DISTRIBUTION OF POINTS ON CYCLIC CURVES OVER FINITE FIELDS

PATRICK MEISNER

Abstract. We determine in this paper the distribution of the number of points on the cyclic covers of \( \mathbb{P}^1(\mathbb{F}_q) \) with affine models \( C : Y^r = F(X) \), where \( F(X) \in \mathbb{F}_q[X] \) and \( r^{th} \)-power free when \( q \) is fixed and the genus, \( g \), tends to infinity. This generalizes the work of Kurlberg and Rudnick and Bucur, David, Feigon and Lalin who considered different families of curves over \( \mathbb{F}_q \). In all cases, the distribution is given by a sum of random variables.

1. Introduction

For any smooth projective, \( C \), of genus \( g \) over a finite field known that
\[
\#C(\mathbb{P}^1(\mathbb{F}_q)) = q + 1 - \sum_{j=1}^{2g} \alpha_j(C)
\]
where the zeta function of \( C \) is
\[
Z_C(u) = \prod_{j=1}^{2g}(1 - u \alpha_j(C))
\]
and \( |\alpha_j(C)| = q^{\frac{g}{2}} \) for \( j = 1, \ldots, 2g \).

The distribution of \( \#C(\mathbb{P}^1(\mathbb{F}_q)) \) when \( C \) varies over families of curves over \( \mathbb{F}_q \) is a classical object of study. For several families of curves over \( \mathbb{F}_q \) Katz and Sarnak [3] showed that when the genus is fixed and \( q \) tends to infinity,
\[
\frac{\sum_{j=1}^{2g} \alpha_j(C)}{\sqrt{q}}
\]
is distributed as the trace of a random matrix in the monodromy group of the family.

The distribution of the number points on families of curves over finite fields with \( q \) fixed while the genus tends to infinity has been a topic of much research recently. It began with Kurlberg and Rudnick [4] determining the distribution of the number of points of hyperelliptic curves. Hyperelliptic curves are in one-to-one correspondence with Galois extensions of \( \mathbb{F}_q(X) \) with Galois group \( \mathbb{Z}/2\mathbb{Z} \). Bucur, David, Feigon and Lalin [1],[2] extended this result to smooth projective curves that are in one-to-one correspondence with Galois extensions of \( \mathbb{F}_q(X) \) with Galois group \( \mathbb{Z}/p\mathbb{Z} \), where \( p \) is a prime such that \( q \equiv 1 \mod p \). Recently Lorenzo, Milione and Meleleo [5] determined the case for Galois group \( \mathbb{Z}/(2\mathbb{Z})^n \). In this paper we determine the case for cyclic Galois groups \( \mathbb{Z}/r\mathbb{Z} \) for any \( q \equiv 1 \mod r \) where \( r \) is not necessarily a prime.

Let \( K = \mathbb{F}_q(X) \) and let \( L \) be a finite Galois extension of \( K \). Let \( r \) be an integer such that \( q \equiv 1 \mod r \). Suppose that \( \text{Gal}(L/K) = \mathbb{Z}/r\mathbb{Z} \). Then there exists a
unique smooth projective curve over \( \mathbb{F}_q \), \( C \), such that \( L \cong K(C) \). Further, \( C \) will have an affine model of the form
\[
Y^r = \alpha F(X), \quad F \in \mathcal{F}_{(d_1, \ldots, d_{r-1})} \subset \mathbb{F}_q[X], \alpha \in \mathbb{F}_q^*
\]
where
\[
\mathcal{F}_{(d_1, \ldots, d_{r-1})} = \{ F = f_1 f_2 \cdots f_{r-1}^{-1} : f_i \in \mathbb{F}_q[X] \text{ are monic, square-free, pairwise coprime,} \}
\]
and \( \deg F_i = d_i \) for \( 1 \leq i \leq r - 1 \).

The Riemann-Hurwitz formula (Theorem 7.16 of [6]) tells us that if we let \( d = \sum_{i=1}^{r-1} id_i \), then the genus \( g \) of the curve \( C \) is given by
\[
2g + 2r - 2 = \sum_{i=1}^{r-1} (r - (r, i))d_i + (r - (r, d))
\]
where \( (r, i) = \gcd(r, i) \). Define now the following sets
\[
\mathcal{F}^j_{(d_1, \ldots, d_{r-1})} = \mathcal{F}_{(d_1, \ldots, d_{j-1}, \ldots, d_{r-1})}
\]
\[
\hat{\mathcal{F}}_{(d_1, \ldots, d_{r-1})} = \{ \alpha F : F \in \mathcal{F}_{(d_1, \ldots, d_{r-1})}, \alpha \in \mathbb{F}_q^* \}
\]
\[
\hat{\mathcal{F}}^j_{(d_1, \ldots, d_{r-1})} = \hat{\mathcal{F}}_{(d_1, \ldots, d_{j-1}, \ldots, d_{r-1})}
\]
\[
\mathcal{F}_{[d_1, \ldots, d_{r-1}]} = \mathcal{F}_{(d_1, \ldots, d_{r-1})} \cup \bigcup_{j=1}^{r-1} \mathcal{F}^j_{(d_1, \ldots, d_{r-1})}
\]
\[
\hat{\mathcal{F}}_{[d_1, \ldots, d_{r-1}]} = \hat{\mathcal{F}}_{(d_1, \ldots, d_{r-1})} \cup \bigcup_{j=1}^{r-1} \hat{\mathcal{F}}^j_{(d_1, \ldots, d_{r-1})}
\]

If we now restrict the \( d_i \) such that \( \sum_{i=1}^{r-1} id_i \equiv 0 \mod r \), then the genus will be invariant over curves with affine models \( Y^r = F(x) \) with \( F(x) \in \hat{\mathcal{F}}_{[d_1, \ldots, d_{r-1}]} \). That is, if we let \( \mathcal{H}_{g, r} \) be the set of curves of genus \( g \) such that \( \text{Gal}(L/K) = \mathbb{Z}/r\mathbb{Z} \), we can write
\[
\mathcal{H}_{g, r} = \bigcup_{\sum_{i=1}^{r-1} id_i \equiv 0 \mod r} \mathcal{H}^{(d_1, \ldots, d_{r-1})}
\]
where \( \mathcal{H}^{(d_1, \ldots, d_{r-1})} \) are the curves with affine models in \( \hat{\mathcal{F}}^{[d_1, \ldots, d_{r-1}]} \). We will discuss the distribution of points not on the whole of \( \mathcal{H}_{g, r} \) but on each \( \mathcal{H}^{(d_1, \ldots, d_{r-1})} \).

