IEICE TRANS. FUNDAMENTALS, VOL.E84–A, NO.10 OCTOBER 2001

LETTER *Special Section on Information Theory and Its Applications*

Fast Encoding of Algebraic Geometry Codes*

Ryutaroh MATSUMOTO[†a)], ***Regular Member***, **Masakuni OISHI**[†], ***Nonmember***, ***and*** **Kohichi SAKANIWA**[†b)], ***Regular Member***

SUMMARY We propose an encoding method for one-point algebraic geometry codes that usually requires less computation than the ordinary systematic encoder.

key words: *encoder, one-point algebraic geometry code*

1. Introduction

For practical use, efficient encoding methods of linear codes are important. But few studies [3], [9] have been done for algebraic geometry codes. Yaghoobian and Blake [9] observed that a codeword in a Hermitian code can be written as a linear combination of vectors represented as a repetition of a codeword in an extended Reed-Solomon code, and proposed an efficient encoding method for Hermitian codes using this fact.

The encoding method of Heegard et al. [3] is applicable to arbitrary linear codes with known automorphism groups. In their method the size of the circuit is smaller than that of a systematic encoder while the number of multiplications is almost the same as that for a systematic encoder.

In this paper, we modify and generalize the method of Yaghoobian and Blake to arbitrary one-point AG codes $C_\Omega(D, mQ)$. The proposed method utilizes the fact that the basis of $\Omega(-Q-D)$ can be taken as a subset of $\{x^i\omega_j \mid 0 \le j \le a-1, 0 \le i\}$, where a is the smallest nonzero nongap at Q, x a function whose pole divisor is aQ, and $\omega_0, \ldots, \omega_{a-1}$ are differentials satisfying certain conditions. We give an algebraic geometry code with which the proposed method can encode 3 times faster than the systematic encoder in the middle information rate.

2. Fast Encoding of One-Point AG Codes

We fix notations used in this paper. K denotes a finite field and F/K an algebraic function field with the full constant field K. We assume that F is not a rational function field because in this case the proposed encoding method becomes the systematic encoding. For a divisor G of F/K, $\Omega(G)$ denotes the linear space consisting of differentials whose divisors $\ge G$ and $\mathcal{L}(G)$ the linear space consisting of elements in F whose divisors $\ge -G$. For a differential ω and for a place P of degree one, $\mathrm{res}_P\omega$ denotes the residue of ω at P. For $f \in F$ and a place P, $f(P)$ denotes the value of f at P and $(f), (f)_0$ and $(f)_\infty$ denote the divisor, the zero divisor and the pole divisor of f, respectively. For an element in F, or a differential, v_P denotes the valuation at a place P.

Let Q, P_1, $\ldots$, P_n be pairwise distinct places of degree one and $D = P_1 + \cdots + P_n$. For a positive integer m, a one-point algebraic geometry code $C_\Omega(D, mQ)$ is defined by

$$\{(\mathrm{res}_{P_1}\omega, \ldots, \mathrm{res}_{P_n}\omega) \mid \omega \in \Omega(mQ - D)\}.$$

We shall first clarify the structure of the generator matrix of an AG code of dimension k. To this end, we want to determine which differentials in $\Omega(mQ-D)$ can be used for the proposed encoding method. Let a be the smallest nonzero element in $\{i \mid \mathcal{L}(iQ) \ne \mathcal{L}((i-1)Q)\}$ and x an element such that $(x)_\infty = aQ$. We define $\Omega(-\infty Q - D) = \bigcup_{i=1}^{\infty} \Omega(-D - iQ)$. For $j = 0, 1, \ldots, a-1$, we define ω_j to be a differential in $\Omega(-\infty Q - D)$ having the maximum valuation at Q among differentials $\omega \in \Omega(-\infty Q - D)$ such that $v_Q(\omega) - j$ is divisible by a.

Lemma 1: Let η_1, η_2 be nonzero differentials such that $v_Q(\eta_1) = v_Q(\eta_2)$. Then there exists $c \in K \setminus \{0\}$ such that $v_Q(\eta_1 - c\eta_2) > v_Q(\eta_1)$.

Proof: Since the differentials form the one-dimensional vector space over F [6, Proposition I.5.9], there exists $f \in F$ such that $f\eta_2 = \eta_1$. Then $v_Q(\eta_1 - f(Q)\eta_2) > v_Q(\eta_1)$. □

Proposition 2: The set

$$\{x^i\omega_j \mid 0 \le i,\ 0 \le j \le a-1,\ v_Q(x^i\omega_j) \ge m\} \quad (1)$$

is a K-basis of $\Omega(mQ - D)$.

