On the Number of Correctable Errors for Some AG-Codes

H. Elbrønd Jensen, T. Høholdt, and J. Justesen

Abstract—**An algorithm that, for codes from a regular plane curve, corrects up to $(d^*/2)-(m^2/8)+(m/4)-(9/8)$ errors, where d^* is the designed distance and m is the degree of the curve was presented in an earlier work. It is now shown, that this bound is the best possible for the algorithm considered.**

Index Terms—**Decoding, algebraic geometry codes.**

I. Introduction

An algorithm for decoding algebraic geometry codes constructed from plane curves was presented in [1]. The idea in the algorithm is to separate the calculation of error positions and error values. The calculation of the (possible) error positions is based upon solving a certain system of linear equations. These equations actually have a structure which makes it possible to find the desired solution by using an algorithm of Sakata, who in [2] gave the proper generalization of the Berlekamp–Massey algorithm to higher dimensions. The observation of this fact is the background for the algorithm presented in [3], which first of all brings down the decoding complexity and moreover gives a better bound for the number of correctable errors.

The subject of this paper is the number of errors, which the algorithm can correct, and to explain things we will first briefly have to describe the code construction and the decoding procedure from [3].

Let $\mathbb{F}_q$ be a finite field with q elements, and let $C(x,y)$ be a polynomial from $\mathbb{F}_q[x,y]$. The curve $C(x,y)=0$ is supposed to be regular, and if m denotes the degree of $C(x,y)$ then $g=(m-1)(m-2)/2$ is the genus of the curve. With $P_1, P_2, \cdots, P_n$ we denote the points on the curve $C(x,y)=0$, for which both coordinates are in $\mathbb{F}_q$ and both are different from zero.

It is convenient to choose an ordering of the pairs of natural numbers, and we choose the so called graduated total degree ordering $<_T$, where $(0,0) <_T (1,0) <_T (0,1) <_T (2,0), \cdots$.

Let j be a natural number $m-2 \leq j \leq \lfloor (n-1)/m \rfloor$ and let $\varphi_0(x,y)$, $\varphi_1(x,y), \cdots, \varphi_s(x,y)$ denote the monomials $x^a y^b$ where $(a,b) \leq_T (0,j)$.

The code $C^*(j)$ is then given by its parity check matrix $\underline{\underline{H}}$

$$\underline{\underline{H}} = \begin{bmatrix} \varphi_0(P_1) \cdots \varphi_0(P_n) \\ \varphi_1(P_1) \cdots \varphi_1(P_n) \\ \vdots \\ \varphi_s(P_1) \cdots \varphi_s(P_n) \end{bmatrix}. \tag{1.1}$$

It now follows from [1] that the dimension of $C^*(j)$ is $n-(mj-g+1)$ and that

$$d_{\min} \geq d^* = mj - 2g + 2.$$

The number d^* is the *designed distance* of the code.

In the decoding situation we receive a word $\underline{r}$, and calculate the syndrome $\underline{s} = \underline{\underline{H}}\,\underline{r}^T$. We number the coordinates in $\underline{s}$ in the same way as we numbered the rows in $\underline{\underline{H}}$, that is $\underline{s} = (s_{ab})$, where $(0,0) \leq_T (a,b) \leq_T (0,j)$.

The idea is now to find solutions $\sigma(x,y) = \sum_{a\,b} \sigma_{ab} x^a y^b$ to

$$\sum_{a\,b} \sigma_{ab} s_{a+\alpha\, b+\beta} = 0, \tag{1.2}$$

where (α, β) runs through all possible values in $\mathbb{N}_0 \times \mathbb{N}_0$. All possible means, that $s_{a+\alpha\, b+\beta}$ must be known, that is $a+\alpha+b+\beta \leq j$ for all a and b in question.

The equations in (1.2) are recursions, and the algorithm of Sakata [2] gives an efficient way to deal with such equations. The result of the algorithm is a list of polynomials $\sigma(x,y)$, which in a certain sense gives minimal solutions to systems of equations (1.2). On this list, we pick out a polynomial $\sigma_0(x,y)$ of smallest degree, which is not the curve $C(x,y)$ itself. One of the main results in [3] is now, that if the number of errors t satisfies

$$t < \frac{d^*}{2} - \frac{m^2}{8} + \frac{m}{4} - \frac{1}{8}, \tag{1.3}$$

then $\sigma_0(x_i, y_i) = 0$ for all errorpoints (x_i, y_i). Consequently the error points are among the points on the intersection between $\sigma_0(x,y)$ and the curve $C(x,y)$, and using this the error vector can be calculated with fairly small complexity.