Kurlberg and Rudnick [4] first investigated the distribution of points for hyperelliptic curves \( (r = 2) \). Bucur, David, Feigon and Lalin [1],[2] then extended this result to the case where \( r = p \), a prime. They noted that the number of points on such a curve will be given by the formula
\[
\#C(\mathbb{P}^1(\mathbb{F}_q)) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{i=0}^{p-1} \chi_p^i(F(x)) = q + 1 + \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \sum_{i=1}^{p-1} \chi_p^i(F(x)),
\]
where \( \chi_p \) is a primitive character on \( \mathbb{F}_q \) of order \( p \). Such a character exists since \( q \equiv 1 \mod p \). This will be determined by the value \( S_p(F) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_q)} \chi_p(F(x)) \) which leads to the result
**Theorem 1.1** (Theorem 1.1 from [1]). If $q$ is fixed and $d_1, \ldots, d_{p-1} \to \infty$ then for any $t \in \mathbb{Z}[\zeta_p]$

$$\frac{|\{F \in \hat{F}_{d_1,\ldots,d_{r-1}} : S_p(F) = t\}|}{|F_{d_1,\ldots,d_{r-1}}|} \sim \text{Prob}\left(\sum_{i=1}^{q+1} X_i = t\right)$$

where the $X_i$ are i.i.d random variables such that

$$X_i = \begin{cases} 0 & \text{with probability } \frac{p-1}{p^2-1} \\ \zeta_p^i & \text{with probability } \frac{q}{p(q+p-1)} \end{cases}$$

For general $r$, we prove in Section 2 a formula for the number of point on the curve with affine model $Y^r = F(X)$. In order to state this formula and our main result, we need some notation. For $d|r$, define

$$F_d(X) = \prod_{i=1}^{d-1} \left( \prod_{j=0}^{r-1} f_{jd+i}(X) \right)^i = \prod_{i=1}^{r-1} f_i(X)^i \mod d.$$ 

Notice that we could write an affine model for our curve as $Y^r = F_1(X)$. Further, the $F_d(X)$ correspond to the subfield extension of $L$. That is if we have $K \subset L \subset L$, then $L' = K(C_d)$, where $C_d$ is a curve with affine model $Y^d = F_d(X)$ for some $d|r$. Then Lemma 2.1 shows that

$$\#C(\mathbb{P}^1(F_q)) = q + 1 + \sum_{d|r} \sum_{(i,d)=1} \sum_{x \in \mathbb{P}^1(F_q)} \chi_d(F_d(x))$$

where $\chi_d$ is a primitive character on $F_q$ of order $d$. Again, such a character exists since $d|r$ and we are assuming that $q \equiv 1 \mod r$. Hence if we define

$$S_d(F_d) = \sum_{x \in \mathbb{P}^1(F_q)} \chi_d(F_d(x))$$

then the number of points on the curve will be determined by the $S_d(F_d)$ for all $d|r$. This leads us to the main theorem

**Theorem 1.2.** Write $r = \prod_{j=1}^{b} p_j^{b_j}$. If $q$ is fixed, then as $d_1, \ldots, d_{r-1} \to \infty$ for any $M_d \in \mathbb{Z}[\zeta_d],$

$$\frac{|\{F \in \hat{F}_{d_1,\ldots,d_{r-1}} : S_d(F_d) \neq M_d, \forall d|r, d \neq 1\}|}{|F_{d_1,\ldots,d_{r-1}}|} \sim \text{Prob}\left(\sum_{i=1}^{q+1} X_{d,i} = M_d, \forall d|r, d \neq 1\right)$$

where $X_{d,i}$ are random variables taking values in $\mu_d \cup \{0\}$ such that

$$\text{Prob}(X_{d,i} = 0) = \frac{r - \frac{d}{q}}{q + r - 1}$$

$$\text{Prob}(X_{d,i} = \epsilon_{d,i} \neq 0) = \frac{q + \frac{r}{d} - 1}{d(q + r - 1)}.$$ 

Moreover, if $i \neq j$ then $X_{d,i}$ and $X_{d,j}$ are independent for all $d,d'|r$. However, if we fix $i$, then for all $d|r$

$$X_{d,i} = \prod_{p|d}(x_{p^{\sigma_p}(d),i})^{\sigma_p} \text{ where } 1 \leq \sigma_p \leq \frac{d}{p^{\nu_p(d)}} \text{ such that } \sigma_p \equiv (p^{\nu_p(d)})^{-1} \mod \frac{d}{p^{\nu_p(d)}}.$$
Further, for all \( p | r \) and \( 1 < s \leq v_p(r) \)
\[
\text{Prob} \left( X_{p^r,i} = 0 | X_{p^r-1,i} = 0 \right) = 1
\]
\[
\text{Prob} \left( X_{p^r-1,i} = \epsilon_{p^r,i} \mid X_{p^r,i} = \epsilon_{p^r,i} \right) = 1.
\]
Finally, if \( d | r \) but \( d \neq r \) then
\[
\text{Prob} \left( X_{p^r,i} = \epsilon_{p^r,i} \neq 0, 1 \leq s \leq v_p(d) \right) \text{ and } X_{p^r,i} = 0, v_p(d) < s \leq v_p(r) \text{ for all } p | r
\]
\[
= \begin{cases} 
\phi(q) - 1 \\
0
\end{cases}
\]
\[
\frac{q}{d(q + r - 1)} \text{ if } \epsilon_{p^r-1,i} = \epsilon_{p^r,i} \text{ for all } p | r, 1 \leq s \leq v_p(d)
\]
and, if \( d = r \),
\[
\text{Prob} \left( X_{p^r,i} = \epsilon_{p^r,i}, s \leq v_p(r) \right) \text{ for all } p | r
\]
\[
= \begin{cases} 
\frac{q}{r(q + r - 1)} \\
0
\end{cases}
\]
\[
\frac{p}{r} \text{ if } \epsilon_{p^r-1,i} = \epsilon_{p^r,i}, 1 \leq s \leq v_p(r), \text{ for all } p | r.
\]

To simplify notation, we will prove this for \( r = p^n \) in full detail in Section 4, and present in Section 5 the proof for general \( r \). Section 6 gives a heuristic which corroborates the results of Theorem 1.2.

