New Linear Codes from Matrix-Product Codes with Polynomial Units

Fernando Hernando and Diego Ruano

***Abstract*—A new construction of codes from old ones is considered, it is an extension of the matrix-product construction. Several linear codes that improve the parameters of the known ones are presented.**

***Index Terms*—Linear Code, Bounds on the minimum distance, Matrix-Product Code, Quasi-Cyclic Code.**

I. Introduction

MATRIX-PRODUCT codes were initially considered in [1], [2]. They are an extension of several classic constructions of codes from old ones. In this article we consider this construction with cyclic codes, extended cyclic matrix-product codes,where the elements of the matrix used to define the codes are polynomials instead of elements of the finite field. The codes obtained with this construction are quasi-cyclic codes [3]. These codes became important after it was shown that some codes in this class meet a modified Gilbert-Varshamov bound [4].

An extension of the lower bound from [2] is obtained. This bound is sharp for a matrix-product code of nested codes, however it is not sharp in this new setting, that is we obtain codes with minimum distance beyond this bound. The decoding algorithm from [5] can be used for the extended cyclic matrix-product code of two nested codes. Finally, by investigating the construction of the words with possible minimum weight of a matrix-product code, we are able to sift an exhaustive search and to obtain three extended matrix-product codes, by extending the $u|u+v$-construction, that improve the parameters of the codes in [6]. Another four linear codes, improving the parameters of the known linear codes, are obtained from the previous ones. Finally, we present a list of new quasi-cyclic codes with good parameters obtained with this construction.

II. Matrix-Product Codes

Let $\mathbb{F}_q$ be the finite field with q elements, $C_1, \ldots, C_s \subset \mathbb{F}_q^m$ linear codes of length m and $A = (a_{i,j}) \in \mathcal{M}(\mathbb{F}_q, s \times l)$ a matrix with $s \leq l$. The matrix-product code $C = [C_1 \cdots C_s] \cdot A$ is the set of all matrix-products $[c_1 \cdots c_s] \cdot A$ where $c_i \in C_i$ is an $m \times 1$ column vector $c_i = (c_{1,i}, \ldots, c_{m,i})^T$ for $i = 1, \ldots, s$.

The i-th column of any codeword is an element of the form $\sum_{j=1}^{s} a_{j,i} c_j \in \mathbb{F}_q^m$, hence reading the entries of the $m \times l$-matrix above in column-major order, the codewords can be viewed as vectors of length ml,

$$c = \left(\sum_{j=1}^{s} a_{j,1} c_j, \ldots, \sum_{j=1}^{s} a_{j,l} c_j \right) \in \mathbb{F}_q^{ml}.$$

A generator matrix of C is of the form:

$$G = \begin{pmatrix} a_{1,1}G_1 & a_{1,2}G_1 & \cdots & a_{1,s}G_1 & \cdots & a_{1,l}G_1 \\ a_{2,1}G_2 & a_{2,2}G_2 & \cdots & a_{2,s}G_2 & \cdots & a_{2,l}G_2 \\ \vdots & \vdots & \cdots & \vdots & \cdots & \vdots \\ a_{s,1}G_s & a_{s,2}G_s & \cdots & a_{s,s}G_s & \cdots & a_{s,l}G_s \end{pmatrix},$$

where G_i is a generator matrix of C_i, $i = 1, \ldots, s$. Moreover, if C_i is a $[m, k_i, d_i]$ code then one has that $[C_1 \cdots C_s] \cdot A$ is a linear code over $\mathbb{F}_q$ with length lm and dimension $k = k_1 + \cdots + k_s$ if the matrix A is full rank and $k < k_1 + \cdots + k_s$ otherwise.

We denote by $R_i = (a_{i,1}, \ldots, a_{i,l})$ the element of $\mathbb{F}_q^l$ consisting of the i-th row of A, for $i = 1, \ldots, s$. We set D_i the minimum distance of the code C_{R_i} generated by $\langle R_1, \ldots, R_i \rangle$ in $\mathbb{F}_q^l$. In [2] the following lower bound for the minimum distance of the matrix-product code C is obtained, $d(C) \geq \min\{d_1 D_1, d_2 D_2, \ldots, d_s D_s\}$, where d_i is the minimum distance of C_i. Furthermore this bound is sharp if $C_1 \supset \cdots \supset C_s$ [5].

III. Extended cyclic matrix-product codes

In this article we consider the case when $C_1, \ldots, C_s$ are cyclic codes. A cyclic code is an ideal in $\mathbb{F}_q[x]/(x^m - 1)$. The matrix-product code $C = [C_1 \cdots C_s] \cdot A$, for a matrix A is a quasi-cyclic code.

