PAPER *Special Section on Information Theory and Its Applications*

Miura's Generalization of One-Point AG Codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization

Ryutaroh MATSUMOTO†, ***Student Member***

SUMMARY Høholdt, van Lint and Pellikaan proposed a generalization of one-point AG codes, called the evaluation codes. We show that an evaluation code from a weight function can be constructed as Miura's generalization of one-point AG codes. Hence we can construct a one-point AG code as good as a given evaluation code from a weight function.

key words: *evaluation codes, one-point AG codes*

1. Introduction

Høholdt, van Lint and Pellikaan proposed a generalization of one-point AG codes called the evaluation codes, and enabled us to construct linear codes from arbitrary algebraic varieties[5], [6]. To construct an evaluation code, we find an appropriate K-algebra R with an order function w and an epimorphism $\varphi : R \to K^n$ of K-algebras, where K is a finite field and n is the code length. Then we define the evaluation code as a dual code of the image of some linear space of R under φ. When the order function w is a weight function, we have a lower bound for the minimum distance of an evaluation code that is a generalization of the Goppa designed minimum distance for algebraic geometry codes. Thus evaluation codes from a weight function are particularly useful, and it is interesting whether we can construct a good evaluation code from a weight function that is never obtained as an algebraic geometry code in terms of information rate and error-correcting capability.

In this paper we show that if a K-algebra R has a weight function then R is the affine coordinate ring of an affine algebraic curve with exactly one place at infinity, and the epimorphism $\varphi : R \to K^n$ is the evaluation of elements in R at K-rational points in the curve, hence the evaluation code from a weight function can be constructed as a linear code on an arbitrary algebraic curve that is proposed by Miura [9], [10]. In Miura's generalization of one-point AG codes, the author showed that we cannot construct a better linear code from a singular curve than the traditional one-point AG code on its normalization in terms of information rate and the Feng-Rao designed minimum distance [8], hence we can construct a one-point AG code as good as a given evaluation code from a weight function in terms of information rate and the Feng-Rao designed minimum distance.

Manuscript received January 20, 1999.
Manuscript revised March 30, 1999.

†The author is with the Sakaniwa Lab., the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo, 152–8552 Japan.

2. Order Functions and Evaluation Codes

In this section we review the evaluation codes. Let K be a finite field. A commutative ring R (and ψ_1) is said to be a *K-algebra* if there exists a ring monomorphism $\psi_1 : K \to R$. We regard the set K^n consisting of n-tuples of K as a commutative ring with the componentwise addition and multiplication. We define a ring monomorphism ψ_2:

$$K \longrightarrow K^n,$$
$$c \longmapsto (c, \ldots, c).$$

We regard K^n as a K-algebra with ψ_2. A ring homomorphism $\varphi : R \to K^n$ is said to be a *homomorphism of K-algebras* if $\psi_2 = \varphi \circ \psi_1$.

$\mathbf{N}_0$ denotes the set of nonnegative integers. A function $w : R \to \mathbf{N}_0 \cup \{-\infty\}$ is said to be an *order function* if it satisfies the conditions (O.0), (O.1), (O.2), (O.3) and (O.4) [6, Definition 3.4], and an order function is said to be a *weight function* if it satisfies (O.5) [6, Definition 3.5]:

(O.0) $w(f) = -\infty$ iff $f = 0$.
(O.1) $w(cf) = w(f)$ for all $c \in K \setminus \{0\}$.
(O.2) $w(f+g) \leq \max\{w(f), w(g)\}$ and equality holds if $w(f) \neq w(g)$.
(O.3) If $w(f) < w(g)$ and $h \neq 0$, then $w(fh) < w(gh)$.
(O.4) If $w(f) = w(g) \neq -\infty$, then there exists $c \in K$ such that $w(f - cg) < w(g)$.
(O.5) $w(fg) = w(f) + w(g)$, where the sum of an integer and $-\infty$ is $-\infty$.

