{2^{n_0-t}}{1+n_0}. \tag{2}$$

On the other hand, since the distance of $\mathcal{C}_i$ is 5, we also have by the sphere-packing bound that

$$\frac{2^{n_0}}{1+n_0+\binom{n_0}{2}} \geq |\mathcal{C}_i|. \tag{3}$$

By (2) and (3) we have

$$\frac{2^{n_0}}{1+n_0+\binom{n_0}{2}} \geq |\mathcal{C}_i| \geq \frac{2^{n_0-t}}{1+n_0}.$$

Therefore,

$$2^t \geq \frac{1+n_0+\binom{n_0}{2}}{1+n_0} = \frac{n_0}{2} + \frac{1}{n_0+1} > \frac{n_0}{2}.$$

Thus, $n_0 \leq 2^{t+1}-1$. Let's denote the maximal redundancy of a code of length n with covering radius R by $r^*(R,n)$. Since $n_0 \leq 2^{t+1}-1$ it follows that

$$r - t \leq r^*(1,n_0) \leq r^*(1,2^{t+1}-1) = t+1.$$

Thus, $r \leq 2t+1$. □

Construction B: For $r \geq 4$, let $\mathcal{B}_i$, $0 \leq i \leq 2^r-1$, be an $(n, 2^{n-r}, 5)3$ code, where $\bigcup_{i=0}^{2^r-1} \mathcal{B}_i = \mathcal{F}_2^n$. For t odd, $r > t \geq 3$, let $\mathcal{Y}_j$, $0 \leq j \leq 2^{r-t}-1$, be an $(n, 2^{n-(r-t)}, 2)1$ code, such that

$$\mathcal{Y}_j = \bigcup_{i=j2^t}^{(j+1)2^t-1} \mathcal{B}_i. \tag{4}$$

We construct the following codes:

$$\tilde{B}_{a2^{2r-t}+b2^r+s2^t+j} = \bigcup_{i=0}^{2^t-1} \mathcal{P}'_{a2^{r-t}+(b+s)2^t+i}(t+1) \times \mathcal{B}_{s2^t+i+j}$$

for $0 \leq a \leq 2^{2t+1-r}-1, 0 \leq b, s \leq 2^{r-t}-1$, and $0 \leq j \leq 2^t-1$, where $i+j$ is taken modulo 2^t and $b+s$ is taken modulo 2^{r-t}, and

$$\tilde{Y}_{a2^{r-t}+b} = \bigcup_{s=0}^{2^{r-t}-1} \bigcup_{j=0}^{2^t-1} \tilde{B}_{a2^{2r-t}+b2^r+s2^t+j}$$

for $0 \leq a \leq 2^{2t+1-r}-1$ and $0 \leq b \leq 2^{r-t}-1$.

In the following theorem, we explain step by step how the codes of Construction B are obtained.

Theorem 3: $\tilde{B}_i, 0 \leq i \leq 2^{\tilde{r}}-1$, is an $(\tilde{n}, 2^{\tilde{n}-\tilde{r}}, 5)3$ code and

$$\bigcup_{i=0}^{2^{\tilde{r}}-1} \tilde{B}_i = \mathcal{F}_2^{\tilde{n}}.$$

$\tilde{Y}_j$, $0 \leq j \leq 2^{\tilde{r}-\tilde{t}}-1$, is an $(\tilde{n}, 2^{\tilde{n}-(\tilde{r}-\tilde{t})}, 2)1$ code, such that

$$\tilde{Y}_j = \bigcup_{i=j2^{\tilde{t}}}^{(j+1)2^{\tilde{t}}-1} \tilde{B}_i$$

where $\tilde{n} = n + 2^{t+1} - 1, \tilde{r} = r+t+1$, and $\tilde{t} = r$.

Proof: For convenience, we denote $\mathcal{P}'_i(t+1)$ by $\mathcal{P}'_i$, and $\mathcal{H}'_i(t+1)$ by $\mathcal{H}'_i$. By the definition of Construction B

$$\tilde{B}_{s2^t+j} = \bigcup_{i=0}^{2^t-1} \mathcal{P}'_{s2^t+i} \times \mathcal{B}_{s2^t+i+j}$$

for $0 \leq s \leq 2^{r-t}-1$, and $0 \leq j \leq 2^t-1$, where $i+j$ is taken modulo 2^t. Fig. 1 describes the 2^r codes which are obtained, where for a given j, the codes $\tilde{B}_{s2^t+j}, 0 \leq s \leq 2^{r-t}-1$, are written in row j.