2. Number of Points on the Curve

Let \( C \) be the smooth projective curve over \( \mathbb{F}_q \) associated to the field \( L = \mathbb{F}_q(X) \left( \sqrt[n]{\alpha f_1(X) f_2^2(X) \ldots f_{r-1}^r(X)} \right) \) where the \( f_i \) are monic, squarefree and pairwise coprime and \( \alpha \in \mathbb{F}_q^* \). Let us determine the smooth affine models of these curves. We first consider the affine model
\[
Y^r = \alpha f_1(X) f_2^2(X) \ldots f_{r-1}^{r-1}(X).
\]
and investigate the smoothness. For any \( j \) such that \( (j, r) = 1 \) we define
\[
F^{(j)} = \alpha^j \prod_{i=1}^{r-1} f_i^{ij} \text{ mod } r.
\]
Then \( F^{(1)} = F \), \( F^j = F^{(j)} H^r \) for some \( H \in \mathbb{F}_q[X] \) and \( Y^r = F^{(j)}(X) \) is another affine model for the curve \( C \).

If \( F(x) \neq 0 \) then any of the models will be smooth at \( x \). If \( f_i(x) = 0 \) for some \( x \in \mathbb{F}_q \) and for some \( i \) such that \( (i, r) = d \) then we can find some \( j \) such that \( (j, r) = 1 \) and \( ij \equiv d \mod r \). Hence \( F^{(j)} \) would have a \( d^{th} \) root at \( x \) and the model \( Y^r = F^{(j)}(X) \) would be smooth at \( x \) if and only if \( d = 1 \).

Now, without loss of generality we may assume we have an affine model \( Y^r = \alpha F(X) \) such that \( f_d(x) = 0 \) for some \( x \in \mathbb{F}_q \) and \( d | r, d \neq 1 \). Moreover, without loss of generality, we may assume \( x = 0 \). Blowing-up the curve at \((0, 0)\) then we get the variety defined by
\[
(Y^r - \alpha f_1^1(X) f_2^2(X) \ldots f_{r-1}^{r-1}(X), Xw - Yz)
\]
where \( w, z \) are projective coordinates. If \( z \neq 0 \), then \( Y = Xw \) and by writing \( f_d(X) = Xf_d^1(X) \) we get
\[
0 = (Xw)^r - X^d \alpha f_1(X) f_2^2(X) \ldots f_d^d(X) \ldots f_{r-1}^{r-1}(X)
\]
\[
= X^d ((X^r - Y)^d - \alpha f_1(X) f_2^2(X) \ldots f_d^d(X) \ldots f_{r-1}^{r-1}(X)).
\]
If we let \( Y' = X^{\frac{q-1}{\alpha}} x^\alpha \), we get the affine model
\[
Y'^{d} = \alpha f_1(X) f_2^d(X) \cdots f_{d-1}^d(X) \cdots f_{r-1}^{r-1}(X)
\]
which is birationally equivalent to
\[
Y^{d} = \alpha \prod_{i=1}^{d-1} \left( \frac{q-1}{\alpha} \prod_{j=0}^{d-1} f_{jd+i}(X) \right)^i = F_{(d)}(X).
\]

Now \( f_d(X) \not| F_{(d)}(X) \), hence \( F_{(d)}(0) \neq 0 \) and the affine model will be smooth at 0.

Further note that \( F_{(r)}(x) = F(x) \).

Further, if \( x_{q+1} \) is the point at infinity then
\[
F_{(d)}(x_{q+1}) = \begin{cases} 
\alpha & F \in F_{(d, \ldots, d, -1)}^{jd}, 1 \leq j \leq r/d - 1 \\
0 & \text{otherwise}
\end{cases}
\]

This leads to the following lemma

**Lemma 2.1.** Let \( C \) be the smooth projective curve associated to the field \( L = F_{q}(X) \left( \sqrt[\alpha]{f_1(X)} f_2^d(X) \cdots f_{r-1}^{r-1}(X) \right) \) then
\[
\#C(\mathbb{P}^1(F_{q})) = q + 1 \sum_{d|r} \sum_{i=1}^{d-1} \sum_{(i,d)=1} \chi_d^i(F_{(d)}(x)).
\]

**Proof.** If \( x \) is not a root of any of the \( f_i \), then there will be \( r \) points lying over \( x \), if \( F_{(r)}(x) \) is an \( r^\text{th} \) power and no points otherwise. We can write this as
\[
1 + \sum_{i=1}^{r-1} \chi_r(F_{(r)}(x)) = 1 + \sum_{d|r} \sum_{i=1}^{d-1} \chi_d^i(F_{(d)}(x)).
\]

If \( f_i(x) = 0 \) for some \( (i, r) = 1 \), then there will be one point lying over \( x \). Further in this case \( F_{d}(x) = 0 \) for all \( d|r \) so we can write this as
\[
1 + \sum_{d|r} \sum_{i=1}^{d-1} \chi_d^i(F_{(d)}(x)).
\]

If \( f_i(x) = 0 \) for some \( (i, r) = d \neq 1 \), then we have to look at the smooth model \( y^d = F_{(d)}(x) \). Thus there will be \( d \) points lying over \( x \) if \( F_{(d)}(x) \) is a \( d^\text{th} \) power and no points otherwise. We can write this as
\[
1 + \sum_{i=1}^{d} \chi_d^i(F_{(d)}^i(x)) = 1 + \sum_{d'|d} \sum_{i=1}^{d'-1} \chi_d^{i}(F_{(d')}(x)).
\]

Further for any \( d'|r \) such that \( d' \not| d \) we get that the exponent of \( f_i \) in \( F_{(d')} \) is non-zero. Hence \( F_{(d')}(x) = 0 \). Therefore, regardless of the behavior at \( x \), the number or points lying above \( x \) is
\[
1 + \sum_{d|r} \sum_{i=1}^{d-1} \chi_d^i(F_{(d)}(x)).
\]
Summing up over all $x$, we find that

$$
\#C(F_q) = \sum_{x \in \mathbb{F}_q} \left(1 + \sum_{d|r} \sum_{i=1}^{d-1} \chi_d^i(F_d(x)) \right)
$$

$$
= q + 1 + \sum_{d|r} \sum_{i=1}^{d-1} \sum_{x \in \mathbb{F}_q} \chi_d^i(F_d(x)).
$$

\[\square\]

### 3. Set Count

First we need two lemmas from other papers. The first one is Lemma 6.4 from [5] saying