If R is a K-algebra with an order function w, then there exists a K-basis $\{f_1, f_2, \ldots\}$ such that $w(f_i) < w(f_{i+1})$ [6, Proposition 3.12]. Suppose that $\varphi : R \to K^n$ is an epimorphism of K-algebras, then the evaluation code C_l is the dual code of the code generated by $\varphi(f_1), \ldots, \varphi(f_l)$. Then the minimum distance of C_l is not less than $d_\varphi(l) = \min\{\#\{(f_i, f_j) \mid w(f_i f_j) = w(f_{m+1})\} \mid m \geq l, C_m \neq C_{m+1}\}$ [6, Theorem 4.13].

When the order function w is a weight function and the set $\mathbf{N}_0 \setminus w(R \setminus \{0\})$ is finite, we have an analogue of the Goppa bound for an algebraic geometry code. Let $g = \#\mathbf{N}_0 \setminus w(R \setminus \{0\})$, then $d_\varphi(l) \geq l + 1 - g$ [6, Theorem 5.24]. We can correct $\lfloor (d_\varphi(l) - 1)/2 \rfloor$ or less errors by the Feng-Rao algorithm [6, Theorem 6.12]. In Example 11 we will show that we can sometimes correct errors more than $\lfloor (d_\varphi(l) - 1)/2 \rfloor$.

3. An Algebra with a Weight Function is a Curve

Let $\bar{K}$ be the algebraic closure of K, χ an affine algebraic curve defined over K. Then there exist a prime ideal I of the polynomial ring $K[X_1, \ldots, X_t]$ such that the ideal of χ is $I\bar{K}[X_1, \ldots, X_t]$. In this paper by the affine coordinate ring of χ, we mean $K[X_1, \ldots, X_t]/I$. Let R be the affine coordinate ring of χ, and F the quotient field of R. F/K is an algebraic function field of one variable. Let Q be a place of F/K. We say that χ *has exactly one place* Q *at infinity* if every nonzero element $f \in R$ has no pole other than Q.

Theorem 1: Let R be a commutative algebra over a finite field K, and w a weight function of R. We assume that there exists $x \in R$ such that $w(x) > 0$.

Then the quotient field F of R is an algebraic function field of one variable over K, and there exists a unique discrete valuation v of F/K and a unique positive integer d such that $w(x) = -dv(x)$ for all $x \in R$. Let Q be the place corresponding to v. Then the degree of Q is one, and R is the affine coordinate ring of an affine algebraic curve defined over K with exactly one place Q at infinity.

Corollary 2: Let R be a K-algebra. If w_1, w_2 are the weight functions of R, then there exists a positive rational number e such that $ew_1 = w_2$.

We divide the proof of the theorem above into several lemmas.

Lemma 3: [9, Lemma 5.2] Let M be a nonzero submonoid of the monoid of nonnegative integers $\mathbf{N}_0$. Then there exists a finite subset $\{a_1, \ldots, a_t\}$ generating M, that is, for any $m \in M$, m can be written as

$$m = n_1 a_1 + \cdots + n_t a_t,\ n_i \in \mathbf{N}_0.$$

Proof: Choose $t \in M \setminus \{0\}$. For $i = 1, \ldots, t$ we define a_i to be the minimum elements in $M \cap \{i + tn \mid n \in \mathbf{N}_0\}$. If $M \cap \{i + tn \mid n \in \mathbf{N}_0\} = \emptyset$, we define a_i to be 0. Then $a_1, \ldots, a_t$ generates M. □

Lemma 4: Let R and w be as in Theorem 1. R is finitely generated as an algebra over K.

Proof: Let $\{a_1, \ldots, a_t\}$ generates the monoid $w(R \setminus \{0\})$. Then there exist elements $f_1, \ldots, f_t$ such that $w(f_i) = a_i$. We claim $R = K[f_1, \ldots, f_t]$.