For details about this whole procedure we refer to [3]. The point here is to emphasize that the polynomial $\sigma_0(x,y)$ is determined as a minimal solution to a system of equations (1.2).

Our aim is to settle the question, whether or not the bound (1.3) is the true bound for the decoding algorithm. The fact, that a certain line of reasoning leads to this bound does of course not exclude, that one by other arguments could improve the bound. As we shall see however, this is basically not possible. The algorithm of Sakata is cumbersome to analyze in detail. To avoid discussions, which are unimportant in this context, we will therefore look at the algorithm from [3] as follows: What we do is to find a solution with smallest possible leading term, not having the curve as a divisor, to systems of the form (1.2). The concept "smallest leading term" refers to the ordering $<_T$ of the exponents of monomials with non-zero coefficients in the considered polynomials cf. [3]. In case there are many such solutions, we pick out one of these at random. The polynomial determined is this way is the output of the algorithm. The algorithm succeeds, if the output has the errorpoints as zeros. If (1.3) holds, this is the case. The algorithm fails, if it is possible, that the output of the algorithm *does not* have the error points as zeros.

II. When Will the Algorithm Fail

We consider a code $C^*(j)$ as previously defined. The positions in codewords and error vectors are numbered by the points $P_1, \cdots, P_n$. So an *error-pattern*, which we denote $\langle x_i, y_i, e \rangle$, $i = 1, \cdots t$, is characterized by a number of rational points (x_i, y_i) on the curve and for each point a corresponding errorvalue e_i.

Let us consider the system (1.2) for a certain errorpattern and for polynomials of degree h. Further, let $\varphi_0(x,y), \cdots, \varphi_1(x,y)$ be the monomials $x^a y^b$, $a+b \leq j-h$, ordered by the ordering $<_T$ of the pairs (a,b). Let $\underline{\underline{F}}_{j-h}$ denote the matrix

$$\underline{\underline{F}}_{j-h} = \{\varphi_s(x_i, y_i)\}, \qquad s = 0, \cdots, 1, \qquad i = 1, \cdots t. \tag{2.1}$$

From Lemma 4.3 [1]) follows, that (1.2) is the same as

$$\underline{\underline{F}}_{j-h}(e_i \sigma(x_i, y_i)) = \underline{0} \tag{2.2}$$

Manuscript received November 5, 1991; revised June 6, 1992. This work was presented in part at ITW-92, Salvador, Bahia, Brazil, June 21–26, 1992.

H. E. Jensen and T. Høholdt are with the Mathematical Institute, The Technical University of Denmark, Bld. 303, DK-2800 Lyngby, Denmark.

J. Justesen is with the Institute of Circuit Theory and Telecommunication, The Technical University of Denmark, Bld. 343, DK-2800 Lyngby, Denmark.

IEEE Log Number 9204212.

0018–9448/93$03.00 © 1993 IEEE

where the vector on the left hand side means the coulumnvector, for which element number i is $e_i\sigma(x_i, y_i)$, $i = 1, \cdots t$.

We use the term *errorlocator* to denote a polynomial $\sigma(x, y)$, which does not have the curve $C(x, y)$ as divisor and for which $\sigma(x_i, y_i) = 0$, $i = 1, \cdots, t$. With $\rho(\underline{\underline{F}}_{j-h})$ we denote the rank of the matrix $\underline{\underline{F}}_{j-h}$.

Lemma 1: Let h be the smallest degree of an errorlocator. The algorithm succeeds in the following two situations:

a) $\rho(\underline{\underline{F}}_{j-h}) = t$,

b) $\rho(\underline{\underline{F}}_{j-h}) < t$, but there are no nonzero vectors of the form $(e_i\sigma(x_i, y_i))$ in the nullspace of $\underline{\underline{F}}_{j-h}$, where $\deg[\sigma(x, y)] \leq h$.

Proof: The output $\sigma_0(x, y)$ of the algorithm is a polynomial with smallest leading term, such that $\sigma_0(x, y)$ does not have the curve as divisor and satisfies the corresponding system of equations (1.2).

