Extended Norm-Trace Codes with Optimized Correction Capability*

Maria Bras-Amorós[1,**] and Michael E. O'Sullivan[2]

[1] Departament d'Enginyeria Informàtica i Matemàtiques
Universitat Rovira i Virgili
maria.bras@urv.cat
[2] Department of Mathematics and Statistics
San Diego State University
mosulliv@sciences.sdsu.edu

Abstract. We consider a generalization of the codes defined by norm and trace functions on finite fields introduced by Olav Geil. The codes in the new family still satisfy Geil's duality properties stated for norm-trace codes. That is, it is easy to find a minimal set of parity checks guaranteeing correction of a given number of errors, as well as the set of monomials generating the corresponding code. Furthermore, we describe a way to find the minimal set of parity checks and the corresponding generating monomials guaranteeing correction at least of *generic* errors. This gives codes with even larger dimensions.

1 Introduction

Let q be a prime power and r an integer greater than or equal to 2. The curve defined over $\mathbb{F}_{q^r}$ with affine equation $x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y$ is called the *norm-trace curve* associated to q and r. In fact, the defining equation is equivalent to $\mathcal{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = \mathcal{T}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$, where, for $x \in \mathbb{F}_{q^r}$, $\mathcal{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x)$ denotes the norm of x over $\mathbb{F}_q$, and for $y \in \mathbb{F}_{q^r}$, $\mathcal{T}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$ denotes the trace of y over $\mathbb{F}_q$. Norm-trace curves were introduced by Geil in [2]. They are a natural generalization of Hermitian curves, these being norm-trace curves resulting from the field extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. Norm-trace curves have a single rational point P_∞ at infinity and $n = q^{2r-1}$ proper rational points.

In this work we consider a somewhat broader family of curves that include norm-trace curves. For example, our family includes $x^u = \mathcal{T}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$, where u divides $(q^r-1)/(q-1)$, and it also includes the maximal curves derived from Hermitian curves studied in [3].

* Part of this work is in the manuscript [1] submitted for publication.

** This work was partly supported by the Catalan Government through a grant BE–2 2006 and a grant 2005 SGR 00446 and by the Spanish Ministry of Education through projects TSI2007-65406-C03-01 E-AEGIS and CONSOLIDER CSD2007-00004 ARES.

S. Boztaş and H.F. Lu (Eds.): AAECC 2007, LNCS 4851, pp. 337–346, 2007.
© Springer-Verlag Berlin Heidelberg 2007

One can check that the new family of curves also fit the conditions for the list decoding algorithm for Hermitian codes using Gröbner basis presented by Lee and O'Sullivan [4].

The codes we obtain from these curves can be seen as codes from order domains. The theory of codes from order domains is developed in [5,6,7,8,9]. For these codes there is a lower bound on the minimum distance and an efficient generalization of the Berlekamp-Massey algorithm based on Sakata's algorithm for finding linear recurrence relations in multidimensional arrays [10]. Using the majority voting method of Feng, Rao, and Duursma, [11,12] the algorithm corrects up to half the above mentioned bound on the minimum distance. Improvements to code dimension, while maintaining a fixed decoding radius were discovered by Feng and Rao [11]. Our earlier work [13] considered a different improvement, based on the observation that the decoding algorithm corrects an error vector based not so much on the weight of the vector but rather the "footprint" of the error locations [14]. For some codes, most error vectors of a given weight t have a particular footprint. Those error vectors are called *generic* and are correctable with fewer check symbols than are required to correct all error vectors of weight t. These results may be combined with the Feng-Rao improvements to increase the dimension of a code while maintaining a desired correction capability.

We show how the codes from the new family of curves still satisfy Geil's duality properties stated for norm-trace codes [2]. That is, it is easy to find a minimal set of parity checks guaranteeing correction of a given number of errors, as well as the set of monomials generating the corresponding code.

Furthermore, following the results in [13] we describe a way to find the minimal set of parity checks and the corresponding generating monomials guaranteeing correction at least of generic errors. This gives codes with larger dimensions.