Proof: Since the elements in the set (1) have pairwise

Manuscript received January 18, 2001.
Manuscript revised April 5, 2001.

[†]The authors are with the Department of Communications and Integrated Systems, Tokyo Institute of Technology, Tokyo, 152-8552 Japan. R. Matsumoto was supported by the JSPS Research Fellowship for Young Scientists during this research.

a) E-mail: ryutaroh@rmatsumoto.org
b) E-mail: sakaniwa@ss.titech.ac.jp

*The results in this paper was partially presented at the IEICE Information Theory Workshop [4].

distinct valuations at Q, they are linearly independent over K and belong to $\Omega(mQ-D)$.

Choose a nonzero differential $\omega \in \Omega(mQ-D)$. Let μ be the maximum valuation of the nonzero differentials in $\Omega(mQ-D)$. For $\ell = v_Q(\omega), v_Q(\omega)+1, \ldots, \mu$, we define $c_\ell \in K$ as follows.

For an integer ℓ, we define $j(\ell)$ to be the remainder of the division of ℓ by a and $i(\ell) = (\ell - j(\ell))/a$. Then $x^{i(\ell)}\omega_{j(\ell)}$ has valuation ℓ at Q.

We set $c_{v_Q(\omega)}$ such that

$$v_Q(\omega - c_{v_Q(\omega)}x^{i(v_Q(\omega))}\omega_{j(v_Q(\omega))}) > v_Q(\omega).$$

For $v_Q(\omega) < \ell \le \mu$, we set c_ℓ such that

$$v_Q\left(\omega - \sum_{\ell'=v_Q(\omega)}^{\ell} c_{\ell'}x^{i(\ell')}\omega_{j(\ell')}\right) > v_Q\left(\omega - \sum_{\ell'=v_Q(\omega)}^{\ell-1} c_{\ell'}x^{i(\ell')}\omega_{j(\ell')}\right).$$

Then the valuation of

$$\omega - \sum_{\ell=v_Q(\omega)}^{\mu} c_\ell x^{i(\ell)}\omega_{j(\ell)}$$

at Q is greater than any nonzero element in $\Omega(mQ-D)$, so $\omega - \sum_{\ell=v_Q(\omega)}^{\mu} c_\ell x^{i(\ell)}\omega_{j(\ell)}$ must be zero. □

We define B as $\{x^i\omega_j \mid 0 \le i,\ 0 \le j \le a-1, (\mathrm{res}_{P_1}x^i\omega_j, \ldots, \mathrm{res}_{P_n}x^i\omega_j) \notin C_\Omega(D, (v_Q(x^i\omega_j)+1)Q)\}$, and for $1 \le k \le n-1$, $B(k)$ as the subset of B consisting of the k differentials having lager valuations at Q than the differentials in $B \setminus B(k)$. For $1 \le k \le n-1$, we define $S = \{j \mid x^i\omega_j \in B(k)\}$ and for $0 \le \ell \le a-1$, $T_\ell = \{i \mid x^i\omega_\ell \in B(k)\}$. Suppose that $\dim C_\Omega(D, mQ) = k$. Then the generator matrix G for $C_\Omega(D, mQ)$ can be written as

$$\begin{pmatrix} \mathrm{res}_{P_1}\omega_0 & \mathrm{res}_{P_2}\omega_0 & \cdots & \mathrm{res}_{P_n}\omega_0 \\ x(P_1)\mathrm{res}_{P_1}\omega_0 & x(P_2)\mathrm{res}_{P_2}\omega_0 & \cdots & x(P_n)\mathrm{res}_{P_n}\omega_0 \\ x(P_1)^2\mathrm{res}_{P_1}\omega_0 & x(P_2)^2\mathrm{res}_{P_2}\omega_0 & \cdots & x(P_n)^2\mathrm{res}_{P_n}\omega_0 \\ \vdots & \vdots & & \vdots \\ \mathrm{res}_{P_1}\omega_1 & \mathrm{res}_{P_2}\omega_1 & \cdots & \mathrm{res}_{P_n}\omega_1 \\ x(P_1)\mathrm{res}_{P_1}\omega_1 & x(P_2)\mathrm{res}_{P_2}\omega_1 & \cdots & x(P_n)\mathrm{res}_{P_n}\omega_1 \\ x(P_1)^2\mathrm{res}_{P_1}\omega_1 & x(P_2)^2\mathrm{res}_{P_2}\omega_1 & \cdots & x(P_n)^2\mathrm{res}_{P_n}\omega_1 \\ \vdots & \vdots & & \vdots \end{pmatrix},$$