Next, we consider the following codes:

$$\tilde{B}_{b2^r+s2^t+j} = \bigcup_{i=0}^{2^t-1} \mathcal{P}'_{(b+s)2^t+i} \times \mathcal{B}_{s2^t+i+j} \tag{5}$$

for $0 \leq b, s \leq 2^{r-t}-1$, and $0 \leq j \leq 2^t-1$, where $i+j$ is taken modulo 2^t, and $b+s$ is taken modulo 2^{r-t}. Fig. 1 describes the codes corresponding to the case $b=0$. For each $b, 1 \leq b \leq 2^{r-t}-1$, we obtain a similar array. Fig. 2 describes

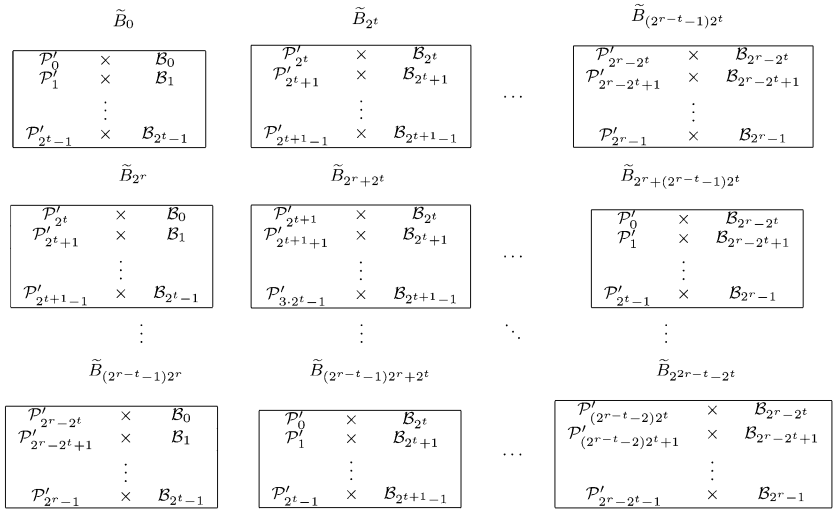

Fig. 2.

the $2^{2(r-t)}$ codes which are obtained for $j = 0$, where for a given b, the codes $\tilde{B}_{b2^r+s2^t}$ are written in row b.

Now, for $0 \le b \le 2^{r-t} - 1$

$$\tilde{Y}_b = \bigcup_{s=0}^{2^{r-t}-1} \bigcup_{j=0}^{2^t-1} \tilde{B}_{b2^r+s2^t+j}. \tag{6}$$

Therefore, from (1), (4), (5), and (6) it follows that

$$\begin{aligned}\tilde{Y}_b &= \bigcup_{s=0}^{2^{r-t}-1} \bigcup_{j=0}^{2^t-1} \bigcup_{i=0}^{2^t-1} \mathcal{P}'_{(b+s)2^t+i} \times \mathcal{B}_{s2^t+i+j} \\ &= \bigcup_{s=0}^{2^{r-t}-1} \bigcup_{i=0}^{2^t-1} \mathcal{P}'_{(b+s)2^t+i} \times \left(\bigcup_{j=0}^{2^t-1} \mathcal{B}_{s2^t+i+j} \right) \\ &= \bigcup_{s=0}^{2^{r-t}-1} \left(\bigcup_{i=0}^{2^t-1} \mathcal{P}'_{(b+s)2^t+i} \right) \times \mathcal{Y}_s \\ &= \bigcup_{s=0}^{2^{r-t}-1} \mathcal{H}'_{b+s} \times \mathcal{Y}_s \end{aligned} \tag{7}$$

and

$$\bigcup_{b=0}^{2^{r-t}-1} \tilde{Y}_b = \bigcup_{b=0}^{2^{r-t}-1} \bigcup_{s=0}^{2^{r-t}-1} \mathcal{H}'_{b+s} \times \mathcal{Y}_s = \left(\bigcup_{b=0}^{2^{r-t}-1} \mathcal{H}'_b \right) \times \mathcal{F}_2^n \tag{8}$$

where $b+s$ is taken modulo 2^{r-t}, and $i+j$ is taken modulo 2^t. Note that $\tilde{Y}_0$ is the union of all the codes which appear in Fig. 1.