The two conditions stated both insures, that any solution to (2.2) of degree h (or smaller) is an errorlocator (consequently there are no solutions with degree smaller than h). This proves the lemma. □

Lemma 2: Let h be the smallest degree of an errorlocator. The algorithm fails, if the following two conditions are satisfied

a) $\rho(\underline{\underline{F}}_{j-h}) < t$,

b) there exists a polynomial $\psi(x, y)$ with deg $[\psi(x, y)] < h$, such that $(e_i\psi(x_i, y_i))i = 1, \cdots, t$ is a non zero vector in the nullspace of $\underline{\underline{F}}_{j-h}$.

Proof: In this situation, there are two possibilities. The first one is, that corresponding to degree $h-1$ or smaller, the system (1.2) has a solution, which does not have the curve as divisor. In this situation, the output $\sigma_0(x, y)$ is clearly *not* an errorlocator, by the definition of h.

Suppose this is not the case and let $\sigma(x, y)$ be an errorlocator with smallest leading term. Then, by (2), the polynomials

$$\sigma(x, y) + \alpha\psi(x, y), \qquad \alpha \in \mathbb{F}_q, \tag{2.3}$$

are all solutions to (1.2) with the same leading term as $\sigma(x, y)$, and only for $\alpha = 0$ such a polynomial is an errorlocator. So either the output has smaller leading term than $\sigma(x, y)$, and is hence not an errorlocator, or $\sigma_0(x, y)$ is picked out from a set of polynomials—at least those in (2.3)—with the same leading term as $\sigma(x, y)$. This proves the lemma. □

Of course, condition b) implies a), but it is not true that given t error positions satisfying a), there always exist error values such that b) holds.

Referring to the above lemma and the proof, it is of course possible, that one in the situation corresponding to (2.3) by chance picks out an errorlocator among the solutions with smallest leading term. But it is very unlikely, and therefore, we say that the algorithm fails in these situations. (Lemma 2.2 is treated as Proposition 4 in [5]).

The important term in the decoding process is the rank of matrices $\underline{\underline{F}}_{j-h}$. The key to estimation of this number is the result in the following lemma, which is based on algebraic geometry. By C', we denote the projective closure of the curve C, and by $\sigma(x, y, z)$ the homogenous version of $\sigma(x, y)$. The errorpoints are $P_i = (x_i, y_i, 1)$, $i = 1, \cdots, t$.

Lemma 3: Let $\sigma(x, y, z)$ be an errorlocator of degree $h \leq j/2$, and let $P_1, \cdots, P_t$, $Q_1, \cdots, Q_u$ be the points in the algebraic closure of $\mathbb{F}_q$, in which $\sigma(x, y, z)$ intersects C'. Suppose, that $j - h \geq m - 2$. Then, for $s = 0$, 1, we have

$$\rho\left(\underline{\underline{F}}_{j-h+s}\right) = t - \rho', \tag{2.4}$$

where ρ' is the dimension of the projective space of homogenous polynomials of degree $m - 3 - (j - 2h) - s$ passing through the points $Q_1, \cdots Q_u$.

Proof: Let $h' = j-h+s$ and let $V_{h'}$ denote the vector space of polynomials, modulo the curve $C'(x, y, z)$, passing through the points $P_1, \cdots, P_t$. The space of all polynomials of degree h', modulo the curve, has dimension $mh' - g + 1$ ([1], Section II. since $h' \geq m - 2$) and hence,

$$\dim(V_{h'}) = mh' - g + 1 - \rho\left(\underline{\underline{F}}_{j-h+s}\right). \tag{2.5}$$

The polynomial $z^{j-2h+s}\sigma(x, y, z)$ belongs to $V_{h'}$, and intersects the curve in mh' points, counted with multiplicity. Let $R_1, \cdots, R_i$ denote the intersection points, which are not the points $P_1, \cdots, P_t$. According to the Riemann–Roch Theorem we have

$$\dim(V_{h'}) = mh' - g + 1 - t + p_1', \tag{2.6}$$

where ρ_1' is the dimension of polynomials of degree $m - 3$ passing through $R_1, \cdots, R_i$. These polynomials are all of the form $z^{j-2h+s}\sigma_1(x, y, z)$, where $\sigma_1(x, y, z)$ has degree $m - 3 - (j - 2h) - s$, and has $Q_1, \cdots, Q_u$ as zeros. Therefore, $\rho_1' = \rho'$ and by comparing (2.5) and (2.6), the lemma follows. □

