Lengthening and the Gilbert-Varshamov bound

Yves Edel and Jürgen Bierbrauer

Abstract

We use lengthening and an enhanced version of the Gilbert-Varshamov lower bound for linear codes to construct a large number of record-breaking codes. Our main theorem may be seen as a closure operation on data bases.

Index Terms

Linear codes, lengthening, Gilbert Varshamov-bound.

1 Introduction

[1] Let q be a prime-power, which will be fixed throughout the discussion. Denote by $\mathbb{F}_q$ the field of q elements and by $V(n,i)$ the number of vectors of weight at most i in $\mathbb{F}_q^n$. It is clear that

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

Let $\mathcal{C}$ be a q-ary code with parameters $[n,k-1,d]$. As $\mathcal{C}$ has q^{k-1} elements it follows that if $q^{k-1}V(n,d-1)<q^n$, then there is a vector $v\in\mathbb{F}_q^n$, which has distance $\geq d$ from every code-word $\in\mathcal{C}$. This leads to the Gilbert-Varshamov bound:

[1] authors'addresses: Yves Edel, Mathematisches Institut der Universität, Im Neuenheimer Feld 288, 69120 Heidelberg (Germany); Jürgen Bierbrauer, Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931 (USA)

Theorem 1 (Gilbert-Varshamov bound) *If* $V(n, d-1) < q^{n-k+1}$, *then a* q*-ary linear code with parameters* $[n, k, d]$ *exists.*

Using orthogonal arrays the following can be proved.

Theorem 2 *If* $V(n-1, d-2) < q^{n-k}$, *then a* q*-ary linear code with parameters* $[n, k, d]$ *exists. Moreover every code* $[n-1, k-1, d]$ *can be embedded in a code* $[n, k, d]$.

This is to be found in the book by Mac Williams and Sloane ([3], page 34). For the sake of completeness we shall give a proof in the final section. It is easy to see that this is always stronger than the Gilbert-Varshamov bound. Combining Theorem 2 with the method of lengthening yields new codes:

Theorem 3 *Assume* $V(n-1, d-2) < q^{n-k}$. *If there exist codes* $[n-i, k-i, d+\delta]$ *and* $[e, i, \delta]$, *then a code* $[n+e, k, d+\delta]$ *can be constructed.*

A proof of Theorem 3 will be given in the following section. It should be noted that Theorem 3 uses only the code parameters. No information on subcodes is needed. We like to think of it as of a closure operation on data bases. In order to illustrate its use we give a binary example: a code $\mathcal{D}$ with parameters $[126, 36, 34]$ is known to exist. It can be derived from a $[128, 36, 36]$ constructed in [4]. As $V(126, 26) < 2^{90}$ it follows from Theorem 2 that $\mathcal{D}$ can be embedded in a code $\mathcal{C}$ with parameters $[127, 37, 28]$. Applying construction X to the pair $\mathcal{C} \supset \mathcal{D}$ with $[6, 1, 6]$ as auxiliary code yields the new code $[133, 37, 34]$.
In Table 1 we list some more applications of Theorem 3. In all cases $i = 1$, so that the auxiliary code is the repetition code $[e, i, \delta] = [\delta, 1, \delta]$. The following parameters are given:

- $q \in \{2, 3, 4\}$,
- the parameters $[n-1, k-1, d+\delta]$ of the known code $\mathcal{D}$,
- δ,
- the parameters $[n, k, d+\delta]$ of the resulting code $\mathcal{E}$.

It is easy to write a program which operates on any given data base and produces the closure of the data base under Theorem 3. All in all Theorem 3 leads to hundreds of improvements in the present version of the data base.