The new approach of this article consists in considering the following construction: we consider the matrix-product code of s cyclic codes of length m with respect a $s \times l$-matrix A whose entries are units in $\mathbb{F}_q[x]/(x^m - 1)$, an element with a inverse, instead of elements in $\mathbb{F}_q$. A unit in $\mathbb{F}_q[X]/(x^m - 1)$ is a polynomial of degree lower than m whose greatest common divisor with $x^m - 1$ is 1 (they are co-primes). We remark, that the cyclic codes generated by f and by fu, with $f \mid x^m - 1$ and $\gcd(u, x^m - 1) = 1$, are the same code.

Hence, we have the so-called extended cyclic matrix-product codes: let $C_1 = (f_1), \ldots, C_s = (f_s) \subset \mathbb{F}_q[x]/(x^m - 1)$ be cyclic codes of length m and a matrix $A = (a_{i,j}) \in$

The work of F. Hernando is supported in part by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006 (Ireland) and by MEC MTM2007-64704 and Junta de CyL VA025A07 (Spain). The work of D. Ruano is supported in part by MEC MTM2007-64704 and Junta de CyL VA065A07 (Spain).

F. Hernando is with the Department of Mathematics, University College Cork, Ireland, e-mail: F.Hernando@ucc.ie

D. Ruano is with DTU-Mathematics, Technical University of Denmark, Matematiktorvet, Building 303, DK-2800, Kgs. Lyngby, Denmark, e-mail: D.Ruano@mat.dtu.dk

$\mathcal{M}((\mathbb{F}_q[X]/(x^m-1)^*, s\times l)$, with $s\leq l$. The extended cyclic matrix-product code $C=[C_1\cdots C_s]\cdot A$ is the set of all matrix-products $[c_1\cdots c_s]\cdot A$ where $c_i\in\mathbb{F}_q[x]$. As for matrix-product codes, if the matrix A is full-rank the dimension of C is the sum of the dimensions of $C_1,\dots,C_s$. An extended cyclic matrix-product code is a quasi-cyclic code.

We denote by $R_i=(a_{i,1},\dots,a_{i,l})$ the element of $(\mathbb{F}_q[x]/(x^m-1))^l$ consisting of the i-th row of A, for $i=1,\dots,s$. We consider C_{R_i}, the $\mathbb{F}_q[x]/(x^m-1)$-submodule of $(\mathbb{F}_q[x]/(x^m-1))^l$ generated by $R_1,\dots,R_i$. In other words, C_{R_i} is a linear code over a ring, and we denote by D_i the minimum Hamming weight of the words of C_{R_i}, $D_i=\min\{wt(x)\mid x\in C_{R_i}\}$.

Then we have a lower bound for the minimum distance of a extended cyclic matrix-product code similar to the one in [2], $d(C)\geq d^*=\min\{d_1D_1,d_2D_2,\dots,d_sD_s\}$. The proof is the same as the one for matrix-product codes.

If we consider $C_1,\dots,C_s$ nested codes, the previous bound is sharp for matrix-product codes. However, if we consider a extended cyclic matrix-product code, then it is not sharp in general, as one can see in the examples. Let us consider the same approach as that of [5] to construct a codeword with minimum weight in this more general setting: set $c_1,\dots,c_p$ such that $c_1=\cdots=c_p$, with $wt(c_p)=d_p$, and $c_{p+1}=\ldots=c_s=0$. Let $r=\sum_{i=1}^p r_iR_i$, with $r_i\in\mathbb{F}_q[x]/(x^m-1)$, be a word in C_{R_p} with weight D_p. If $c_i'=r_ic_i$ then

$$[c_1'\cdots c_s']\cdot A=c_1\left(\sum_{j=1}^p a_{j,1}r_j,\dots,\sum_{j=1}^p a_{j,l}r_j\right)=c_pr.$$

Although, for a cyclic code C and a unit g in $\mathbb{F}_q[x]/(x^m-1)$, $C=\{cg\mid c\in C\}$, the weight of c is different from the one of cg, in general. Hence, the weight of c_pr is greater than or equal to d_pD_p. We remark that this phenomenon allows us to obtain codes with minimum distance beyond the lower bound.