2 Codes from Extended Norm-Trace Curves

A linearized polynomial over $\mathbb{F}_q$—also called a q polynomial—is a polynomial over $\mathbb{F}_q$ whose terms all have degree a power of q [15, §3.4]. Let $L(y) = \sum_{i=0}^{d} a_i y^{q^i}$ be a linearized polynomial such that a_0, a_d are nonzero and such that $L(y) = 0$ has q^d distinct solutions in $\mathbb{F}_{q^r}$. Then L gives a q^d-to-one map from $\mathbb{F}_{q^r}$ into itself [15].

Let η be a primitive element of $\mathbb{F}_{q^r}$. Let v be any factor of $q^r - 1$ and let D be the powers of η^v, along with 0: $D = \{0\} \cup \{\eta^{vm} : m \in \{1, \ldots, \frac{q^r-1}{v}\}\}$. We will assume that $L(\mathbb{F}_{q^r}) \supseteq D$. Then for any u dividing v we consider the curve $x^u = L(y)$ whose coordinate ring is $A = \dfrac{\mathbb{F}_{q^r}[x, y]}{x^u - L(y)}$.

A basis of A as a vector space over $\mathbb{F}_{q^r}$ is given by the images in A of the set of monomials $\mathcal{B} = \{x^a y^b : b < q^d\}$. Consider $\ll$ the total ordering on A determined by the (q^d, u) weighted degree, $\deg_{q^d,u} x^a y^b = q^d a + ub$. One can check that any monomial in $\mathbb{F}_q[x, y]$ has the same weighted degree as exactly one monomial in $\mathcal{B}$. In particular, no two monomials from $\mathcal{B}$ have the same weighted degree. Let z_i be the ith monomial in $\mathcal{B}$ with respect to $\ll$, starting with $z_0 = 1$. Notice that

if z_i divides z_j then $i \leqslant j$. We say that a set of monomials W is *divisor-closed* if $z_i \in W$ whenever z_i divides a monomial in W.

Since u is coprime to q, this curve has a unique point at infinity. We consider all points (α, β) on the curve such that $\alpha^u = L(\beta) \in D$. Thus we have α is either 0 or $\alpha \in \{\eta^{mv/u} : m \in \{1, \ldots, \frac{(q^r-1)u}{v}\}\}$. There are $n = q^d(\frac{(q^r-1)u}{v} + 1)$ such points, $P_1, \ldots, P_n$.

Let $\varphi : A \longrightarrow \mathbb{F}_q^n$ be such that $f \mapsto (f(P_1), \ldots, f(P_n))$ and let W be a set of monomials in $\mathcal{B}$. We call E_W the linear code spanned by $\{\varphi(z_i) : z_i \in W\}$ and C_W the dual code.

Given W define W_φ as the set $\{z_i \in W : \varphi(z_i)$ is not in the span of $\varphi(z_j), j \in W, j < i\}$ and let $\mathcal{M} = \{x^a y^b : a \leqslant \frac{(q^r-1)u}{v}, b < q^d\}$. The next proposition shows how the set W defining a code can be reduced to its intersection with $\mathcal{M}$. For the sake of brevity, the proof of this proposition has been omitted.

Proposition 1. – *If $W \subseteq \mathcal{M}$ then $W_\varphi = W$.*
– *If W is divisor-closed then $W_\varphi = W \cap \mathcal{M}$.*

The next proposition shows how to find the set $W^\perp$ defining the dual code of the code defined by W. As before, for the sake of brevity, the proof of this proposition has been omitted. The proofs of both propositions is in [1].

Proposition 2. *Suppose that the prime divisor of q also divides $v-u$. If $W \in \mathcal{M}$ is divisor-closed then $C_W = E_{W^\perp}$ where*

$$W^\perp = \mathcal{M} \setminus \{x^{\frac{(q^r-1)u}{v}-a} y^{q^d-1-b} : x^a y^b \in W\}.$$

Example 1. Let q be a prime power, let i, j, k be positive integers with $j, k > 1$ and let r be a common multiple of ij and k. Consider the curve with affine equation $x^{\frac{q^{ij}-1}{q^i-1}} = y^{q^{k-1}} + y^{q^{k-2}} + \cdots + y^{q^2} + y^q + y$. We may write this as $\mathcal{N}_{\mathbb{F}_{q^{ij}}/\mathbb{F}_{q^i}}(x) = \mathcal{T}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(y)$ which is illustrated in the diagram of fields in Figure 1.

