Inverting construction Y_1.

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)

July 15, 2002

Abstract

We introduce a computer-based method for extending linear codes, which can be viewed as an inverse of the familiar construction Y_1. As a result codes with record-breaking parameters are constructed.

1 Introduction

Let $\mathcal{C}$ be a q-ary linear code with parameters $[n, k, d]$. Let v be a code-word of the dual code $\mathcal{C}^{\perp}$, of weight w. Then the subcode of $\mathcal{C}$, which consists of the words having vanishing entry at the support of v has parameters $[n - w, k - w + 1, d]$. This observation is known as **construction** Y_1. We ask when this operation can be inverted. So let a code $\mathcal{C}$ with parameters $[n, k, d]$ be given, let H be a check matrix of $\mathcal{C}$. Let H' be obtained by adding a row with entries 0 to H. We want to try and lengthen H' by adding l columns (elements of $\mathbb{F}_q^{n+1-k}$) to H' such that the resulting matrix still has

the property that any $d-1$ columns are linearly independent. The lengthened matrix is then the parity check matrix of a code $[n+l, k+l-1, d]$.
Naturally we wish to find as many new columns as possible. $e = 1$ can always be obtained. This leads to a code $[n+1, k, d]$, which can trivially be obtained from $\mathcal{C}$. In our setting it suffices to choose as new column just any vector with nonzero entry in the last row.
This procedure seems to be called for when $\mathcal{C}$ does not admit an extension to a code $[n+1, k+1, d]$. It is an easily checked folklore fact among coding theorists that this is equivalent with the covering radius of $\mathcal{C}$ satisfying $\rho(\mathcal{C}) < d-1$. In that case our construction can be seen as a tentative to construct a code $[n+1, k, d]$ of covering radius $\geq d-1$, in fact with many vectors at distance $\geq d-1$ from the code. In that case the columns added to H' will have nonzero entries in the last row. Application of construction Y_1 to the last row of the check matrix leads back to code $\mathcal{C}$.
In table I we give a list of codes with new parameters obtained by applying this procedure.

Complete information on these codes, including a check matrix, is to be found on the first author's homepage [1]. Observe that it suffices to give a check matrix for the longest code in each chain. Some words about the codes we start from. Codes $[127, 106, 7]_2$ and $[63, 39, 9]_2$ are primitive BCH-codes, $[45, 24, 9]_2$ is obtained from the quadratic-residue code $[48, 24, 12]_2$. The ternary code $[24, 12, 9]_3$ is a quadratic-residue code and $[22, 12, 7]_3$ is obtained from it by truncation. A code $[85, 74, 6]_3$ was constructed in [3] as a computer-generated extension of the dual $[81, 70, 6]_3$ of the extended primitive BCH-code $[81, 11, 45]_3$. Code $[85, 70, 7]_3$ is constructed in [2] by applying construction X to a pair of dual BCH-codes. Codes $[65, 57, 5]_4$ and $[81, 70, 6]_4$ are taken from [2], $[20, 13, 6]_4$ was constructed by computer and $[19, 10, 7]_4$ was obtained as a truncation from a double circulant code $[20, 10, 8]_4$. Most of the remaining codes of departure were constructed by computer, the exceptions being $[26, 16, 8]_5$ (obtained by construction XX from a primitive BCH-code $[24, 16, 6]_5$,) the Reed-Solomon code $[6, 2, 5]_5$ and $[17, 10, 7]_9$, obtained by truncation from a quadratic-residue code $[20, 10, 10]_9$. Start codes $[30, 24, 5]_5$, $[28, 21, 6]_5$, $[27, 18, 7]_5$, $[14, 7, 7]_7$ and $[16, 10, 6]_8$ are new codes.
Two of the binary codes yield dense sphere packings, via the coset-code method (see [4]). In dimension 156 we can use $[156, 133, 8]_2$ together with $[156, 57, 32]_2$, the repetition code and the all-even code, to construct a sphere packing with center density $\delta = 2^{112}$. In dimension 163 the same method,

Table I

$[127, 106, 7]_2$	$\rightarrow$	$[155, 133, 7]_2$	$\rightarrow$	$[162, 139, 7]_2$		
$[45, 24, 9]_2$	$\rightarrow$	$[49, 27, 9]_2$				
$[63, 39, 9]_2$	$\rightarrow$	$[72, 47, 9]_2$	$\rightarrow$	$[77, 51, 9]_2$		
$[85, 74, 6]_3$	$\rightarrow$	$[95, 83, 6]_3$	$\rightarrow$	$[103, 90, 6]_3$		
$[22, 12, 7]_3$	$\rightarrow$	$[27, 16, 7]_3$	$\rightarrow$	$[34, 22, 7]_3$	$\rightarrow$	$[42, 29, 7]_3 \rightarrow$
						$[53, 39, 7]_3$
$[85, 70, 7]_3$	$\rightarrow$	$[92, 76, 7]_3$	$\rightarrow$	$[108, 91, 7]_3$		
$[24, 12, 9]_3$	$\rightarrow$	$[29, 16, 8]_3$	$\rightarrow$	$[35, 21, 8]_3$		
$[65, 57, 5]_4$	$\rightarrow$	$[87, 78, 5]_4$	$\rightarrow$	$[145, 135, 5]_4$		
$[20, 13, 6]_4$	$\rightarrow$	$[27, 19, 6]_4$	$\rightarrow$	$[36, 27, 6]_4$		
$[81, 70, 6]_4$	$\rightarrow$	$[106, 94, 6]_4$				
$[19, 10, 7]_4$	$\rightarrow$	$[26, 16, 7]_4$				
$[6, 2, 5]_5$	$\rightarrow$	$[12, 7, 5]_5$				
$[30, 24, 5]_5$	$\rightarrow$	$[44, 37, 5]_5$	$\rightarrow$	$[78, 70, 5]_5 \rightarrow$		$[137, 128, 5]_5$
$[28, 21, 6]_5$	$\rightarrow$	$[33, 24, 6]_5$	$\rightarrow$	$[44, 35, 6]_5$	$\rightarrow$	$[68, 58, 6]_5 \rightarrow$
						$[102, 91, 6]_5$
$[27, 18, 7]_5$	$\rightarrow$	$[33, 23, 7]_5$	$\rightarrow$	$[45, 34, 7]_5$		
$[26, 16, 8]_5$	$\rightarrow$	$[33, 22, 8]_5$				
$[14, 7, 7]_7$	$\rightarrow$	$[19, 11, 7]_7$				
$[16, 10, 6]_8$	$\rightarrow$	$[26, 19, 6]_8$	$\rightarrow$	$[44, 36, 6]_8$		
$[15, 8, 7]_8$	$\rightarrow$	$[21, 13, 7]_8$				
$[17, 10, 7]_9$	$\rightarrow$	$[22, 14, 7]_9$				

based on $[163, 39, 8]_2$ and $[163, 63, 32]_2$, yields center density $2^{120.5}$.

References

[1] Our homepages are http://www.mathi.uni-heidelberg.de/∼yves/ and http://www.math.mtu.edu/∼jbierbra/Home.html

[2] J.Bierbrauer and Y.Edel: *New code parameters from Reed-Solomon subfield codes,* *IEEE Transactions on Information Theory* **43** (1997),953-968.

[3] J.Bierbrauer and Y.Edel: *Extending and lengthening BCH-codes,* *Finite Fields and Their Applications* **3**(1997),314-333.

[4] J.Bierbrauer and Y.Edel: *Dense sphere packings from new codes,* submitted for publication in *Journal of Algebraic Combinatorics.*

[5] 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.

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