We can consider the algorithm [5, Algorithm 1] to decode extended cyclic matrix-product codes up to $\lfloor\frac{d^*-1}{2}\rfloor$ errors, for $s=2$ and $l\geq 2$. Algorithm in [5] assumes that A is a non-singular by columns matrix, in this setting, it just means that the first row of A has non-zero elements and the 2-dimensional minors of A are full rank in $\mathbb{F}_q[x]/(x^m-1)$,

For $s\geq 3$, we cannot use this algorithm since the units of $\mathbb{F}_q[x]/(x^m-1)$ are not an additive group, that is the sum of two units is not a unit in general. For instance, 1 and x are units in $\mathbb{F}_q[x]/(x^m-1)$ and $x-1$ is not a unit, for any finite field $\mathbb{F}_q$ and $m>1$. Hence, we can only perform the Gaussian elimination (i.e., lines 10 and 11 of [5, Algorithm 1]) for two rows.

IV. New linear codes

Obtaining a sharper bound than the one in the previous section is a very tough problem, actually it is the same question as the computation of the minimum distance of a quasi-cyclic code. However, by analyzing the lower bound d^* we have performed a search to find codes with good parameters. An exhaustive search in this family is only feasible if one considers some extra conditions, this conditions are necessary for having good parameters, but not sufficient. We will assume further particular conditions that allowed us to achieve successfully a search, discarding a significant amount of cases. We have used the structure obtained in the previous section for extended matrix-product codes from nested codes and we have obtained some binary linear codes improving the parameters of the codes previously known.

Let $s=l=2$, and A the matrix

$$A=\begin{pmatrix} g_1 & g_2\\ 0 & g_4\end{pmatrix},$$

where g_1,g_2,g_4 are units in $\mathbb{F}_2[x]/(x^m-1)$, in this way A is full rank over $\mathbb{F}_2[x]/(x^m-1)$ with $D_1=2$ and $D_2=1$. We may also consider this family of codes as an extension of the $u\mid u+v$-construction.

For nested matrix-product codes, the lower bound for the minimum distance $d^*=\min\{d_1D_1,\dots,d_sD_s\}$ is sharp. Furthermore, by theorem [5, Theorem 1] we have some words with weight d_iD_i for $i=1,\dots,s$. We follow the construction of these words and consider a matrix A in a such a way that they have weight larger than d_iD_i. Let $C_1=(f_1)$ and $C_2=(f_2)$, with $f_1\mid f_2$ (that is, $C_1\supset C_2$). We consider $h_1,h_2\in\mathbb{F}_2[x]$ such that $wt(f_1h_1)=d_1$ and $wt(f_2h_2)=d_2$. The words of $C=[C_1C_2]A$ considered in [5, Theorem 1] are $c_1=(f_1h_1,0)$ and $c_2=(f_2h_2r_1,f_2h_2r_2)$, where $r_1R_1+r_2R_2$, with $r_1,r_2\in\mathbb{F}_2[x]/(x^m-1)$, is a codeword with minimum weight in C_{R_2}, namely it has weight 1.

We have that $c_1A=(f_1h_1g_1,f_1h_1g_2)$ and $c_2A=(f_2h_2r_1g_1,f_2h_2(r_1g_2+r_2g_4))$. The words with minimum weight in C_{R_2} are generated by R_2 and $g_4R_1-g_2R_2$. Therefore, the words with possible minimum weight from [5] are: $(f_1h_1g_1,f_1h_1g_2)$, $(0,f_2h_2g_4)$ and $(f_2h_2g_1g_4,0)$. Hence, we want to get $f_1h_1g_1$ or $f_1h_1g_2$ with weight greater than d_1 and $f_2h_2g_4$ and $f_2h_2g_1g_4$ with weight greater than d_2.

We shall assume also that $d_2>2d_1$, therefore we only should have $f_1h_1g_1$ or $f_1h_1g_2$ with weight greather than d_1 in order to have a chance to improve the lower bound for matrix-product code.

Summarizing, we have performed a sifted search following the criteria: we consider extended cyclic matrix-product codes $C=[C_1C_2]A$, where C_1,C_2 are cyclic nested codes, with same length and d_2 *"much larger"* than $2d_1$, and a matrix

$$A=\begin{pmatrix} g_1 & g_2\\ 0 & 1\end{pmatrix},$$

with g_1,g_2 units in $\mathbb{F}_2[x]/(x^m-1)$ such that $wt(f_1h_1g_1)>d_1$ or $wt(f_1h_1g_2)>d_1$.

