Portugal. Math. (N.S.)
Vol. 68, Fasc. 1, 2011, 103–107
DOI 10.4171/PM/1882

Portugaliae Mathematica

Special divisors of large dimension on curves with many points over finite fields

José Felipe Voloch*

(Communicated by Arnaldo Garcia)

Abstract. We prove a non-existence result for special divisors of large dimension on curves over finite fields with many points. We also give a family of examples where such divisors exist under less stringent hypotheses.

Mathematics Subject Classification (2010). Primary 14H25; Secondary 11F11, 11G20.
Keywords. Algebraic curves over finite fields, special divisors, modular forms.

1. Introduction

The purpose of this note is to study a hypothesis of Ben-Aroya and Ta-Shma [2] on the existence of special divisors of large dimension on curves with many points over finite fields. Their work was motivated by an application to the construction of binary error correcting codes with good properties by concatenating codes from large alphabets (such as algebraic geometry codes) with a Hadamard code. They remarked that, if divisors with certain properties could be constructed on curves meeting the Drinfeld–Vladut bound ([4], Theorem 9.37) their construction could be improved. Unfortunately, we show in this note that such divisors do not exist. We also give a construction of special divisors on modular curves which, although not quite reaching the demands of Ben-Aroya and Ta-Shma, do have large dimension and might be useful for similar constructions. This example also restricts how much our result can be improved. In the course of our proof we also obtain a version of Castelnouvo's genus bound valid for all curves in arbitrary characteristic.

*I would like to thank Amnon Ta-Shma for asking me about this question and various conversations and Gabor Wiese for many pointers to the literature. I would also like to acknowledge the support of my research by NSA grant MDA904-H98230-09-1-0070.

By a curve we always mean an irreducible projective algebraic curve over a field. When talking about genus or rational points on a curve, we mean the corresponding notions on a smooth model of the curve. By a strange curve, we mean a curve embedded in some projective space all of whose tangents at smooth points pass through a fixed point of the ambient space.

2. Main result

Lemma 2.1. *Let X be a curve, D a positive divisor on X such that the linear system defined by D embeds X in $\mathbf{P^n}$ as a strange curve, for some $n > 1$. Then $2D$ embeds X in $\mathbf{P^s}$ where $s \geq 2n - 1$ and such that the image is not a strange curve.*

Proof. Recall that, by definition, all tangents of a strange curve pass through a fixed point, called its nucleus. Replacing, if necessary, D by a linearly equivalent divisor, we may assume that the nucleus of the image of X in $\mathbf{P^n}$ is $(0 : 1 : 0 : \ldots : 0)$, so the embedding is given by $(1 : x : y_2 : \ldots : y_n)$, where x is a separating variable on X and $dy_i/dx = 0$ for all i, as follows from the condition that the tangents pass through the nucleus. I claim that the elements $1, x, y_2, \ldots, y_n, xy_2, \ldots, xy_n$ of $L(2D)$ are linearly independent. Indeed, if that is not the case, there exists a linear combination $y \neq 0$ of $y_2, \ldots, y_n$ such that $xy = a + bx + \sum c_i y_i$ with a, b, c_i constants. Differentiating this equation gives $y = b$ contradicting the fact that $1, x, y_2, \ldots, y_n$ are linearly independent. This shows the first claim. If the image were strange, so is the curve traced out by $1, x, y_2, \ldots, y_n, xy_2, \ldots, xy_n$ and its nucleus has to be of the form $(0 : 1 : 0 : \ldots : 0 : b_2 : \ldots : b_n)$ for some constants b_i and the condition that the tangents all go through the nucleus gives $d(xy_i)/dx = b_i$. But $d(xy_i)/dx = y_i$ and they cannot be constants, as noted above. This completes the proof. □

Remark 2.2. If the characteristic is not 2, then we could include x^2 among the list of linearly independent elements of $L(2D)$, with a similar proof and conclude $s \geq 2n$.

