Finite Fields and Their Applications ••• (••••) ••••••

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Corrigendum

Corrigendum to "Artin's primitive root conjecture for function fields revisited" [Finite Fields Appl. 67 (2020) 101713] ☆

Seoyoung Kim *, M. Ram Murty

Department of Mathematics and Statistics, Queen's University, Kingston, ON K7L 3N6, Canada

ARTICLE INFO

Article history:
Received 3 September 2021
Accepted 9 November 2021
Available online xxxx
Communicated by Stephen D. Cohen

MSC:
11R58
11M41

Keywords:
Artin's conjecture
Function fields
Finite fields

The proof of Corollary 8 as given on page 13 of our paper [5] is not complete. Corollary 6 as stated is not correct. We thank Igor Shparlinski for pointing this out.

The first sentence of Corollary 6 in [5] should be "Let χ be a non-trivial character defined over $\mathbb{F}_{q^n}$ which is of the form $\chi^{(n)} = \chi \circ N$ as given in (4.17), which is not quadratic." With this change, the proof of Corollary 6 is valid.

DOI of original article: https://doi.org/10.1016/j.ffa.2020.101713.

☆ Research of the author was partially supported by an NSERC Discovery grant.

* Corresponding author.
E-mail addresses: sk206@queensu.ca (S. Kim), murty@queensu.ca (M.R. Murty).

https://doi.org/10.1016/j.ffa.2021.101963

Please cite this article in press as: S. Kim, M.R. Murty, Corrigendum to "Artin's primitive root conjecture for function fields revisited" [Finite Fields Appl. 67 (2020) 101713], Finite Fields Appl. (2022), https://doi.org/10.1016/j.ffa.2021.101963

Let $d|(q-1)$. Then, there are precisely d characters χ of $\mathbb{F}_q^*$ satisfying $\chi^d = 1$. Any character χ of $\mathbb{F}_{q^n}^*$ of order d is necessarily of the form $\chi \circ N$ where N is the norm map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. This is because the norm map is surjective (the norm of a generator of $\mathbb{F}_{q^n}^*$ is a generator of $\mathbb{F}_q^*$). With this observation, the proof of Corollary 8 is valid. However, the condition $d|(q-1)$ may not be always met. To rectify this, we proceed as follows.

Let $a(x)$ be a polynomial of degree K as alluded to in Corollary 8. Let χ be a character of $\overline{\mathbb{F}}_q$. The L-function attached to χ is

$$L(s,\chi) := \exp\left(\sum_{n=1}^{\infty} N_n(\chi)t^n/n\right), \qquad t = q^{-s},$$

where

$$N_n(\chi) := \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)).$$

This is the "geometric" form of the L-function that appears on page 103 of [2]. The reader can find a more modern presentation in [1]. This is the same L-function that appears in our paper and as noted there, is a polynomial in t of degree at most $K-1$ *provided* $(d, q-1) \neq 1$. It is well-known how this L-function changes via base change (see Theorem 8.15 on page 109 of [6] for instance). More precisely, the L-function over $\mathbb{F}_{q^r}$ is simply the L-function over $\mathbb{F}_q$ twisted by r-th roots of unity. Importantly, the absolute value of the zeros is unchanged by base change. Thus, our estimate for the zeros given in Theorem 4 can be applied in deriving the estimate (4.27) in the case $(d, q-1) \neq 1$.

The difficulty arises when $(d, q-1) = 1$. If $a(x)$ is linear, there is no difficulty since the character sums corresponding to non-trivial characters are simply zero. If $a(x)$ is quadratic, the elementary method in Jensen-Murty [4] paper deals with this case. Henceforth, we assume $K := \deg a \geq 3$ and that it is a squarefree polynomial. To prove Corollary 8, we apply a rudimentary sieve. For each d, we define $f(d)$ to be the order of $q \pmod{d}$. For d squarefree, $f(d)$ is simply the least common multiple of $f(\ell)$ for all primes ℓ dividing d. To avoid the difficulty described above, we should work over $\mathbb{F}_{q^{f(d)}}$ as our base field. With this understanding, we then have by applying Theorem 4:

Lemma 0.1. *The number of irreducible polynomials in $\mathbb{F}_q[x]$ of degree n for which $a(x)$ is a d-th power is*

$$\frac{q^n}{ndf(d)} + O(q^n e^{-n/f(d)(K-1)}).$$

Some remarks are in order. In the lemma we are counting polynomials not weighted by degree and so this explains n in the denominator in the main term. Also, as we are counting polynomials instead of elements of $\mathbb{F}_{q^n}$, this explains $df(d)$ in the denominator of the main term.

Please cite this article in press as: S. Kim, M.R. Murty, Corrigendum to "Artin's primitive root conjecture for function fields revisited" [Finite Fields Appl. 67 (2020) 101713], Finite Fields Appl. (2022), https://doi.org/10.1016/j.ffa.2021.101963

