Mathematical Research Letters **8**, 689–691 (2001)

CORRECTIONS TO: SPACE FILLING CURVES OVER FINITE FIELDS

Nicholas M. Katz

1. Introduction

Ofer Gabber has kindly pointed out to me that the proof of Lemma 5 in my article, "Space filling curves over finite fields," which appeared in *Mathematical Research Letters,* Volume 6, Number 5-6, pp. 613–624, is wrong. The error occurs in the last paragraph of the proof. The first sentence of that paragraph makes a false statement about Frobenius elements (starting with "so every..."). This false statement is used in the following sentence ("Therefore...") to assert that, for $r \geq r_0$, the conditions $(\star\star\, r, \mathcal{D}_r, \mathcal{C}_r)$ and $(\star\star\, r, \mathcal{E}/W)$ are equivalent. It is indeed trivially true that the first condition implies the second, but the converse need only hold if in addition r is divisible by N, the order of the cyclic group Γ/Γ_{geom}. The effect of correcting this error is that in Lemmas 4, 5, and 6, and in Corollary 7, what is asserted to hold for r sufficiently large holds only for r sufficiently large *and sufficiently divisible*. Indeed, Gabber has constructed examples to show that Lemma 6 and Corollary 7 can be false without this extra proviso. In the corrections below, we also modify the statement of Lemma 5 so that its new, weaker conclusion applies in a more general setting.

2. Corrections and modifications to statements of results

page 616, assertion 2) of Lemma 4: should read "For all sufficiently large *and sufficiently divisible* r, D_r/k is geometrically connected.".

page 617, lines 7-8 of the statement of Lemma 5 (i.e., lines 13-14 on the page): should read "$r \geq r_0$, a smooth, geometrically connected *k-scheme $\mathcal{C}_r$ and a k-morphism $i_r : \mathcal{C}_r \to W$ which is surjective on k_r-valued points.* Form the fibre"

page 617, line 12 of the statement of Lemma 5 (i.e., line 18 on the page): the label of the map in the diagram should be i_r and not $i_{r,W}$.

page 617, last line of the statement of Lemma 5: should read "Then for r sufficiently large *and sufficiently divisible* , the fibre product $\mathcal{D}_r/k$ is geometrically connected."

page 619, assertion a) of Lemma 6: should read "For r sufficiently large *and sufficiently divisible* , we have an equality of images of geometric fundamental

Received September 1, 2001.

groups

$$\rho_r(\pi_1^{geom}(\mathcal{C}_r, c_r)) = \rho(\pi_1^{geom}(W, w))$$

(equality inside G)."

page 619, assertion b) of Lemma 6: should read (in its entirety) "For r sufficiently large *and sufficiently divisible*, we have an equality of images of fundamental groups

$$\rho_r(\pi_1(\mathcal{C}_r, c_r)) = \rho(\pi_1(W, w))$$

(equality inside G)."

page 620, lines -5 and -2 in the statement of Corollary 7 (i.e. lines -10 and -6 on the page): should read respectively "Then (resp. then) for r sufficiently large *and sufficiently divisible*, the pullback sheaf $(f_r)^\star(\mathcal{F})$ on $\mathcal{C}_r$ has the same..."

3. Corrections to the proof of Lemma 5

page 618, line 15: should read "We will show that for any $r \geq r_0$ *which is divisible by* N *and which is* large enough that $(\star\star\, r, \mathcal{E}/W)$ holds, $\mathcal{D}_r$ is"

page 618, line -2, through page 619, line 2: Delete the last paragraph of the proof. Replace it by the following text.

We will show that for any $r \geq r_0$ which is divisible by N and for which $(\star\star\, r, \mathcal{E}/W)$ holds, the condition $(\star\star\, r, \mathcal{D}_r, \mathcal{C}_r)$ holds. We now fix one such r.

The subgroup $\pi_1(W \otimes_k k_r, w)$ of $\pi_1(W, w)$ maps, by ρ, to the subgroup $\Gamma(0) = \Gamma_{geom}$, simply because N divides r . Because this subgroup contains $\pi_1^{geom}(W, w)$, it maps onto Γ_{geom}. This subgroup contains all the Frobenius elements in $\pi_1(W, w)$ attached to k_r-valued points of W. By $(\star\star\, r, \mathcal{E}/W)$, the images of these elements fill Γ_{geom}. By the spacefilling property, each of these elements is $\pi_1(W \otimes_k k_r, w)$-conjugate to the image of a Frobenius element in $\pi_1(\mathcal{C}_r \otimes_k k_r, c_r)$ attached to a k_r-valued point of $\mathcal{C}_r$. The group $\pi_1(\mathcal{C}_r \otimes_k k_r, c_r)$ maps to Γ_{geom}, and the images of its Frobenius elements attached to k_r-valued points of $\mathcal{C}_r$ meet every conjugacy class in Γ_{geom}. So by Jordan's theorem, we conclude that $\pi_1(\mathcal{C}_r \otimes_k k_r, c_r)$ maps onto Γ_{geom}. Thus every element in Γ_{geom} is the image of a $\pi_1(\mathcal{C}_r \otimes_k k_r, c_r)$-conjugate of some Frobenius element attached to a k_r-valued point of $\mathcal{C}_r$ (because the images of these Frobenius elements meet every conjugacy class in Γ_{geom}, and $\pi_1(\mathcal{C}_r \otimes_k k_r, c_r)$ maps onto Γ_{geom}.) But the $\pi_1(\mathcal{C}_r \otimes_k k_r, c_r)$-conjugates of Frobenius elements attached to k_r-valued points of $\mathcal{C}_r$ are themselves such Frobenius elements, and thus $(\star\star\, r, \mathcal{D}_r, \mathcal{C}_r)$ holds.