**Lemma 3.1** (Lemma 6.4 from [5]). Let $d_1, \ldots, d_n$ be positive integers. For $0 \leq \ell \leq q$ let $x_1, \ldots, x_\ell$ be distinct elements of $\mathbb{F}_q$. Let $U \in \mathbb{F}_q[x]$ be such that $U(x_i) \neq 0$ for $1 \leq i \leq \ell$. Let $a_{i,1}, \ldots, a_{i,n}, \ldots, a_{\ell,1}, \ldots, a_{\ell,n} \in \mathbb{F}_q^*$. Then the size of

$$
\{(f_1, \ldots, f_n) \in \mathbb{F}_{d_1} \times \cdots \times \mathbb{F}_{d_n} : (f_i, f_j) = (f_i, U) = 1, f_j(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\}
$$

is

$$
P_n^U(\ell) := \frac{L_n-1}{\zeta_q(2)} q^{d_1+\cdots+d_n} \left(\frac{q}{(q-1)^n(q+n)}\right)^\ell \prod_{p \mid |U|} \frac{|P|}{|P| + n} \left(1 + O\left(q^{-\min(d_1,2)}\right)\right)
$$

where

$$
L_n = \prod_{j=1}^n K_j
$$

and

$$
K_j = \prod_{P} \left(1 - \frac{j}{(|P|+1)(|P|+j)}\right).
$$

From now on, if $K_j$ or $L_n$ appears elsewhere in the paper, it will be the same formula that appears in the above Lemma 3.1. The next lemma is Lemma 3.2 from [1]

**Lemma 3.2** (Lemma 3.2 from [1]). Fix $x_1, \ldots, x_\ell \in \mathbb{F}_q$ and let $U$ be a polynomial of degree $u$ with $U(x_i) \neq 0, 1 \leq i \leq \ell$. Define the multiplicative function

$$
c_{ij}^U(F) = \begin{cases} 
\mu^2(F) \prod_{p \mid F} (1 + j|P|^{-1})^{-1} & F(x_i) \neq 0, 1 \leq i \leq \ell, (F,U) = 1 \\
0 & \text{otherwise}
\end{cases}
$$

Then for any $0 < \epsilon < 1$

$$
\sum_{\deg(F) = d} c_{ij}^U(F) = \frac{K_j g^d}{\zeta_q(2)} q^{j+1} \left(\frac{q+j+1}{q+j}\right)^\ell \prod_{p \mid |U|} \left(\frac{|P|+j+1}{|P|+j}\right) \left(1 + O\left(q^{-(d+u+\ell)-d}\right)\right).
$$

We use these two lemmas to prove the following lemma.
Lemma 3.3. Let $d_{1,1}, \ldots, d_{t,1}, \ldots, d_{1,n}, \ldots, d_{r,n-1,1}$ be positive integers. For $0 \leq \ell \leq q$ let $x_1, \ldots, x_\ell$ be distinct elements of $\mathbb{F}_q$. Let $U \in \mathbb{F}_q[x]$ be such that $U(x_i) \neq 0$ for $1 \leq i \leq \ell$. Let $a_{1,1}, \ldots, a_{t,1}, \ldots, a_{1,n}, \ldots, a_{t,n} \in \mathbb{F}_q^\ast$. Then the size of

$$\{(F_1, \ldots, F_n) \in \mathcal{F}_{d_{1,1}, \ldots, d_{t,1,-1}} \times \cdots \times \mathcal{F}_{d_{1,n}, \ldots, d_{t,n-1,1}} : (F_j, U) = 1, F_j(x_i) = a_{i,j},$$

$$1 \leq i \leq \ell, 1 \leq j, k \leq n, j \neq k\}$$

is

$$T_n^U(\ell) := \frac{L_{r_1 + \cdots + r_n - n - 1} q^{d_{1,1} + \cdots + d_{r,n-1,1}}}{\zeta_q(2)^{r_1 + \cdots + r_n - n}} \left(\frac{q}{(q - 1)^{n(q + r_1 + \cdots + r_n - n)}}\right)^\ell \prod_{P \mid U} \frac{|P|}{|P| + r_1 + \cdots + r_n - n} \left(1 + O\left(q^{\frac{-\min d_{i,j}}{2}}\right)\right).$$

Proof. If we write $F_i = \prod_{j=1}^{r_i-1} f_{i,j}^j$ then,

$$T_n^U(\ell) = \sum_{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1} R_n^U \prod_{j \neq 1} f_{i,j}(\ell)$$

$$= \sum_{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1} L_n q^{d_{1,1} + \cdots + d_{1,n}} \left(\frac{q}{(q - 1)^{n(q + n)}}\right)^\ell \prod_{P \mid U, j \neq 1} \frac{|P|}{|P| + n} \left(1 + O\left(q^{\frac{-\min d_{i,j}}{2}}\right)\right) \sum_{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1} \prod_{P \mid U, j \neq 1} \frac{|P|}{|P| + n}$$

Lemma 3.2 shows that

$$\sum_{f_{i,j} \in \mathcal{F}_{d_{i,j}}, j \neq 1} \prod_{P \mid U, j \neq 1} \frac{|P|}{|P| + n} = \sum_{\deg(f_{2,1}) = d_{2,1}} c_n^U(f_{2,1}) \sum_{\deg(f_{2,2}) = d_{2,2}} c_n^U(f_{2,2}) \cdots$$

$$\sum_{\deg(f_{r_n-1,n}) = d_{r_n-1,n}} c_n^U \prod_{j \neq 1} f_{i,j}(f_{r_n-1,n})$$

$$= \frac{L_{r_1 + \cdots + r_n - n - 1} q^{d_{1,1} + \cdots + d_{r,n-1,1}}}{\zeta_q(2)^{r_1 + \cdots + r_n - n}} \left(\frac{q}{(q - 1)^{n(q + r_1 + \cdots + r_n - n)}}\right)^\ell \prod_{P \mid U} \frac{|P|}{|P| + r_1 + \cdots + r_n - n} \left(1 + O\left(q^{\frac{-\min d_{i,j}}{2}}\right)\right).$$

Thus, for an appropriate choice of $\epsilon$, we get the result.\[\square\]