Corollary 2.3. *The genus g of X satisfies $g \leq m(m-1)(n-1) + m(2r+1)$, where $d - 1 = m(n-1) + r$, $0 \leq r \leq n - 2$.*

Proof. We have the Castelnuovo bound ([4], Theorem 7.111, [5], Theorem 2.9) which states that, if Y is a curve embedded in $\mathbf{P^n}$ of degree k, not contained in a hyperplane, not strange, and $k - 1 = m(n-1) + r$, $0 \leq r \leq n - 2$, then the genus of Y is at most $m(m-1)(n-1)/2 + mr$. Applying this bound to $X \subset \mathbf{P^s}$ as in the lemma proves the corollary. □

Consider now a curve of genus g and a divisor D on it with $\deg D = d$, $l(D) = n + 1$, $n \geq 0$. By the Riemann–Roch theorem we have $n \geq d - g$. When

$n > d - g$, then D is called a special divisor and we must have $d \leq 2g - 2$ and $n = 0$ or $n \leq d/2$ (Clifford's theorem). In this note we want to consider special divisors for which n is large, namely n/d is bounded below by some constant. We are particularly interested in curves over finite fields of large genus with many points in the sense of approaching the Drinfeld–Vladut bound.

We use the Vinogradov notation $f \ll g$ to mean $f \leq cg$ for some constant $c > 0$ where f, g are positive functions of some parameters. Naturally, $g \gg f$ means $f \ll g$. The symmetrical nature of the notation makes it preferable here to the common alternative $f = O(g)$.

Theorem 2.4. *Suppose that we have a sequence q_i of prime powers such that, for each $q = q_i$, we are given a curve of genus g over $\mathbb{F}_q$ such that $g/\sqrt{q} \to \infty$ as $i \to \infty$ and such that the curve has $N \gg g\sqrt{q}$ points over $\mathbb{F}_q$, and a divisor D with $\deg D = d$, $l(D) = n + 1$ satisfying $d/n \ll 1$. Then $g \ll n$. In particular, if $n \ll g/\sqrt{q}$, then q is bounded.*

Remark 2.5. Ben-Aroya and Ta-Shma ([2], Hypothesis 12) specifically ask for a situation as in the theorem. The condition $d/n \ll 1$ translates to their requirement that the divisors are c-dense for some $c > 0$. They also require $N/d > \beta q$ for some $\beta > 0$ (a βq gap). This forces g large (unless d is uniformly bounded, which they exclude). Under these conditions, $g\sqrt{q} \gg N > d\beta q > n\beta q$, so $n \ll g/\sqrt{q}$. They also require q unbounded. The theorem implies that this is not possible. In a personal communication, Ta-Shma noted that interesting results can still be obtained under a less stringent hypothesis. We offer some examples below but it's unclear how they impact the constructions envisaged in [2].

Proof. Let X be the curve postulated in the theorem. The divisor D defines a map $\phi : X \to \mathbf{P^n}$ and we let Y be the image of ϕ. If s is the degree of the induced map $X \to Y$, then Y has degree $k = d/s$. As $n \leq k$ since Y is not contained in a hyperplane, we get $s \ll 1$ under our assumptions, so $N \ll \#Y(\mathbb{F}_q) \ll q + g_Y\sqrt{q}$, where g_Y is the genus of Y, by the Weil bound. We consider two possibilities, $g_Y \leq \sqrt{q}$ or not. If $g_Y \leq \sqrt{q}$ then $N \ll q$, which by our hypothesis that $N \gg g\sqrt{q}$, gives $g \ll \sqrt{q}$, contradicting another of our hypotheses. So, $g_Y > \sqrt{q}$ and $N \ll g_Y\sqrt{q}$. Now we apply the Castelnuovo bound (or the corollary above, if Y is strange), noting that $m \leq (k-1)/(n-1) \ll 1$, so $g_Y \ll n$, therefore $N \ll g_Y\sqrt{q} \ll n\sqrt{q}$. Hence, if we assume that $N \gg g\sqrt{q}$, we get $g \ll n$, as claimed. The second statement clearly follows from the first and this proves the theorem. □

3. Examples

Ben-Aroya and Ta-Shma use, in [2], the Fermat curve of degree $p + 1$ over $\mathbb{F}_{p^2}$. This curve has genus $p(p-1)/2$, $p^3 + 1$ rational points and, for each $k \leq p$, the

divisor kH, where H is the intersection of the curve with the line at infinity, has dimension $\binom{k+2}{2}$.