We remark that from the fact that $\pi_1(\mathcal{C}_r \otimes_k k_r, c_r)$ maps onto Γ_{geom}, it follows that $\pi_1(\mathcal{C}_r, c_r)$ maps onto Γ, simply because any element of degree one in the source maps onto a generator of the cyclic quotient Γ/Γ_{geom}.

4. Correction to the proof of Lemma 6

page 619, line -3: the sentence should end "for r *divisible by* N *and* $r \gg 0$."

page 619, line -1: the sentence should end "whence a) *and b), cf. the corrected proof of Lemma 5.*"

page 620, delete lines 1-4.

page 620, line 10: add the words "*and sufficiently divisible*" after the phrase "for $r \gg 0$".

5. Correction to the proof of Theorem 8

page 621, line 7: should read "By Lemma 4, for large r *which is sufficiently divisible*, this closed subscheme $\mathcal{D}_{rd}$ of V is a smooth"

6. Counterexamples

In this section, we construct, following ideas of Ofer Gabber, counterexamples to the uncorrected versions of Lemma 6 and Corollary 7. We work over the finite field $k = \mathbb{F}_q$. Let G/k be a smooth, geometrically connected, commutative group-scheme of dimension $n \geq 1$, and

$$\phi : G \to G$$

a finite etale homomorphism of k-group-schemes of degree $deg(\phi) \geq 2$ with the following property: the finite etale commutative k-group-scheme $Ker(\phi)$ has no nontrivial k-rational points, i.e., $Ker(\phi)(k) = \{e\}$. Here are three elementary examples of such situations (G, ϕ).

(1) Pick $\alpha \neq 1$ in $\mathbb{F}_q^\times$, take $G = \mathbb{G}_a, \phi(x) := x^q - \alpha x$. Here $deg(\phi) = q$.
(2) Pick a prime number $l \geq q+1$, take $G = \mathbb{G}_m, \phi(x) := x^l$. Here $deg(\phi) = l$.
(3) Pick a prime number $l \geq 2 + q + 2\sqrt{q}$ and an elliptic curve $E/\mathbb{F}_q$, take $G = E, \phi(P) := lP$. Here $deg(\phi) = l^2$.

The geometric Frobenius F_k in $Gal(\bar{k}/k)$ acts as a group-automorphism of the finite group $Ker(\phi)(\bar{k})$. Denote by N the order of this automorphism. By hypothesis, F_k has no fixed points in $Ker(\phi)(\bar{k}) - \{e\}$. Therefore, for any integer $r \geq 1$ with $(r, N) = 1$, $(F_k)^r$ has no fixed points in $Ker(\phi)(\bar{k}) - \{e\}$. So for any such r, $Ker(\phi)(k_r) = \{e\}$, i.e., the map

$$\phi : G \to G$$

is injective, and hence bijective, on k_r-valued points.

In the notations of Lemma 6 and Corollary 7, take $W = G$, with base point $w = e$. For $r \geq 1$ with $(r, N) = 1$, take $f_r : \mathcal{C}_r \to W$ to be $\phi : G \to G$; for other r, take it to be $id : G \to G$. Take $c_r = e$ as base point in $\mathcal{C}_r = G$, and take as "chemin" from $f_r(c_r) = e$ to e the identity. To make counterexamples to Lemma 6 and Corollary 7, we need only exhibit a finite etale covering

$$\pi : \mathcal{E} \to G$$

which is geometrically nontrivial, but whose pullback by $\phi : G \to G$ is geometrically trivial. For the monodromy representation of such a covering will violate conclusion a) of Lemma 6 for every $r \geq 1$ with $(r, N) = 1$, and the lisse sheaf $\mathcal{F} := \pi_\star \bar{\mathbb{Q}}_l$ on G will violate the first conclusion of Lemma 7 for the same r. Such a $\pi : \mathcal{E} \to G$ is given by $\phi : G \to G$.