By Lemma 4, $t+1 \ge r-t$. If $t+1 = r-t$, then it follows from (8) that $\bigcup_{b=0}^{2^{r-t}-1} \tilde{Y}_b = \mathcal{F}_2^{2^{t+1}-1} \times \mathcal{F}_2^n$, and we have considered all the codes obtained in Construction B. If $t+1 > r-t$, then we have considered the codes from Construction B which correspond to $a = 0$. Clearly

$$\mathcal{F}_2^{2^{t+1}-1} = \bigcup_{a=0}^{2^{2t+1-r}-1} \bigcup_{b=0}^{2^{r-t}-1} \mathcal{H}'_{a2^{r-t}+b}. \tag{9}$$

For $0 \le a \le 2^{2t+1-r} - 1, 0 \le b, s \le 2^{r-t} - 1$, and $0 \le j \le 2^t - 1$, where $i+j$ is taken modulo 2^t and $b+s$ is taken modulo 2^{r-t}, consider the code

$$\tilde{B}_{a2^{2r-t}+b2^r+s2^t+j} = \bigcup_{i=0}^{2^t-1} \mathcal{P}'_{a2^{r-t}+(b+s)2^t+i} \times \mathcal{B}_{s2^t+i+j}.$$

For $0 \le a \le 2^{2t+1-r} - 1$ and $0 \le b \le 2^{r-t} - 1$ consider the code

$$\tilde{Y}_{a2^{r-t}+b} = \bigcup_{s=0}^{2^{r-t}-1} \bigcup_{j=0}^{2^t-1} \tilde{B}_{a2^{2r-t}+b2^r+s2^t+j}.$$

One can easily verify from (7) that

$$\tilde{Y}_{a2^{r-t}+b} = \bigcup_{s=0}^{2^{r-t}-1} \mathcal{H}'_{a2^{r-t}+b+s} \times \mathcal{Y}_s \tag{10}$$

where $b+s$ is taken modulo 2^{r-t}. Thus, it follows from (8)–(10) that

$$\begin{aligned}&\bigcup_{a=0}^{2^{2t+1-r}-1} \bigcup_{b=0}^{2^{r-t}-1} \tilde{Y}_{a2^{r-t}+b} \\ &= \bigcup_{a=0}^{2^{2t+1-r}-1} \bigcup_{b=0}^{2^{r-t}-1} \bigcup_{s=0}^{2^{r-t}-1} \mathcal{H}'_{a2^{r-t}+b+s} \times \mathcal{Y}_s \\ &= \left(\bigcup_{a=0}^{2^{2t+1-r}-1} \bigcup_{b=0}^{2^{r-t}-1} \mathcal{H}'_{a2^{r-t}+b} \right) \times \mathcal{F}_2^n = \mathcal{F}_2^{2^{t+1}-1} \times \mathcal{F}_2^n. \end{aligned}$$

It is easy to verify that $\tilde{B}_i \cap \tilde{B}_j = \varnothing$ for $i \ne j$, and hence, $\bigcup_{i=0}^{2^{\tilde{n}}-1} \tilde{B}_i = \mathcal{F}_2^{\tilde{n}}$.

Next, we compute the parameters of these codes. $\mathcal{Y}_0 = \bigcup_{i=0}^{2^t-1} \mathcal{B}_i$, and hence, the subnorm of the family $\{\mathcal{B}_i : 0 \le i \le 2^t - 1\}$ is 4. The subnorm of the family $\{\mathcal{P}'_i(t+1) : 0 \le i \le 2^t - 1\}$ is 3. Thus, by Theorem 1, the code $\tilde{B}_0$ has the following parameters:

$$\begin{aligned}&\tilde{n} = n + 2^{t+1} - 1, \quad d = 5, \quad R = 3 \\ &|\tilde{B}_0| = |\mathcal{B}_0| \cdot |\mathcal{P}'_0(t+1)| \cdot 2^t \\ &\qquad = 2^{n-r} \cdot 2^{2^{t+1}-2(t+1)} \cdot 2^t = 2^{\tilde{n}-(r+t+1)}. \end{aligned}$$