As a consequence, $\rho(\underline{\underline{F}}_{j-h}) = t$ if $\rho' = 0$, and the simplest way to insure that $\rho' = 0$ is to demand that

$$m(m - 3 - (j - 2h)) < mh - t, \tag{2.7}$$

According to the theorem of Bezout, the left-hand side of (2.7) is the number of points in which a polynomial of degree $m - 3 - (j - 2h)$ intersects the curve C', and the right-hand side is the number of points $Q_1, \cdots, Q_u$. So clearly, if (2.7) holds, we have $\rho' = 0$. The bound (1.3)—and the bound in [1]—is based on this line of reasoning.

But (2.7) is a sufficient, not a necessary condition for $\rho' = 0$. If you run the algorithm on a computer, which we have done for a specific code $C^*(j)$, you will observe that in general the algorithm corrects errors up to half the minimum distance, and even beyond half the minimum distance. The reason for this seems to be, that in general at least one of the conditions in Lemma 1 holds. Actually, an errorpattern shall be rather cleverly selected to make the algorithm break down. One way to do this is explained in the next section.

III. The Construction

In this section, we consider codes $C^*(j)$ constructed from a Hermitian curve (cf. [1])

$$y^{r+1} - x^r - x = 0 \tag{3.1}$$

of degree $m = r + 1$. Over the field GF$[r^3]$ this curve has r^3 rational points, of which $r^3 - r$ has both coordinates different from zero. The code considered has therefore length $n = r^3 - r$. An important property is that the n rational points lie on $r^2 - r$ lines, where each line intersects the curve in m rational points. We denote these lines $\ell_1(x, y), \cdots, \ell_a(x, y)$. These lines have no rational points in common.

Lemma 4: Let p be a number with $1 \leq p < m$, and let $v = (1/2)p(p + 1)$. Then there exist rational points $P_1', \cdots, P_v'$ on the curve C, such that any polynomial passing through $P_1', \cdots, P_v'$ has degree at least p.

Proof: Let $\underline{\underline{G}}$ be the matrix (2.1) corresponding to $j-h=p-1$ and some points $P_1', \cdots, P_v'$. Looking for a polynomial $\sigma(x,y) = \sum \sigma_{ab} x^a y^b$, $a+b \le p-1$, passing through $P_1', \cdots, P_v'$, is the same as looking for solutions to

$$\underline{\underline{G}}^T \underline{\sigma} = \underline{0}, \tag{3.2}$$

where $\underline{\sigma} = (\sigma_{ab})$ is the vector of coefficients in the polynomial. The matrix $\underline{\underline{G}}$ is an $v \times v-$matrix, so the points $P_1', \cdots, P_v'$ must be chosen in such a way, that the rank of $\underline{\underline{G}}$ equals v. Suppose, that this is not the case for the points considered, and let s denote the first row in $\underline{\underline{G}}^T$, which is dependent of the proceeding rows. This means, that any polynomial of degree $p-1$ or smaller, which passes through $P_1', \cdots, P_{s-1}'$, also has P_s' as a zero. The number of points P_s' with the property is at most $(p-1)m$, by the theorem of Bezout. Therefore we can find a rational point P_s'' on the curve, such that there exists a polynomial of degree $\le p-1$, passing through $P_1', \cdots, P_{s-1}'$, but not passing through P_s''. By substituting P_s' with P_s'', the first s rows in $\underline{\underline{G}}^T$ are then linearly independent, and continuing in this way, the lemma follows.

We are now ready to introduce our construction. We consider $C^*(j)$, where as usual $m-2 \le j < r^2 - r$, $m = r+1$. Choose first $p_2 < m$ and take points $P_1', \cdots, P_v'$ where $v = (1/2)p_2(p_2+1)$ with the property in lemma 3.1. Let $\psi(x,y)$ be a polynomial of degree p_2 passing through these points. Among the lines $\ell_1(x,y), \cdots, \ell_a(x,y)$ we choose p_1 lines, which does not pass through any of the intersection points of $\psi(x,y)$ with the curve $C(x,y)$. Let $P_1, \cdots, P_k$, where $k = p_1 m$, be the k rational points from the curve on the lines. The points

$$P_1, \cdots, P_k, \qquad P_1', \cdots, P_v' \tag{3.3}$$

are then the type of errorpoints we consider. For any choice of error values we have the following lemma. □

Lemma 5: The smallest degree of an errorlocator is $h = p_1 + p_2$.

