Asymptotic improvement of the Gilbert-Varshamov bound for linear codes

Philippe Gaborit[*]   Gilles Zémor[†]

August 29, 2007

Abstract

The Gilbert-Varshamov bound states that the maximum size $A_2(n,d)$ of a binary code of length n and minimum distance d satisfies $A_2(n,d) \geq 2^n/V(n,d-1)$ where $V(n,d) = \sum_{i=0}^{d} \binom{n}{i}$ stands for the volume of a Hamming ball of radius d. Recently Jiang and Vardy showed that for binary non-linear codes this bound can be improved to

$$A_2(n,d) \geq cn \frac{2^n}{V(n,d-1)}$$

for c a constant and $d/n \leq 0.499$. In this paper we show that certain asymptotic families of linear binary $[n, n/2]$ random double circulant codes satisfy the same improved Gilbert-Varshamov bound. These results were partially presented at ISIT 2006 [3].

Index terms: Double circulant codes, Gilbert-Varshamov bound, linear codes, random coding.

1 Introduction

The Gilbert-Varshamov bound asserts that the maximum size $A_q(n,d)$ of a q-ary code of length n and minimum Hamming distance d satisfies

$$A_q(n,d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i}(q-1)^i}. \tag{1}$$

This result is certainly one of the most well-known in coding theory, it was originally stated in 1952 by Gilbert [5] and improved by Varshamov in [15]. In 1982 Tsfasman, Vladuts and Zink [14] improved the GV bound on the number of codewords by an exponential factor in the block length, but this spectacular result only holds for some classes of non-binary codes. Recently Jiang and

---

[*]XLIM, Université de Limoges, 123, Av. Albert Thomas, 87000 Limoges, France. `gaborit@unilim.fr`

[†]Université de Bordeaux 1, Institut de Mathématiques de Bordeaux, 351 cours de la Libération, 33405 Talence. `zemor@math.u-bordeaux1.fr`

Vardy [6] improved the GV bound for non-linear binary codes by a linear factor in the block length n to

$$A_2(n, d) \geq cn \frac{2^n}{V(n, d-1)}, \qquad (2)$$

for $d/n \leq 0.499$, for a constant c that depends only on the ratio d/n and where $V(n, d) = \sum_{i=0}^{d} \binom{n}{i}$ stands for the volume of a Hamming ball of radius d. This new bound asymptotically surpasses previous improvements of the binary Gilbert-Varshamov bound which only managed to multiply the right hand side in (1) by a constant (see [6] for references). The method used by Jiang and Vardy relies on a graph-theoretic framework and more specifically on locally sparse graphs which are used to yield families of non-linear codes (their result was later slighlty improved in [16]). In this paper we also improve on the the the Gilbert-Varshamov bound by a linear factor in the block length but for **linear** codes, thereby solving one of the open problems of [6]. The method we use is not related to graph theory and relies on double circulant random codes.

Double circulant codes are $[2n, n]$ codes which are stable under the action of permutations composed of two circular permutations of order n acting simultaneously on two differents halves of the coordinate set. These codes can also be seen as quasi-cyclic codes, a natural generalization of cyclic codes [13]. Their study started in 1969 in [8] and since they gave some very good codes it was natural to wonder whether they could be made to satisfy the Gilbert-Varshamov bound. A first step in that direction was made by Chen, Peterson and Weldon in [1] who prove that when 2 is a primitive root of the ring $\mathbb{Z}/p\mathbb{Z}$ for p a prime, double circulant $[2p, p]$ random codes satisfy the Gilbert-Varshamov bound; unfortunately it is still unknown (this is Artin's celebrated conjecture, 1927) whether an infinity of such p exists. Later Kasami [9], building on this idea, extended the result of [1] to the case of powers of such p, and obtained a bound which is worse than the Gilbert-Varshamov bound by an exponential factor in the block length (though a very small one). Later Kasami's work was generalized to other cases in [7, 11, 12], and, in particular in [2], bounds were proven for certain classes of quasi-cyclic codes that are worse than the Gilbert-Varshamov bound only by a subexponential factor in the block length. In this paper, building anew on Kasami's idea we prove, by using a probabilistic approach, that randomly chosen double circulant codes not only satisfy the Gilbert-Varshamov bound with high probability, but also the same linear improvement as that of Jiang and Vardy (2).

The paper is organized as follows: in Section 2 we cover the main ideas involved. We start by recalling the probabilistic method for deriving lower bounds on the minimum distance of linear codes (section 2.0), then we introduce double circulant codes in section 2.1 and derive (5) an upperbound on the probability that a random double circulant code contains a non-zero vector of weight not more than a given w. In section 2.2 we study the probability that a given vector belongs to a randomly chosen double circulant code. Finally in section 2.3 we derive our improved lower bound on the minimum distance in the simple case when the codelength is $2p$ and 2 is a primitive root of $\mathbb{Z}/p\mathbb{Z}$: the result is given in Theorem 4.

in Section 3, we develop our method in the more complicated case of block-lengths $2p^m$, p a "Kasami" prime, in order to obtain an infinite family of double circulant codes with an improved minimum distance. Section 3.1 starts by giving an informal sketch of the content of section 3, which is intended to give some guidance to the reader and discuss the technical issues involved. Section 3.2 shows how to derive our main result, which is Theorem 8, from a proposition on the weight distribution of a certain class of cyclic codes. Finally section 3.3 is devoted to a proof of this last proposition.

Section 4 concludes by some comments and side results.

2   Overview of the method, the simple cases

2.0   The Gilbert Varshamov bound for linear codes and its improvement

To put the rest of the paper into perspective and introduce notation, let us recall how the probabilistic method derives the Gilbert Varshamov bound for linear codes. Rather than bounding the code size from below by a function of the minimum distance, as in (2), we fix a lower bound on the code rate and find a lower bound on the minimum distance. We limit ourselves to the rate $1/2$ case because it will be our main object of study.