We have compared the minimum distance of these binary linear codes with the ones in [6] using [7]. We pre-compute a table containing all the cyclic codes up to length 110, their parameters and their words of minimum weight. We obtained the following linear codes whose parameters are better than the ones previously known:

From [6]	New codes
$[94,25,26]$	$\mathcal{C}_1=[94,25,27]$
$[102,28,27]$	$\mathcal{C}_2=[102,28,28]$
$[102,29,26]$	$\mathcal{C}_3=[102,29,28]$

$\mathcal{C}_1 = [C_1, C_2]A$, where $C_1 = (f_1)$ and $C_2 = (f_2)$ with:

- $f_1 = x^{23} + x^{22} + x^{21} + x^{20} + x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^5 + x^4 + 1$,
- $f_2 = (x^{47} - 1)/(x + 1)$,
- $g_1 = 1$,
- $g_2 = x^{20}+x^{19}+x^{13}+x^{12}+x^{11}+x^9+x^7+x^4+x^3+x^2+1$.

$\mathcal{C}_2 = [C_1, C_2]A$, where $C_1 = (f_1)$ and $C_2 = (f_2)$ with:

- $f_1 = x^{25} + x^{23} + x^{22} + x^{21} + x^{20} + x^{18} + x^{16} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$,
- $f_2 = (x^{51} - 1)/(x^2 + x + 1)$,
- $g_1 = 1$,
- $g_2 = x^{20} + x^{15} + x^{14} + x^{10} + x^9 + x^7 + 1$.

$\mathcal{C}_3 = [C_1, C_2]A$, where $C_1 = (f_1)$ and $C_2 = (f_2)$ with:

- $f_1 = x^{24} + x^{23} + x^{21} + x^{19} + x^{18} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^4 + 1$,
- $f_2 = (x^{51} - 1)/(x^2 + x + 1)$,
- $g_1 = x^{12} + x^6 + 1$,
- $g_2 = x^{40} + x^{24} + 1$.

Moreover operating on C_3 we get four more codes.

From [6]	New codes	Method
$[101, 29, 26]$	$\mathcal{C}_4 = [101, 29, 27]$	PunctureCode($\mathcal{C}_3$,102)
$[101, 28, 26]$	$\mathcal{C}_5 = [101, 28, 28]$	ShortenCode($\mathcal{C}_3$,101)
$[100, 28, 26]$	$\mathcal{C}_6 = [100, 28, 27]$	PunctureCode($\mathcal{C}_5$,101)
$[103, 29, 27]$	$\mathcal{C}_7 = [103, 29, 28]$	ExtendCode($\mathcal{C}_3$)

Also a good number of new quasi-cyclic codes reaching the best known lower bounds [8] are achieved with this method, cyclic extended matrix-product codes are quasi-cyclic codes. The codes marked in bold already exist but with a different construction. The construction of the codes can be found in *http://euclid.ucc.ie/pages/staff/Fernando/*.

n	k	d
4	3	2
6	4	2
8	3	4
8	5-6-7	2
10	6	3
10	9	2
12	5-7	4
12	9-10-11	2
14	5	6
14	9	4
14	11-13	2
16	3	8
16	**4**	**8**
16	9-10-11	4
16	12-13-14-15	2
18	8	6
18	10-11	4
18	15-16-17	2
20	11	5
20	12-13-14	4
20	16-18-19	2
22	12	6
22	21	2
24	**4**	**12**
24	**8**	**8**
24	13	6
24	15-16-17	4
24	20-21-22-23	2
26	14	6
26	25	2
28	**6**	**12**
28	15	6
28	**16**	**6**
28	19-20-22	4
28	24-25-26-27	2
30	**6**	**14**
30	7	12
30	16	7
30	17	6
30	**18 – 19**	**6**
30	20	5
30	21-22-23-24	4
30	26-27-28-29	2
32	**4**	**16**
32	18-19	6
32	23	4
32	27-28-29-30-31	2
34	24-25-26	4
34	33	2
36	19	8
36	26-27-28	4
36	31-32-33-34-35	2
36	37	2
40	18	10
40	21-22-23	8
40	30-31-32-33	4
40	35-36-37-38-39	2
42	18	12
42	22-23-24-25	8
42	27-28-29	6
42	32-33-34-35	4
42	37-38-39-40-41	2
44	23	9
44	24	8
44	42-43	2
46	24	10
46	33	6
46	45	2
48	**4**	**24**
48	25	10
48	27-28-29-30	8
48	32-33	6
48	37-38-39-40-41	4
48	43-44-45-46-47	2
50	28-29	8
50	45-46-49	2
52	27	10
52	50-51	10
54	28-29	10
54	51-52-53	2
56	23	14
56	24-25-26-27	12
56	30	10
56	33-34-35-36-37	8
56	40-41	6
56	45-46-47-48-49	4
56	51-52-53-54-55	2
56	57	2
60	22	16
60	28-29	12
60	37-38-39-40	8
60	44-45	6
60	49-50-51-52-53	4
60	55-56-57-58-59	2
62	7	30
62	22	16
62	30	12
62	36	10
62	40-41	8
62	46	6
62	51-52-55-57	4
62	61	2
64	31-33	12
64	58-59-60-61-62	12
66	**22**	**18**
66	25	16
66	34-35	12
66	40	10
66	42-43-44-45	8
66	50-51-52	6
66	54-55	4
66	63-64-65	2
68	26	16
68	35	12
68	44	8
68	51	6
68	56-57-58	4
68	66-67	2
70	22	20
70	37	12
70	42	10
70	46-47-49	8
70	52-53-54	6
70	58-59-60-61-62	4
70	63	3
70	64-65-66-67-69	2
72	29-30	16
72	38-39	12
72	48	8
72	60-61-62-63	4
72	66-67-68-69-70	2
72	71	2
74	73	2
76	40	12
76	74-74	12
78	41-42	12
78	48-49	10
78	52-53-54	8
78	60-61-62-63	6
78	75-76-77	2