Proof: Suppose, that $\sigma(x,y)$ is an errorlocator, and let $\sigma_1(x,y)$ be the product of the polynomials corresponding to the p_1 lines. It follows from the theorem of Noether, that $\sigma(x,y) = \sigma_1(x,y)\sigma_2(x,y)$. Since $\sigma_2(x,y)$ has the points $P_1', \cdots, P_v'$ as zeros, it follows from Lemma 4, that the degree of $\sigma(x,y)$ is at least p_2. This proves the lemma. □

Let us now especially suppose that

$$h = p_1 + p_2 \le j/2, \qquad p_2 = m - 3 - (j - 2h). \tag{3.4}$$

We have an errorlocator $\sigma(x,y) = \sigma_1(x,y)\sigma_2(x,y)$ as in the proof of Lemma 5, and h is the smallest degree of an errorlocator. Now, consider Lemma 3 in the situation $s=0$. For the term ρ' we have $\rho' > 0$, because $\sigma_2(x,y,z)$, the homogenous version of $\sigma_2(x,y)$, is an element in the vectorspace for which ρ' denotes the dimension. Consequently,

$$\rho(\underline{\underline{F}}_{j-h}) < t, \tag{3.5}$$

which means that the first condition in Lemma 2 is satisfied. Therefore, we first find the smallest number of points for which the above construction is possible. The number of errorpoints is $t = p_1 m + (1/2)p_2(p_2+1)$, which we under the conditions (3.4) can rewrite as

$$\begin{aligned} t &= (h - m + 3 + j - 2h)m \\ &\quad + \frac{1}{2}(m - 3 - j + 2h)(m - 3 - j + 2h + 1). \end{aligned} \tag{3.6}$$

Considered as a function of h, this is a polynomial of degree two of the form $2h^2 + (-m + 2m - 6 - 2j + 1)h + \cdots$. Without restrictions, the minimum value of (3.6) is therefore obtained for

$$\begin{aligned} h &= \frac{j}{2} - \frac{m-3}{4} + \frac{1}{2}, \qquad p_2 = \frac{m-3}{2} + 1, \\ p_1 &= \frac{j}{2} - \frac{3(m-3)}{4} - \frac{1}{2}. \end{aligned} \tag{3.7}$$

Inserting this in $t = p_1 m + (1/2)p_2(p_2+1)$, we find the minimum value

$$\begin{aligned} t_0 &= \frac{mj}{2} - \frac{3m(m-3)}{4} - \frac{m}{2} \\ &\quad + \frac{1}{2}\left(\frac{m-3}{2} + 1\right)\left(\frac{m-3}{2} + 2\right) \\ &= \frac{mj}{2} - \frac{m(m-3)}{2} - \frac{m^2}{4} + \frac{3m}{4} \\ &\quad - \frac{m}{2} + \frac{1}{8}(m-3)^2 + \frac{3(m-3)}{4} + 1 \\ &= \frac{mj}{2} - \frac{2g-2}{2} - \frac{m^2}{8} + \frac{m}{4} - \frac{1}{8}, \end{aligned}$$

that is,

$$t_0 = \frac{d^*}{2} - \frac{m^2}{8} + \frac{m}{4} - \frac{1}{8}, \tag{3.8}$$

when m and j are given; it is a course not always possible to obtain (3.8) with natural numbers h, p_1, and p_2. The bound will be somewhat greater. But to avoid unnecessary details we formulate the result as follows.

Theorem 1: Consider a Hermitian curve C of degree m, where m is odd, and a code $C^*(j)$, where $j - \frac{m-1}{2}$ is even and where $(3/2)m - (3/2) \le j < m^2 - 3m + 2$. If

$$t \ge \frac{d^*}{2} - \frac{m^2}{8} + \frac{m}{4} - \frac{1}{8}, \tag{3.9}$$

there exists an errorpattern $\langle x_i, y_i, e_i \rangle$, $i = 1, \cdots, t$, for which the decoding algorithm fails.