This curve matches the former scheme with $v = \frac{q^r-1}{q-1}$ and $u = \frac{q^{ij}-1}{q^i-1}$. In this case $D = \{0\} \cup \{\eta^{vm} : m \in \{1, \ldots, q-1\}\} = \mathbb{F}_q$, and we can verify that u divides v since $v/u = \frac{q^r-1}{q-1} \cdot \frac{q^i-1}{q^{ij}-1} = \frac{q^r-1}{q^{ij}-1} \cdot \frac{q^i-1}{q-1}$ is an integer. Furthermore,

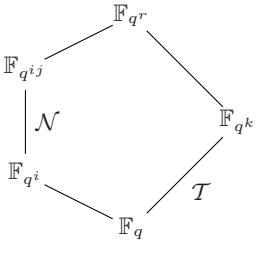


Fig. 1. Field extensions defining the curve of Example 1

both u and v are 1 modulo q so q divides $v-u$. Thus the assumptions of this section are fulfilled. Because of our choice of D, the only points on the curve that we are considering are in $\mathbb{F}_{q^{ij}} \times \mathbb{F}_{q^k}$ and there are $q^{k-1}(1+(q-1)u)$ of them. There may be other points on the curve, but we have not been able to show that the duality properties of this section can be extended to a larger set of points.

Norm-trace curves as defined in [2] correspond to the curves in this example when $i=1$ and $j=k=r$, and Hermitian curves correspond to the case when $i=1$ and $j=k=2$. Other curves can be obtained which are not Hermitian curves or norm-trace curves as in [2]. In Table 1 we list the possible norm and trace functions for all the extensions of finite fields contained in $\mathbb{F}_{2^8}$.

As an example, the curve with affine equation

$$x^3 = y^8 + y^4 + y^2 + y$$

over $\mathbb{F}_{2^4}$ is obtained taking $q=2$, $i=1$, $j=2$, $k=4$ and $r=4$. In this case $u=3$ and $v=15$ and the number of points in $\mathbb{F}_4 \times \mathbb{F}_{16}$ is 32. Considering $\mathbb{F}_{16} = \mathbb{Z}_2/(X^4+X+1)$ and taking $\alpha = [X]$, these 32 points are $(0,0)$, $(0,1)$, $(0,\alpha)$, $(0,\alpha^2)$, $(0,\alpha^4)$, $(0,\alpha^5)$, $(0,\alpha^8)$, $(0,\alpha^{10})$, $(1,\alpha^3)$, $(1,\alpha^6)$, $(1,\alpha^7)$, $(1,\alpha^9)$, $(1,\alpha^{11})$, $(1,\alpha^{12})$, $(1,\alpha^{13})$, $(1,\alpha^{14})$, (α^5,α^3), (α^5,α^6), (α^5,α^7), (α^5,α^9), (α^5,α^{11}), (α^5,α^{12}), (α^5,α^{13}), (α^5,α^{14}), (α^{10},α^3), (α^{10},α^6), (α^{10},α^7), (α^{10},α^9), $(\alpha^{10},\alpha^{11})$, $(\alpha^{10},\alpha^{12})$, $(\alpha^{10},\alpha^{13})$, $(\alpha^{10},\alpha^{14})$.

Table 1. For the field $\mathbb{F}_{256}$ the norm and trace functions appearing in Example 1 are listed. The curves considered are obtained for a fixed q by setting any norm function equal to any trace function.