Let C_{rand} be the random code of length $2n$ and dimension $k \geq n$ obtained by choosing randomly and uniformly a $n \times 2n$ parity-check matrix in $\{0,1\}^{n \times 2n}$. The probability that a given nonzero vector $\mathbf{x} = (x_1 \ldots x_{2n})$ is a codeword is clearly $1/2^n$. Let w be a positive number, not necessarily an integer. We are interested in the random variable $X(w)$ equal to the number of nonzero codewords of C_{rand} of weight not more than w. In other words

$$X(w) = \sum_{\mathbf{x} \in B_{2n}(w)} X_{\mathbf{x}} \tag{3}$$

where $B_{2n}(w)$ denotes the set of nonzero vectors $\mathbf{x}$ of $V_{2n} = \{0,1\}^{2n}$ of weight at most w, and $X_{\mathbf{x}}$ is the Bernoulli random variable equal to 1 if $\mathbf{x} \in C_{\mathrm{rand}}$ and equal to zero otherwise. Now whenever we prove that the probability $\mathrm{P}(X(w) > 0)$ is less than 1, we prove the existence of a $[2n, k, d]$ code with $k \geq n$ and $d > w$. Since the variable $X(w)$ is integer valued we have

$$\mathrm{P}(X(w) > 0) \leq \mathrm{E}\left[X(w)\right] \;=\; \sum_{\mathbf{x} \in B_{2n}(w)} \mathrm{E}\left[X_{\mathbf{x}}\right] = |B_{2n}(w)| \mathrm{P}(\mathbf{x} \in C_{\mathrm{rand}})$$

$$=\; |B_{2n}(w)| \frac{1}{2^n}.$$

Hence, for every positive integers n and w satisfying $|B_{2n}(w)| < 2^n$ there exists a linear code of parameters $[2n, n, d > w]$. Reworded, we have the following lower bound on d, essentially equivalent to (1).

Theorem 1 (GV bound) *For every positive integer n there exists a linear code of parameters $[2n, n, d]$ satisfying*

$$|B_{2n}(d)| \geq 2^n.$$

In the present paper we shall prove :

Theorem 2 *There exists a positive constant b and an infinite sequence of integers n and $[2n, n, d]$ linear codes satisfying*

$$|B_{2n}(d)| \geq bn2^n.$$

This result, equivalent to (2) for rate 1/2, will be obtained by again choosing random matrices, but from a restricted class, namely the set of parity-check matrices of double circulant codes.

2.1   Double circulant codes

A binary *double circulant code* is a $[2n, n]$ linear code C with a parity-check matrix of the form $\mathbf{H} = [\mathbf{I}_n \,|\, \mathbf{A}]$ where $\mathbf{I}_n$ is the $n \times n$ identity matrix and

$$\mathbf{A} = \begin{bmatrix} a_0 & a_{n-1} & \ldots & a_1 \\ a_1 & a_0 & \ldots & a_2 \\ a_2 & a_1 & \ldots & a_3 \\ \cdots\cdots\cdots\cdots\cdots \\ a_{n-1} & a_{n-2} & \ldots & a_0 \end{bmatrix}.$$

There is a natural action of the group $\mathbb{Z}/n\mathbb{Z}$ on the space $V_{2n} = \{0,1\}^{2n}$ of vectors $\mathbf{x} = (x_1 \ldots x_n, x_{n+1} \ldots x_{2n})$ namely,

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \times V_{2n} &\rightarrow V_{2n} \\ (j, \mathbf{x}) &\mapsto j \cdot \mathbf{x} \end{aligned}$$

where

$$1 \cdot \mathbf{x} = (x_n, x_1 \ldots x_{n-1}, x_{2n}, x_{n+1}, \ldots x_{2n-1})$$

and $j \cdot \mathbf{x} = (j-1) \cdot (1 \cdot \mathbf{x})$. The double circulant code C is clearly invariant under this group action. Consider now C to be the random code C_{rand} obtained by choosing the vector $\mathbf{a} = (a_0 \ldots a_{n-1})$ randomly and uniformly in $\{0,1\}^n$. As before, we are interested in the random variable $X(w)$ defined by (3) and equal to the number of nonzero codewords of C_{rand} of weight not more than w. We are interested in the maximum value of w for which we can claim that $\mathrm{P}(X(w) > 0) < 1$, for this will prove the existence of codes of parameters $[2n, n, d > w]$. The core remark is now that, if $\mathbf{y} = j \cdot \mathbf{x}$, then

$$X_{\mathbf{y}} = X_{\mathbf{x}}$$

where $X_{\mathbf{x}}$ ($X_{\mathbf{x}}$) is the Bernoulli random variable equal to 1 if $\mathbf{x} \in C_{\mathrm{rand}}$ ($\mathbf{y} \in C_{\mathrm{rand}}$) and equal to zero otherwise. Let now $B'_{2n}(w)$ be a set of representatives of the orbits of the elements of $B_{2n}(w)$, i.e. for any $\mathbf{x} \in B_{2n}(w)$, $|\{j \cdot \mathbf{x}, j \in \mathbb{Z}/n\mathbb{Z}\} \cap B'_{2n}(w)| = 1$. We clearly have $X(w) > 0$ if and only if $X'(w) > 0$ where

$$X'(w) = \sum_{\mathbf{x} \in B'_{2n}(w)} X_{\mathbf{x}}.$$

4

Denote by $\ell(\mathbf{x})$ the length (size) of the orbit of $\mathbf{x}$, i.e. $\ell(\mathbf{x}) = \#\{j \cdot \mathbf{x}, j \in \mathbb{Z}/n\mathbb{Z}\}$. We have

$$X'(w) = \sum_{\mathbf{x} \in B_{2n}(w)} \frac{X_{\mathbf{x}}}{\ell(\mathbf{x})} \tag{4}$$

By writing $P(X(w) > 0) = P(X'(w) > 0) \leq E[X'(w)]$, together with (4) we obtain

$$P(X(w) > 0) \leq \sum_{d|n} \sum_{\substack{\mathrm{wt}(\mathbf{x}) \leq w \\ \ell(\mathbf{x})=d}} \frac{E[X_{\mathbf{x}}]}{d}. \tag{5}$$

Suppose in particular that n is a prime, in that case orbits are of size 1 or n, and if $w < n$ then clearly the orbit of $\mathbf{x}$ has size n for any $\mathbf{x} \in B_{2n}(w)$, so that (5) becomes

$$P(X(w) > 0) \leq E[X(w)]/n.$$

If we can manage to prove that

$$E[X(w)] \leq |B_{2n}(w)| \frac{c}{2^n} \tag{6}$$

for constant c, then we will have proved the existence of double circulant codes of parameters $[2n, n, d > w]$, for any w such that $|B_{2n}(w)| < \frac{1}{c} n 2^n$.

