Sixth International Workshop on Optimal Codes and Related Topics
June 16-22, 2009, Varna, Bulgaria *pp. 145-150*

Additional relations between coefficients of error locator polynomial

Valeriy Lomakov vl@guap.ru
St. Petersburg State University of Aerospace Instrumentation
190000, Bolshaya Morskaya, 67, St. Petersburg, Russia

Abstract. A method is described for obtaining additional relations between coefficients of the error locator polynomial. The obtained relations are used for list correcting, in polynomial time, +1 error with cyclic codes.

1 Introduction

Several procedures for decoding cyclic codes beyond the BCH bound were presented. Most of them use special techniques to determine the unknown syndromes from Newton's identities (see [1–4]) or some other syndrome relations (see [5, Ch. 10.5] and [1, 6]) by means of the known syndromes. Thus, the decoding capabilities of these procedures are limited to half the minimum distance. In contrast to these procedures, list decoding procedures break away this restriction at the cost of complexity of bivariate polynomial factorization (see [7, 8]). The aim of this paper is not to describe a faster procedure but point out a method to obtain additional relations between coefficients of the error locator polynomial without determination of the unknown syndromes.

2 Preliminaries

Denote by L the set of all roots of unity of degree n over the field $\mathbb{F}_q$: $L = \{\alpha_i\}_1^n$, $\alpha_i = \alpha^i$, where α is a primitive root of $x^n - 1 = 0$. The field $\mathbb{F}_{q^m}$ is obtained from $\mathbb{F}_q$ by adjoining to $\mathbb{F}_q$ a primitive zero of $x^n - 1$, i. e., $L \subset \mathbb{F}_{q^m}$.

Suppose the error vector $\mathbf{e} = (e_0, e_1, \ldots, e_{n-1})$, $e_i \in \mathbb{F}_q$, has nonzero components $e_{i_1}, e_{i_2}, \ldots, e_{i_t}$, where $t = \mathrm{wt}(\mathbf{e})$ is the Hamming weight of $\mathbf{e}$, and no other. If we associate with $\mathbf{e}$ the elements of L: $X_1, X_2, \ldots, X_t$, where $X_j = \alpha_{i_j}$, then we say that $\sigma(x)$ is the error locator polynomial and write

$$\sigma(x) = \prod_{j=1}^{t}(X_j x - 1) = \sum_{j=0}^{t} \sigma_j x^j,\ \sigma_0 = 1. \tag{1}$$

Without loss of generality we can assume that $t = \deg \sigma(x) \leq n - 1$.

Let the $n \times n$ Hankel matrix S associated with $\sigma(x)$ has the form

$$S = \begin{pmatrix} \sigma_0 & \sigma_1 & \sigma_2 & \dots & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & \sigma_3 & \dots & \sigma_0 \\ \sigma_2 & \sigma_3 & \sigma_4 & \dots & \sigma_1 \\ \dots & \dots & \dots & \dots & \dots \\ \sigma_{n-1} & \sigma_0 & \sigma_1 & \dots & \sigma_{n-2} \end{pmatrix}, \tag{2}$$

where $\sigma_l = 0$, $\forall l > t$. We introduce a concise notation for minors of order l of S formed by $i_1, i_2, \dots, i_l$ rows and $j_1, j_2, \dots, j_l$ columns:

$$D^{(l)} = S \begin{pmatrix} i_1 & i_2 & \dots & i_l \\ j_1 & j_2 & \dots & j_l \end{pmatrix}.$$

By $D_1, D_2, \dots, D_n$ denote consistent principal minors of S.

3 Additional relations

By definition,

$$\mathrm{GCD}\,(\sigma(x),\, x^n - 1) = \frac{\sigma(x)}{\sigma_t}. \tag{3}$$

The following generalization of König-Rados theorem [9, Th. 6.1] provides a way to use this property for obtaining additional relations between σ_i.

Theorem 1. *Suppose $\sigma(x)$ is a polynomial denoted in* (1)*. Then*

$$\exists\, D^{(n-t)} \neq 0, \tag{4}$$

$$D^{(l)} = 0, \quad \forall l \geqslant n - t + 1. \tag{5}$$

Proof. Use the elements of L to set up the nonsingular ($\alpha_i \neq \alpha_j$, $\forall i \neq j$) Vandermonde matrix [10, Ch. 4, § 8, L. 17]

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \dots & \dots & \dots & \dots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix}.$$