$q=2$			
i,j	Norm functions on x	k	Trace functions on y
1,2	x^3	2	y^2+y
1,4	x^{15}	4	$y^8+y^4+y^2+y$
1,8	x^{255}	8	$y^{128}+y^{64}+y^{32}+y^{16}+$
2,2	x^5		$+y^8+y^4+y^2+y$
2,4	x^{85}		
4,2	x^{17}		

$q=4$			
i,j	Norm functions on x	k	Trace functions on y
1,2	x^5	2	y^4+y
1,4	x^{85}	4	$y^{64}+y^{16}+y^4+y$
2,2	x^{17}		

$q=16$			
i,j	Norm functions on x	k	Trace functions on y
1,2	x^{17}	2	$y^{16}+y$

3 Correction-Capability-Optimized Evaluation Codes

Given a field $\mathbb{F}$ and an $\mathbb{F}$-algebra A, an *order function* on A is a map $\rho : A \longrightarrow \mathbb{N}_{-1}$ which satisfies: i) the set $L_m = \{f \in A : \rho(f) \leqslant m\}$ is an $m+1$ dimensional vector space over $\mathbb{F}$; ii) if $f, g, z \in A$ and z is nonzero then $\rho(f) > \rho(g) \Longrightarrow \rho(zf) > \rho(zg)$ [6,5,16]. The pair A, ρ is often called an order domain. It is easy to show that ρ must be surjective. The ring A defined in Section 2 admits an order function in which z_i has order i. That is, we may define ρ by i) $\rho(0) = -1$, ii) $\rho(z_i) = i$, iii) $\rho(\sum_{i \in I} a_i z_i) = \max I$, where the $a_i's$ are assumed to be nonzero. Notice that in this case two elements f, g in A have the same order if and only if $v_{P_\infty}(f) = v_{P_\infty}(g)$.

Given an order function ρ an operation $\oplus$ in $\mathbb{N}_0$ can be well defined by $i \oplus j = \rho(fg)$ where f and g are such that $\rho(f) = i$ and $\rho(g) = j$. In our example, $i \oplus j = k$ is equivalent to $v_{P_\infty}(z_i) + v_{P_\infty}(z_j) = v_{P_\infty}(z_k)$. In fact $\mathbb{N}_0, \oplus$ is a commutative semigroup. We can define a partial ordering $\preccurlyeq$ on $\mathbb{N}_0$ by setting $i \preccurlyeq j$ if and only if there exists $k \in \mathbb{N}_0$ such that $i \oplus k = j$. When $i \preccurlyeq j$ we must also have $i \leqslant j$. An important parameter for decoding is $\nu_i = |\{j \in \mathbb{N}_0 : j \preccurlyeq i\}|$.

Codes from order domains are defined by means of a surjective map $\varphi : A \longrightarrow \mathbb{F}^n$. Consider a basis $\mathcal{B}$ of A with an element of each order. Given a subset W of $\mathcal{B}$, define the *order-prescribed evaluation code* related to W as the $\mathbb{F}$-subspace E_W generated by $\{\varphi(z_i) : z_i \in W\}$ and define C_W to be its dual code. For the codes considered here we take φ as the map which takes $f \in A$ to $(f(P_1), \ldots, f(P_n))$, where $P_1, \ldots, P_n$ are the points of the curve different than the one at infinity.

The subsets W can be defined in order to achieve optimal correction capability. The two results on decoding performance that we need are

Theorem 1. *[11] All error vectors of weight t can be corrected by C_W if W contains all elements z_i with $\nu_i < 2t + 1$.*

Theorem 2. *[13] All generic error vectors of weight t can be corrected by C_W if W contains all elements z_i with $i \notin \{j \oplus k : j, k \geqslant t\}$.*

Theorem 1 can be used to design an optimal order-prescribed evaluation code correcting t errors. Indeed, take $\widetilde{R}(t) = \{z_i \in \mathbb{N}_0 : \nu_i < 2t + 1\}$ and use the code $C_{\widetilde{R}(t)}$. This construction is due to Feng and Rao [11]. Theorem 2 can be used to design an optimal order-prescribed evaluation code correcting all generic errors of weight t. Indeed, take $C_{\widetilde{R}^*(t)}$ where $\widetilde{R}^*(t)$ is $\mathbb{N}_0 \setminus \{i \oplus j : i, j \geqslant t\}$. This construction was introduced in [13].

