Some remarks on the BGS tower over finite cubic fields

Yasutaka Ihara (Chuo University)

§1 The "second basement" of the tower

We shall give some remarks related to the tower of function fields constructed by Bezerra, Garcia and Stichtenoth [1] (see also [2]).

Let $k = \mathbb{F}_q$ be any finite field, and x_1, x_2 be variables over k subject to the relation (the equation (0.7) of [1] for $i = 1$)

$$y_1 := \frac{x_1^q + x_1 - 1}{x_1} = \frac{1 - x_2}{x_2^q}. \tag{1}$$

Put

$$y_2 = \frac{x_2^q + x_2 - 1}{x_2}. \tag{2}$$

We choose a separable closure $k(x_1)^{sep}$ of $k(x_1)$, and any automorphism σ of $k(x_1)^{sep}(= k(x_2)^{sep})$ over k^{sep} that maps x_1 to x_2. Note that σ maps y_1 to y_2. We go down further to "the basement B2" of the BGS-tower. To "switch on the light for the floor B2", just note that $k(y_1) \cap k(y_2)$ is generated over k by the following element z_1.

$$z_1 := \frac{-y_1^q}{(1 - y_1)^{q+1}} = \frac{y_2 - 1}{y_2^{q+1}}. \tag{3}$$

(The proof will be indicated later.) Put

$$z_2 = \sigma(z_1) = \frac{-y_2^q}{(1 - y_2)^{q+1}}. \tag{4}$$

We have the following inclusion relations among these function fields.

$$\begin{tikzcd}[column sep=small]
k(x_1) \arrow[dr, dash] & & k(x_2) \arrow[dl, dash] \arrow[dr, dash] & & & \text{(extension degree } q\text{)} \\
& k(y_1) \arrow[dr, dash] & & k(y_2) \arrow[dl, dash] \arrow[dr, dash] & & \text{(extension degree } q+1\text{)} \\
& & k(z_1) & & k(z_2) &
\end{tikzcd}$$

Since $x_2 = (1-y_1)/(1-y_1+y_1y_2)$ and $y_2 = (1-z_2^{-1})/(1-z_1)$, $k(y_1,y_2) = k(x_2)$ and $k(z_1,z_2) = k(y_2)$ hold; hence the field generated over k by $\sigma^i(z_1)(i \in \mathbb{Z})$ is the same as that generated over k by $\sigma^i(x_1)(i \in \mathbb{Z})$.

That z_1 generates $k(y_1) \cap k(y_2)$ follows from the fact that the (degree $q+1$) extension $k(y_2)/k(z_1)$ has a point with ramification index q (see below §3) and hence cannot have any proper intermediate fields.

There are some advantages of going down to the second basement, the fields $k(z_1), k(z_2) \subset k(y_2)$. One is related to a group theoretic way of looking at the tower and the rational points over the cubic extension of k. The second is to show the existence of an invariant differential in the tower which shows up with a simple expression in terms of z_i.

§2 A group-theoretic way to see why the tower has many rational points over $\mathbb{F}_{q^3}$

Let T denote the field automorphism of $K = k(y_2)$ over k defined by

$$T(y_2) = 1 - y_2^{-1}. \tag{5}$$

Then (3)(4) can be rewritten respectively as

$$z_1 = T(y_2)/y_2^q, \tag{6}$$

$$z_2 = T(z_1). \tag{7}$$

Put $K_1 = k(z_1), K_2 = k(z_2)$, and let K^T denote the fixed field of T in K. Let M be the smallest Galois extension of K which is Galois both over K_1 and K^T. It is the composite of the tower of extensions of K obtained by first taking the Galois closure of K over K_1, then its Galois closure over K^T, then over K_1, and so on.

The key properties of the extension M/K comes from the following two key properties of the extension K/K_1 which is separable with degree q+1.

