数理解析研究所講究録
631巻 1987年 35-42

The rank of Hasse-Witt matrix and a periodic solution of some congruences

Saga Univ. Fac. Sci. Engrg. Toru Nakahara
中原 徹

§1. Introduction

Let f and p be odd primes and relatively prime. First we consider the next simultaneous congruences:

$$pj_k \equiv j_{k+1} \bmod f \qquad (1)_r$$

where $\{j_k\}_{k \bmod r} \subset \{1, \ldots, (f-1)/2\}$, $r = \mathrm{Ind}_f p$.
When there exists such a solution $\{j_k\}$ of 'positive' absolutely least residues modulo f, we say that the congruences $(1)_r$ have a periodic solution and r is the length of the period.

In §2 we can solve the congruences $(1)_r$ for $r = 3$ and odd numbers $r \geqq 3$.

Our aim is to give some algebraic function fields whose Hasse-Witt matrices do not have the full rank but have a positive rank. In §3 we can characterize the fields by applying a periodic solution of $(1)_r$.

§2. A periodic solution

We denote by $R^\times$ the group of the reduced residue classes modulo f and identify the class and its representative. Let w be a primitive root modulo f. For any a, b $\in R^\times$ there exist α, β such that $a \equiv w^\alpha$, $b \equiv w^\beta \bmod f$. By setting that

$$\alpha \equiv \beta \bmod \frac{f-1}{r} \longleftrightarrow \text{a and b are equivalent}$$

we can define an equivalence relation in $R^\times$. Then

$$R^\times = \bigcup_{a \in R^\times} C_a \quad \text{(disjoint)} \tag{2$_r$}$$

where $C_a = \{a, pa, \ldots, p^{r-1}a\}$.

When the length r of $(1)_r$ is even, we have no solution. Hence r is odd.

<u>Proposition 1</u> When the length r of the period in $(1)_r$ is equal to 3, we can get a periodic solution of $(1)_3$ for all primes $f \equiv 1 \bmod 6$ up to $f = 7$.

<u>Proof</u> Let p be a prime congruent to $w^{(f-1)/3}$ or $w^{2(f-1)/3}$ modulo f. Then there exist uniquely a, b $\in [1, g]$, $g = (f-1)/2$ such that $1 \pm a \pm b \equiv 1 + p + p^2 \equiv 0 \bmod f$. It is enough for us to consider the case of $p \equiv a$, $p^2 \equiv -b \bmod f$, namely

$$C_1 = \{1, a, -b\} \text{ and } 1 + a - b = 0. \tag{3}$$

Because in the case of $p \equiv -a$, $p^2 \equiv b \bmod f$, we may consider replacing p by p^2. For a class $C_j = \{j, pj, p^2j\}$ in the partition $(2)_3$ and an integer c, cC_j means the class $\{c, cpj, cp^2j\}$ and $C_i + C_j$ the class $\{i + j, p(i + j), p^2(i + j)\}$.

Now we select a class $C_a + C_b = C_a + (-C_{-b})$

$= \{a + b, - b - 1, 1 - a\}$.

i) For $a + b > g$, $b < g$, we have a solution $-(C_a + C_b)$ $= \{-(a + b), b + 1, - 1 + a\} = \{f - (a + b), b + 1, - 1 + a\}$ of $(1)_3$.

ii) For $a + b > g$, $b = g$, it holds $a = g - 1$. Since $- b \equiv a^2$, $0 \equiv g^2 - 3g \bmod f$ holds. Then $0 \equiv 4(g^2 - 3g) \equiv (2g + 1)^2 - 16g - 1$ $\equiv 7 \bmod f$. This implies $f = 7$, which is the exceptional case.

