Note on Kim & Murty, *Artin's primitivie root conjecture for function fields revisited.*[2, 3]

Javier López-Contreras

October 2022

1 Introduction

As I communicated in a very brief email some days ago I believe there is a flaw in [2] which invalidates the proof of Artin's conjecture over Function Fields as is detailed in [3] and [2].

For the sake of brevity, I wasn't able to fully expose the details of the possible flaw in the email. I am writting this note with that precise objective, hoping it will make it easier for you to weight in.

2 Details

Definition 1. The second page of the corrigendum [2] introduces the following L-function. Given a fix $a \in \mathbb{F}_q[x]$ monic[1] of degree K and an arbitrary character of the algebraic closure $\chi : \overline{\mathbb{F}_q} \to \mathbb{C}$, define

$$L(s, \chi) := \exp\left(\sum_{n \geq 1} N_n(\chi) \frac{q^{-sn}}{n}\right)$$

with

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

- The next paragraph states that this L-function is another form of the L-function given in the original paper [3]. I believe the error is in this equality of L-functions.

[1] Although it is not explicitly specified [3] or [2], you can always assume monic in the Artin's conjecture setting as any non-monic polynomial will never be a primitive root modulo any $p \in \mathbb{F}_q[x]$

Definition 2. The L-function of the original paper is defined as follows. Given an r-tuple of characters $\chi_i' : \mathbb{F}_q \to \mathbb{C}$ and an r-tuple of monic irreducible polynomials $f_i \in \mathbb{F}_q[x]$, define

$$\begin{aligned} \widehat{\chi} : \mathbb{F}_q[x] &\to \mathbb{C} \\ g &\mapsto \prod_{i=1}^{r} \chi_i'(\ (f_i, g)\ ) \end{aligned}$$

where (f_i, g) indicates the resultant. Then, define

$$\mathcal{L}'(s, \widehat{\chi}) = \sum_{\substack{g \in \mathbb{F}_q[x] \\ \text{monic}}} \frac{\widehat{\chi}(g)}{(q^{\deg g})^s}$$

- To equalize Definition 2 with Definition 1, I understand that the natural choice is to take $r = \#$irreducible factors of a, $(f_1, \ldots, f_r)$ the irreducible components of a.
- Setting the $\chi_i' = \chi$ doesn't work as, to start, the χ_i should be characters of $\mathbb{F}_q$ and χ is a character of $\overline{\mathbb{F}}_q$. Even if we stretch the Definition 2 to include characters of $\overline{F}_q$, this choice of χ_i will still not work, as I will show in a moment. For now, let's just set them all equal to each other $\chi_i' = \chi'$, letting χ' be an arbitrary character of $\mathbb{F}_q$ (possibly a character of $\overline{F}_q$, if we need to stretch the definition).
- Note that we have $\widehat{\chi}(g) = \chi'(\ (a, g)\ )$ as $a = \prod f_i$. We have split a into irreducible components just to match the conditions of the Definition 2.

Question, is $\mathcal{L} = \mathcal{L}'$?

- Taking the logarithm of the Euler product of second L-function, we get

$$\begin{aligned} \log \mathcal{L}'(s, \widehat{\chi}) &= \sum_{\substack{v \in \mathbb{F}_q[x] \\ \text{monic irreducible}}} -\log\left(1 - \frac{\widehat{\chi}(v)}{q^{\deg v s}}\right) \\ &= \sum_{\substack{v \in \mathbb{F}_q[x] \\ \text{monic irreducible}}} \sum_{k \geq 1} \frac{1}{k} \cdot \left(\frac{\widehat{\chi}(v)}{q^{\deg v s}}\right)^k \\ &= \sum_{m \geq 1} \sum_{\substack{v \in \mathbb{F}_q[x] \\ \text{monic irreducible} \\ \deg v = m}} \sum_{k \geq 1} \frac{1}{k} \cdot \widehat{\chi}(v)^k q^{-mk \cdot s} \\ &= \sum_{n \geq 1} \left(\sum_{m \mid n} \sum_{\substack{v \in \mathbb{F}_q[x] \\ \text{monic irreducible} \\ \deg v = m}} m \cdot \widehat{\chi}(v)^{n/m} \right) \frac{q^{-sn}}{n} \end{aligned}$$

where, in the last equality, we have set $n = mk$

- For this to be equal to Definition 1, we would need the equality of all the coefficients. Namely, $\forall n \geq 1$

$$N_n(\chi) = \sum_{\theta \in \mathbb{F}_{q^n}} \chi(a(\theta)) \stackrel{?}{=} \sum_{m|n} \sum_{\substack{v \in \mathbb{F}_q[x] \\ \text{monic irreducible} \\ \deg v = m}} m \cdot \chi'(\ (a,v)\ )^{n/m}$$