2.2 The behaviour of $P(\mathbf{x} \in C_{\mathrm{rand}})$

To prove equality (6) we need to study carefully the quantities $E[X_{\mathbf{x}}]$, for $\mathbf{x} \in B_{2n}(w)$, since

$$E[X(w)] = \sum_{\mathbf{x} \in B_{2n}(w)} E[X_{\mathbf{x}}].$$

For $\mathbf{x} \in V_{2n}$, let us write $\mathbf{x} = (\mathbf{x}_L, \mathbf{x}_R)$ with $\mathbf{x}_L, \mathbf{x}_R \in \{0,1\}^n$. Consider the syndrome function σ

$$\begin{aligned} \sigma : V_{2n} &\rightarrow V_n \\ \mathbf{x} &\mapsto \sigma(\mathbf{x}) = \mathbf{x}\,{}^t\mathbf{H} = \sigma_L(\mathbf{x}) + \sigma_R(\mathbf{x}) \end{aligned}$$

where $\sigma_L(\mathbf{x}) = \mathbf{x}_L$ and $\sigma_R(\mathbf{x}) = \mathbf{x}_R\,{}^t\mathbf{A}$.

For any binary vector of length n, $\mathbf{u} = (u_0, \ldots, u_{n-1})$, denote by $\mathbf{u}(Z) = u_0 + u_1 Z + \cdots + u_{n-1}Z^{n-1}$ its polynomial representation in the ring $\mathbb{F}_2[Z]/(Z^n + 1)$. For any $\mathbf{u} \in V_n$, let $C(\mathbf{u})$ denote the cyclic code of length n generated by the polynomial representation $\mathbf{u}(Z)$ of $\mathbf{u}$. Since $\sigma_R(\mathbf{x})$ has polynomial representation equal to $\mathbf{x}_R(Z)\mathbf{a}(Z)$, we obtain easily

Lemma 3 *The right syndrome $\sigma_R(\mathbf{x})$ of any given $\mathbf{x} \in V_{2n}$ is uniformly distributed in the cyclic code $C(\mathbf{x}_R)$. Therefore, the probability $P(\mathbf{x} \in C_{\mathrm{rand}})$ that $\mathbf{x}$ is a codeword of the random code C_{rand} is*

- $P(\mathbf{x} \in C_{\mathrm{rand}}) = 1/|C(\mathbf{x}_R)|$ *if* $\mathbf{x}_L \in C(\mathbf{x}_R)$,
- $P(\mathbf{x} \in C_{\mathrm{rand}}) = 0$ *if* $\mathbf{x}_L \notin C(\mathbf{x}_R)$.

2.3 The case n prime and 2 primitive modulo n

If n is prime and 2 is primitive modulo n then, over $\mathbb{F}_2[Z]$, the factorization of $Z^n + 1$ into irreducible polynomials is

$$Z^n + 1 = (1 + Z)(1 + Z + Z^2 + \cdots + Z^{n-1})$$

and there is only one non-trivial cyclic code of length n, namely the $[n, n - 1, 2]$ even-weight code. Therefore $\mathrm{P}(X(w) > 0) = \mathrm{P}(X'(w) > 0) \leq \mathrm{E}\,[X'(w)]$ together with (4) and Lemma 3 give

$$\mathrm{P}(X(w) > 0) \quad \leq \quad \sum_{\substack{\mathrm{wt}(\mathbf{x}_L) + \mathrm{wt}(\mathbf{x}_R) \leq w \\ \mathrm{wt}(\mathbf{x}_R) \text{ odd}}} \frac{1}{n2^n} + \sum_{\substack{\mathrm{wt}(\mathbf{x}_L) + \mathrm{wt}(\mathbf{x}_R) \leq w \\ \mathrm{wt}(\mathbf{x}_R) \text{ even} \\ \mathrm{wt}(\mathbf{x}_L) \text{ even}}} \frac{1}{n2^{n-1}} \qquad (7)$$

$$\mathrm{P}(X(w) > 0) \quad \leq \quad 2|B_{2n}(w)| \frac{1}{n2^n}.$$

We therefore have the following result:

Theorem 4 *If p is prime and 2 is primitive modulo p, then there exist double circulant codes of parameters $[2p, p, d > w]$ for any positive number w such that*

$$2|B_{2p}(w)| < p2^p.$$

Unfortunately, it is not known (though it is conjectured) whether there exists an infinite family of primes p for which 2 is primitive modulo p. Therefore, to obtain Theorem 2 we will envisage cases when n is non-prime. This will involve two technical difficulties, namely dealing with non-trivial divisors d of n in (5), and non-trivial cyclic codes $C(\mathbf{x}_R)$ of length n in Lemma 3.

3 An infinite family of double circulant codes

3.1 Preview

In this section we will study the behaviour of the minimum distance of random double circulant codes for the infinite sequences of blocklengths $2n$ introduced by Kasami : we will have $n = p^m$ for suitably chosen p. We will first specialise inequality (5) to this case, for which all the possible orbit sizes ℓ are powers of p, p^s, $s \leq m$. Applying Lemma 3 will lead us to an upper bound (13) on $\mathrm{P}(X(w) > 0)$ that involves the weight distributions of the cyclic codes of length n. This upper bound can be essentially thought of as the same as (7), plus a number of parasite terms involving all vectors $\mathbf{x} = (\mathbf{x}_L, \mathbf{x}_R)$ of $B_{2n}(w)$ for which both $\mathbf{x}_L$ and $\mathbf{x}_R$ are codewords of some cyclic code of length n that is neither the whole space $\{0, 1\}^n$ nor the $[n, n - 1, 2]$ even-weight subcode. The problem at hand is to control the parasite terms so that they do not pollute too much the main term i.e. the right hand side of (7). To do this, the crucial part will be to bound from above with enough precision terms of the form

$$\sum_{i+j \leq w} A_i(C) A_j(C) \frac{1}{|C|} \qquad (8)$$

where C is a cyclic code of length n and $A_i(C)$ is the number of codewords of weight i. In section 3.2 we shall state such an upper bound, namely Proposition 5, and show how it leads to the desired result which will be embodied by Theorem 8.