Proof: Suppose first that $t = t_0$ in (3.9). Using the previously stated construction with p_1 and p_2 from (3.7), we obtain t points $\langle x_i, y_i \rangle$. Remark first, that p_1 and p_2 are indeed natural numbers. Moreover, it follows from the inequality $j < m^2 - (3/2)m + (1/2)$ that

$$(m-1)(m-2) - m\left(\frac{m-3}{2} + 1\right) > \frac{j}{2} - \frac{3(m-3)}{4} - \frac{1}{2},$$

which shows that it is possible to choose the p_1 lines as wanted. The smallest degree of an errorlocator is $h = p_1 + p_2$, and as proved before in (3.5) we have $\rho(\underline{\underline{F}}_{j-h}) < t$. Consequently there exists a vector $\boldsymbol{c} = (c_i) \ne \underline{0}$, such that $\underline{\underline{F}}_{j-h}\underline{c} = \underline{0}$. Therefore, if we for some errorvalues e_i can prove, that there exists a polynomial $\psi(x,y)$ with $\deg[\psi(x,y)] < h$ and

$$e_i \psi(x_i, y_i) = c_i, \qquad i = 1, \cdots, t, \tag{3.10}$$

then, by Lemma 2, the theorem is proved in the case $t = t_0$. We will prove, that the polynomial $\psi(x,y)$ introduced just before Lemma 5 will do the job. To see this, consider first any index i corresponding to one of the "independent" points $P_1', \cdots, P_v'$. And let us suppose that $c_i \ne 0$. This means, that column number i in the matrix $\underline{\underline{F}}_{j-h}$ is a linear combination of the other columns. This again means, that any polynomial of degree $j-h$ or smaller passing through the other errorpoints necessarily also passes through P_i'. However, this contradicts the way in which the points $P_1', \cdots, P_v'$ are chosen. Therefore $c_i = 0$. Now, consider (3.10). We have just proved, that for any i corresponding to $P_1', \cdots, P_v'$ the equality is satisfied for any choice of the e_i. For the remaining points, we put

$e_s = c_s/\psi(x_s, y_s)$, and here $\psi(x_s, y_s) \neq 0$ by the choice of the points $P_1, \cdots, P_k$. Remark, that $\deg[\psi(x,y)] = p_2 < h$, by the assumption $j \geq (3/2)\,m-(3/2)$. If $t > t_0$ we simply add points with errorvalue zero to the previously stated construction. This concludes the proof of the theorem. □

We have used the Hermitian curve because the rational points on this are so easy to handle, but this is probably also the case for many other curves.

For a code $C^*(j)$ from a Hermitian curve, we have however more information in the decoding situation than the syndromes $S_{ab},\ a + b \leq j$, and this can be used to get a minor improvement. This fact has no influence on the general results for the algorithm as previously described, but since the extra information is readily available in this specific situation we will make some comments about it.

From the curve equation $y^{r+1} - x^r - x = 0$ follows, in general, that

$$S_{a\,b+r+1} = S_{a+r\,b} + S_{a+1\,b}.$$

Therefore, when we are decoding a code $C^*(j)$, we know the syndromes $S_{a\,b},\ a + b \leq j$ and $S_{0\,j+1},\ S_{1\,j}, \cdots, S_{j-r\,r+1}$. Using all these syndromes as input to the algorithm one can realize, either by theoretical arguments or by experiments in concrete situations, that an error pattern as the one in Theorem 1 will be correctly decoded. To construct examples where the algorithm breaks down also with this extended input, one must change things a little.

We choose the error points in the same way as before, but such that the smallest degree h of an error locator satisfies

$$h = p_1 + p_2,\ p_2 = m - 3 - (j - 2h) - 1. \tag{3.11}$$

Let us now imagine, that we run the algorithm with all syndromes $S_{a\,b},\ a+b \leq j+1$, as input. Then, with notation as above, because of (3.11) the rank of the matrix $\underline{\underline{F}}_{j+1-h}$ is smaller that t (cf. Lemma 3). One can then, as before, find an error pattern for which the algorithm fails, and therefore of course the algorithm also fails if the input is the syndromes $S_{a\,b},\ a + b \leq j$, and $S_{0\,j+1}, \cdots, S_{j-r\,r+1}$. To find the smallest number of points for which this construction is possible, we shall minimize an expression corresponding to (3.6). Carrying out the calculations one obtains

$$t_1 = \frac{d^*}{2} - \frac{m^2}{8} + \frac{3m}{4} - \frac{1}{8}, \tag{3.12}$$

which is a somewhat greater bound than (3.8). But the difference is not significant compared to the bound itself, and we will not discuss this problem further.