Multiplying S and A and using $\alpha_i^n = 1$, $\forall \alpha_i \in L$, we get

$$SA = \begin{pmatrix} \sigma(\alpha_1) & \sigma(\alpha_2) & \dots & \sigma(\alpha_n) \\ \alpha_1^{-1}\sigma(\alpha_1) & \alpha_2^{-1}\sigma(\alpha_2) & \dots & \alpha_n^{-1}\sigma(\alpha_n) \\ \alpha_1^{-2}\sigma(\alpha_1) & \alpha_2^{-2}\sigma(\alpha_2) & \dots & \alpha_n^{-2}\sigma(\alpha_n) \\ \dots & \dots & \dots & \dots \\ \alpha_1^{-(n-1)}\sigma(\alpha_1) & \alpha_2^{-(n-1)}\sigma(\alpha_2) & \dots & \alpha_n^{-(n-1)}\sigma(\alpha_n) \end{pmatrix}.$$

Find the rank of SA. First note that $\mathbf{v}$ has no $n-t+1$ zero components, i.e., $\exists \alpha_{i_j} \in L\colon \sigma(\alpha_{i_j}) = 0$. Then any minor of SA of order $l \geq n-t+1$ has at least one zero column. Hence the rank of SA is at most $n-t$. Otherwise write the minor of SA of order $n-t$ formed by $1, 2, \ldots, n-t$ rows and $i_1, i_2, \ldots, i_{n-t}$ columns of SA

$$\prod_{j=1}^{n-t} \sigma(\alpha_{i_j}) \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_{i_1}^{-1} & \alpha_{i_2}^{-1} & \ldots & \alpha_{i_{n-t}}^{-1} \\ \alpha_{i_1}^{-2} & \alpha_{i_2}^{-2} & \ldots & \alpha_{i_{n-t}}^{-2} \\ \multicolumn{4}{c}{\dotfill} \\ \alpha_{i_1}^{-(n-t-1)} & \alpha_{i_2}^{-(n-t-1)} & \ldots & \alpha_{i_{n-t}}^{-(n-t-1)} \end{vmatrix},$$

If $i_1, i_2, \ldots, i_{n-t}$ are indices of zero components of $\mathbf{v}$ ($\sigma(\alpha_{i_j}) \neq 0$), then this minor is nonzero. Therefore the rank of SA is $n-t$.

But A is nonsingular, hence SA and S have the same rank. Thus $\exists\, D^{(n-t)} \neq 0$ and $D^{(l)} = 0$, $\forall l \geq n-t+1$. $\square$

4 Correcting +1 error

Let the $e(x) = \sum_{j=0}^{t} e_{i_j} x^{i_j}$, $e_{i_j} \neq 0$, be the error polynomial associated with the vector $\mathbf{e}$. Suppose $t = \frac{\delta'}{2} + 1$, where $\delta' = 2\left\lfloor \frac{\delta-1}{2} \right\rfloor$ and δ is the BCH bound of a cyclic code with minimum distance $d \geq \delta$. Then write

$$\sigma_j = \Phi_j(S_1, \ldots, S_{\delta'}, z),\ j \in \{1, \ldots, t\}, \tag{6}$$

where Φ_j is a function of given syndromes $\{S_i\}_1^{\delta'}$ and unknown $z \in \mathbb{F}_{q^m}$. The function Φ_j is a linear function of z [5, Ch. 7.3]. Find z using relation (5)

$$D^{(n-t+1)} = F(\sigma_1, \ldots, \sigma_t) = \sum_i c_i \prod_{j=1}^{t} \sigma_j^{b_{ij}} = 0, \tag{7}$$

where F is a function of σ_j, $c_i \in \mathbb{F}_q$ and b_{ij} are some degrees. We are interested in nontrivial ($\exists i\colon c_i \neq 0$) relation (7). Taking into account $F(\sigma_1, \ldots, \sigma_t) = F_1(\sigma_1, \ldots, \sigma_{t-1}) + \sigma_t F_2(\sigma_1, \ldots, \sigma_t)$, find it by the following theorem.

Theorem 2. *Suppose $\sigma_t = 0$, $\sigma_{t-1} \neq 0$, $1 \leq t \leq \frac{n-1}{2}$, and*

$$D^{(n-t+1)} = S\begin{pmatrix} 1 & \ldots & t & 2t & \ldots & n \\ 1 & \ldots & t & 2t & \ldots & n \end{pmatrix}.$$

Then at least one of D_{n-t+1} and $D^{(n-t+1)}$ is nonzero.