Choose nonzero $x \in R$. Then there exists $f_1^{n_1} \cdots f_t^{n_t}$ having the same weight as x. By the definition of the weight function, there exists $c \in K$ such that

$$w(x - cf_1^{n_1} \cdots f_t^{n_t}) < w(x).$$

Repeating the same argument on $x - cf_1^{n_1} \cdots f_t^{n_t}$, we get

$$w(x - \sum c_{n_1, \ldots, n_t} f_1^{n_1} \cdots f_t^{n_t}) < 0,$$

which implies

$$x = \sum c_{n_1, \ldots, n_t} f_1^{n_1} \cdots f_t^{n_t}.$$

□

Example 5: [4] In contrast to the weight function, we can construct a K-algebra with an order function that is not finitely generated over K. Let R be the K-linear subspace of $K[X, Y]$ generated by $\{X^i Y^j \mid j = 0 \text{ or } (j > 0 \text{ and } i > 0)\}$. Then R is a subring of $K[X, Y]$ and not finitely generated over K. Since $K[X, Y]$ has an order function, R has an order function.

Lemma 6: [6, Lemma 5.6] Let R, w be as in Theorem 1, $f \in R \setminus K$, and (f) be the ideal of R generated by f. Then the residue class ring $R/(f)$ is a nonzero finite-dimensional K-linear space.

Lemma 7: Let R, w be as in Theorem 1. R is an integral domain [6, Proposition 3.10]. Let F be the quotient field of R. F is an algebraic function field of one variable over K.

Proof: Since R is finitely generated over K, it is enough to show that the transcendence degree of F over K is one, which equals to the Krull dimension of the ring R [2, Theorem A, Chapter 13].

For $f \in R \setminus K$, $R/(f)$ is of Krull dimension 0 by the previous lemma, thus R is of Krull dimension 1 [2, Corollary 13.11]. □

Lemma 8: Let I be a prime ideal of $K[X_1, \ldots, X_t]$ and suppose that the Krull dimension of $R := K[X_1, \ldots, X_t]/I$ is 1. Let $\bar{R}$ is the integral closure of R in its quotient field. Then $\bar{R}$ modulo R is a finite-dimensional K-linear space.

Proof: $\bar{R}$ is finitely generated as an R-module [2, Corollary 13.13]. Thus there exists a prime ideal $\bar{I}$ of $K[X_1, \ldots, X_u]$ such that $\bar{R} = K[X_1, \ldots, X_u]/\bar{I}$. Let A be the annihilator of the R-module $\bar{R}$ modulo R, that is, $\{x \in R \mid x\bar{R} \subseteq R\}$. Then A is a nonzero ideal of $\bar{R}$ [7, Chapter X]. Let J be the ideal of $K[X_1, \ldots, X_u]$ containing $\bar{I}$ such that $J \bmod \bar{I} = A$. Then the number of zeros of J in the algebraic closure of K is finite, so the vector space dimension of $K[X_1, \ldots, X_u]/J = \bar{R}/A$ is finite [1, Theorem 2.2.7]. Hence $\bar{R}$ modulo R is finite-dimensional. □

Proof of Theorem 1: Let d be the greatest common divisor of $w(R) \setminus \{0, -\infty\}$. We define a function

v from F such that $v(f/g) = \frac{w(g)-w(f)}{d}$ for nonzero $f, g \in R$ and $v(0) = \infty$. Then v is a discrete valuation of the algebraic function field F/K in the sense of Stichtenoth [12, Definition I.1.9]. Let O_Q be the valuation ring corresponding to v, and Q the place of O_Q. By the definition (O.4) of the weight function, the residue field O_Q/Q is isomorphic to K, so the degree of Q is one.

Let $\mathbf{P}_F$ be the set of places in F/K, $\bar{R}$ the integral closure of R in F, and $S(R) := \{P \in \mathbf{P}_F \mid O_P \supset R\}$. Then $\bar{R} = \bigcap_{P \in S(R)} O_P$ [12, Theorem III.2.6]. We will show that $S(R) = \mathbf{P}_F \setminus \{Q\}$. Let $W := \{x \in \bar{R} \mid v_Q(x) > 0\}$. Then W is a K-linear space. Since the vector space dimension of $\bar{R}$ modulo R is finite and $R \cap W = \{0\}$, $\dim W < \infty$. Suppose that there exists $T \in \mathbf{P}_F \setminus (S(R) \cup \{Q\})$. By the strong approximation theorem of the discrete valuations [12, Theorem I.6.4], we can find $x_i \in F$ for $i = 1, 2, \ldots$ such that $v_Q(x_i) = i$ and $v_P(x_i) \geq 0$ for all $P \in \mathbf{P}_F \setminus \{T\}$. Then $x_i \in \bigcap_{P \in S(R)} O_P = \bar{R}$ and $x_i \in W$. $x_1, x_2, \ldots$ are linearly independent over K, which contradicts $\dim W < \infty$.