iii) $a + b < g$. In this case we choose the smallest integer d such that $d(a + b) > f/2$, then we obtain a solution $- d(C_a + C_b)$ $= \{f - d(a + b), d(b + 1), d(- 1 + a)\}$. The condition $d(b + 1) < f/2$ is valid for $b \geqq 5$. In fact $2d(b + 1) \leqq 2(d - 1)(a + b)$ holds if and only if $2 + (3/(b - 2)) \leqq d$ does. For $b \geqq 5$ the value $d = 3$ satisfies the final inequality. On the other hand the situation (3) implies $b \neq 1, 2$. For the case of $d = 3$ and $b = 3$, $- b \equiv a^2$, hence $-3 \equiv 4 \bmod f$, namely $f = 7$, which is impossible because of the same reason as ii). For the case of $d = 3$ and $b = 4$, we get $f = 13$. In the case of $d = 2$ if $d(b + 1) > f/2$, it holds that $4b + 4 > f > 4b - 2$. The last inequality follows from the definition of d. For the case of $f = 4b + 3$, $4b + 1$ and $4b - 1$, it follows that $f = 19$, 23 and 5 or 7 respectively. Finally we can see a solution of $(1)_3$ for $f = 13$ or 19 as follows:

$f = 13$	$C_2 = \{2, 6, 5\}$	$p \equiv 3, - 4 \bmod 13$
$f = 19$	$C_4 = \{4, 9, 6\}$	$p \equiv 7, - 8 \bmod 19$.

By i), ii) and iii) we have finished a proof of Proposition 1.

<u>Proposition 2</u> Let $f = 1 + a + \ldots + a^{r - 1}$ be a prime for $a > 2$. Then the length $r > 1$ of period in $(1)_r$ is odd, we can

get a periodic solution of $(1)_r$.

Proof[2] Let p be a prime congruent to a. C_1 denotes an equivalence class $\{1, a, a^2, \dots, a^{r-1}\}$ of $(2)_r$.

i) a is an odd number. In this case $\frac{a+1}{2}C_1$ gives a solution

$$\left\{ \frac{a+1}{2}, \frac{a+1}{2}a, \dots, \frac{a+1}{2}a^{r-2}, \frac{a+1}{2}a^{r-1} - \frac{a+1}{2}f \right\} \text{ of } (1)_r$$

with the length r of the period.

ii) a is an even number. In the case we can find a solution

$$\frac{3a+2}{2}C_1 = \left\{\frac{3a+2}{2}, \frac{3a+2}{2}a, \dots, \frac{3a+2}{2}a^{r-3}, \frac{3a+2}{2}a^{r-2} - f, \frac{3a+2}{2}a^{r-1} - \frac{3a-2}{2}f\right\} \text{ of } (1)_r.$$

§3. The rank of Hasse-Witt matrix

Let K be a finite field of characteristic $p > 2$ and $A_f = K(x, y)$ an algebraic function field over K defined by $y^2 = x^f + a$ ($a \in K$, $a \neq 0$), where $(p, f) = 1$ and $f = 2g + 1$ is a prime.

Let $\omega_1 = dx/y$, $\omega_2 = xdx/y$, $\dots$, $\omega_g = x^{g-1}dx/y$ be a basis f the K-module of holomorphic differentials in A_f. Then he Hasse-Witt matrix of A_f is defined by the representation matrix ver K of the Cartier operator C with respect to a basis $\{\omega_j\}_{1 \leq j \leq g}$ [1], [5], [6]:

$${}^t(C(\omega_1), \dots, C(\omega_g)) = M^t(\omega_1, \dots, \omega_g).$$

For any differential $\omega = (a_0^p + a_1^p + \dots + a_{p-1}^p x^{p-1})dx$ ($a_i \in A_f$), the operator C is defined by

$$C(\omega) = a_{p-1}dx.$$

Then we have

$$\omega_j = x^{j-1}dx/y = \sum_{k=0}^{\ell} \binom{\ell}{k} a^{\ell - k} x^{j + fk - 1} dx/y^p, \quad p = 2\ell + 1$$

and

$$C(x^{i + fk - 1}dx) = \begin{cases} x^{((i + fk)/p) - 1}dx, & i + fk \equiv 0 \bmod p \\ 0 & , \text{ otherwise} \end{cases}.$$

Recently T. Kodama and T. Washio obtained the next three lemmas[6].

Lemma 1 (i) The Hasse-Witt matrix M has at most one non-zero element in each row and in each column

(ii) rank $M = \#\{(i, k) \mid i + fk \equiv 0 \bmod f, (i, k) \in [1, g] \times [0, \ell]\}$.

(iii) rank $M = \#\{(i, j) \mid i \equiv pj \bmod f, (i, j) \in [1, g] \times [1, g]\}$.