Section 3.3 will then be devoted to proving Proposition 5. It is not easy in general to estimate the weight distribution of cyclic codes that don't have extra properties, but it turns out that for these particular code lengths of the form $n = p^m$, all cyclic codes C have a special degenerate structure. Either C consists of a collection of vectors of the form $(x, x, \ldots, x)$ where x is a subvector of length n/p and is repeated p times, or C is the dual of such a code. Section 3.2 will have reduced the problem to the latter class of cyclic codes only. Ideally, we would like to claim that the cyclic codes C have a binomial distribution of weights, i.e. $A_i(C) \approx \frac{|C|}{2^n} \binom{n}{i}$, however this is not true, the cyclic codes C have many more low-weight codewords than would be dictated by the binomial distribution. The problem of the unbalanced couples (i, j), (i small and j large or vice versa) in the sum (8) is therefore dealt with by the trivial upper bound $A_i(C) \leq \binom{n}{i}$: Lemma 11 will show that these terms account for a sufficiently small fraction of $|B_{2n}(w)|/2^n$. Lemma 10 is the central result of section 3.3 which gives a more refined upper bound on $A_i(C)$ for i well enough separated from 0, i.e. $i \geq \kappa n$ for constant positive κ. Fortunately, we do not need $A_i(C)$ to be too close to the binomial distribution, and the cruder upper bound of Lemma 11 will suffice to derive Proposition 5.

3.2 Reducing the problem to the study of the weight distribution of certain cyclic codes

Following Kasami [9], let us consider n of the form $n = p^m$ where 2 is primitive modulo p and $2^{p-1} \neq 1 \bmod p^2$. It will be implicit that all the primes p considered in the remainder of section 3 will satisfy this property. Let us also suppose $m \geq 2$, since the case $m = 1$ is covered by Theorem 4.

It is known [9] that the irreducible factors of $Z^n + 1$ in $\mathbb{F}_2[Z]$ are $1 + Z$ together with all the polynomials of the form

$$1 + Q(Z) + Q(Z)^2 + \cdots Q(Z)^{p-1} \tag{9}$$

for $Q(Z) = Z, = Z^p, Z^{p^2}, \ldots, Z^{p^{m-1}}$.

Since n is a prime power, (5) gets rewritten through Lemma 3 as:

$$P(X(w) > 0) \leq \sum_{s=1}^{m} \sum_{\substack{\mathrm{wt}(\mathbf{x}) \leq w \\ \ell(\mathbf{x}) = p^s \\ C(\mathbf{x}_L) \subset C(\mathbf{x}_R)}} \frac{1}{p^s |C(\mathbf{x}_R)|} \tag{10}$$

Note that $\mathbf{x} \in V_{2n}$ has orbit length $\ell(\mathbf{x}) < n$ if and only if both $\mathbf{x}_L$ and $\mathbf{x}_R$ are made up of p successive identical subvectors of length n/p. Equivalently $\mathbf{x}_L$ and $\mathbf{x}_R$ each belong to the cyclic code generated by the polynomial

$$P_n(Z) = 1 + Z^{n/p} + Z^{2n/p} + \cdots + Z^{(p-1)n/p}. \tag{11}$$

Let $\mathcal{C}_n$ denote the set of those cyclic codes of length n whose generator poly-nomial is *not* a multiple of $P_n(Z)$. All the other cyclic codes of length n are obtained by duplicating p times some cyclic code of length n/p. Therefore, for $s = m$, the inner sum in (10) can be bounded from above by:

$$\sum_{C \in \mathcal{C}_n} \sum_{i+j \leq w} A_i(C) A_j(C) \frac{1}{n|C|} \tag{12}$$

where $A_i(C)$ denotes the number of codewords of C of weight i. Applying (12) recursively, we obtain from (10)

$$\mathrm{P}(X(w) > 0) \leq \sum_{s=0}^{m-1} \sum_{C \in \mathcal{C}_{n/p^s}} \sum_{i+j \leq w/p^s} A_i(C) A_j(C) \frac{1}{|C| n/p^s}. \tag{13}$$

We now proceed to evaluate the righthandside of (13). The most technical part of our proof of Theorem 2 is contained in the following Proposition.

Proposition 5 *There exist positive constants q, K, c_1 and $\gamma < 1$ such that, for any $n = p^m$ with $p \geq q$, we have $|B_{2n}(2Kn)| \leq 2^n$ and for any positive real number w, $K \leq w/2n \leq 1/4$, and for any cyclic code C of $\mathcal{C}_n$, we have*

$$\sum_{i+j \leq w} A_i(C) A_j(C) \frac{1}{|C|} \leq c_1 \frac{|B_{2n}(w)|}{2^n} \gamma^{n - \dim C}.$$

Suitable numerical values of the constants are $q = 14^3$, $K = 0.1$, $\gamma = 1/2^{1/5}$, $c_1 = 2^{6/5}$.

Before proving Proposition 5, let us derive the consequences on the proba-bility $\mathrm{P}(X(w) > 0)$. That will lead us to our main result, namely Theorem 8, the consequence of which is Theorem 2. We have:

Lemma 6 *There exists a constant c_2 such that, for any $n = p^m$, $p > q$, and for any $K \leq w/2n \leq 1/4$,*

$$\sum_{C \in \mathcal{C}_n} \sum_{i+j \leq w} A_i(C) A_j(C) \frac{1}{|C|} \leq c_2 \frac{|B_{2n}(w)|}{2^n}.$$

A suitable numerical value for c_2 is $c_2 = 4.3$.