Table 1:

q	$\mathcal{D}$	δ	$\mathcal{E}$
2	[123,29,39]	8	[132,30,39]
2	[126,29,42]	10	[137,30,42]
2	[135,29,45]	10	[146,30,45]
2	[197,65,41]	3	[201,66,41]
2	[206,96,31]	3	[210,97,31]
3	[40,24,9]	2	[43,25,9]
3	[43,24,10]	2	[46,25,10]
3	[52,13,22]	3	[56,14,22]
3	[59,32,13]	2	[62,33,13]
3	[64,17,24]	2	[67,18,24]
3	[65,16,25]	2	[68,17,25]
3	[81,16,41]	10	[92,17,41]
3	[83,16,42]	10	[94,17,42]
4	[44,22,14]	3	[48,23,14]
4	[40,14,15]	1	[42,15,15]
4	[42,14,17]	2	[45,15,17]
4	[59,27,17]	2	[62,28,17]
4	[63,27,21]	4	[68,28,21]
4	[65,27,23]	5	[71,28,23]

2 Proofs

Let $\mathcal{A}$ be a linear subspace of dimension $n-k$ of $\mathbb{F}_q^{n-1}$, which is an orthogonal array of strength t, and let A be a generator matrix of $\mathcal{A}$. We wish to add an additional column to A such that the resulting subspace of $\mathbb{F}_q^n$ still is an orthogonal array of strength t. The columns which do not do the job are precisely those vectors in $\mathbb{F}_q^{n-k}$, which can be written as linear combinations of at most $t-1$ columns of A. The number of such linear combinations is at most $\sum_{i=0}^{t-1}\binom{n-1}{i}(q-1)^i$. This number happens to equal $V(n-1,t-1)$. Thus, if $V(n-1,t-1) < q^{n-k}$, then our orthogonal array can be extended in the required manner. By Delsarte theory a linear subspace of $\mathbb{F}_q^n$ is an orthogonal array of strength t if and only if its dual has minimum distance $\geq t+1$. Considering duals we see that we have proved the following: if there is a code $\mathcal{C}$ with parameters $[n-1,k-1,d]$ and if $V(n-1,d-2) < q^{n-k}$, then $\mathcal{C}$ can be extended to a code $[n,k,d]$. Just as in the case of the Gilbert-Varshamov bound it is easy to see by induction that the condition of the existence of an $[n-1,k-1,d]$ is not needed. Theorem 2 is proved.
In order to show that Theorem 2 is always better than Theorem 1 it suffices to show the inequality

$$qV(n-1,d-2) < V(n,d-1). \tag{2}$$

In fact, consider the $V(n-1,d-2)$ vectors of length $n-1$ and weight $\leq d-2$. Adding a coordinate and extending each of these vectors in all q possible ways yields $qV(n-1,d-2)$ different (but obviously not all) vectors of length n and weight $\leq d-1$. This proves our last claim concerning Theorem 2.
Consider Theorem 3: we use a basic fact on lengthening known as construction X ([3], see also [1]):

Lemma 1 (construction X) *Let $\mathcal{C}$ be a q-ary code with parameters $[n,k,d]$ and $\mathcal{D}$ a subcode of $\mathcal{C}$ of codimension κ and minimum distance $\geq d+\delta$ for some $\delta > 0$. If there is a code with parameters $[e,\kappa,\delta]$ then there is a code $[n+e,k,d+\delta]$ which projects onto $\mathcal{C}$.*

The assumptions of Theorem 3 show that the code $[n-i,k-i,d+\delta]$ can be embedded in a code $[n,k,d]$. Application of construction X to this pair of codes leads to the conclusion of Theorem 3.

References

[1] J.Bierbrauer and Y.Edel, *Extending and lengthening BCH-codes,* manuscript.

[2] A.E. Brouwer, *Data base of bounds for the minimum distance for binary, ternary and quaternary codes,*
URL http://www.win.tue.nl/win/math/dw/voorlincod.html or
URL http://www.cwi.nl/htbin/aeb/lincodbd/2/136/114 or
URL ftp://ftp.win.tue.nl/pub/math/codes/table[234].gz.

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

[4] D.Schomaker and M.Wirtz, *On binary cyclic codes of length from 101 to 127, IEEE Transactions on Information Theory* **38**(1992), 516-518.