Therefore we conclude $S(R) = \mathbf{P}_F \setminus \{Q\}$, which implies that R is the affine coordinate ring of an affine algebraic curve with exactly one place Q of degree one at infinity.

Recall that $w = -dv$ as a function from R. We will show the uniqueness of d and v $(= v_Q)$. Suppose that there exist a positive integer d_1 and a discrete valuation v_1 of F/K such that $w(x) = -d_1 v_1(x)$ for all $x \in R$. Then by the definition of the discrete valuation [12, Definition I.1.9] there exist $f, g \in R \setminus \{0\}$ such that $1 = v_1(f/g) = v_1(f) - v_1(g) = (w(f) - w(g))/d_1$. So d_1 must be the greatest common divisor of $w(R) \setminus \{0, -\infty\}$ and $d_1 = d$. Let Q_1 be the place of v_1. Then $Q_1 \in \mathbf{P}_F \setminus S(R)$ and $Q_1 = Q$. □

4. Evaluation Codes from a Weight Function can be Constructed as Miura's Generalization of One-Point AG Codes

Miura [9], [10] generalized the construction of the improved one-point AG codes [3] to an arbitrary singular curve with exactly one place of degree one at infinity. In this section we review Miura's generalization of one-point AG codes, then we show that evaluation codes from a weight function can be constructed as Miura's generalization.

Let R be the affine coordinate ring of an affine algebraic curve defined over K with exactly one place Q of degree one at infinity. Miura's generalization of one-point AG codes is as follows [9], [10]. v_Q denotes the discrete valuation at Q, and there exists a K-basis of R

$$\{f_1, f_2, \ldots\} \tag{1}$$

such that $v_Q(f_i) > v_Q(f_{i+1})$. Let $M_1, \ldots, M_n$ be the pairwise distinct maximal ideals of R such that $R/M_i = K$ for $i = 1, \ldots, n$. We define the homomorphism of K-algebras τ as

$$\begin{array}{ccc} R & \longrightarrow & K^n, \\ f & \longmapsto & (f \bmod M_1, \ldots, f \bmod M_n). \end{array} \tag{2}$$

τ is an epimorphism of K-algebras, because by the Chinese Remainder Theorem the image of τ is isomorphic to $R/M_1 \times \cdots \times R/M_n$, which is isomorphic to K^n.

We define the subset $\{g_1, \ldots, g_n\}$ of the basis (1) inductively as follows. $g_1 = f_1$. g_i is defined as the element f_j having the smallest index such that $\tau(f_j)$ is linearly independent of $\tau(g_1), \ldots, \tau(g_{i-1})$. Choose a nonempty proper subset $B \subset \{g_1, \ldots, g_n\}$. The linear code $C(B)$ is defined as the dual code of the linear space generated by $\tau(B)$. It is a generalization of the improved one-point AG codes proposed by Feng and Rao [3], and if we define a weight function $w(f) = -v_Q(f)$ and take B as the first r elements of $\{g_1, g_2, \ldots, g_n\}$, then $C(B)$ is an evaluation code.