Lemma 3.3 deals with the case where the $F_i$ are all coprime. We want, however the case where they are not necessarily coprime. Suppose now that we have
Then if we define \( F_n = \prod_{k=1}^{r_j-1} f_{j,k} \) and we want to rewrite the \( F_j \) as products of square-free polynomials that are all coprime to one another. For example, if \( n = 2, r_1 = r_2 = 4 \) then we would have
\[
F_1 = f_{1,1} f_{1,2} f_{1,3} \quad F_2 = f_{2,1} f_{2,2} f_{2,3}.
\]
Then if we define
\[
f_{(i,j)} = \gcd(f_{1,i}, f_{2,j}), \quad 1 \leq i, j \leq 3
\]
and
\[
f_{(i,0)} = \frac{f_{1,i}}{f_{(i,1)} f_{(i,2)} f_{(i,3)}} \quad f_{(0,j)} = \frac{f_{2,j}}{f_{(1,j)} f_{(2,j)} f_{(3,j)}}, \quad 1 \leq i, j \leq 3.
\]
Then we can call all the \( f_{(i,j)} \) are square-free and coprime to one another. Moreover
\[
F_1 = f_{(1,0)} f_{(1,1)} f_{(1,2)} f_{(1,3)} f_{(2,0)} f_{(2,1)} f_{(2,2)} f_{(2,3)} f_{(3,0)} f_{(3,1)} f_{(3,2)} f_{(3,3)} = \prod_{i=0}^{3} \prod_{j=0}^{3} f_{(i,j)}
\]
\[
F_2 = f_{(0,1)} f_{(1,1)} f_{(2,1)} f_{(3,1)} f_{(0,2)} f_{(1,2)} f_{(2,2)} f_{(3,2)} f_{(0,3)} f_{(1,3)} f_{(2,3)} f_{(3,3)} = \prod_{i=0}^{3} \prod_{j=0}^{3} f_{(i,j)}.
\]

In general, define
\[
\mathcal{R} = [0, \ldots, r_1 - 1] \times \cdots \times [0, \ldots, r_n - 1] \setminus \{(0, \ldots, 0)\}
\]
and write \( \vec{\alpha} \in \mathcal{R} \) as \( \vec{\alpha} = (\alpha_1, \ldots, \alpha_n) \). Define also \( f_{\vec{\alpha}} \) to be the largest polynomial such that
\[
f_{\vec{\alpha}} \text{ divides } \gcd \left( f_{j,\alpha_j} \right) \quad \text{and} \quad \left( f_{\vec{\alpha}}, \prod_{j=1}^{n} F_j \right) = 1.
\]

With this definition we get if \( \vec{\alpha} \neq \vec{\beta} \) then \( (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \). Indeed, suppose we have \( \alpha_j \neq \beta_j \) and \( \alpha_j, \beta_j \neq 0 \). Then \( f_{\vec{\alpha}} \mid f_{j,\alpha_j} \) and \( f_{\vec{\beta}} \mid f_{j,\beta_j} \) and since \( (f_{j,\alpha_j}, f_{j,\beta_j}) = 1 \), we get that \( (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \). On the other hand suppose we have \( \alpha_j = \beta_j = 0 \). Then \( f_{\vec{\alpha}} \mid f_{j,\alpha_j} \mid F_j \) but \( (f_{\vec{\beta}}, F_j) = 1 \) hence \( (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \).

Now, define \( \vec{\beta} = (0, \ldots, 0, k, 0, \ldots, 0) \), where the \( k \) is in the \( j^{th} \) position. Then \( f_{\vec{\beta}} \) is the largest polynomial that divides \( f_{j,k} \) that is coprime to all the other \( f_{j',k'} \). If \( f_{\vec{\beta}} \neq f_{j,k} \) then
\[
\prod_{\substack{\vec{\alpha} \neq \vec{\beta} \alpha_j = k}} f_{\vec{\alpha}}
\]
is the largest polynomial that divides \( f_{j,k} \) that is not coprime to at least one of the other \( f_{j',k'} \). If \( f_{\vec{\beta}} = f_{j,k} \), then \( f_{\vec{\alpha}} = 1 \) for all \( \vec{\alpha} \neq \vec{\beta} \) such that \( \alpha_j = k \). In either case we get
\[
f_{j,k} = f_{\vec{\beta}} \prod_{\substack{\vec{\alpha} \neq \vec{\beta} \alpha_j = k}} f_{\vec{\alpha}} = \prod_{\alpha_j = k} f_{\vec{\alpha}}.
\]
We then rewrite
\[ F_j = \prod_{k=1}^{r_j-1} f_{j,k}^{k} \quad \text{as} \quad F_j = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}. \]

Define \( \vec{d}(\vec{\alpha}) := (d(\vec{\alpha}))_{\vec{\alpha} \in \mathcal{R}} \) to be an integer vector with non-negative entries indexed by the vectors of \( \mathcal{R} \). Further, define the set
\[ \mathcal{F}_{\vec{d}(\vec{\alpha})} = \{(f_{\vec{\alpha}})_{\vec{\alpha} \in \mathcal{R}} \in \prod_{\vec{\alpha} \in \mathcal{R}} \mathcal{F}_{\vec{d}(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1 \text{ for all } \vec{\alpha} \neq \vec{\beta} \in \mathcal{R} \}. \]

To ease notation, we will write just \( (f_{\vec{\alpha}}) \) instead of \( (f_{\vec{\alpha}})_{\vec{\alpha} \in \mathcal{R}} \) if it is clear what set the indices \( \vec{\alpha} \) run over. Hence,
\begin{align*}
\{ (F_1, \ldots, F_n) &\in \mathcal{F}_{d_1,1} \times \cdots \times \mathcal{F}_{d_{n-1},n} : F_j(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n \} \\
&= \bigcup_{\vec{d}(\vec{\alpha})} \{ (f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n \}
\end{align*}

This leads to Proposition 3.4

**Proposition 3.4.** Let \( \vec{d}(\vec{\alpha}) \) be as above. For \( 0 \leq \ell \leq q \) let \( x_1, \ldots, x_{\ell} \) be distinct elements of \( \mathbb{F}_q \). Let \( a_{1,1}, \ldots, a_{\ell,1}, \ldots, a_{1,n}, \ldots, a_{\ell,n} \in \mathbb{F}_q^* \). Then the size of
\[ \{ (f_{\vec{\alpha}}) \in \mathcal{F}_{\vec{d}(\vec{\alpha})} : F_j(x_i) := \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j}(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n \} \]
is
\[ S_n(\ell) := \frac{L_{r_1 \cdots r_n - 2 \sum_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}}}{\zeta_q(2)^{r_1 \cdots r_n - 1}} \left( \frac{q}{(q-1)^{n(q+r_1 \cdots r_n - 1)}} \right)^{\ell} \left( 1 + O \left( q^{-\min_{\vec{\alpha} \in \mathcal{R}} d_{\vec{\alpha}}} \right) \right). \]