Lemma 2 The rank of M is equal to g if and only if $p \equiv 1 \bmod f$. In this case

$$M = \begin{bmatrix} a_{11} & & \\ & \ddots & \\ & & a_{gg} \end{bmatrix},$$

where $a_{jj} = \binom{\ell}{k} a^{(\ell - k)/p}$ and $k = (p - 1)j/f$.

In this case it is called that the algebraic function field A_f is normal. When A_f is not normal, we say that A_f is singular.

Lemma 3 The rank of M is zero if and only if $p \equiv -1 \bmod f$.

It is known that the algebraic function field with M of rank zero is supersingular[3], [4], [7].

We shall construct some type of algebraic function fields which are singular but not supersingular. Finding a periodic solution $\{j_k\}_{k \bmod r}$, $1 \leqq j_k \leqq g$, $j_i \not\equiv j_k \bmod f$ $(i \not\equiv k \bmod r)$ of the congruences

$$pj_k \equiv j_{k+1} \bmod f, \qquad (1)_r$$

we can pursue our purpose.

Proposition 3 If the simultaneous congruences

$$pj_1 \equiv j_2,\ pj_2 \equiv j_3, \ldots,\ pj_r \equiv j_1 \bmod f$$
$$1 \leqq j_k \leqq g \quad (k \bmod r)$$

have a periodic solution $\{j_k\}_{k \bmod r}$, where $r = \mathrm{Ind}_f p$, then the rank of arbitrary power of the Hasse-Witt matrix M is not smaller than the length r of the period.

Proof By Lemma 1 and the assumption, in any j_k-th row of M only the (j_k, j_{k-1})-component has non-zero element. Then because of a solution $C_{j_1} = \{j_k\}$ we obtain the diagonal matrix M^r whose rank is at least r.

Remark 1 From the above proof the rank of M^r is a multiple of r. On the other hand when we have no solution of $(1)_r$, the rank of M^r is equal to 0.

Theorem 1 There exist infinitely many algebraic function fields A_f whose Hasse-Witt matrices are singular but have the rank at least 3 for all primes $f \equiv 1 \bmod 6$ up to $f = 7$.

Proof From Propositions 1, 3 and Lemma 2 Theorem 1 follows.

Remark 2 In the exceptional case we have no solution of $(1)_3$ for $g = 3$. Thus the algebraic function field A_7 is supersingular from Remark 1[7].

Combining Propositions 2, 3 and Lemma 2 we obtain the next theorem.

Theorem 2 Let $f = 1 + a + \dots + a^{r-1}$ be a prime number for an integer $a > 2$ and an odd number $r > 1$. Then there exists an algebraic function field A_f whose Hasse-Witt matrix is singular but has the rank at least r.

Remark 3 From Theorems 1, 2 and Proposition 3 it is shown that there exist infinitely many algebraic function fields which are singular but not supersingular.

Problem 1 Are there infinitely many such fields A_f with rank $M \geqq 5$?

Problem 2 Find a dencity relation between the length r and primes f.

Remark 4 Recently Prof. H. Niederreiter told to the author that if r and f satisfy Prop. 2, then necessarily $r = O(\sqrt{f}\log f)$ holds.

References

[1] T. Kodama, On the rank of the Hasse-Witt matrix, Proc. Japan Acad. Ser. A Math. Sci., 60(1984), 165-167.

[2] T. Nakahara, On a periodic solution of some congruences, Rep. Fac. Sci. Engrg. Saga Univ. Math., 14(1986), 1-5.

[3] M. Rosen, The asymptotic behavior of the class group of a function field over a finite field, Arch. Math., 24(1974), 287-296.

[4] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986, New York Berlin Heidelberg Tokyo.

[5] H. Stichtenoth, Die Hasse-Witt Invariante eines Kongruenzfunktionenkörpers, Arch. Math., 33(1979), 357-360.

[6] T. Washio and T. Kodama, Hasse-Witt matrices of hyperelliptic function fields, Sci. Bull. Fac. Ed. Nagasaki Univ., 37(1986), 9-15.

[7] T. Washio and T. Kodama, A note on a supersingular function field, ibid., 37(1986), 17-21.

Department of Mathematics
Faculty of Science and Engineering
Saga University
Saga 840
Japan