(I) Ramifications in K/K_1. The only ramifications are:
Above $z_1 = 0$; $\quad y_2 = 1, \infty$ with ramification indices $1, q$, respectively;
Above $z_1 = \infty$; $\quad y_2 = 0$ with ramification index $q+1$.
The set of ramified points upstairs in K is thus $0, 1, \infty$ which is stable under T.

(II) Decomposition in K/K_1. All points of K above $z_1 = 1$ are $\mathbb{F}_{q^3}$-rational. Note that,in view of (6), this is an immediate consequence of the fact $T^3 = 1$.

Moreover, the set of all points of K above $z_1 = 1$ is stable under the action of T (because of (6) for $z_1 = 1$, and because T commutes with the q-th power Frobenius morphism of K).

The set of points of $k(x_1)$ lying above $z_1 = 1$ coincides with that defined in [1](§3) by $x_1 = \omega \in \Omega$.

Proposition 1 *The Galois extension M/K has the following properties.*

(i) It is unramified outside $y_2 = 0, 1, \infty$, and ramified above $0, 1, \infty$ with infinite ramification indices.

(ii) All points above the point $z_1 = 1$ of K_1 are rational over $\mathbb{F}_{q^3}$.

(iii) $M^\sigma = M$, and hence M contains $x_i = \sigma^i(x_1)$ (and also $y_i = \sigma^i(y_1)$, $z_i = \sigma^i(z_1)$) for all $i \in \mathbb{Z}$.

Thus, M contains the BGS tower. It is Galois also over K_2.

Proof (i) Let $e_i (i = 0, 1, \infty)$ be the ramification index of $y_2 = i$ in M/K. Then, as M/K^T is Galois, $e_0 = e_1 = e_\infty$, and as M/K_1 is Galois, $e_1 = q.e_\infty$ (if finite); hence they must be infinite. The rest of (i)(ii) is clear from the above (I)(II). (iii) By (7), $\sigma = T \circ g$ with some $g \in Gal(K^{sep}/K_1)$. As M is Galois over K_1, M is g-invariant, and as M is Galois over K^T, it is T-invariant. Therefore, M is σ-invariant. The rest follows immediately.

Corollary 1 *M/K is an infinite Galois extension. Accordingly, $K_1 \cap K^T = k$.*

Remark One can probably show that $k(z_1) \cap k(z_2) = k$, so that there is no lower basement “B3”.

Let G denote the subgroup of the field automorphism group of M over k generated by $U_1 = Gal(M/K_1)$ and $U^T = Gal(M/K^T)$, or what amounts to the same, generated by U_1 and σ. The group G is locally compact and non-compact with respect to the natural Krull topology.

[Problems] *Find the explicit structure of G, the inertia groups in G, and decide whether G is the free product of U_1 and U^T with amalgamated subgroup $U = Gal(M/K)$, or some non-trivial quotient of it.*

Note that the decomposition group over $z_1 = 1$ is generated by an element of order 3.

One may replace T by a more general element of $PGL(2, k)$, consider y_2 as a new variable, and use the equations (6)(7) as the starting point. Then the points above $z_1 = 1$ are all rational over $\mathbb{F}_{q^n}$, where n is the order of T in $PGL(2, k)$, and this point set is stable under the action of T. But the trouble in the general case is with ramifications. In general, the set of points of K above the ramification locus (below) of K/K_1 does not seem to be stable under T, so the ramification in M/K does not seem to be so easily controllable.

§3 The invariant differential ω

By a differential of order d ($d \in \mathbb{N}$) of a function field K, we simply mean an element of the d-th tensor power of the module of rational differentials of K (tensored over K). It turns out that the following differential of order $q^2 - 1$ of our function field $k(z_1)$ is σ-invariant and hence belongs to $k(z_i)$ for any $i \in \mathbb{Z}$ (!).