$\mathcal{F}_2^n = \bigcup_{s=0}^{2^{r-t}-1} \mathcal{Y}_s$, and hence, the subnorm of the family $\{\mathcal{Y}_s : 0 \le s \le 2^{r-t}-1\}$ is 1. On the other hand, the subnorm of family $\{\mathcal{H}_i'(t+1) : 0 \le i \le 2^{r-t}-1\}$ is 1 if $r = 2t+1$, and 2 if $r < 2t+1$. Therefore, by Theorem 1, the code $\tilde{Y}_0$ has the following parameters:

$$\tilde{n} = n + 2^{t+1} - 1, \quad d = 2, \quad R = 1$$
$$|\tilde{Y}_0| = |\tilde{B}_0| \cdot 2^t \cdot 2^{r-t} = 2^{\tilde{n}-(r+t+1-r)} = 2^{\tilde{n}-(t+1)}.$$

Note that $\tilde{B}_i$ and $\tilde{Y}_j$ have the same parameters as $\tilde{B}_0$ and $\tilde{Y}_0$, respectively, for all i and j. Let us denote $\tilde{r} = r + t + 1$ and $\tilde{t} = r$. Furthermore, by definition

$$\tilde{Y}_j = \bigcup_{i=j2^{\tilde{t}}}^{(j+1)2^{\tilde{t}}-1} \tilde{B}_i, \qquad 0 \le j \le 2^{\tilde{r}-\tilde{t}} - 1. \qquad \square$$

Let $f_{i+2} = f_{i+1} + f_i$, $i \ge 0$, where $f_0 = f_1 = 1$, be the Fibonacci's sequence.

Theorem 4: For $r_0 \ge 5, r_0$ is odd, let $\mathcal{B}_i^0, 0 \le i \le 2^{r_0}-1$, be an $(n_0, 2^{n_0-r_0}, 5)3$ code, where

$$\bigcup_{i=0}^{2^{r_0}-1} \mathcal{B}_i^0 = \mathcal{F}_2^{n_0}.$$

For t_0 odd, $r_0 > t_0 \ge 3$, let $\mathcal{Y}_j^0, 0 \le j \le 2^{r_0-t_0} - 1$, be an $(n_0, 2^{n_0-(r_0-t_0)}, 2)1$ code, such that

$$\mathcal{Y}_j^0 = \bigcup_{i=j2^{t_0}}^{(j+1)2^{t_0}-1} \mathcal{B}_i^0.$$

Then there exists an infinite family of codes $\{\mathcal{B}^l : l \ge 0\}$, where $\mathcal{B}^l$ is a code with the following parameters:

$$\left(n_l = \sum_{i=0}^{l-1} 2^{t_i+1} + n_0 - l, 2^{n_l-r_l}, 5 \right) 3$$

where $r_l = f_l(r_0+1) + f_{l-1}(t_0+1) - 1$ and $t_l = r_{l-1}$, for $l \ge 1$.

Proof: We apply Construction B recursively with initial two sets of codes

$$\{\mathcal{B}_i^0 : 0 \le i \le 2^{r_0} - 1\}$$

and

$$\{\mathcal{Y}_j^0 : 0 \le j \le 2^{r_0-t_0} - 1\}$$

and obtain two sets of codes $\{\mathcal{B}_i^l : 0 \le i \le 2^{r_l} - 1\}$ and $\{\mathcal{Y}_j^l : 0 \le j \le 2^{r_l-t_l} - 1\}$ for each $l, l \ge 1$, where $\mathcal{B}_i^l$ is an $(n_l, 2^{n_l-r_l}, 5)3$ code and $\mathcal{Y}_j^l$ is an $(n_l, 2^{n_l-(r_l-t_l)}, 2)1$ code, with $t_l = r_{l-1}, r_l = r_{l-1} + t_{l-1} + 1$, and $n_l = n_{l-1} + 2^{t_{l-1}+1} - 1$ by Theorem 3. Then the parameters of the obtained codes satisfy the following recursive equations:

