On the existence of dimension zero divisors on curves over finite fields

Christophe Ritzenthaler
Joint work with Stéphane Ballet and Robert Rolland

Institut de Mathématiques de Luminy

Workshop on sequences, codes and curves (Antalya)
September 25 - 29, 2009

Riemann-Roch theorem

C/K a curve of genus g and κ its canonical divisor.

Theorem

Let D be a divisor of C and

$$\mathcal{L}(D) = \{f \in K(C) \mid \operatorname{div}(f) + D \geq 0\} \cup \{0\}.$$

Then

$$\dim D := \dim \mathcal{L}(D) = \deg D - g + 1 + \dim \mathcal{L}(\kappa - D).$$

Dimension zero divisor: $\dim D = 0 \iff \nexists D' \geq 0$ such that $D' \sim D$.

In particular, if $D' \sim D$ then D' has dim. 0 iff D has.

Elementary consequences

- if $\deg D < 0$, $\dim D = 0$;
- if $\deg D = 0$ then $\dim D = 0$ iff D is not principal ;
- if $\deg D \geq g$, $\dim D > 0$.

Particular case $\deg D = g - 1$:

$$\dim D = 0 \iff i(D) = \dim \mathcal{L}(\kappa - D) = 0$$

The integer $i(D)$ is called the index of speciality.
A divisor D such that $i(D) = 0$ is called non special.

Rem: If there is $P \in C(K)$ and if D is a dim. 0 divisor of degree $g - 1$, then there exists a dim. 0 divisor of degree $g - k$ for all $k > 0$.

Geometric interpretation

Conclusion : geometrically, dim. 0 divisor are not rare !

Behavior over $\mathbb{F}_q$

Let C be a genus g curve over $\mathbb{F}_q$.
Let A_m be the number of effective divisor of degree m and $h = \#(\mathrm{Jac}\, C)(\mathbb{F}_q)$.

Lemma

If $m \leq g-1$ and $A_m < h$, there exists a dim. 0 divisor of degree m.

Rem: it is not an equivalence.

Lachaud (asymptotics): proportion of (classes of) dim. 0 divisor of degree $g-k$ over $\mathbb{F}_q$

$$1 - \frac{1}{q^k} + \mathcal{O}\left(\frac{1}{q^{k+1}}\right).$$

What can be said for a fixed q ?

Main result

Let $C/\mathbb{F}_q$ be a curve of genus $g \geq 2$.

Theorem

There exists a dim. 0 divisor of degree $g-k$ over $\mathbb{F}_q$ if

1. $q = 2$ *and* $k \geq 5$;
2. $q = 3$ *and* $k \geq 2$;
3. $q \geq 4$ *and* $k \geq 1$.

The result for $q \geq 4$ were already known by Ballet-Le Brigand.

We can even get lower bound for the number of such divisors (but these bounds are not optimal).

Can we improve this result in the cases $q = 2, 3$?

There are exceptions (Ballet-Le Brigand)

For the following values of g, k and q, there are curves $C/\mathbb{F}_q$ of genus g without any dim. 0 divisor of degree $g-k$

- For $g=1$ (and $k=1$), 3 (isomorphism classes of) elliptic curves (with $q=2,3,4$);
- For $g=2$ and $k=2$ (resp. $k=1$), 2 curves over $\mathbb{F}_2$ (resp. 1 curve over $\mathbb{F}_2$);
- For $g=3$ and $k=1$, 3 (resp. 6) hyperelliptic (resp. non-hyperelliptic) curves over $\mathbb{F}_2$.

Question: are there infinitely many exceptions ?

Points on the curve

1. If $\#C(\mathbb{F}_q) > 0$ and if there is a dim. 0 divisor of degree $g-1$, then for all $k \geq 1$, there is a dim. 0 divisor of degree $g-k$.
2. If $\#C(\mathbb{F}_q) > g$ then, for all $k \geq 1$, there is a dim. 0 divisor of degree $g-k$ (Ballet-Le Brigand).
3. If $q = 2$ and $\#C(\mathbb{F}_q) > 2$, then for all $k \geq 2$, there is a dim. 0 divisor of degree $g-k$.

Relation with the p-rank

Definition

The p-rank $0 \leq \gamma \leq g$ of C is defined as $(\mathrm{Jac}\, C)[p](\bar{\mathbb{F}}_q) = p^\gamma$.

If $Z(C,t) = \frac{L(t)}{(1-t)(1-qt)}$ then $\gamma = \deg(L(t) \pmod p)$.

Proposition

Let $C/\mathbb{F}_q$ be a curve of p-rank γ. There exists a dim. 0 divisor of degree $\gamma - 1$.

For $p = 2$ and $\gamma = g$ (generic case), such divisor can be taken as $\frac{1}{2}\,\mathrm{div}(df)$ for any $f \in K(C) \setminus K$.

Proof

Let $L(t) = \sum_{i=0}^{2g} a_i t^i$, $h = L(1)$ and $h_{m,i}$ the order of the set of classes of divisors of degree m and dimension i.

$$Z(C,t) = \sum_{i=0}^{\infty} A_i t^i \Rightarrow A_m = \sum_{i=0}^{m} \frac{q^{m-i+1}-1}{q-1} a_i \Rightarrow A_m \equiv \sum_{i=0}^{m} a_i \pmod{p},$$

$$A_m = \sum_{i=1}^{\infty} \frac{q^i - 1}{q-1} h_{m,i} \Rightarrow A_m \equiv \sum_{i=1}^{\infty} h_{m,i} \pmod{p},$$

$$h = \sum_{i=0}^{\infty} h_{m,i} \text{ and } h \equiv \sum_{i=0}^{\gamma} a_i \pmod{p}.$$

For $m = \gamma - 1$,

$$h_{m,0} = h - \sum_{i=1}^{\infty} h_{m,i} \equiv h - A_m \equiv \sum_{i=0}^{\gamma} a_i - \sum_{i=0}^{\gamma-1} a_i \equiv a_\gamma \not\equiv 0 \pmod{p}.$$

Institut de Mathématiques de Luminy

Does arithmetic rule geometry ?

Theorem

If $q > 3$ (resp. $q = 2$) and

$$q^{-k+1} \sum_{i=0}^{g+k-1} a_i + \sum_{i=0}^{g-k} a_i \geq 0 \ \ (resp. \ > 0)$$

then there is a dim. 0 divisor of degree $g - k$.
Moreover, if C is hyperelliptic then there is a dim. 0 divisor of degree $g - k$ iff

$$\sum_{i=g-k+1}^{g} a_i + \sum_{i=g-k}^{g-1} q^{g-i} a_i + (q^k - 1) \sum_{i=0}^{g-k-1} q^{g-i-k} a_i > 0.$$

The second result is proved thanks to earlier results by Pellikaan.

Rem.: There is no such result for non hyperelliptic curves.

Where to look for counter-examples if $q = 2$ and $g > 3$?

If a curve $C/\mathbb{F}_2$ of genus g has no dim. 0 divisor of degree $g-1$ then

- The 2-rank of C is less than g;
- $\#C(\mathbb{F}_2) \leq g$ points;
- If C is hyperelliptic then

$$a_g + 2a_{g-1} + \sum_{i=0}^{g-2} 2^{g-i-1} a_i = 0.$$

Can one construct such a curve for infinitely many values of g ?

Thank you for your attention !

(and visit `www.manypoints.org`)