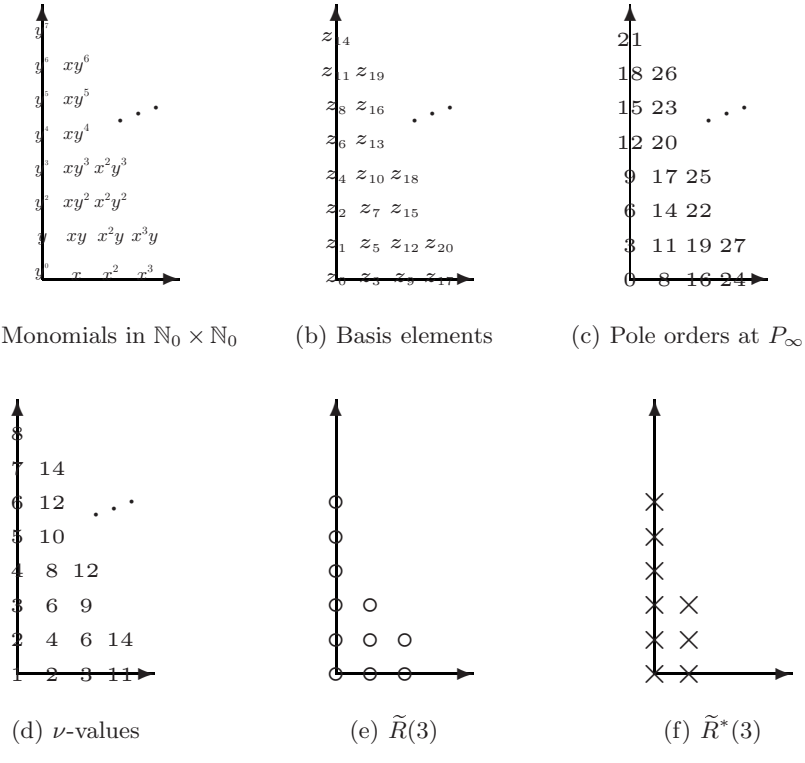
Example 2. Consider the codes over the curve with affine equation $x^3 = y^8 + y^4 + y^2 + y$ over $\mathbb{F}_{16}$. The monomials in A are ordered by their $(q^d, u) = (8, 3)$ graded degree, which in turn is the pole order of each monomial at infinity. Thus, $z_0 = 1$, $z_1 = y$, $z_2 = y^2$, $z_3 = x$, $z_4 = y^3$, $z_5 = xy$, etc.

The parity checks $\varphi(x^a y^b)$ can be represented by the corresponding monomials $x^a y^b$ and each monomial $x^a y^b$ can be represented by the point with coordinates (a, b) in the $\mathbb{N}_0 \times \mathbb{N}_0$ grid. This is illustrated in Figure 2(a) and Figure 2(b).

Figure 2(c) represents the pole order at infinity of each monomial represented in Figure 2(a). In this case the ν-value corresponding to the monomial z_i is the number of monomials z_j, z_k with $v_{P_\infty}(z_j) + v_{P_\infty}(z_k) = v_{P_\infty}(z_i)$. Figure 2(d) represents these ν-values.

Suppose we want to correct 3 errors. Theorem 1 says that the minimum set of parity checks that we need corresponds exactly to those monomials whose ν-value is at most 6. This gives the set $\widetilde{R}(3) = \{ z_0 = 1, z_1 = y, z_2 = y^2, z_3 = x, z_4 = y^3, z_5 = xy, z_6 = y^4, z_7 = xy^2, z_8 = y^5, z_9 = x^2, z_{12} = x^2 y\}$. These monomials are represented in Figure 2(e).