**Proof.** We will split the \( F_j := \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j} \) into their coprime parts. In order to do this we will need some new notation. Define
\[ S_j := \{(0, \ldots, 0, \alpha_j, 0, \ldots, 0) : 1 \leq \alpha_j \leq r_j - 1 \} \subset \mathcal{R} \]
where the non-zero entry is in the \( j^{th} \) coordinate. Define,
\[ S = \bigcup_{j=1}^{n} S_j. \]

Then the factor of \( F_j = \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{\alpha_j} \) that is coprime to all \( F_i \) such that \( i \neq j \) will be \( \prod_{\vec{\alpha} \in S_j} f_{\vec{\alpha}}^{\alpha_j} \). Further for any subset \( \mathcal{R}' \subset \mathcal{R} \), define
\[ \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{R}'} = \{(f_{\vec{\alpha}}) \in \prod_{\vec{\alpha} \in \mathcal{R}} \mathcal{F}_{\vec{d}(\vec{\alpha})} : (f_{\vec{\alpha}}, f_{\vec{\beta}}) = 1, \text{ for } \alpha \neq \beta \in \mathcal{R}' \}. \]

We will denote this as just \( \mathcal{F}_{\vec{d}(\vec{\alpha})}^{\mathcal{R}'} \) with the understanding that in this context \( \vec{d}(\vec{\alpha}) \) is indexed by \( \mathcal{R}' \) instead of \( \mathcal{R} \). Then,
\[ S_n(\ell) = |\{(f_{\vec{\alpha}}) \in \mathcal{F}_{d(\vec{\alpha})} : \prod_{\vec{\alpha} \in \mathcal{R}} f_{\vec{\alpha}}^{a_{i,j}}(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n\}| \]

\[ = \sum_{(f_{\vec{\alpha}}) \in \mathcal{F}_{d(\vec{\alpha})}} \mathcal{P}_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} \prod_{\vec{\alpha} \in \mathcal{S}} f_{\vec{\alpha}}^{b_{i,j}}(x_i) = b_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell | \]

\[ = \sum_{(f_{\vec{\alpha}}) \in \mathcal{F}_{d(\vec{\alpha})}} T_n^{\Pi_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} f_{\vec{\alpha}}}(\ell) \]

where \( T_n^{\Pi_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} f_{\vec{\alpha}}}(\ell) \) is as in Lemma 3.3 and

\[ b_{i,j} = a_{i,j} \prod_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} f_{\vec{\alpha}}(x_i)^{-a_{i,j}}. \]

Thus, similarly to the previous lemma,

\[ S_n(\ell) = \sum_{(f_{\vec{\alpha}}) \in \mathcal{F}_{d(\vec{\alpha})}} \mathcal{P}_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} \prod_{\vec{\alpha} \in \mathcal{S}} f_{\vec{\alpha}}^{a_{i,j}}(x_i) = a_{i,j}, 1 \leq i \leq \ell, 1 \leq j \leq n | \]

\[ \times \prod_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} \mathcal{P}_{f_{\vec{\alpha}}}(x_i) = 0 \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{S}} d_{\vec{\alpha}}}{2}}\right)\right) \]

\[ = M \sum_{(f_{\vec{\alpha}}) \in \mathcal{F}_{d(\vec{\alpha})}} \prod_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} \mathcal{P}_{f_{\vec{\alpha}}}(x_i) = 0 \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{S}} d_{\vec{\alpha}}}{2}}\right)\right) \]

By the same reasoning as in the proof of Lemma 3.3 we get

\[ M = \sum_{(f_{\vec{\alpha}}) \in \mathcal{F}_{d(\vec{\alpha})}} \prod_{\vec{\alpha} \in \mathcal{R} \setminus \mathcal{S}} \mathcal{P}_{f_{\vec{\alpha}}}(x_i) = 0 \left(1 + O\left(q^{-\frac{\min_{\vec{\alpha} \in \mathcal{S}} d_{\vec{\alpha}}}{2}}\right)\right) \]

Therefore, if we choose an appropriate \( \epsilon \), we get the result.

\[ \square \]

4. The case \( r = p^n \)

In order to apply the counting formula of Proposition 3.4 we want to write the \( n \) functions defined by

\[ F_{(p)}(X) = \prod_{i=1}^{p^n-1} f_i^{a_{i,j}} \mod p^j \quad 1 \leq j \leq n \]

in terms of coprime functions.