Let $B_0 = \{0\}$ and B_i the linear space generated by $\tau(g_1), \ldots, \tau(g_i)$. We define $M(s) := \{(g_i, g_j) \mid \tau(g_i g_j) \in B_s \setminus B_{s-1}$ and for $1 \leq u \leq i$, $1 \leq v \leq j$, $(u, v) \neq (i, j)$, $\tau(g_u g_v) \in B_{s-1}\}$ and

$$d_M(B) := \min\{\#M(s) \mid g_s \notin B\}.$$

Then the minimum distance of $C(B)$ is not less than $d_M(B)$ and we can correct $\lfloor (d_M(B) - 1)/2 \rfloor$ or less errors by the Feng-Rao algorithm. A fast error-and-erasure decoding algorithm is also available [11]. If we define $g = \#(\mathbf{N}_0 \setminus -v_Q(R \setminus \{0\}))$, then $\#M(s) \geq s - g$, which corresponds to the Goppa designed minimum distance of an algebraic geometry codes. If the affine curve corresponding to R is nonsingular, then g equals to the genus of the curve.

To show that an evaluation code can be obtained in this way, it is enough to show that if $\varphi : R \to K^n$ is an epimorphism of K-algebras, then φ is of the form (2).

Theorem 9: Let R be a K-algebra and $\varphi : R \to K^n$ is an epimorphism of K-algebras. Then there exists distinct maximal ideals $M_1, \ldots, M_n$ such that $R/M_i = K$ and φ equals to

$$\begin{array}{l} R \longrightarrow K^n, \\ x \longmapsto (x \bmod M_1, \ldots, x \bmod M_n). \end{array}$$

Proof: Let ρ_i be

$$\begin{array}{l} K^n \longrightarrow K, \\ (c_1, \ldots, c_n) \longmapsto c_i, \end{array}$$

for $i = 1, \ldots, n$. Let $M_i := \ker(\rho_i \circ \varphi)$. Then $R/M_i = K$ for $i = 1, \ldots, n$ and φ equals to

$$\begin{array}{l} R \longrightarrow K^n, \\ x \longmapsto (x \bmod M_1, \ldots, x \bmod M_n). \end{array}$$

$M_1, M_2, \ldots, M_n$ are pairwise distinct, otherwise φ is

not an epimorphism. □

We will clarify the relation between d_φ and d_M when $B = \{g_1, g_2, \ldots, g_r\}$.

Theorem 10: Let R be the affine coordinate ring of an affine algebraic curve with exactly one place Q of degree one at infinity, $w = -v_Q$ a weight function of R, $\{f_1, f_2, \ldots\}$ a K-basis of R such that $w(f_i) < w(f_{i+1})$, and $M_1, \ldots, M_n$ maximal ideals of R whose residue fields are K. We define φ as (2) and $\{g_1, \ldots, g_n\}$, d_φ, d_M as above. We choose B as the first r elements of $\{g_1, \ldots, g_n\}$ and suppose that $f_l = g_r$. Then $d_M(B) \geq d_\varphi(l)$.

Proof: We will show that if $w(f_i f_j) = w(f_{m+1})$ and $C_m \neq C_{m+1}$ then $f_i, f_j \in \{g_1, \ldots, g_n\}$. Suppose that $f_i \notin \{g_1, \ldots, g_n\}$. Then $\varphi(f_i)$ can be written as a linear combination of $\varphi(f_1), \ldots, \varphi(f_{i-1})$, which implies $\varphi(f_{m+1})$ can be written as a linear combination of $\varphi(f_1), \ldots, \varphi(f_m)$ that contradicts $C_m \neq C_{m+1}$.

Thus $\{(f_i, f_j) \mid w(f_i f_j) = w(f_{m+1})\} \subseteq \{(g_i, g_j) \mid \varphi(g_i g_j) \in B_s \setminus B_{s-1}$ and for $1 \leq u \leq i$, $1 \leq v \leq j$, $(u, v) \neq (i, j)$, $\varphi(g_u g_v) \in B_{s-1}\}$ with $f_{m+1} = g_s$. Therefore $d_M(B) \geq d_\varphi(l)$. □

The reader might think that $d_\varphi = d_M$. But we can construct an (abnormal) example such that $d_\varphi < d_M$.