Proof. The proof is completed by showing that $D^{(n-t+1)} \neq 0$, if $D_{n-t+1} = 0$. For this evaluate $D_t, D_{t+1}, \ldots, D_{n-t}$:

$$D_t = (-1)^{\lfloor \frac{t}{2} \rfloor} \sigma_{t-1}^t \neq 0,$$
$$D_{t+1} = (-1)^{\lfloor \frac{t+1}{2} \rfloor} \sigma_t^{t+1} = 0.$$

If $n > 7$

$$D_{t+2} = \ldots = D_{n-t-1} = 0,$$

because these minors have at least one zero column. And

$$D_{n-t} = (-1)^{\frac{n-2t-1}{2}} D_{t+1} = 0.$$

I. e., $D_t \neq 0$, $D_{t+1} = \cdots = D_{n-t+1} = 0$, hence it follows from Frobenius's theorem [11, Ch. X, Th. 23] that $D^{(n-t+1)} \neq 0$. □

Substituting (6) for σ_j in nontrivial relation (7) and fixing $\{S_i\}_1^{\delta'}$ for a certain $\mathbf{e}$, we get

$$F(\sigma_1, \ldots, \sigma_t) = F\left(\Phi_1(z), \ldots, \Phi_t(z)\right) = \Phi(z) = 0, \tag{8}$$

where Φ is a function of z and only. Suppose $\Phi_t(z) = az + b$; then denote by L^* the set of n elements $\left\{a^{-1}(\alpha_i - b)\right\}_1^n$. We now present algorithm for correcting all patterns of t and fewer errors, using $\sigma_t \in L$.

Algorithm

1. Compute the syndromes $\{S_i\}_1^{\delta'}$.
2. If $S_1 = S_3 = 0$, then $\sigma(x) = 1$. Go to step 7.
3. Determine $\Phi(z)$ from (8).
4. Use the Chein search to find roots ξ_i of $\Phi(z)$ in L^*. If $\exists \xi_i \in L^*: \ \Phi(\xi_i) = 0$, go to step 6.
5. Using $\Phi_t(z) = 0$, we get $z = -\frac{b}{a}$. Substituting $-\frac{b}{a}$ for z in $\sigma_j = \Phi_j(z)$, we get $\sigma^{(1)}(x)$. Go to step 7.
6. Output all polynomials $\sigma^{(i)}(x) = \sum_{j=1}^{t} \Phi_j(\xi_i) x^j + 1$ such that (3) holds.
7. Use the Chein search to find roots of $\sigma^{(i)}(x)$ in L.

Remark. If $t = \left\lfloor \frac{d-1}{2} \right\rfloor + 1$, then output $\sigma^{(i)}(x)$ from steps 5 and 6 such that (3) holds for maximum likelihood decoding.

5 Examples

Unique correction Consider the (39, 15, 10) binary cyclic code with $\delta = 7$ [12, p. 496]. It has roots α, α^3, where $\alpha = \beta^{105}$ and β is a primitive element of $\mathbb{F}_{2^{12}}$ such that $\beta^{12}+\beta^7+\beta^6+\beta^5+\beta^3+\beta+1=0$. Suppose $e(x) = x^{34}+x^{13}+x^{10}+x^9$; then the sequence of syndromes is $\{\beta^{354}, \beta^{708}, \beta^{476}, \beta^{1416}, \beta^{1068}, \beta^{952}\}$.

Consider $z = S_7$. By applying Berlekamp's algorithm [5, 7.4] one step further we get $\Phi_1(z) = \beta^{354}$, $\Phi_2(z) = \beta^{1028}z + \beta^{3216}$, $\Phi_3(z) = \beta^{1382}z + \beta^{4031}$, $\Phi_4(z) = \beta^{1160}z + \beta^{2226}$. Further note that $F(\sigma_1, \sigma_2, \sigma_3, \sigma_4) = D_{36}$. That is

$$\begin{aligned}\Phi(z) = {} & \beta^{1099}z^{20} + \beta^{2135}z^{19} + \beta^{2334}z^{18} + \beta^{434}z^{17} + \beta^{2166}z^{16} + \beta^{2033}z^{15} + \\ & + \beta^{1849}z^{14} + \beta^{45}z^{13} + \beta^{156}z^{12} + \beta^{1493}z^{11} + \beta^{1373}z^{10} + \beta^{3370}z^{9} + \\ & + \beta^{3779}z^{8} + \beta^{658}z^{7} + \beta^{2493}z^{6} + \beta^{1903}z^{5} + \beta^{1558}z^{4} + \beta^{3492}z^{3} + \\ & + \beta^{2916}z^{2} + \beta^{1309}z + \beta^{4081}.\end{aligned}$$

Thus the only root of $\Phi(z)$ in $L^* = \left\{\beta^{-1160}(\alpha_i + \beta^{2226})\right\}_1^{39}$ is β^{45}. Finally, we obtain $\sigma(x) = \alpha^{27}x^4 + \beta^{405}x^3 + \beta^{3686}x^2 + \beta^{354}x + 1$, which corresponds to $e(x) = x^{34} + x^{13} + x^{10} + x^9$.