Proof: From Proposition 5 it is enough to show that the sum $\sum_{C \in \mathcal{C}_n} \gamma^{n - \dim C}$ is upperbounded by a constant for any $\gamma < 1$. Choosing a code C in $\mathcal{C}_n$ is equivalent to choosing its generator polynomial, and from the list (9) of irreducible factors of $Z^n + 1$, we see that if we order all possible generator polynomials by increasing degrees, we have 1 and $1 + Z$, then 2 polynomials of degree at least $p - 1$, then 4 polynomials of degree at least $p(p - 1)$, ... then 2^i

8

polynomials of degree at least $p(p-1)^{i-1}$ and so on. Therefore, since $n - \dim C$ equals the degree of the generator polynomial, we obtain

$$
\begin{aligned}
\sum_{C \in \mathcal{C}_n} \gamma^{n-\dim C} &\leq 1 + \gamma + 2\gamma^{p-1} + \sum_{i \geq 2} 2^i \gamma^{p(p-1)^{i-1}} \\
&\leq 1 + \gamma + 2\gamma^{p-1} + \left(\frac{2}{p-1}\right)^2 \sum_{i \geq 2} (p-1)^i \gamma^{(p-1)^i} \\
&\leq 1 + \gamma + 2\gamma^{p-1} + \left(\frac{2}{p-1}\right)^2 \sum_{j \geq 1} j\gamma^j \\
&\leq 1 + \gamma + 2\gamma^{p-1} + \left(\frac{2}{p-1}\right)^2 \frac{\gamma}{(1-\gamma)^2}.
\end{aligned}
$$

With the values $\gamma = 2^{1/5}$, $c_1 = 2^{6/5}$ and $p \geq 14^3$ given in Proposition 5 we obtain that $c_2 = 4.3$ is suitable. ∎

From (13) and Lemma 6 we obtain that

$$
\mathrm{P}(X(w) > 0) \leq c_2 \frac{1}{n} \frac{|B_{2n}(w)|}{2^n} + c_2 \sum_{s=1}^{m-1} \frac{p^s}{n} \frac{|B_{2n/p^s}(w/p^s)|}{2^{n/p^s}} \tag{14}
$$

to deal with this last sum we invoke:

Lemma 7 *For any prime $p > 14^3$ and for any positive number w such that $|B_{2n}(w)| \leq n2^n$, we have*

$$
\sum_{s=1}^{m-1} \frac{p^s}{n} \frac{|B_{2n/p^s}(w/p^s)|}{2^{n/p^s}} \leq \frac{2}{p}
$$

Proof: Choose p times a vector of length $2n/p$ and weight not more than w/p: concatenate the resulting vectors and one obtains a vector of length $2n$ and weight not more than w. Therefore $|B_{2n/p}(w/p)|^p \leq |B_{2n}(w)|$ and we have

$$
\sum_{s=1}^{m-1} \frac{p^s}{n} \frac{|B_{2n/p^s}(w/p^s)|}{2^{n/p^s}} \leq \sum_{s=1}^{m-1} \frac{p^s}{n} \left(\frac{|B_{2n}(w)|}{2^n}\right)^{1/p^s} \leq \sum_{s=1}^{m-1} \frac{p^s}{n} n^{1/p^s}.
$$

The result follows from routine computations. ∎

We see therefore from (14) and Lemma 7 that, if we choose w such that $|B_{2n}(w)| \leq bn2^n$, for $b < 1$, then, provided the conditions of Proposition 5 are satisfied, we have $\mathrm{P}(X(w) > 0) \leq bc_2 + 2c_2/p$. For $c_2 = 4.3$ and any $p > 14^3$ this quantity is less than 1 when $b \leq 0.23$. The largest w for which $|B_{2n}(w)| \leq bn2^n$ is readily seen to satisfy $K \leq \frac{w}{2n} \leq \frac{1}{4}$ which means that all conditions of Proposition 5 are satisfied, so that we have proved:

Theorem 8 *There exist positive constants $b \leq 0.23$ and q, such that for any prime $p \geq q$ such that 2 is primitive modulo p and $2^{p-1} \neq 1 \bmod p^2$, and for any power $n = p^m$ of p, there exist double circulant codes of parameters $[2n, n, d > w]$ for any w such that $|B_{2n}(w)| \leq bn2^n$. A suitable value of q is $q = 14^3$ and the first suitable prime p is $p = 2789$.*

3.3 Proof of Proposition 5

Our remaining task is now to prove Proposition 5. We start by noting that Proposition 5 is stated with a positive real number w, because the discussion starting from (13) involves balls of non-integer radius. However, it clearly is enough to prove it only for integer values of w.

The crucial part of the proof will be to bound from above the weight distribution of C, for $C \in \mathcal{C}_n$. Let us note that, since the polynomial $P_n(Z)$ defined in (11) is an irreducible factor of $Z^n + 1$, the code C belongs to $\mathcal{C}_n$ if and only if $P_n(Z)$ divides the generator polynomial of the dual code $C^\perp$. This means that any codeword of $C^\perp$ must be obtained by repeating p times a subvector of length n/p. Equivalently, a generating matrix of $C^\perp$, i.e. a parity-check matrix of C is of the form

$$\mathbf{H}_C = [\mathbf{A} \mid \mathbf{A} \mid \cdots \mid \mathbf{A}]$$

meaning that it equals the concatenation of p identical copies of an $r \times n/p$ matrix $\mathbf{A}$.

We shall need the following lemma.

Lemma 9 *Let $\mathbf{H}_{tr} = [\mathbf{I}_r \mid \mathbf{I}_r \mid \cdots \mid \mathbf{I}_r]$ be the $r \times tr$ matrix obtained by concatenating t copies of the $r \times r$ identity matrix. Let σ_{tr} be the associated syndrome function:*

$$\sigma_{tr} : \{0,1\}^{tr} \to \{0,1\}^r$$
$$\mathbf{x} \mapsto \sigma_{tr}(\mathbf{x}) = \mathbf{x}\,{}^t\mathbf{H}_{tr}.$$

Let $w \leq tr$ be an integer. Then, for any $\mathbf{s} \in \{0,1\}^r$, the number of vectors of length tr and of weight w that map to $\mathbf{s}$ by σ_{tr} is not more than:

$$\sqrt{2rt}\left(\frac{1 + |1 - 2\omega|^t}{2}\right)^r \binom{tr}{w}$$

where $w = \omega tr$.