where each row in G corresponds to a differential in $B(k)$. We used the fact that $\mathrm{res}_{P_1}x^i\omega_j = x(P_1)^i\mathrm{res}_{P_1}\omega_j$ [6, Proof of Theorem II.2.8 and Theorem IV.3.2]. Let $\boldsymbol{i} = (i_1, \ldots, i_k) \in K^k$ be an information. Then the codeword is $\boldsymbol{i}G$. But we can compute the codeword $\boldsymbol{i}G$ in a different way.

For $\ell \in S$, let $T_\ell = \{t_{\ell,1}, t_{\ell,2}, \ldots, t_{\ell,\sharp T_\ell}\}$ such that $t_{\ell,1} < t_{\ell,2} < \cdots < t_{\ell,\sharp T_\ell}$, where $\sharp$ denotes the number of elements in a set. Let G_ℓ be the $\sharp T_\ell \times n$ matrix $(x^{t_{\ell,i}}(P_j))_{1\le i\le \sharp T_\ell, 1\le j\le n}$. Define a diagonal matrix M_ℓ by

$$M_\ell = \begin{pmatrix} \mathrm{res}_{P_1}\omega_\ell & & & \\ & \mathrm{res}_{P_2}\omega_\ell & & \\ & & \ddots & \\ & & & \mathrm{res}_{P_n}\omega_\ell \end{pmatrix}.$$

Then the codeword can be also obtained as $(i_1, \ldots, i_{\sharp T_0})G_0M_0 + (i_{\sharp T_0+1}, \ldots, i_{\sharp T_0+\sharp T_1})G_1M_1 + \cdots + (i_{k-\sharp T_{\max S}+1}, \ldots, i_k)G_{\max S}M_{\max S}$, where $\max S$ denotes the maximum integer in S. Since many columns in the matrix G_ℓ are the same, we can compute many columns in $(i_{\sharp T_0+\cdots+\sharp T_{\ell-1}+1}, \ldots, i_{\sharp T_0+\cdots+\sharp T_\ell})G_\ell$ by copying the values from other column in $(i_{\sharp T_0+\cdots+\sharp T_{\ell-1}+1}, \ldots, i_{\sharp T_0+\cdots+\sharp T_\ell})G_\ell$. But we can further reduce the encoding complexity by performing elementary row operations on G_ℓ.

Let $\delta = \sharp\{x(P_i) \mid i = 1, \ldots, n\}$. By an appropriate permutation of indices of $P_1, \ldots, P_n$, we may assume that $x(P_1), x(P_2), \ldots, x(P_\delta)$ are pairwise distinct. Then there exists a $\sharp T_\ell \times \sharp T_\ell$ nonsingular matrix N_ℓ such that

$$G'_\ell = \begin{pmatrix} 1 & & O & \cdots \\ & \ddots & & \cdots \\ O & & 1 & \cdots \end{pmatrix} = N_\ell G_\ell.$$

Consider the linear map from K^k to K^n defined by

$$\begin{aligned}(i_1, \ldots, i_{\sharp T_0})&G'_0M_0 \\ &+ (i_{\sharp T_0+1}, \ldots, i_{\sharp T_0+\sharp T_1})G'_1M_1 + \cdots \\ &+ (i_{k-\sharp T_{\max S}+1}, \ldots, i_k)G'_{\max S}M_{\max S}. \qquad (2)\end{aligned}$$

The linear code defined by the linear map (2) is the same as $C_\Omega(D, G)$, because the linear map (2) is obtained by multiplying the information word by the matrix NG from right, where

$$N = \begin{pmatrix} N_0 & & & \\ & N_1 & & \\ & & \ddots & \\ & & & N_{\max S} \end{pmatrix},$$

and is nonsingular.