List correction Consider the $(33, 12, 10)$ binary cyclic code with the BCH bound $\delta = 10$ [12, p. 495]. It has roots 1, α, α^3, where $\alpha = \beta^{31}$ and β is a primitive element of $\mathbb{F}_{2^{10}}$ such that $\beta^{10} + \beta^6 + \beta^5 + \beta^3 + \beta^2 + \beta + 1 = 0$. Suppose $e(x) = x^{30} + x^{18} + x^{12} + x^7 + x^4$; then the sequence of syndromes is $\{\beta^{845}, \beta^{312}, \beta^{934}, \beta^{467}, 1, \beta^{622}, \beta^{221}, \beta^{777}\}$.

By [13], it follows that $\sigma(x) = \sum_{i=1}^{3} c_i\sigma_i(x)$, where c_i are some unknowns and $\sigma_i(x)$ are the polynomials obtained by an extension of the Euclidean algorithm ($\deg \sigma_i(x) = i + 2$). Combining this with $\sigma_0 = 1$, $\sigma_1 = S_6$, we get $\Phi_1(z) = \beta^{622}$, $\Phi_2(z) = \beta^{43}z + \beta^{221}$, $\Phi_3(z) = \beta^{665}z + \beta^{777}$, $\Phi_4(z) = \beta^{198}z$, $\Phi_5(z) = \beta^{754}z$. Further note that $F(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5) = D_{29}$. That is

$$\begin{aligned}\Phi(z) = {} & \beta^{504}z^{17} + \beta^{781}z^{16} + \beta^{728}z^{15} + \beta^{213}z^{14} + \beta^{292}z^{13} + \beta^{305}z^{12} + \\ & + \beta^{516}z^{11} + \beta^{562}z^{10} + \beta^{905}z^{9} + \beta^{27}z^{8} + \beta^{964}z^{7} + \beta^{119}z^{6} + \\ & + \beta^{924}z^{5} + \beta^{277}z^{4} + \beta^{191}z^{3}.\end{aligned}$$

The function $\Phi(z)$ has roots β^{424} and β^{889} in $L^* = \left\{\beta^{-754}\alpha_i\right\}_1^{33}$; hence, we get $\sigma^{(1)} = \alpha^5z^5 + \beta^{622}z^4 + \beta^{87}z^3 + \beta^{893}z^2 + \beta^{622}z + 1$ and $\sigma^{(2)} = \alpha^{20}z^5 + \beta^{64}z^4 + \beta^{180}z^3 + \beta^{242}z^2 + \beta^{622}z + 1$, which correspond to $e^{(1)}(x) = x^{30} + x^{18} + x^{12} + x^7 + x^4$ and $e^{(2)}(x) = x^{31} + x^{26} + x^{20} + x^8 + x$, respectively, with the same sequence of syndromes.

References

[1] C. R. P. Hartmann, "Decoding beyound the BCH bound," *IEEE Trans. Inform. Theory*, vol. 18, pp. 441–444, May 1972.

[2] M. Elia, "Algebraic decoding of the (23, 12, 7)-Golay code," *IEEE Trans. Inform. Theory*, vol. 33, pp. 150–151, Jan. 1987.

[3] P. Stevens, "Extension of the BCH decoding algorithm to decode binary cyclic codes up to their maximum error correction capacities," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1332–1340, Sept. 1988.

[4] P. Bours, J. C. M. Janssen, M. van Asperdt, and H. C. A. van Tilborg, "Algebraic decoding beyond e_{BCH} of some binary cyclic codes, when $e > e_{BCH}$," *IEEE Trans. Inform. Theory*, vol. 36, pp. 214–222, Jan. 1990.

[5] E. R. Berlekamp, *Algebraic coding theory.* New York: McGraw-Hill, 1968.

[6] G.-L. Feng and K. K. Tzeng, "A new procedure for decoding cyclic and BCH codes up to actual minimum distance," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1364–1374, Sept. 1994.

[7] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon codes and algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1757–1767, Sept. 1999.

[8] Y. Wu, "New list decoding algorithm for Reed-Solomon and BCH codes," *IEEE Trans. Inform. Theory*, vol. 54, pp. 3611–3630, Aug. 2008.

[9] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed. Cambridge: Cambridge University Press, 1997.

[10] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes.* Amsterdam: North-Holland, 1977.

[11] F. R. Gantmakher, *The theory of matrices*, 2nd ed. Providence: AMS Chelsea Publishing, 2000.

[12] W. W. Peterson and E. J. Weldon, Jr., *Error-correcting codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.

[13] S. Bezzateev and M. Bossert, "Decoding of interleaved RS codes with the Euclidean algorithm," *IEEE International Symposium on Inform. Theory 2008*, Toronto, pp. 1803–1807, 6-11 July, 2008.