- If $\chi = \chi' \circ N_{\mathbb{F}_q^n/\mathbb{F}_q}$, this is true. For any $v \in \mathbb{F}_q[x]$ irreducible polynomial of degree m, let $\theta_1, \ldots, \theta_m$ be its roots. Now

$$\begin{aligned}
\chi(a(\theta_1)) + \cdots + \chi(a(\theta_m)) &= \chi'(N(a(\theta_1))) + \cdots + \chi'(N(a(\theta_m))) \\
&= \sum_i \chi' \left(\left(\prod_j a(\theta_j) \right)^{n/m} \right) \\
&= m \cdot \chi' \left(\prod_i a(\theta_i) \right)^{n/m} \\
&= m \cdot \chi'(\ (a,v)\ )^{n/m}
\end{aligned}$$

  Adding over all conjugation classes, we get the desired identity.

- But, given an arbitrary $\chi : \overline{F}_q \to \mathbb{C}$ which is not the lift of any character on the base field, there doesn't seem to be a natural choice of χ' that makes the identity true.

3 Flaw in the proof of Artin's conjecture

The equality of the two L-functions is not merely a presentation problem. It is logically used in the proof of Artin's conjecture.

- To prove Artin's conjecture it is sufficient to see that for any $a \in \mathbb{F}_q[x]$ monic, for all n big enough and all $\chi : \mathbb{F}_{q^n} \to \mathbb{C}$, there is an upper bound to the following character sum.

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

- Davenport [1] proves that the L-function on Definition 2 is a polynomial. Only in the case $\chi = \chi' \circ N$ he uses this to find and equality of these character sum with a sum over the zeroes of the L-function.

- For $\chi \neq \chi' \circ N$, the character sum that one needs to bound doesn't even come up as a coefficient in the L-series of Definition 2. It only comes up as a coefficient in the Definition 1, which, a priori, is not a polynomial nor does it follow an equality similar to the one found by Davenport.

4 Brief comment on another potential issue

For the sake of completeness, let me express another smaller remark. It is about the original paper[3], but doesn't seem to be corrected in the corrigendum.

The Main Theorem (Theorem 4 [3]) is not needed in the Proof of Corollary 8 even when $\chi = \chi' \circ N$, which, as corrected in the corrigenum, is the only family of character bounds that the original paper proves correctly, a priori. This result is still cited in the corrigendum for the case $(d, q-1) \neq 1$, so I thought it might be significant to point it out.

- The Main Theorem is used to give a non-trivial upper bound to the character sum in the non-quadratic case, namely $q^n e^{\frac{-cn}{K-1}}$ for any c such that $c_1 > c > 0$, where c_1 is the constant given by Theorem 4 and K is the degree of the polynomial a.
- For the quadratic case, a worse bound is given using the classical methods, namely q^{nB} for some $B < 1$.
- But then, to make $q^n e^{\frac{-cn}{K-1}}$ upper bound q^{nB}, the paper makes $c \to 0$, choosing a $0 < c < (K-1)(1-B)\log q$. Making $c \to 0$ just makes the non-trivial bound at least as bad as the classical one.
- Hence, the classical bound is already enough if used for both cases.

The proof for the case of $\chi = \chi' \circ N$ is still correct but there is no need to give a non-trivial bound. The bound obtained with the classical method is enough.

References

[1] H Davenport. "On character sums in finite fields". In: *Acta Math.* 71 (1939), pp. 99–121.

[2] Seoyoung Kim and M. Ram Murty. "Corrigendum to "Artin's primitive root conjecture for function fields revisited" [Finite Fields Appl. 67 (2020) 101713]". In: *Finite Fields and Their Applications* 78 (2022), p. 101963. ISSN: 1071-5797. DOI: `https://doi.org/10.1016/j.ffa.2021.101963`. URL: `https://www.sciencedirect.com/science/article/pii/S107157972100157X`.

[3] Seoyoung Kim and M. Ram Murty. "Artin's primitive root conjecture for function fields revisited". In: *Finite Fields and Their Applications* 67 (2020), p. 101713. ISSN: 1071-5797. DOI: `https://doi.org/10.1016/j.ffa.2020.101713`. URL: `https://www.sciencedirect.com/science/article/pii/S1071579720300824`.