$$r_{l+2} = r_{l+1} + r_l + 1, \quad n_l = n_{l-1} + 2^{t_{l-1}+1} - 1$$

with initial conditions $n_0, t_0, r_0, r_1 = r_0 + t_0 + 1$. One can verify that the solutions for these recursive equations are

$$r_l = f_l(r_0+1) + f_{l-1}(t_0+1) - 1$$

and

$$n_l = \sum_{i=1}^{l-1} 2^{f_{i-1}(r_0+1)+f_{i-2}(t_0+1)} + 2^{t_0+1} + n_0 - l,$$

for $l \ge 1$, where $f_{-1} = 0$. $\square$

Corollary 2: The $(n_l, 2^{n_l-r_l}, 5)3$ codes $\mathcal{B}^l, l \ge 1$, obtained in Theorem 4 have odd redundancy.

The following examples apply Construction B recursively.

Example 1: Take $\mathcal{B}_0^0$ be $\mathcal{P}_0'(m)$ and $\mathcal{Y}_0^0$ be $\mathcal{H}_0'(m)$. In this case, $n_0 = 2^m - 1, r_0 = 2m - 1$, and $t_0 = m - 1$. Note that these codes meet the two bounds of Lemma 4. Thus, by Theorem 4, we have the following.

Corollary 3: For each even integer $m, m \ge 4$, there exists an infinite family of quasi-perfect codes $\{\mathcal{PD}^l(m) : l \ge 0\}$, where $\mathcal{PD}^l(m)$ is an

$$\left(n_l = \sum_{i=0}^{l} 2^{f_i m} - l - 1, 2^{n_l-(f_{l+2}m-1)}, 5 \right) 3$$

code.

Example 2: Take $\mathcal{B}_0^0$ be the code $\{000000, 111111\}$, and $\mathcal{Y}_0^0$ be the punctured Hamming code $(6, 2^4, 2)1$. In this case, $n_0 = 6, r_0 = 5$, and $t_0 = 3$. Thus, we obtain an infinite family of codes $\{\mathcal{B}^l : l \ge 0\}$, where $\mathcal{B}^l, l \ge 1$, is an

$$\left(n_l = \sum_{i=1}^{l-1} 2^{6f_{i-1}+4f_{i-2}} - l + 22, 2^{n_l-(6f_l+4f_{l-1}-1)}, 5 \right) 3$$

code.

Example 3: Let $\mathcal{B}_0^0$ be the linear code $(20, 2^{11}, 5)3$, obtained by Wagner [16] via computer search. The following matrix is a parity-check matrix H for this code which is equivalent to one found by Wagner

$$H = \left[\begin{array}{c|c} 00011111110 & 101111111 \\ 11101111111 & 010000000 \\ 11101000100 & 001000000 \\ 11011100010 & 000100000 \\ 11011010101 & 000010000 \\ 10111100101 & 000001000 \\ 10111001000 & 000000100 \\ 01111010010 & 000000010 \\ 01111001011 & 000000001 \end{array}\right].$$

Let $\mathcal{Y}_0^0$ be the $(20, 2^{18}, 2)1$ linear code with the following parity-check matrix:

$$\tilde{H} = \left[\begin{array}{c|c} 00011111110 & 101111111 \\ 11101111111 & 010000000 \end{array}\right]$$

which obtained by deleting seven rows from H. In this case, $n_0 = 20, r_0 = 9$, and $t_0 = 7$. Thus, we obtain an infinite family of codes $\{\mathcal{B}^l : l \ge 0\}$, where $\mathcal{B}^l, l \ge 1$, is an

$$\left(n_l = \sum_{i=1}^{l-1} 2^{10f_{i-1}+8f_{i-2}} - l + 276, 2^{n_l-(10f_l+8f_{l-1}-1)}, 5 \right) 3$$

code.

The following construction is due to Zaitsev *et al.*[17].