We analyze the number of multiplications in K required to compute (2). The computation of $(i_{\sharp T_0+\cdots+\sharp T_{\ell-1}+1}, \cdots, i_{\sharp T_0+\cdots+\sharp T_\ell})G'_\ell$ requires at most $\sharp T_\ell(\delta - \sharp T_\ell)$ (not $\sharp T_\ell n$) multiplications and $n-\delta$ copies of one component in the codeword to other columns. Computing $(i_{\sharp T_0+\cdots+\sharp T_{\ell-1}+1}, \cdots, i_{\sharp T_0+\cdots+\sharp T_\ell})G_\ell M_\ell$ requires at most n multiplications. Thus the total number of multiplications is at most

$$n\sharp S + \sum_{\ell\in S}\sharp T_\ell(\delta - \sharp T_\ell) = n\sharp S + k\delta - \sum_{\ell\in S}(\sharp T_\ell)^2. \quad (3)$$

On the other hand, the number of multiplications required in the systematic encoding of $C_\Omega(D, mQ)$ is at

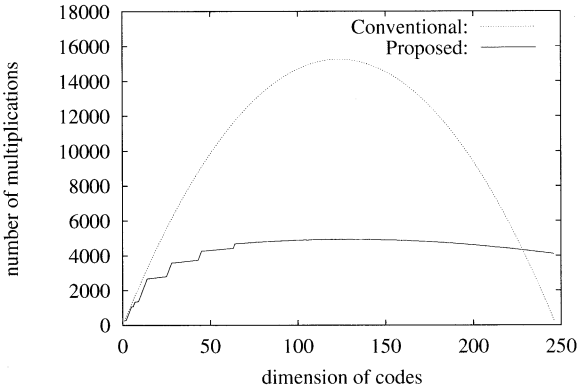

Fig. 1 Number of multiplications in encoding the Garcia-Stichtenoth codes.

most $k(n-k)$.

Since the amount of storage used by an encoder depends on its implementation (e.g. parallelized implementation versus serialized one), we do not analyze in detail the amount of storage used by the proposed encoder and the systematic one. However, the proposed encoder does not use large amount of precomputed data and it does not require much more memory than the systematic one.

We give an example demonstrating how much encoding is speeded up.

Example 3: Let $E = \mathbf{F}_{16}(y_1, y_2, y_3)$ with

$$y_2^4 + y_2 + y_1^5 = 0,\ y_3^4 + y_3 + (y_2/y_1)^5 = 0,$$

which is a function field discovered by Garcia and Stichtenoth [2]. The number of poles of y_1 is 1 [2], and is denoted by Q. Umehara and Uyematsu [7] showed how to construct one-point algebraic geometry codes on this function field, based on the results by Voss and Høholdt [8]. Let $P_1, \ldots, P_{247}$ be an enumeration of all places of degree one except Q in E and $D = P_1 + \cdots + P_{247}$. $k(n-k)$ and Eq.(3) are compared in Fig. 1.

Remark 4: We could not prove rigorously that the number of multiplications in the proposed encoder is always less than the systematic one in a wide range of code dimension. However, in all the examples verified by us, the proposed encoder requires less multiplications in most information rate. In particular, for the Hermitian codes the ratio of their numbers of multiplications in the middle information rate increases as the code length increases.

Remark 5: An algebraic geometry code $C_{\mathcal{L}}(D, mQ)$, which is the dual of $C_\Omega(D, mQ)$, is defined by

$$\{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(mQ)\}.$$

One can also efficiently encode $C_{\mathcal{L}}(D, mQ)$ in a similar way to $C_\Omega(D, mQ)$ as shown below. Let a be as above and $b_j = \min\{i \mid \mathcal{L}(iQ) \neq \mathcal{L}((i-1)Q)$ and $i \equiv j \pmod a\}$ for $j = 0, \ldots, a-1$. Choose elements $f_j \in F$ such that $(f_j)_\infty = b_j Q$. We define $\mathcal{B}$ as $\{x^i f_j \mid 0 \leq i,\ 0 \leq j \leq a-1,\ (x^i f_j(P_1), \ldots, x^i f_j(P_n)) \notin C_{\mathcal{L}}(D, (-v_Q(x^i f_j) - 1)Q)\}$, and for $1 \leq k \leq n-1$, $\mathcal{B}(k)$ as the subset of $\mathcal{B}$ consisting of the k elements having larger valuations at Q than the elements in $\mathcal{B} \setminus \mathcal{B}(k)$. Then a generator matrix of $C_{\mathcal{L}}(D, mQ)$ of dimension k can be written as

