ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Mathematics 285 (2004) 345–347

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Note

Linear codes with complementary duals meet the Gilbert–Varshamov bound

Nicolas Sendrier

Projet CODES, INRIA UR Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France

Received 4 February 2003; received in revised form 18 December 2003; accepted 7 May 2004

Abstract

Using the hull dimension spectra of linear codes, we show that linear codes with complementary dual meet the asymptotic Gilbert–Varshamov bound.

Keywords: Error correcting codes; Hull; LCD codes; Gilbert–Varshamov bound

1. Introduction

Linear codes with complementary duals (LCD codes) were introduced by James Massey in 1992 [4]. In that paper, the author shows that LCD codes are asymptotically good and raises the question of whether or not they reach the Gilbert–Varshamov bound. The purpose of this note is to prove that they do.

The hull [1] of a linear code C is defined to be its intersection with its dual, $\mathscr{H}(C) = C \cap C^{\perp}$. The LCD codes are the linear codes with a hull of dimension zero. The complete hull dimension spectra of linear codes is given in [5]. In particular the proportion of q-ary linear codes having a hull of dimension l tends towards a positive constant (only dependent of q and l).

2. Hull dimension

Throughout the paper, GF(q) will denote the finite field with q elements and unless specified otherwise we will consider q-ary codes. An $[n,k]$ code will be a q-ary linear code of length n and dimension k and an $[n,k,d]$ code will be an $[n,k]$ code of minimum distance d. We denote by $\mathscr{L}_{n,k}$ the set of all $[n,k]$ codes and by $\mathscr{H}_l$ the set of q-ary linear codes whose hull has dimension l. We have

Theorem 1 (Sendrier [5]). *For all* $l \geqslant 0$, *all* q *and any rate* $0 < R < 1$.

$$\lim_{n\to\infty} \frac{|\mathscr{H}_l \cap \mathscr{L}_{n,\lceil Rn\rceil}|}{|\mathscr{L}_{n,\lceil Rn\rceil}|} = \frac{\tau_0}{(q^l-1)(q^{l-1}-1)\cdots(q-1)} = \tau_l,$$

where $\tau_0 = \prod_{i>0}(1+q^{-i})^{-1}$.

It is remarkable that this number does not depend on the rate R.

E-mail address: Nicolas.Sendrier@inria.fr (N. Sendrier).

0012-365X/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.05.005

The proportion of $[n,k]$ LCD codes among $[n,k]$ codes is τ_0. For $q=2$, about 41.9% of the linear codes have a complementary dual. This proportion increases with q, we have for instance $\tau_0=0.639$ for $q=3$ or $\tau_0=0.996$ for $q=256$. More generally, $\tau_0 \approx 1-1/q$ when q grows to infinity.

3. The Gilbert–Varshamov bound

Theorem 2 (Gilbert–Varshamov lower bound). *An $[n,k,d]$ code exists if*

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k}. \tag{1}$$

Using the q-ary entropy function, defined for all x with $0 \leqslant x \leqslant 1$ by

$$H_q(x) = -x \log_q \frac{x}{q-1} - (1-x)\log_q(1-x)$$

and an adequate inequality on binomial coefficients (see [3, p. 310]), we obtain from (1) another sufficient condition for the existence of an $[n,k,d]$ code

$$(n-1)H_q\left(\frac{d-2}{n-1}\right) < n-k. \tag{2}$$

From this the asymptotic version of the bound can be derived.

Theorem 3 (Gilbert–Varshamov asymptotic lower bound). *For each δ such that $0 \leqslant \delta \leqslant (q-1)/q$ there exists a sequence of $[n_i,k_i,d_i]$ codes such that*:

(1) $\lim_{i\to\infty} n_i = \infty$,
(2) $\liminf_{i\to\infty} d_i/n_i \geqslant \delta$,
(3) $\limsup_{i\to\infty} k_i/n_i \geqslant 1 - H_q(\delta)$.

A family of code is asymptotically good if there exists two positive numbers R and δ such that $R\delta > 0$ and an infinite sequence of $[n,k,d]$ codes in the family such that $d/n \geqslant \delta$ and $k/n \geqslant R$. Meeting the asymptotic Gilbert–Varshamov bound will mean something like that with an additional condition between R and δ.