If we just want to guarantee correction of generic errors, Theorem 2 says that the minimum set of parity checks that we need corresponds exactly to those monomials whose pole order at infinity is not the sum of the pole orders of two monomials in $z_3, z_4, z_5, \ldots$. This gives the set $\widetilde{R}^*(3) = \{z_0 = 1, z_1 = y, z_2 = y^2, z_3 = x, z_4 = y^3, z_5 = xy, z_6 = y^4, z_7 = xy^2, z_8 = y^5\}$. These monomials are represented in Figure 2(f). Notice that $\widetilde{R}^*(3) \subseteq \widetilde{R}(3)$ and that $\widetilde{R}(3)$ has two more monomials than $\widetilde{R}^*(3)$.



(a) Monomials in $\mathbb{N}_0 \times \mathbb{N}_0$ (b) Basis elements (c) Pole orders at P_∞

(d) ν-values (e) $\widetilde{R}(3)$ (f) $\widetilde{R}^*(3)$

Fig. 2.

Dimension and Generating Matrices of Correction-Capability-Optimized Codes from Extended Norm-Trace Curves

In this subsection we see how the sets of check monomials giving correction-capability-optimized codes from extended norm-trace curves behave well in the sense that they are divisor-closed. Hence, we can find nice ways to determine the actual dimensions of the codes, their parity-check matrices and their generating matrices.

Lemma 1. *The sets $\widetilde{R}(t)$ and $\widetilde{R}^*(t)$ are divisor-closed.*

Proof. Notice that for a subset W being divisor-closed is equivalent to being $\preccurlyeq$-closed, that is, $i \in W$ for all $i \preccurlyeq j$ with $j \in W$. If $i \preccurlyeq j$ and $j \in \widetilde{R}(t)$ then $\nu_i \leqslant \nu_j < 2t+1$, so $i \in \widetilde{R}(t)$. Thus $\widetilde{R}(t)$ is closed under $\preccurlyeq$. To prove that $\widetilde{R}^*(t)$ is closed under $\preccurlyeq$ notice that, if $i \preccurlyeq j$ then $j = i \oplus s$ for some $s \in \mathbb{N}_0$. Suppose $i \notin \widetilde{R}^*(t)$. Then $i = k \oplus l$ with $k, l \geqslant t$ and $j = i \oplus s = k \oplus (l \oplus s)$ and so $j \notin \widetilde{R}^*(t)$.

Corollary 1. $\widetilde{R}_\varphi(t) = \widetilde{R}(t) \cap \mathcal{M}$, $\widetilde{R}^*_\varphi(t) = \widetilde{R}^*(t) \cap \mathcal{M}$.

Corollary 2. $C_{\widetilde{R}(t)} = C_{\widetilde{R}_\varphi(t)} = E_{\widetilde{R}_\varphi(t)^\perp}$, $C_{\widetilde{R^*}(t)} = C_{\widetilde{R^*}_\varphi(t)} = E_{\widetilde{R}^*_\varphi(t)^\perp}$.

Example 3. Consider the codes $C_{\widetilde{R}(3)}$ and $C_{\widetilde{R}^*(3)}$ over the curve $x^3 = y^8 + y^4 + y^2 + y$ represented in Figure 2(e) and Figure 2(f). In this case $\frac{(q^4-1)u}{v} = 3$ and $q^d - 1 = 7$, so $\mathcal{M} = \{x^a y^b : 0 \leqslant a \leqslant 3, 0 \leqslant b \leqslant 7\}$ (see Figure 3(a)). Since all checks in $\widetilde{R}(3)$ (resp. $\widetilde{R}^*(3)$) are inside $\mathcal{M}$, by Corollary 1, they are all linearly independent. So the dimension of $C_{\widetilde{R}(3)}$ is $32 - 11 = 21$ and the dimension of $C_{\widetilde{R}^*(3)}$ is $32 - 9 = 23$.

Now we can use Corollary 2 to derive, from $\widetilde{R}(3)$ and $\widetilde{R}^*(3)$, the set of monomials $x^a y^b$ such that the vectors $\varphi(x^a y^b)$ generate $C_{\widetilde{R}(3)}$ and $C_{\widetilde{R}^*(3)}$. In Figure 3(b) we represented all these sets. In Figure 4 and Figure 5 we give the explicit parity check matrices and generating matrices for these codes.