Example 11: Let $\mathbf{F}_4$ be the finite field with 4 elements, and consider $R = \mathbf{F}_4[X, Y]/(Y^5 + Y + X^6)$. $x, y \in R$ denote the elements represented by X, Y. The affine algebraic set defined by $Y^5 + Y + X^6$ is an affine algebraic curve with exactly one place Q of degree one at infinity, and $v_Q(x) = -5, v_Q(y) = -6$ [9], [10]. We define the weight function $w = -v_Q$. Then $\{f_1, f_2, \ldots, f_{10}, \ldots\} = \{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, \ldots\}$ is a $\mathbf{F}_4$-basis of R whose elements have pairwise distinct weights. The curve has 8 $\mathbf{F}_4$-rational points in the affine plane, and let $M_1, \ldots, M_8$ be the corresponding maximal ideals of R. We define φ as $R \to \mathbf{F}_4^8$, $x \mapsto (x \bmod M_1, \ldots, x \bmod M_8)$. Then $\{g_1, \ldots, g_8\} = \{1, x, y, x^2, xy, y^2, x^2y, y^3\}$. If we take B as the first r elements, then d_φ and d_M are as follows.

l	1	2	3	4	5	6	8
r	1	2	3	4	5	6	7
$d_\varphi(l)$	2	2	3	3	3	6	8
$d_M(B)$	2	2	3	4	5	6	8

5. Conclusion

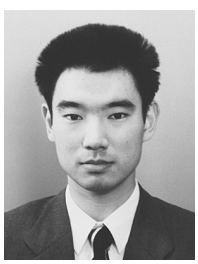
Miura [9], [10] and Høholdt, van Lint and Pellikaan [5], [6] generalized one-point AG codes in two different ways, and the former seems to be a special case of the latter. In this paper we showed that they are same. Hence we can construct a one-point AG code as good as a given evaluation code from a weight function in terms of information rate and the Feng-Rao designed minimum distance.

Acknowledgments

The author thanks Prof. Pellikaan for teaching Example 5 and pointing a logical gap in the proof, Dr. Umehara for suggesting the construction of algebraic curves such that $d_\varphi < d_M$, Dr. Shibuya for pointing English errors, and Prof. Sakaniwa and the members in the Sakaniwa laboratory for providing a good environment for this research.

References

[1] W.W. Adams and P. Loustaunau, "An introduction to Gröbner bases," Graduate Studies in Mathematics, vol.3, American Mathematical Society, 1994.
[2] D. Eisenbud, "Commutative algebra with a view toward algebraic geometry," Graduate Texts in Mathematics, vol.150, Springer-Verlag, Berlin, 1995.
[3] G.L. Feng and T.R.N. Rao, "Improved geometric Goppa codes part I, basic theory," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1678–1693, Nov. 1995.
[4] O. Geil and R. Pellikaan, "On the existence of order domains," preprint, 1999.
[5] T. Høholdt, J.H. van Lint, and R. Pellikaan, "Order functions and evaluation codes," Proc. AAECC-12, Lecture Notes in Computer Science, vol.1255, pp.138–150, Springer-Verlag, 1997.
[6] T. Høholdt, J.H. van Lint, and R. Pellikaan, "Algebraic geometry codes," in Handbook of Coding Theory, eds. V. Pless and W.C. Huffman, pp.871–961, Elsevier, 1998.
[7] S. Lang, Algebra, 3rd ed., Addison-Wesley, 1993.
[8] R. Matsumoto, "Linear codes on nonsingular curves are better than those on singular curves," IEICE Trans. Fundamentals, vol.E82-A, no.4, pp.665–670, April 1999.
[9] S. Miura, Ph.D. thesis, Univ. Tokyo, May 1997.
[10] S. Miura, "Linear codes on affine algebraic curves," IEICE Trans., vol.J81-A, no.10, pp.1398–1421, Oct. 1998.
[11] S. Sakata, D.A. Leonard, H.E. 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.
[12] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag, Berlin, 1993.



Ryutaroh Matsumoto received the B.E. degree in computer science and M.E. degree in information processing from Tokyo Institute of Technology in 1996 and 1998 respectively. He is currently a Ph.D student in the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology. His current research interest includes algebraic geometry codes. E-mail: ryutaroh@ss.titech.ac.jp