TABLE II

redundancy r	lower bound on $n^*(3,5,r)$	construction	packing density of the family
$r \equiv 0 (mod\ 8)$	$2^{\frac{r}{2}} + 2^{\frac{r}{4}} - 1$	$\mathcal{A}(\frac{r}{2}, \frac{r}{4})$	$1/2$
$r \equiv 4 (mod\ 8)$	$2^{\frac{r}{2}} + 1$	Zetterberg[11]	$1/2$
$r \equiv 2 (mod\ 4)$	$2^{\frac{r}{2}}$	Irred. Goppa[11]	$1/2$
$r \equiv 3 (mod\ 4)$	$2^{\frac{r+1}{2}} - 1$	$\mathcal{P}'_0(\frac{r+1}{2})$	1

redundancy r	upper bound on $l^*(3,5,r)$	construction	covering density of the family
$r \equiv 0 (mod\ 6)$	$2^{\frac{r+3}{3}} - 1$	$\mathcal{A}(\frac{r}{3}, \frac{r}{3})$	$4/3$
$r \equiv 2 (mod\ 6)$	$5 \cdot 2^{\frac{r-2}{3}} - 1$	$\mathcal{A}(\frac{r+4}{3}, \frac{r-2}{3})$	$125/24$
$r \equiv 4 (mod\ 6)$	$3 \cdot 2^{\frac{r-1}{3}} - 2$	Struik[15]	$9/4$
$r \equiv 5 (mod\ 6)$	$2^{\frac{r+4}{3}} - 2$	$\mathcal{PD}^1(\frac{r+1}{3})$	$8/3$

Construction C: Let $r \geq 3$ be an odd integer and $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{2^r}$ be disjoint $(n, 2^{n-r}, 5)3$ codes, such that

$$\bigcup_{i=0}^{2^r-1} \mathcal{C}_i = \mathcal{F}_2^n.$$

Define

$$\bigcup_{i=0}^{2^r-1} \mathcal{C}_i \times \mathcal{P}_i(r+1).$$

Theorem 5: [17] The code defined by Construction C is an $(n + 2^{r+1}, 2^{n+2^{r+1}-2(r+1)}, 5)3$ code, with packing density greater than $1/2$.

All the codes obtained in Theorem 4 (e.g., the codes from Examples 1–3) can be used in Construction C. Hence, we obtain many codes with various lengths and density greater than $1/2$.

To end this section, we give another construction for $(3,5)$ codes. The following lemma is well known [12], [14].

Lemma 5:

$$\mathcal{H}'(m+1) = \bigcup_{i=0}^{2^m-1} \mathcal{H}'_i(m) \times \mathcal{H}^e_i(m).$$

Lemma 6: For every even integer $m, m \geq 4$, $\mathcal{H}'(m+1)$ is a union of 2^{2m-1} disjoint $(2^{m+1} - 1, 2^{2^{m+1}-1-3m}, 5)3$ codes.

Proof: Since

$$\bigcup_{i=0}^{2^{m-1}-1} \mathcal{P}'_i(m) = \mathcal{H}'_0(m), \qquad \bigcup_{i=0}^{2^{m-1}-1} \mathcal{P}_i(m) = \mathcal{H}^e_0(m)$$

it follows by Lemma 2 that

$$\mathcal{H}'_0(m) \times \mathcal{H}^e_0(m) = \bigcup_{j=0}^{2^{m-1}-1} \bigcup_{i=0}^{2^{m-1}-1} \mathcal{P}'_i(m) \times \mathcal{P}_{i+j}(m)$$

where

$$\bigcup_{i=0}^{2^{m-1}-1} \mathcal{P}'_i(m) \times \mathcal{P}_i(m) = \mathcal{D}(m)$$

is the code defined in [5] with parameters $(2^{m+1} - 1, 2^{2^{m+1}-1-3m}, 5)3$, and by Lemma 5

$$\mathcal{H}'_0(m+1) = \bigcup_{i=0}^{2^m-1} \mathcal{H}'_i(m) \times \mathcal{H}^e_i(m)$$

which completes the proof. □

Let $\mathcal{D}_0(m) = \mathcal{D}(m)$ and $\{\mathcal{D}_i(m)\}_{i=0}^{2^{2m-1}-1}$ be a set of disjoint $(2^{m+1} - 1, 2^{2^{m+1}-1-3m}, 5)3$ codes such that

$$\bigcup_{i=0}^{2^{2m-1}-1} \mathcal{D}_i(m) = \mathcal{H}'_0(m+1).$$

Corollary 4: The family of sets $\{\mathcal{D}_i(m) : 0 \leq i \leq 2^{2m-1} - 1\}$ has subnorm 4.