To apply the results of Section 3 we define, in this context

\[ \mathcal{R} = [0, \ldots, p-1]^n \setminus \{(0, \ldots, 0)\}. \]
If \( \alpha \in \mathcal{R} \) we will denote it \( \check{\alpha} = (\alpha_1, \ldots, \alpha_n) \). Rewrite
\[
F := \prod_{\alpha \in \mathcal{R}} f_{\alpha_{1} + \ldots + \alpha_{n}}^{\alpha_{1} + \ldots + \alpha_{n}}.
\]
That is we make the identification \( f_{\alpha_{1} + \ldots + \alpha_{n}} \rightarrow f_{(\alpha_{1}, \ldots, \alpha_{n})} \)
Recall the notation in Section 2 where we denoted, for \( d \mid r \),
\[
F_{(d)}(X) := \prod_{i=1}^{r-1} \left( \prod_{j=0}^{d-1} f_{j}^{i+1}(X) \right)^{i} = \prod_{i=1}^{r-1} f_{i}(X)^{i \mod d}.
\]
and we have
\[
F_{(p^{j})}(X) = \prod_{\alpha \in \mathcal{R}} f_{\alpha}(X)^{\alpha_{1} + \ldots + \alpha_{n}}
\]
for \( j = 1, \ldots, n \). Further, if necessary, we denote \( F_{(1)}(X) = 1 \).
Define \( d_{1} := d(1, 0, \ldots, 0) \). Also use the notation \( f_{1} = f_{(1,0,\ldots,0)} \). We will redefine the sets in Section 1 using this new notation.
\[
\mathcal{R}' = \mathcal{R} \setminus \{(1,0,\ldots,0)\}
\]
\[
\hat{\mathcal{F}}_{d(\check{\alpha})} = \{(f_{1}, f_{\check{\alpha}}) \in \hat{\mathcal{F}}_{d_{1}} \times \prod_{\check{\alpha} \in \mathcal{R}'} \hat{\mathcal{F}}_{d(\check{\alpha})} : (f_{\check{\alpha}}, f_{\check{\beta}}) = 1 \text{ for all } \check{\alpha} \neq \check{\beta}\}
\]
Let
\[
\delta(\check{\alpha}, \check{\beta}) = \begin{cases} 1 & \check{\alpha} = \check{\beta} \\ 0 & \check{\alpha} \neq \check{\beta} \end{cases}.
\]
Then define
\[
\mathcal{F}_{d(\check{\alpha})}^{\check{\beta}} = \{(f_{\check{\beta}}, f_{\check{\alpha}}) \in \mathcal{F}_{d(\check{\beta})} \times \prod_{\check{\alpha} \neq \check{\beta}} \mathcal{F}_{d(\check{\alpha})} : (f_{\check{\alpha}}, f_{\check{\beta}}) = 1, \check{\alpha} \neq \check{\beta} \in \mathcal{R}\}.
\]
Likewise define \( \hat{\mathcal{F}}_{d(\check{\alpha})}^{\check{\beta}} \) to be elements of \( \mathcal{F}_{d(\check{\alpha})}^{\check{\beta}} \) where \( f_{1} \) is not necessarily monic. Further, define
\[
\mathcal{F}_{d(\check{\alpha})} = \mathcal{F}_{d(\check{\alpha})}^{\check{\beta}} \cup \bigcup_{\check{\beta} \in \mathcal{R}} \mathcal{F}_{d(\check{\beta})}^{\check{\alpha}}
\]
\[
\hat{\mathcal{F}}_{d(\check{\alpha})} = \hat{\mathcal{F}}_{d(\check{\alpha})}^{\check{\beta}} \cup \bigcup_{\check{\beta} \in \mathcal{R}} \hat{\mathcal{F}}_{d(\check{\beta})}^{\check{\alpha}}.
\]
Now, if \( x_{q+1} \) is the point at infinity, then,
\[
F_{(p^{j})}(x_{q+1}) = \begin{cases} \text{leading coefficient of } f_{1} & (f_{\check{\alpha}}) \in \hat{\mathcal{F}}_{d(\check{\alpha})}^{\check{\beta}} \\ 0 & \text{otherwise} \end{cases}
\]
where \( \check{\beta} = (\beta_{1}, \ldots, \beta_{n}) \in \mathcal{R} \) is any tuple such that \( \beta_{i} = 0 \) for all \( i \neq j \).

**Proposition 4.1.** Let \( a_{i,j} \in \mathbb{F}_{q}^{*}, 1 \leq j \leq n, 1 \leq i \leq \ell \) such that \( a_{i,j} = a_{i,j-1}(b_{i,j})^{p^{j-1}} \)
for some \( b_{i,j} \in \mathbb{F}_{q}^{*} \). We let \( a_{i,0} = 1 \) so that \( a_{i,1} = b_{i,1} \). Then
\[
|\{(f_{\check{\alpha}}) \in \hat{\mathcal{F}}_{d(\check{\alpha})} : F_{(p^{j})}(a_{i}) = a_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell\}| = \frac{L_{p^{n-2}q^{\sum_{\check{\alpha} \in \mathcal{R}} d(\check{\alpha})}}{\zeta_{q}(2)p^{n-1}} \frac{p^{n(n-1)}q}{(q-1)^{n}(q+p^{n}-1)} \left(1 + O \left(q^{-\frac{\min_{\check{\alpha} \in \mathcal{R}} d(\check{\alpha})}{2}} \right)\right). \]
Proof. For \( j = 1, \ldots, n \) define \( F_j = 1 - \prod_{x \in \mathbb{R}} f^{p_j}_x \). Then we can write \( F_{(p')} = F_{(p'-1)}F_{p-1}^{p-1} \), where, again, we have \( F_1 = 1 \). Then \( F_{(p')}(x_i) = \alpha_{i,j} \) for all \( i,j \) is equivalent to \( F_j(x_i) = \epsilon_{i,j} \) for all \( i,j \) for some \( \epsilon_{i,j} \in \mu_{p-1} \). Hence,

\[
\left| \{(f_{\alpha}) \in \mathcal{F}_{d(\alpha)} : F_{(p')}(x_i) = \alpha_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell \} \right| = \left| \{(f_{\alpha}) \in \mathcal{F}_{d(\alpha)} : F_j(x_i) = \epsilon_{i,j}b_{i,j}, \epsilon_{i,j} \in \mu_{p-1}, 1 \leq j \leq n, 1 \leq i \leq \ell \} \right|
\]

\[
= \frac{Lp^{n-2q \sum_{\alpha \in \mathbb{R}} d(\alpha)}}{\zeta_q(2)^{p-1}} \left( \frac{p^{\frac{n(n-1)}{2}q}}{(q-1)^n(q + p^n - 1)} \right)^\ell \left( 1 + O \left( q^{-\min_{\alpha \in \mathbb{R}} d(\alpha)} \right) \right) .
\]

Where the second equality comes from Proposition 3.4 and that there are \( (p^{n(n-1)/2})^\ell \) different choices for the \( \epsilon_{i,j} \).

Now let us look at what happens if some of the \( a_{i,j} = 0 \). Note that if \( a_{i,j} = 0 \) then \( a_{i,j+1} = 0 = F_{p'}|F_{p'+1} \). Thus we have

Corollary 4.2. Let \( a_{i,j} \in \mathbb{F}_q \), \( 1 \leq j \leq n, 1 \leq i \leq \ell \) such that

\[
a_{i,1}, \ldots, a_{i,k} \neq 0 \quad \text{and} \quad a_{i,k+1}, \ldots, a_{i,n} = 0 \quad \text{for} \quad \sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k
\]

for \( k = 0, \ldots, n-1 \) and \( a_{i,j} \neq 0 \) for all \( j \) for \( \sum_{i=0}^{n-1} m_i + 1 \leq i \leq \ell \). Further, if \( a_{i,j} \neq 0 \) then \( a_{i,j} = a_{i,j-1}(b_{i,j})^{p_{j-1}} \) for some \( b_{i,j} \in \mathbb{F}_q \). Then

\[
\left| \{(f_{\alpha}) \in \mathcal{F}_{d(\alpha)} : F_{(p')}(x_i) = \alpha_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell \} \right|
\]

\[
= \frac{Lp^{n-2q \sum_{\alpha \in \mathbb{R}} d(\alpha)}}{\zeta_q(2)^{p-1}} \prod_{k=0}^{n-1} \left( \frac{(p-1)p^{n-k-1}(q-1)^n}{p^{\frac{n(n-k)}{2}}q} \right)^{m_k} \times \left( \frac{p^{\frac{n(n-1)}{2}q}}{(q-1)^n(q + p^n - 1)} \right)^\ell \left( 1 + O \left( q^{-\min_{\alpha \in \mathbb{R}} d(\alpha)} \right) \right) .
\]