80	41	14
80	43-44	12
80	68-69-70	4
80	74-75-76-77-78	2
80	79	2
82	22	24
82	60	8
82	81	2
84	23-24-25	24
84	30	20
84	43-44	14
84	46-47-48-49	12
84	52-53	10
84	58-59-60-61	8
84	66-67-68	6
84	71-72-73-74-75	4
84	76	4
84	78-79-80-81-82	2
84	83	2
86	16	32
86	56-57	10
86	70-71	6
86	72	5
86	85	2
88	32	20
88	46-47	14
88	75	4
88	84-85-86-87	2
90	26	24
90	46-47-48	14
90	52-53-54	12
90	57-58-59-60	10
90	64-65-66	8
90	71-72-73	6
90	77-78-79-80	4
90	84-85-86-87-88	2
90	89	2
92	24-25	26
92	47-48	14
92	55	12
92	66-67-68-69	8
92	79	4
92	90-91	2
94	25	26
94	48	15
94	69-70	8
96	36-37-38	20
96	50-51-52	14
96	56-57	12
96	83-84-85	4
96	90-91-92-93-94	2
96	95	2
98	52-54	14
98	92-94-95-97	2
100	53-54	14
100	94-95-96-98-99	2
102	**9**	**48**
102	28	27
102	29	26
102	**34**	**24**
102	42	20
102	53	16
102	56-57	14
104	56	16
104	100-101-102	2
104	103	2
106	105	2
108	46-47	20
108	56-57	16
110	58-59	16
110	71	12
110	85	8
110	105-106-109	2

V. Conclusion

The new construction presented in this paper produces codes with good parameters. We expect that one can find more new codes with larger length and over other finite fields.

Acknowledgment

The authors would like to thank P. Beelen and T. Høholdt for helpful comments on this paper.

References

[1] T. Blackmore and G. H. Norton, "Matrix-product codes over $\mathbb{F}_q$," *Appl. Algebra Engrg. Comm. Comput.*, vol. 12, no. 6, pp. 477–500, 2001.

[2] F. Özbudak and H. Stichtenoth, "Note on Niederreiter-Xing's propagation rule for linear codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 13, no. 1, pp. 53–56, 2002.

[3] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes," *Discrete Appl. Math.*, vol. 111, no. 1-2, pp. 157–175, 2001.

[4] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate $1/2$," *IEEE Trans. Information Theory*, vol. IT-20, p. 679, 1974.

[5] F. Hernando, K. Lally, and D. Ruano, "Construction and decoding of matrix-product codes from nested codes," *Submitted to Appl. Algebra Engrg. Comm. Comput.*, 2008, 11 pages.

[6] M. Grassl, "Bounds on the minimum distance of linear codes," Online available at http://www.codetables.de, 2007, accessed on 2009-3-27.

[7] W. Bosma, J. Cannon, and C. Playoust, "The magma algebra system. I. the user language," *J. Symbolic Comput.*, vol. 24(3-4), pp. 235–265, 1997.

[8] E. Z. Chen, "Web database of binary QC codes," Online available at http://www.tec.hkr.se/~chen/research/codes/searchqc2.htm, accessed on 2009-3-27.