Definition 4. A family $\mathscr{F}$ of q-ary linear codes meets the Gilbert–Varshamov bound (in the strong sense) if for each number δ with $0 \leqslant \delta \leqslant (q-1)/q$ it contains a sequence of $[n_i,k_i,d_i]$ codes such that

(1) $\lim_{i\to\infty} n_i = \infty$,
(2) $\liminf_{i\to\infty} d_i/n_i \geqslant \delta$,
(3) $\limsup_{i\to\infty} k_i/n_i \geqslant 1 - H_q(\delta)$.

A family can meet the bound in a weaker sense if the statements of the theorem do not hold for each δ. For instance, self-dual codes do meet the Gilbert–Varshamov bound, but only for $\delta = H_q^{-1}(\frac{1}{2})$. Note also that in this weaker sense, we must not allow $\delta=0$ or $(q-1)/q$ or we might have asymptotically bad families of codes meeting the Gilbert–Varshamov bound.

Not only there are linear codes that meet the bound, but almost all of them do (see [2, Section 1] for instance). Formally, this can be can stated as follows:

Lemma 5. *For all $\varepsilon > 0$ and all R with $0 < R < 1$ we have*

$$\lim_{n\to\infty} \frac{|\mathscr{G}_{n,\lceil Rn\rceil}(\varepsilon)|}{|\mathscr{L}_{n,\lceil Rn\rceil}|} = 1,$$

where $\mathscr{G}_{n,k}(\varepsilon)$ the set of all $[n,k,d]$ codes such that $k/n + H_q(d/n) \geqslant 1-\varepsilon$.

Theorem 6. *Let $\mathscr{F}$ denote a family of q-ary codes. If for each number R with $0 < R < 1$ we have*

$$\limsup_{n\to\infty} \frac{|\mathscr{F} \cap \mathscr{L}_{n,\lceil Rn\rceil}|}{|\mathscr{L}_{n,\lceil Rn\rceil}|} > 0, \tag{3}$$

then $\mathscr{F}$ meets the Gilbert–Varshamov bound in the strong sense.

Proof. For all n, all k and all $\varepsilon > 0$ we have $(\mathscr{F} \cap \mathscr{L}_{n,k}) \backslash (\mathscr{F} \cap \mathscr{G}_{n,k}(\varepsilon)) \subset \mathscr{L}_{n,k} \backslash \mathscr{G}_{n,k}(\varepsilon)$, $\mathscr{F} \cap \mathscr{G}_{n,k}(\varepsilon) \subset \mathscr{F} \cap \mathscr{L}_{n,k}$ and $\mathscr{G}_{n,k}(\varepsilon) \subset \mathscr{L}_{n,k}$. And thus we can write

$$\frac{|\mathscr{F} \cap \mathscr{L}_{n,k}|}{|\mathscr{L}_{n,k}|} - \frac{|\mathscr{F} \cap \mathscr{G}_{n,k}(\varepsilon)|}{|\mathscr{L}_{n,k}|} \leqslant 1 - \frac{|\mathscr{G}_{n,k}(\varepsilon)|}{|\mathscr{L}_{n,k}|}.$$

From (3) we easily derive that for all R with $0 < R < 1$ and all $\varepsilon > 0$

$$\limsup_{n \to \infty} \frac{|\mathscr{F} \cap \mathscr{G}_{n,\lceil Rn \rceil}(\varepsilon)|}{|\mathscr{L}_{n,\lceil Rn \rceil}|} > 0.$$

Thus for all R with $0 < R < 1$ and all $\varepsilon > 0$ there exists (infinitely many) codes in $\mathscr{F}$ whose parameters verify $k = \lceil Rn \rceil$ and $k/n + H_q(d/n) \geqslant 1 - \varepsilon$. From that we can construct the sequences required to comply with Definition 4. □

4. Codes with prescribed hull dimension

Theorem 7. *Linear codes with prescribed hull dimension meet the Gilbert–Varshamov bound in the strong sense.*

Proof. A direct consequence of Theorem 1 and Theorem 6. □

Corollary 8. *LCD codes meet the Gilbert–Varshamov bound in the strong sense.*

References

[1] E.F. Assmus Jr., J.D. Key, Affine and projective planes, Discrete Math. 83 (1990) 161–187.

[2] A. Barg, Complexity issues in coding theory, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Vol. I, North-Holland, Amsterdam, 1998, pp. 649–754 (Chapter 7).

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

[4] J.L. Massey, Linear codes with complementary duals, Discrete Math. 106/107 (1992) 337–342.

[5] N. Sendrier, On the dimension of the hull, SIAM J. Discrete Math. 10(2) (1997) 282–293.