This situation can only occur if $m \geq 6$, so the smallest case in characteristic 2 is $r = 8$, which gives codes of length 504 over GF(64).

The bound (3.9) is the same as the bound (1.3), and hence the results in this correspondence shows, that the bound obtained in [2] in the general case is the optimal one for the method considered.

References

[1] J. Justesen, K.J. Larsen, A. Havemose, H.E. Jensen and T. Høholdt, "Construction and decoding of a class of algebraic geometry codes," *IEEE Trans. Inform. Theory,* vol. 35, pp. 811–821, July 1989.

[2] S. Sakata, "Extension of the Berlekamp–Massey algorithm to N dimensions," *Inform. Computat.,* vol. 84, no. 2, pp. 207–239, Feb. 1990.

[3] J. Justesen, K.J. Larsen, H. Jensen, and T. Høholdt, "Fast decoding of codes from algebraic plane curves," *IEEE Trans. Inform. Theory,* vol. 38, pp. 111–120, Jan. 1992.

[4] A.N. Skorobogatov and S.G. Vlădut, "On the decoding of algebraic–geometric codes," *IEEE Trans. Inform. Theory,* vol. 36, pp. 1051–1061, Sept. 1990.

[5] I.M. Duursma, "Algebraic decoding using special divisors," preprint, Eindhoven Univ. of Technol., The Netherlands, 1991.

Phased Burst Error-Correcting Array Codes

Rodney M. Goodman, Robert J. McEliece, and Masahiro Sayano

Abstract—**Various aspects of single phased burst error-correcting array codes are explored. These codes are composed of two-dimensional arrays with row and column parities with a diagonally cyclic readout order; they are capable of correcting a single burst error along one diagonal. Optimal codeword sizes are found to have dimensions $n_1 \times n_2$ such that n_2 is the smallest prime number larger than n_1. These codes are capable of reaching the Singleton bound. A new type of error, approximate errors is defined; in q-ary applications, these errors cause data to be slightly corrupted and thererfore still close to the true data level. Phased burst array codes can be tailored to correct these codes with even higher rates than before.**

Index Terms—**Error-correcting codes, array codes, phased burst correction, approximate errors.**

I. Introduction

In computer memory and communications applications, information can be corrupted by bursts of noise which occur within one of many predetermined sectors or time intervals. These noise patterns will be called phased burst errors [1] because although the noise pattern may be random at each burst, its duration and starting points are restricted to certain intervals. Noise sources which can generate these errors include line noise, synchronization errors in demodulation, timing errors in multivalued memories, and backscatter radar signals. These errors are often periodic in time (or, in the case of memories, in position) and can be long in duration. (See Fig. 1).

A motivation for studying this problem is the encoding of multilevel random access memories, where each cell contains more than one bit of data. These memories use dynamic RAM cells to store one of several discrete voltages. An experimental 4-Mbit chip with 16 possible voltage levels (4 bits worth of data) stored in each cell was reported in [2]. Voltage levels in each cell are stored and sensed by ramping the voltages on pertinent row and column select lines.

Manuscript received November 4, 1991. R.M. Goodman and M. Sayano are supported in part by NSF Grant MIP-8711568. R.J. McElliece was supported by AFOSR Grant 91-0037 and a grant from Pacific Bell. This work was presented in part at the IEEE/CAM Information Theory Workshop, Cornell University, Ithaca, NY, June 25–29, 1989, in part at the International Symposium on Information Theory, San Diego, CA, January 14–19, 1990, and in part at the IEEE International Symposium on Information Theory, Budapest, Hungary, June 24–28, 1991.

R.M. Goodman and R.J. McEliece are with The Department of Electrical Engineering, California Institute of Technology, Mail Code 116–81, Pasadena, CA 91125.

M. Sayano was with The Department of Electrical Engineering, California Institute of Technology, Mail Code 116–81, Pasadena, CA 91125. He is now with The Aerospace Corporation, El Segundo, CA 90009–2957.

IEEE Log Number 9204213.

0018–9448/93$03.00 © 1993 IEEE