Now we provide some examples of curves with many points and special divisors of large dimension based on the following proposition. Let $X_0(\ell)$ (where ℓ is a prime number) denote as usual the modular curve parametrising elliptic curves together with a subgroup of order ℓ.

Proposition 3.1. *Let g be the genus of $X_0(\ell)$, $\ell \equiv -1 \bmod 12$. Then $X_0(\ell)$ has a divisor D with $\deg D = g - 1$ which satisfies, for any fixed $\varepsilon > 0$, $l(D) \gg \ell^{1/2-\varepsilon}$.*

Proof. The proposition is a consequence of the results of Hecke [3]. (For a modern exposition, valid in arbitrary characteristic, see [6]). Namely, consider dihedral modular forms of weight one attached to unramified extensions of the imaginary quadratic field of discriminant ℓ. These are cusp forms for $\Gamma_1(\ell)$ of weight one, so sections of a line bundle on $X_1(\ell)$ of degree $g_1 - 1$, where g_1 is the genus of $X_1(\ell)$. They are also Hecke eigenforms, so linearly independent. Additionally, there are at least as many forms as the class number of $\mathbb{Q}(\sqrt{-\ell})$ minus one, so the number of forms is $\gg \ell^{1/2-\varepsilon}$, as follows from the Brauer-Siegel theorem.

These dihedral forms can be viewed as cusp forms for $\Gamma_0(\ell)$ of weight one and quadratic character $(-l\,|\,\cdot)$, Now, we fix one such form f_0 and look at f/f_0 for f varying among these dihedral forms. As the forms all have the same character, their ratio descends to a function on $X_0(\ell)$. As $X_1(\ell) \to X_0(\ell)$ is unramified under our assumptions, we get that these functions are in $L(D)$ for some divisor D of degree $g - 1$ on $X_0(\ell)$ and, from the above, $l(D) \gg \ell^{1/2-\varepsilon}$. □

Remark 3.2. The space of cusp forms of weight one on $X_0(\ell)$ often contains forms other than those constructed in the proof of the proposition. However, these extra forms are not expected to be enough to change the asymptotic behaviour of the dimension. For liftable forms, a precise conjecture is made in [1], conjecture 1.1, where also some results towards that conjecture are obtained. Non-liftable forms seem to be even rarer, see e.g. the numerical evidence in [6].

We know that g is $(\ell + 1)/12$ and that $X_0(\ell)$ has at least $g\sqrt{q}$ points over $\mathbb{F}_q$ if $q = p^2$, where $p \neq \ell$ is another prime. The condition $g/\sqrt{q} \to \infty$ can be satisfied with suitable choices of p, ℓ. However, for the divisor constructed in the proposition, d/n is not expected to be bounded above, so our theorem should not apply. In itself, our theorem is not strong enough to bound the number of non-liftable forms.

References

[1] M. Bhargava and E. Ghate, On the average number of octahedral newforms of prime level. *Math. Ann.* **344** (2009), 749–768. Zbl 05586453 MR 2507622

[2] A. Ben-Aroya and A. Ta-Shma, Constructing small-bias sets from algebraic-geometric codes. 50th Annual IEEE Symposium on Foundations of Computer Science (*FOCS* 2009), IEEE Computer Soc., Los Alamitos, CA, 2009, 191–197. MR 2648401

[3] E. Hecke, Zur Theorie der elliptischen Modulfunktionen, *Math. Ann.* **97** (1926), 210–242. JFM 52.0377.04 MR 1512360

[4] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic curves over a finite field*. Princeton Ser. Appl. Math., Princeton University Press, Princeton, NJ, 2008. Zbl 1200.11042 MR 2386879

[5] J. Rathmann, The uniform position principle for curves in characteristic *p*. *Math. Ann.* **276** (1987), 565–579. Zbl 0595.14041 MR 879536

[6] G. Wiese, Dihedral Galois representations and Katz modular forms. *Doc. Math.* **9** (2004), 123–133. Zbl 1119.14019 MR 2054983

Received February 22, 2010; revised May 23, 2010

J. F. Voloch, Department of Mathemtics, University of Texas, Austin, TX 78712, U.S.A.
E-mail: voloch@math.utexas.edu