We now write $q^n - 1$ as AB where A is composed of primes $\ell < y$ and B is composed of primes $\geq y$, with y a parameter to be chosen. For each character χ of order d with d squarefree and dividing A, we have $f(d) < e^{Cy}$ for an absolute constant C, by a simple application of Chebycheff's theorem. By Theorem 4, each character sum corresponding to a non-trivial character is

$$O(q^n e^{-n/f(d)(K-1)}).$$

Thus, choosing $y = c \log\log n$ with c sufficiently small, ensures that the error term is

$$O(q^n e^{-n/(\log n)^v})$$

with $v < 1$. The number of squarefree divisors of A is at most $2^{\pi(y)}$. Now the number of irreducible polynomials $P(x)$ for which $a(x)$ is not a d-th power for all $d|A$ is by the inclusion-exclusion principle and Lemma 0.1,

$$\sum_{d|A} \frac{\mu(d)}{df(d)} \frac{q^n}{n} + O(q^n e^{-n/(\log n)^v})$$

If we let

$$N_\ell := \#\{P(x) \in \mathbb{F}_q[x] : P(x) \text{ is irreducible and } a(x) \text{ is an } \ell\text{-th power mod } P(x)\},$$

then the number of polynomials $P(x)$ for which $a(x)$ is a primitive root is at least

$$\sum_{d|A} \frac{\mu(d)}{df(d)} \frac{q^n}{n} + O(q^n e^{-n/(\log n)^v}) - \sum_{y<\ell<z} N_\ell - \sum_{\ell>z} N_\ell. \tag{1}$$

We apply the ℓ-th power reciprocity law to estimate N_ℓ (see Proposition 3.6 of [6]):

Lemma 0.2.

$$N_\ell \leq q^n/\ell^K.$$

Proof. We first treat the case $\deg a$ is even. Let d be the degree of θ over $\mathbb{F}_q$ and $P(x)$ its irreducible polynomial. To say $a(\theta)$ is an ℓ-th power is tantamount to saying $a(x)$ is an ℓ-th power (mod $P(x)$). By Proposition 3.6 of [6] $a(x)$ is an ℓ-th power if and only if $P \equiv a_i (\bmod\, a)$ where a_i are the classes mod a which are ℓ-th powers. Thus $P - a_i$ is divisible by a and the number of such polynomials is at most q^{d-K}. As the number of a_i is $\Phi(a)/\ell^K$ and $\Phi(a) \leq q^K$ we get q^d/ℓ^K and as $d \leq n$, the result is now clear. The case of $\deg a$ being odd is similar. □

Please cite this article in press as: S. Kim, M.R. Murty, Corrigendum to "Artin's primitive root conjecture for function fields revisited" [Finite Fields Appl. 67 (2020) 101713], Finite Fields Appl. (2022), https://doi.org/10.1016/j.ffa.2021.101963

An immediate consequence of the lemma is that the last sum in (1) is $O(q^n/(z^{K-1}\log z))$, because the tail is over primes $\ell > z$. As $K \geq 3$, choosing $z = n^{1-\epsilon}$ ensures the error is under control.

Finally, the middle sum in (1) is bounded by (applying Lemma 0.1):

$$\sum_{y<\ell<z} \frac{q^n}{n\ell f(\ell)} + O(q^n e^{-n/f(\ell)(K-1)}).$$

As $f(\ell) < \ell < z = n^{1-\epsilon}$ and the number of summands is at most z, the error is under control. Finally, the sum is the tail of a convergent series by a well-known theorem of Romanoff (see Theorem 108 on page 157 of [6] for example), and so this error is too under control.

Finally, to show the first term of (1) dominates, we apply Lemma 10.16 of [6] (due to Heilbronn [3]) which we state for the convenience of the reader: let $x_1, x_2, ..., x_n$ be real numbers with $0 \leq x_i \leq 1$ for each i. Let $a_1, ..., a_n$ be a finite set of natural numbers. Then,

$$1 - \sum_{i=1}^{n} \frac{x_i}{a_i} + \sum_{1\leq i<j\leq n} \frac{x_i x_j}{[a_i, a_j]} - \cdots + (-1)^n \frac{x_1 x_2 \cdots x_n}{[a_1, a_2, ..., a_n]} \geq \prod_{i=1}^{n} \left(1 - \frac{x_i}{a_i}\right).$$

Here, $[a_1, ..., a_r]$ denotes the least common multiple of $a_1, ..., a_r$. We apply this with $x_i = 1/\ell_i$ and $a_i = f(\ell_i)$ with the ℓ_i ranging over the prime divisors of A. We then have

$$\sum_{d|A} \frac{\mu(d)}{df(d)} \geq \prod_{\ell|A} \left(1 - \frac{1}{\ell f(\ell)}\right) \geq \prod_{\ell|A} \left(1 - \frac{1}{\ell}\right) \geq \prod_{\ell|q^n-1} \left(1 - \frac{1}{\ell}\right)$$
$$= \frac{\varphi(q^n-1)}{q^n-1} \gg \frac{1}{\log n + \log\log q}$$

by an elementary estimate for the Euler φ-function. Thus, the first term in (1) dominates the other two terms. This completes the proof Corollary 4 in [5].

References

[1] A. Adolphson, S. Sperber, Character sums in finite fields, Compos. Math. 52 (1984) 325–354.
[2] H. Davenport, On character sums in finite fields, Acta Math. 71 (1939) 99–121.
[3] H. Heilbronn, On an inequality in the elementary theory of numbers, Proc. Camb. Philol. Soc. 33 (1937) 207–209.
[4] E. Jensen, M. Ram Murty, Artin's conjecture for polynomials over finite fields, in: R.P. Bambah, V.C. Dumir, R.J. Hans-Gill (Eds.), Number Theory, Hindustan Book Agency, Indian National Science Academy, 2000, pp. 167–181.
[5] S. Kim, M. Ram Murty, Artin's primitive root conjecture for function fields revisited, Finite Fields Appl. 67 (2020) 101713.
[6] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

Please cite this article in press as: S. Kim, M.R. Murty, Corrigendum to "Artin's primitive root conjecture for function fields revisited" [Finite Fields Appl. 67 (2020) 101713], Finite Fields Appl. (2022), https://doi.org/10.1016/j.ffa.2021.101963