Theorem 1 *Put*

$$\omega = \frac{(1-z_1)^{q+2}}{z_1^{q(q+1)}}(dz_1)^{\otimes(q^2-1)}. \tag{8}$$

Then as a differential of M of order q^2-1, it is G-invariant, in particular, σ-invariant;

$$\omega = \frac{(1-z_i)^{q+2}}{z_i^{q(q+1)}}(dz_i)^{\otimes(q^2-1)} \qquad (i \in \mathbb{Z}). \tag{9}$$

If L is any subfield of M containing any one of z_i , ω can be regarded as a differential of order q^2-1 of L. Let S_L (resp. T_L) denote the set of all geometric points of L obtained as the restriction to L of any extension of the point $z_1 = 1$ (resp. $z_1 = 0, \infty$) to M. Then the divisor $(\omega)_L$ of ω has support in $S_L \cup T_L$, and $ord_P(\omega)_L = q+2$ when $P \in S_L$; hence

$$(\omega)_L = (q+2)\sum_{P\in S_L} P + \sum_{P \in T_L} b(P)P \tag{10}$$

with some integers $b(P)$. In particular, whenever L satisfies

$$\sum_{P\in T_L} b(P) \leq 0, \tag{11}$$

one has an "individual" (Zink and) BGS-inequality

$$|S_L| \geq \frac{q^2-1}{q+2}(2g_L - 2), \tag{12}$$

for L, where g_L is the genus of L.

Proof Simple direct calculations. In fact, we have

$$\omega = \sigma(\omega) = \frac{(y_2^{q+1} - y_2 + 1)^{q+2}}{(y_2(1-y_2))^{q(q+1)}}(dy_2)^{\otimes(q^2-1)}. \tag{13}$$

Note also that

$$deg(\omega)_L = (q^2 - 1)(2g_L - 2), \tag{14}$$

and that if L'/L is a finite extension in M, and Q is a point of L' above a point P of L, then for any differential ω of order d on L,

$$ord_Q\omega = e(Q/P)ord_P\omega + d.\delta(Q/P), \tag{15}$$

where $e(Q/P)$ (resp. $\delta(Q/P)$) denote the ramification index (resp. the different exponent) of Q/P.

Recall that in the case of modular or Shimura curves over $\mathbb{F}_{q^2}$, the tower has an invariant differential ω of order $q-1$ having zeros of order 2 at every special $\mathbb{F}_{q^2}$-rational point, and that the existence of this differential is related to the liftability of the curve over $\mathbb{F}_{q^2}$ together with the sum of the graphs of the Frobenius correspondence and its transpose, to characteristic 0 (the first infinitesimal step for this) (cf. [3],[4],[5]). It seems also interesting to find out what the existence of ω in this case implies with regard to liftings especially to the original Zink's construction [6].

References

[1] J.Bezerra,A.Garcia,H.Stichtenoth, An explicit tower of function fields over cubic fields and Zink's lower bound, J.reine angew.Math. 589 (2005), 159-199.
[2] A.Bassa,H.Stichtenoth, A simplified proof for the limit of a tower over cubic finite fields, to appear in J.Number theory.
[3] Y.Ihara, On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations, J.Fac.Sci.Univ.Tokyo IA 21 (1974), 309-332.
[4] Y.Ihara, On the Frobenius correspondences of algebraic curves, Proc.Internat.Symp.on Algebraic Number Theory, S.Iyanaga ed., Kyoto (1976); 67-98, Japan Society of Promotion of Sciences.
[5] Y.Ihara, Lifting curves over finite fields together with the characteristic correspondences $\Pi + \Pi'$, J.Algebra 75 (1982),445-451.
[6] Th.Zink, Degeneration of Shimura surfaces and a problem in coding theory, in: Fundamentals of Computation Theory (Cottbus), L.Budach, ed., Springer-Verlag, New York (1985), 503-511.

Yasutaka Ihara (COE, Chuo University, and RIMS,Kyoto University (as P.E))
email: ihara@math.chuo-u.ac.jp, ihara@kurims.kyoto-u.ac.jp