Construction D: For each even $m, m \geq 4$, define

$$\mathcal{E}(m) = \bigcup_{i=0}^{2^{2m-1}-1} \mathcal{P}'_i(2m) \times \mathcal{D}_i(m).$$

By Theorem 1 we have the following.

Theorem 6: $\mathcal{E}(m)$ is a

$$(2^{2m} + 2^{m+1} - 2, 2^{2^{2m}+2^{m+1}-2-5m}, 5)3$$

code.

B. Dense and Sparse Codes

Table II presents the known lower bounds on $n^*(3,5,r)$ (top) and the known upper bounds on $l^*(3,5,r)$ (bottom).

The only codes with odd redundancy which were known are the punctured Preparata codes and the Wagner's codes [16]. We have constructed many new codes with odd redundancy (see Corollary 2). In fact, no family of codes with redundancy $r \equiv 1 \pmod 4$ was known. The code $\mathcal{PD}^j(m)$, $j \geq 0$, has redundancy $f_{j+2}m - 1$. When $j \equiv 1, 2 \pmod 3$ and $m \equiv 2 \pmod 4$, then $f_{j+2}m - 1 \equiv 1 \pmod 4$. In this way, we obtain codes for each redundancy $r > 10$, where $r \equiv 5 \pmod{12}$ or $r \equiv 9 \pmod{20}$, and so on. Unfortunately, the packing density of this family is 0 and the covering density is ∞ (unless $j = 1$).

V. Conclusion and Open Problems

Several new constructions for quasi-perfect codes with radius $R = 2, R = 3$, and distance $d = 4, d = 5$, respectively, are given. We summarized by presenting the known bounds on $l^*(R, d, r)$ and $n^*(R, d, r)$. The BDS construction has an important role in our constructions. The distance and covering radius of the code obtained is computed by Theorem 1. But the bounds of this theorem are not always tight as can be seen from the following example. Let $\mathcal{C}_0$ be a linear $(n, 2^{n-r}, 4)2$ code and $\{\mathcal{C}_i : 0 \leq i \leq 2^r - 1\}$ be the family of codes which contains $\mathcal{C}_0$ and its $2^r - 1$ cosets. Let $\mathcal{C}_i^e, 0 \leq i \leq 2^r - 1$, be the set of codewords of $\mathcal{C}_i$ with even weight. The code $\bigcup_{i=0}^{2^r-1} \mathcal{C}_i \times \mathcal{C}_i^e$ is a $(2, 4)$ code. This can be verified by noting that if H is the parity-check matrix of $\mathcal{C}_0$, then

$$\begin{bmatrix} 0 \ldots 0 & 1 \ldots 1 \\ H & H \end{bmatrix}$$

is the parity-check matrix of $\bigcup_{i=0}^{2^r-1} \mathcal{C}_i \times \mathcal{C}_i^e$. The subnorm of the family $\{\mathcal{C}_i : 0 \leq i \leq 2^r - 1\}$ is 2 and one can verify that the subnorm of the family $\{\mathcal{C}_i^e : 0 \leq i \leq 2^r - 1\}$ is at least 6 (unless $\mathcal{C}_0$ is the extended Hamming code). Thus, by Theorem 1, the distance of the code $\bigcup_{i=0}^{2^r-1} \mathcal{C}_i \times \mathcal{C}_i^e$ is at least 3 and the covering radius is at most R, where $R \geq 4$, and hence the bounds of Theorem 1 are not tight. This leads to the obvious question when the bounds of Theorem 1 can be improved. We conclude this paper with a list of open problems and more suggestions for future research.

Codes with large distance: Except for the repetition codes, the $(24, 2^{12}, 8)4$ extended Golay code, and the $(22, 2^{12}, 6)3$ punctured Golay code no quasi-perfect codes are known with distance greater than 5. Thus, the first problem we suggest is to find such codes or to prove that they do not exist.