Proof: Let $\mathbf{X}$ be a random vector of length tr obtained by choosing independently each of its coordinates to equal 1 with probability ω. The probabilities that any given coordinate of $\sigma_{tr}(\mathbf{X})$ equals 0 or 1 are those of a sum of t independent Bernoulli random variables of parameter ω, namely:

$$\frac{1 + (1 - 2\omega)^t}{2} \qquad \text{and} \qquad \frac{1 - (1 - 2\omega)^t}{2}.$$

Since all the coordinates of $\sigma_{tr}(\mathbf{X})$ are clearly independent,

$$\max_{\mathbf{s} \in \{0,1\}^r} \mathrm{P}(\sigma_{tr}(\mathbf{X}) = \mathbf{s}) = \left(\frac{1 + |1 - 2\omega|^t}{2}\right)^r. \tag{15}$$

Now let $W = \mathrm{wt}\,(\mathbf{X})$ be the weight of $\mathbf{X}$. We have

$$\mathrm{P}(W = w) = \binom{tr}{w}\omega^w(1 - \omega)^{tr-w} = \binom{tr}{\omega tr}2^{-trh(\omega)}$$

where h denotes the binary entropy function, $h(x) = -x \log_2 x - (1-x) \log_2(1-x)$. By a variant of Stirling's formula [13][Ch. 10,§11,Lemma 7]

$$\binom{n}{w} \geq 2^{nh(\omega)}/\sqrt{8n\omega(1-\omega)}, \qquad (16)$$

therefore:

$$P(W = w) \geq \frac{1}{\sqrt{8tr\omega(1-\omega)}} \geq \frac{1}{\sqrt{2tr}}.$$

For given $\mathbf{s}$, let N_w denote the number of vectors of length tr and weight w that have syndrome $\mathbf{s}$. Since $P(\sigma_{tr}(\mathbf{X}) = \mathbf{s} \mid W = w) = N_w/\binom{tr}{w}$ we have

$$P(\sigma_{tr}(\mathbf{X}) = \mathbf{s}) \geq P(\sigma_{tr}(\mathbf{X}) = \mathbf{s} \mid W = w) P(W = w) \geq \frac{N_w}{\binom{tr}{w}} \frac{1}{\sqrt{2tr}}.$$

Hence, by (15),

$$N_w \leq \sqrt{2tr} \left(\frac{1 + |1 - 2\omega|^t}{2}\right)^r \binom{tr}{w}$$

which is the claimed result. ∎

Lemma 10 *Let $0 < \kappa < 1/4$. There exist q, such that for any $p > q$, $n = p^m$, and for any code $C \in \mathcal{C}_n$, the following holds:*

- *either $C = \{0,1\}^n$ or C equals the even-weight code,*

- *or, the weight distribution of C satisfies, for any i, $\kappa n \leq i \leq n/2$,*

$$A_i(C) \leq \frac{1}{2^{3r/5}} \binom{n}{i}$$

where $r = n - \dim C$.

For $\kappa = 0.07$ a suitable value of q is $q = 14^3$.

Proof: If $r = 0$ or $r = 1$, i.e. C equals the whole space $\{0,1\}^n$ or the even-weight code, there is nothing to prove. Suppose therefore $r > 1$. From the factorization (9) of $Z^n + 1$ into irreducible factors we see that we must have $r \geq p - 1$. From the discussion preceding Lemma 9 we must have

$$r \leq n - p^{m-1}(p - 1) = n/p \qquad (17)$$

and a parity-check matrix of C is made up of p identical copies of some $r \times n/p$ matrix $\mathbf{A}$. Therefore, after permuting coordinates, there exists a parity-check matrix of C of the form

$$\mathbf{H}_C = [\mathbf{B} \mid \mathbf{I}_r \mid \mathbf{I}_r \mid \cdots \mid \mathbf{I}_r]$$

where $\mathbf{B}$ is some $r \times (n - rt)$ matrix and is followed by t copies of the $r \times r$ identity matrix. The integer t can be chosen to take any value such that $1 \leq t \leq p$: we shall impose the restriction

$$t \leq p^{1/3}. \qquad (18)$$

For any $\mathbf{x} \in \{0,1\}^n$, write $\mathbf{x} = (\mathbf{x}_1, \mathbf{x}_2)$ where $\mathbf{x}_1$ is the vector made up of the first $n - tr$ coordinates of $\mathbf{x}$ and $\mathbf{x}_2$ consists of the remaining tr coordinates Now the syndrome function σ associated to $\mathbf{H}_C$ takes the vector $\mathbf{x} \in \{0,1\}^n$ to $\sigma(\mathbf{x}) = \mathbf{x}_1{}^t B + \sigma_{tr}(\mathbf{x}_2)$ where σ_{tr} is the function defined in Lemma 9. The code C is the set of vectors $\mathbf{x}$ such that $\sigma(\mathbf{x}) = 0$, therefore by partitioning the set of vectors of weight i into all possible values of $\mathbf{x}_1$ we have, from Lemma 9:

$$A_i(C) \leq \sqrt{2tr} \sum_{j=0}^{tr} \left(\frac{1 + |1 - 2\frac{j}{tr}|^t}{2} \right)^r \binom{tr}{j} \binom{n - tr}{i - j} \tag{19}$$

for any i such that

$$i \geq tr. \tag{20}$$

Notice that:

$$\binom{tr}{j} \binom{n - tr}{i - j} = \frac{\binom{i}{j} \binom{n-i}{tr-j}}{\binom{n}{tr}} \binom{n}{i}$$

so that (19) becomes

$$A_i(C) \leq \sqrt{2tr} \sum_{j=0}^{tr} \left(\frac{1 + |1 - 2\frac{j}{tr}|^t}{2} \right)^r \frac{\binom{i}{j} \binom{n-i}{tr-j}}{\binom{n}{tr}} \binom{n}{i}$$

$$\leq \sqrt{2tr}(tr + 1) \binom{n}{i} \max_{0 \leq j \leq tr} \left(\frac{1 + |1 - 2\frac{j}{tr}|^t}{2} \right)^r \frac{\binom{i}{j} \binom{n-i}{tr-j}}{\binom{n}{tr}}. \tag{21}$$