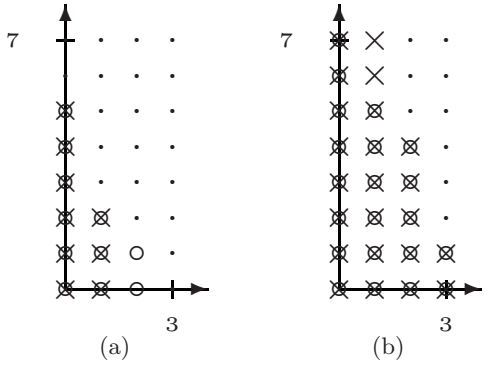


Fig. 3. Obtaining $\widetilde{R}(3)^\perp$ and $R^*_\varphi(3)^\perp$ from $\widetilde{R}_\varphi(3)$ and $R^*_\varphi(3)$, respectively

Fig. 4. Parity check matrix (above) and generating matrix (below) of $C_{\tilde{R}(3)}$

Fig. 5. Parity check matrix (above) and generating matrix (below) of $C_{\tilde{R}^*(3)}$

4 Conclusion

We described a new family of curves generalizing the norm-trace curves introduced by Geil. We showed how the associated correction-capability-optimized codes behave well in the sense that the set of defining check monomials is divisor-closed. This enables us to exactly determine the dimension of the codes and to construct a parity check matrix and a generating matrix.

References

1. Bras-Amorós, M., O'Sullivan, M.E.: Duality for Some Families of Correction Capability Optimized Evaluation Codes (2007)
2. Geil, O.: On Codes From Norm-Trace Curves. Finite Fields Appl. 9(3), 351–371 (2003)
3. Koetter, R.: On the Determination of Error Values for Codes From a Class of Maximal Curves. In: Proc. 35-th Allerton Conference on Communication, Control, and Computing, pp. 44–53 (1997)
4. Lee, K., O'Sullivan, M.E.: List Decoding of Hermitian Codes Using Groebner Bases (2006)
5. Hoeholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic Geometry Codes. In: Handbook of Coding Theory, vol. I, pp. 871–961. North-Holland, Amsterdam (1998)
6. O'Sullivan, M.E.: New Codes for the Berlekamp-Massey-Sakata Algorithm. Finite Fields Appl. 7(2), 293–317 (2001)
7. Geil, O., Pellikaan, R.: On the Structure of Order Domains. Finite Fields Appl. 8(3), 369–396 (2002)
8. Geil, O.: Codes Based on an F_q-Algebra. PhD thesis, Aalborg University (1999)
9. Little, J.B.: The Ubiquity of Order Domains for the Construction Of Error Control Codes. Adv. Math. Commun. 1(1), 151–171 (2007)
10. Sakata, S.: Extension of Berlekamp-Massey Algorithm to n Dimensions. IEEE Trans. Inform. Theory 34(5), 1332–1340 (1988)
11. Feng, G.L., Rao, T.R.N.: Improved Geometric Goppa codes. I. Basic Theory. IEEE Trans. Inform. Theory 41(6, part 1), 1678–1693 (1995)
12. Duursma, I.M.: Majority Coset Decoding. IEEE Trans. Inform. Theory 39(3), 1067–1070 (1993)
13. Bras-Amorós, M., O'Sullivan, M.E.: The Correction Capability of the Berlekamp-Massey-Sakata Algorithm With Majority Voting. Appl. Algebra Engrg. Comm. Comput. 17(5), 315–335 (2006)
14. Geil, O., Hoeholdt, T.: Footprints or Generalized Bezout's Theorem. IEEE Trans. Inform. Theory 46(2), 635–641 (2000)
15. Lidl, R., Niederreiter, H.: Introduction to Finite Fields and Their Applications, 1st edn. Cambridge University Press, Cambridge (1994)
16. Bourbaki, N.: Commutative Algebra, ch. 1–7. Elements of Mathematics. Springer, Berlin (1998)