Codes with $R = 2$ and $d = 3$: In this case, we could not find shorter codes than the nonlinear $(2, 4)$ codes obtained in Section III. However, for $r \equiv 2 \pmod 4, r = 2m + 2, m$ is even, $m \geq 4$, the $(27 \cdot 2^{m-3} - 1, 2^{27 \cdot 2^{m-3} - 3 - 2m}, 3)2$ linear codes were constructed in [3] with covering density $\frac{729}{512}$, which is smaller then the one obtained by Case B in Section III. The longest code with redundancy r is the Hamming code of length $2^r - 1$ (for which $R = 1$). Given a linear $(n, 2^{n-r}, 3)2$ code, one can obtain an $(n + i, 2^{n+i-r}, 3)2$ code for any i such that $n + i \leq 2^r - 2$ by adding i distinct columns to the parity-check matrix of the $(n, 2^{n-r}, 3)2$ code. Thus, the main two problems which remain are to find linear and nonlinear codes shorter than the known ones.

Codes with $R = 2$ and $d = 4$: We would like to see improvements on the bounds given in Section III. The main problem we suggest is to prove or disprove that there exists an n_0 such that for any given $n \geq n_0$ there exists a $(2, 4)$ code of length n. The redundancy of these codes might not be an integer. Also, we note that linear $(n, M, 4)2$ codes correspond to complete caps in projective spaces [4].

Codes with $R = 3$ and $d = 5$: We would like to see any new $(3, 5)$ codes, especially families with redundancy r congruent to 1 or 3 modulo 6 and finite covering density, and with redundancy r congruent to 1 modulo 4 and finite packing density.

Codes with noninteger redundancies: As we mentioned in the Introduction, all our codes have integer redundancies. Finding infinite families of codes with noninteger redundancies is an interesting task for itself.

Acknowledgment

The authors would like to thank two anonymous reviewers whose comments have contributed for improving the paper.

References

[1] R. A. Brualdi, V. S. Pless, and R. M. Wilson, "Short codes with a given covering radius," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 99–109, Jan. 1989.

[2] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, 1997.

[3] A. A. Davydov and A. Yu. Drozhzhina-Labinskaya, "Constructions, families, and tables of binary linear covering codes," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1270–1279, Jul. 1994.

[4] A. A. Davydov and L. M. Tombak, "Quasiperfect linear binary codes with distance 4 and complete caps in projective geometry," *Probl. Inf. Transm.*, vol. 25, no. 4, pp. 265–275, 1989.

[5] T. Etzion and G. Greenberg, "Constructions for perfect mixed codes and other covering codes," *IEEE Trans. Inf. Theory*, vol. 39, no. 1, pp. 209–214, Jan. 1993.

[6] E. M. Gabidulin, A. A. Davydov, and L. M. Tombak, "Linear codes with covering radius 2 and other new covering codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 219–224, Jan. 1991.

[7] D. C. Gorenstein, W. W. Peterson, and N. Zierler, "Two-error correcting Bose-Chaudhuri codes are quasi-perfect," *Inf. Contr.*, vol. 3, pp. 291–294, 1960.

[8] I. Honkala, "On (k,t)-subnormal covering codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 4, pp. 1203–1206, Jul. 1991.

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

[10] O. Moreno, "Further results on quasi-perfect codes related to the Goppa codes," *Congressus Numerantium*, vol. 40, pp. 249–256, 1983.

[11] ——, private communication.

[12] K. T. Phelps, "A combinatorial construction of perfect codes," *SIAM J. Alg. Discr. Meth.*, vol. 4, pp. 398–403, 1983.

[13] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 4, pp. 503–510, Jul. 1972.

[14] F. I. Solov'eva, "On binary nongroup codes" (in Russian), in *Methody Diskr. Analiza*, vol. 37, 1981, pp. 65–76.

[15] R. Struik, "Covering Codes," Ph.D. dissertation, Eindhoven Univ. Technol., Eindhoven, The Netherlands, 1994.

[16] T. J. Wagner, "A search technique for quasi-perfect codes," *Inf. Contr.*, vol. 9, pp. 94–99, 1966.

[17] 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 *Proc. 2nd Int. Symp. Information Theory*, B. N. Petrov and F. Csáki, Eds. Budapest, Hungary: Akadémiai Kiadó, 1973, pp. 257–263.