Set $i = \iota n$ and $j = \alpha tr$, we have:

$$\frac{\binom{i}{j} \binom{n-i}{tr-j}}{\binom{n}{tr}} \leq \frac{i^j (n-i)^{tr-j}}{\binom{n}{tr} j! (tr-j)!}$$

$$\leq \frac{\iota^j (1 - \iota)^{tr-j} n^{tr}}{\binom{n}{tr} j! (tr-j)!}$$

$$\leq \frac{\iota^j (1 - \iota)^{tr-j} n^{tr}}{(n - tr)^{tr} \binom{tr}{j}^{-1}} \qquad \text{since } \binom{n}{tr} \geq (n - tr)^{tr}/(tr)!$$

$$\leq \frac{\iota^j (1 - \iota)^{tr-j} \binom{tr}{j}}{(1 - \frac{tr}{n})^{tr}}.$$

We have seen (17) that $r \leq n/p$ and $t \leq p^{1/3}$ (condition (18)), therefore $tr/n \leq 1/p^{2/3} \leq 1/2$: by using the inequality $1 - x \geq 2^{-2x}$, valid whenever $0 \leq x \leq 1/2$, we therefore have

$$\frac{\binom{i}{j} \binom{n-i}{tr-j}}{\binom{n}{tr}} \leq 2^{2t^2 r^2/n} \iota^j (1 - \iota)^{tr-j} \binom{tr}{j}$$

and by using $\binom{tr}{j} \leq 2^{trh(\alpha)}$ we finally get

$$\frac{\binom{i}{j} \binom{n-i}{tr-j}}{\binom{n}{tr}} \leq 2^{tr(\frac{2tr}{n} - D(\alpha||\iota))}$$

where $D(x||y) = x \log_2 \frac{x}{y} + (1 - x) \log_2 \frac{1-x}{1-y}$. Together with (21) we get:

$$A_i(C) \leq 2^{r(\beta + f(\iota))} \frac{1}{2^r} \binom{n}{i}$$

with

$$f(\iota) = \max_{0 \leq \alpha \leq 1} g(\alpha, \iota) \tag{22}$$

$$\text{where} \qquad g(\alpha, \iota) = \log_2(1 + |1 - 2\alpha|^t) - tD(\alpha||\iota) \tag{23}$$

and $\beta = \frac{1}{r} \log_2 \sqrt{2tr} + \frac{1}{r} \log_2(tr + 1) + 2t^2 r/n$. Write $\log_2(tr + 1) \leq 1 + \log_2 tr$ to get $\beta \leq (\frac{3}{2} + \frac{3}{2} \log_2(tr))/r + 2t^2 r/n$. By using $t < p^{1/3}$ and $p - 1 \leq r \leq n/p$, we get

$$\frac{3}{2} \frac{\log_2 tr}{r} < \frac{3}{2} \frac{\log_2(r+1)^{4/3}}{r} = 2 \frac{\log_2(r+1)}{r} \leq 2 \frac{\log_2 p}{p-1}$$

and

$$\beta \leq \frac{3}{2(p-1)} + \frac{2 \log_2 p}{p-1} + \frac{2}{p^{1/3}}.$$

We see that β can be made arbitrarily small by increasing the value of p. A numerical computation gives us $\beta < 0.152$ for all $p > 14^3$.

Since we have supposed $i \leq n/2$, we have $\iota \leq 1/2$ so that the definition (22) and (23) of f can be replaced by the equivalent

$$f(\iota) = \max_{0 \leq \alpha \leq \iota} g(\alpha, \iota)$$

$$g(\alpha, \iota) = \log_2(1 + (1 - 2\alpha)^t) - tD(\alpha||\iota)$$

from which we easily see that g and f are decreasing functions of ι. We see that $f(\kappa)$ can be made arbitrarily small, for all $\kappa > 0$, by choosing t big enough. Numerically, by choosing $t = 14$, $\kappa = 0.07$ and $p > 14^3$, we see that (20) is satisfied and we get, for all $0.07 \leq \iota$, $f(\iota) \leq f(\kappa) \leq 0.24$. We obtain therefore that, for all $\kappa n \leq i \leq n/2$,

$$A_i(C) \leq 2^{-0.608r} \binom{n}{i}$$

which proves the lemma. ∎

To prove Proposition 5, we need a final technical lemma, of a purely enumerative nature.

Lemma 11 *Let $0 < \kappa < K < 1/4$. There exist an integer n_0 and $\varepsilon > 0$ such that, for any $n \geq n_0$, $w = 2\omega n$ with $K \leq \omega < 1/4$,*

$$2 \sum_{\substack{i+j \leq w \\ i < \kappa n}} \binom{n}{i} \binom{n}{j} \leq \frac{1}{2^{\varepsilon n}} |B_{2n}(w)|.$$

For $\kappa = 0.07$, $K = 0.1$, $n_0 = 14^3$, a suitable value of ε is $\varepsilon = 0.004$.

Proof: Clearly we have:

$$2 \sum_{\substack{i+j \leq w \\ i < \kappa n}} \binom{n}{i}\binom{n}{j} \; \leq \; \kappa n^2 \binom{n}{\kappa n}\binom{n}{w - \kappa n}$$

$$\leq \; \kappa n^2 2^{n(h(\kappa)+h(2\omega-\kappa))} = \frac{\kappa n^2 2^{2nh(\omega)}}{2^{n(2h(\omega)-h(\kappa)-h(2\omega-\kappa))}}$$

$$\leq \; \kappa n^2 \frac{2^{2nh(\omega)}}{2^{n(2h(K)-h(\kappa)-h(2K-\kappa))}}$$

since $2h(\omega) - h(\kappa) - h(2\omega - \kappa)$ is an increasing function of ω. By (16) we have $2^{2nh(\omega)} \leq \sqrt{16n}|B_{2n}(w)|$, so that we obtain, since $\kappa \leq 1/4$,

$$2 \sum_{\substack{i+j \leq w \\ i < \kappa n}} \binom{n}{i}\binom{n}{j} \leq n^{5/2} \frac{|B_{2n}(w)|}{2^{n(2h(K)-h(\kappa)-h(2K-\kappa))}} \leq \frac{|B_{2n}(w)|}{2^{\varepsilon n}}$$

for any $n \geq n_0$ with $\varepsilon \leq 2h(K) - h(\kappa) - h(2K - \kappa) - \frac{5}{2}\frac{\log_2 n_0}{n_0}$. ∎

Proof of Proposition 5:   If $C = \{0,1\}^n$ or if C is the even-weight subcode, then $A_i(C) \leq \binom{n}{i}$, and $\sum_{i+j \leq w} A_i(C)A_j(C) \leq \sum_{i+j \leq w} \binom{n}{i}\binom{n}{j} = |B_{2n}(w)|$. The result clearly holds for any $c_1 \geq 2/\gamma$.