$$\begin{pmatrix} f_0(P_1) & f_0(P_2) & \cdots & f_0(P_n) \\ x(P_1)f_0(P_1) & x(P_2)f_0(P_2) & \cdots & x(P_n)f_0(P_n) \\ x(P_1)^2 f_0(P_1) & x(P_2)^2 f_0(P_2) & \cdots & x(P_n)^2 f_0(P_n) \\ \vdots & \vdots & & \vdots \\ f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ x(P_1)f_1(P_1) & x(P_2)f_1(P_2) & \cdots & x(P_n)f_1(P_n) \\ x(P_1)^2 f_1(P_1) & x(P_2)^2 f_1(P_2) & \cdots & x(P_n)^2 f_1(P_n) \\ \vdots & \vdots & & \vdots \end{pmatrix},$$

where each row corresponds to an element in $\mathcal{B}(k)$. We can get a similar expression for the number of multiplications required for encoding $C_{\mathcal{L}}(D, mQ)$.

Remark 6: In order to estimate the encoding complexity (3) of our method, we do not have to find vectors $(\mathrm{res}_{P_1}\omega_j, \ldots, \mathrm{res}_{P_n}\omega_j)$. When we construct the one-point algebraic geometry code $C_\Omega(D, mQ)$ and decode errors with the Feng-Rao [1] or the Sakata decoding algorithm [5], we know the set $\mathcal{W} = \{i \mid C_{\mathcal{L}}(D, iQ) \neq C_{\mathcal{L}}(D, (i-1)Q)\}$. So we can know $v_Q(B)$ because $v_Q(B) = \{i - 1 \mid i \in \mathcal{W}\}$. $v_Q(B(k))$ can be easily seen from $v_Q(B)$. We have $\sharp S = \sharp\{i \bmod a \mid i \in v_Q(B(k))\}$ and $\sharp T_\ell = \sharp\{i \in v_Q(B(k)) \mid i - \ell$ is divisible by $a\}$.

Remark 7: To construct an encoder, we have to find vectors $(\mathrm{res}_{P_1}\omega_j, \ldots, \mathrm{res}_{P_n}\omega_j)$ for $j = 0, \ldots, a-1$. By the definition of ω_j, $(\mathrm{res}_{P_1}\omega_j, \ldots, \mathrm{res}_{P_n}\omega_j)$ may be taken as any element in $C_\Omega(D, v_Q(\omega_j)Q) \setminus C_\Omega(D, (v_Q(\omega_j)+1)Q)$. Note that $v_Q(\omega_j)$ can be easily calculated as described in the previous remark.

Acknowledgment

The authors would like to thank Dr. Shibuya for reading and criticizing the preliminary manuscript.

References

[1] G.L. Feng and T.R.N. Rao, "Decoding algebraic geometric codes up to the designed minimum distance," IEEE Trans. Inf. Theory, vol.39, no.1, pp.36–47, 1993.
[2] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields, attaining the Drinfeld-Vladut bound," Invent. Math., vol.121, no.1, pp.211–222, 1995.
[3] C. Heegard, J. Little, and K. Saints, "Systematic encoding via Gröbner bases for a class of algebraic-geometric Goppa codes," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1752–1761, Nov. 1995.
[4] R. Matsumoto, M. Oishi, and K. Sakaniwa, "Fast encoding of algebraic geometry codes," IEICE Technical Report, IT99-3, May 1999.

[5] S. Sakata, D.A. Leonard, H. Elbrønd Jensen, and T. Høholdt, "Fast erasure-and-error decoding of algebraic geometry codes up to the Feng-Rao bound," IEEE Trans. Inf. Theory, vol.44, no.4, pp.1558–1564, July 1998.
[6] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, Berlin, 1993.
[7] D. Umehara and T. Uyematsu, "One-point algebraic geometric codes from Artin-Schreier extensions of Hermitian function fields," IEICE Trans. Fundamentals, vol.E81-A, no.10, pp.2025–2031, Oct. 1998.
[8] C. Voß and T. Høholdt, "An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound," IEEE Trans. Inf. Theory, vol.43, no.1, pp.128–135, Jan. 1997.
[9] T. Yaghoobian and I.F. Blake, "Hermitian codes as generalized Reed-Solomon codes," Des. Codes Cryptogr., vol.2, pp.5–17, 1992.