Let $C \in \mathcal{C}_n$ with $r = n - \dim C > 1$. Let us write:

$$\frac{1}{|C|} \sum_{i+j \leq w} A_i(C)A_j(C) = S_1 + S_2$$

with

$$S_1 = \frac{1}{|C|} \sum_{\substack{i+j \leq w \\ \kappa n \leq i,j}} A_i(C)A_j(C) \qquad \text{and} \qquad S_2 = \frac{2}{|C|} \sum_{\substack{i+j \leq w \\ i < \kappa n}} A_i(C)A_j(C).$$

By Lemma 10 we have

$$S_1 \leq \frac{1}{|C|} \sum_{i+j \leq w} \binom{n}{i}\binom{n}{j}\frac{1}{2^{6r/5}} \leq \frac{|B_{2n}(w)|}{2^n}\frac{1}{2^{r/5}}.$$

To upperbound S_2 we simply write $A_i(C) \leq \binom{n}{i}$. By Lemma 11, we have

$$S_2 \leq \frac{|B_{2n}(w)|}{2^n}\frac{2^r}{2^{\varepsilon n}} = \frac{|B_{2n}(w)|}{2^n}\frac{2^r}{(2^{\varepsilon p})^{n/p}} \leq \frac{|B_{2n}(w)|}{2^n}\frac{2^r}{(2^{\varepsilon p})^r}$$

since we have seen (17) that $r \leq n/p$. By choosing $p \geq \frac{6}{5\varepsilon}$ we obtain

$$S_2 \leq \frac{|B_{2n}(w)|}{2^n}\frac{1}{2^{r/5}}.$$

This proves the result with $\gamma = 1/2^{1/5}$ and $c_1 = 2^{6/5}$. ∎

4   Comments

The probabilistic method we used easily shows that almost all double circulant codes of the asymptotic family presented here satisfy an improved bound of the form (2). Actually we suspect that this is also the case for most choices of n : this is suggested by computer experiments with randomly chosen double circulant codes of small blocklengths.

We have tried to strike a balance between giving readable proofs and deriving a non-astronomical lower bound on the prime p in Theorem 8. In principle, the numerical values could be refined. In particular, the constant b of Theorem 8 could be made to approach $1/2$ (as in Theorem 4) but at the cost of a larger p. If we convert the formulation of Theorem 8 in the form (2) (which just involves switching from $|B_{2n}(d)|$ in Theorem 2 to $|B_{2n}(d-1)|$ in (2)) we obtain a constant c which is of the same order of magnitude, but somewhat worse, than the improved constant $c \approx 0.102$ of [16] for Jiang and Vardy's method.

In this paper we only consider the binary case with codes of rate $1/2$ but the method can be straightforwardly generalized to the case of different alphabets and to quasi-cyclic codes of any rational rate (though at the cost of a worsening of the constant b) by considering for parity check matrices vertical and horizontal concatenations of random circulant matrices.

Finally, a natural question is to wonder whether the ideas developed in this paper can be extended to Euclidean lattices in a way similar to the generalization of Jiang and Vardy's method to sphere-packings of Euclidean spaces [10]. A positive answer to this question is given in the paper [4].

References

[1] C. L. Chen, W. W. Peterson and E. J. Weldon, "Some results on quasi-cyclic codes," *Inform. Control*, Vol. 15, no. 5, pp. 407–423, 1969.

[2] V. V. Chepyzhov, "New lower bounds for minimum distance of linear quasi-cyclic and almost linear cyclic codes," *Problemy Peredachi Informatsii*, Vol. 28, no 1, pp. 39–51, 1992.

[3] P. Gaborit and G. Zémor, "Asymptotic improvement of the Gilbert-Varshamov bound for linear codes", ISIT 2006, Seattle, p.287-291.

[4] P. Gaborit and G. Zémor, "On the construction of dense lattices with a given automorphism group," *Annales de l'Institut Fourier*, vol. 57 No. 4 (2007), pp. 1051–1062.

[5] E. N. Gilbert, " A comparison of signalling alphabets", *Bell. Sys. Tech. J.*, **31**, pp. 504-522, 1952.

[6] T. Jiang and A. Vardy, "Asymptotic improvement of the Gilbert-Varshamov bound on the size of binary codes," *IEEE Trans. Inf. Theory*, Vol. 50, no. 8, pp. 1655–1664, 2004.

[7] G. A. Kabatiyanskii, "On the existence of good cyclic almost linear codes over non prime fields", *Problemy Peredachi Informatsii*, Vol. 13, no 3, pp. 18–21, 1977.

[8] M. Karlin, " New binary coding results by circulant", *IEEE Trans. Inform. Theory* **15**, pp. 81–92, 1969.

[9] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2," *IEEE Trans. Inf. Theory*, Vol. 20, no. 5, pp. 679–679, 1974.

[10] M. Krivelevich, S. Litsyn, A. Vardy, "A lower bound on the density of sphere packings via graph theory", *Int. Math. Res. Not*, no. 43, 2271–2279, 2004.

[11] E. Krouk, "On codes with prescribed group of symmetry," *Voprosy Kibernetiki*, Vol. 34, pp. 105–112, 1977.

[12] E. Krouk and S. Semenov, "On the existence of good quasi-cyclic codes," proc. of 7th joint Swedish-Russian International Workshop on Information Theory, St-Petersburg, Russia, june 1995, pp. 164–166.

[13] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam 1977.

[14] M. A. Tsfasman, S.G. Vladuts and Zink, "Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound", *Math. Nach.*, **104**, pp. 13–28, 1982.

[15] R.R. Varshamov, "Estimate of the number of signals in error-correcting codes", *Dokl. Acad. Nauk*, **117**, pp. 739–741, 1957 (in Russian).

[16] V. Vu and L. Wu, "Improving the Gilbert-Varshamov bound for q-ary codes", *IEEE Trans. Inf. Theo.*, **51** (9), pp. 3200–3208, 2005