Proof. Consider \( i \) such that \( \sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k \). Then \( f_{\alpha}(x_i) = 0 \) for some \( \alpha \) such that \( \alpha_{k+1} \neq 0 \) but \( \alpha_j = 0 \) for all \( j < k+1 \). There are \( (p-1)p^{n-j-1} \) different such \( \alpha \). Fix a partition \( m_k := \sum_{\alpha} m_k, \alpha \) where the sum is over all such \( \alpha \) defined above and \( m_k, \alpha \) is the number of times \( f_{\alpha}(x_i) = 0 \).

Define \( f_{\bar{\alpha}} \) as \( f_{\alpha} \) divided by its roots and \( F_{(p')} \) as the corresponding product of the \( f_{\bar{\alpha}} \). Now \( F_{(p')}(x_i) \) is determined by \( F_{(p')}(x_i) \) for \( j \leq k \). \( F_{(p')}(x_i) \) will be fixed, up to a \( p^{j-1} \)th root of unity, for \( j+1 \leq k \leq n \). Thus we get a factor of

\[
\left( \prod_{j=k+1}^{n} \frac{q-1}{p^{j-1}} \right)^{m_k} = \left( \frac{(q-1)^{n-k}}{p^{\frac{q-1}{2}n(n-k)}} \right)^{m_k} .
\]
Summing up over all the partitions of $m_k$ we get
\[
\left| \{(f_{\vec{a}}) \in \mathcal{F}_{d(\vec{a})} : \ell_{F_{p^j}}(x_i) = a_{i,j}, 0 \leq j \leq n, 1 \leq i \leq \ell \} \right|
= \prod_{k=0}^{n-1} \left( (p-1)p^{n-k-1} \right)^{m_k} L_{p^n-2q^{\sum_{\vec{a} \in \mathbb{R}} d(\vec{a})}} \prod_{k=0}^{n-1} \left( \frac{(q-1)^{n-1} - \sum_{k=0}^{n-1} m_k}{p^{n-k-1}} \right) \left( \frac{p^{\frac{n(n-1)}{2}}}{(q-1)^n (q + p^n - 1)} \right) \ell \left( 1 + O \left( q^{\frac{\min_{\vec{a} \in \mathbb{R}^d} d(\vec{a})}{2}} \right) \right)
\]
\[
= L_{p^n-2q^{\sum_{\vec{a} \in \mathbb{R}} d(\vec{a})}} \prod_{k=0}^{n-1} \left( \frac{(p-1)p^{n-1} (q-1)^{n-k}}{q} \right)^{m_k} \left( \frac{q}{p^n (q + p^n - 1)} \right) \ell \left( 1 + O \left( q^{\frac{\min_{\vec{a} \in \mathbb{R}^d} d(\vec{a})}{2}} \right) \right).
\]

Corollary 4.3. Let $\epsilon_{i,j} \in \mu_{p^j} \cup \{0\}$, $1 \leq j \leq n, 1 \leq i \leq \ell$ such that
\[
\epsilon_{i,1}, \ldots, \epsilon_{i,k} \neq 0 \text{ and } \epsilon_{i,k+1}, \ldots, \epsilon_{i,n} = 0 \text{ for } \sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k
\]
for $k = 0, \ldots, n-1$ and $\epsilon_{i,j} \neq 0$ for all $j$ for $\sum_{i=0}^{n-1} m_i + 1 \leq i \leq \ell$. Further, if $\epsilon_{i,j} \neq 0$ then $\epsilon_{i,j-1} = (\epsilon_{i,j})^p$. Then
\[
\left| \{(f_{\vec{a}}) \in \mathcal{F}_{d(\vec{a})} : \ell_{F_{p^j}}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell \} \right|
= \left( q - 1 \right)^{\sum_{k=0}^{n-1} m_k} L_{p^n-2q^{\sum_{\vec{a} \in \mathbb{R}} d(\vec{a})}} \prod_{k=0}^{n-1} \left( \frac{(p-1)p^{n-k-1} (q-1)^{n-k}}{q} \right)^{m_k} \left( \frac{q}{p^n (q + p^n - 1)} \right) \ell \left( 1 + O \left( q^{\frac{\min_{\vec{a} \in \mathbb{R}^d} d(\vec{a})}{2}} \right) \right).
\]

Proof. For $k = 1, \ldots, n$, $F_{p^k}(x_i) = 0$ for $1 \leq i \leq \sum_{j=0}^{k-1} m_j$, so for $\sum_{j=0}^{k-1} m_j + 1 \leq i \leq \ell$, $F_{p^k}(x_i)$ has $\frac{q-1}{p^k}$ choices. Hence
\[
\left| \{(f_{\vec{a}}) \in \mathcal{F}_{d(\vec{a})} : \ell_{F_{p^j}}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq \ell \} \right|
= \left( q - 1 \right)^{\sum_{k=0}^{n-1} m_k} L_{p^n-2q^{\sum_{\vec{a} \in \mathbb{R}} d(\vec{a})}} \prod_{k=0}^{n-1} \left( \frac{(p-1)p^{n-k-1} (q-1)^{n-k}}{q} \right)^{m_k} \left( \frac{q}{p^n (q + p^n - 1)} \right) \ell \left( 1 + O \left( q^{\frac{\min_{\vec{a} \in \mathbb{R}^d} d(\vec{a})}{2}} \right) \right).
\]

Up until now, we have been looking only at points in $F_q$. What we need to look at however, is points in $\mathbb{P}^1(F_q)$. This is taken care of my the following corollary

Corollary 4.4. Let $\epsilon_{i,j} \in \mu_{p^j} \cup \{0\}$, $1 \leq j \leq n, 1 \leq i \leq q + 1$ such that
\[
\epsilon_{i,1}, \ldots, \epsilon_{i,k} \neq 0 \text{ and } \epsilon_{i,k+1}, \ldots, \epsilon_{i,n} = 0 \text{ for } \sum_{i=0}^{k-1} m_i + 1 \leq i \leq \sum_{i=0}^{k-1} m_i + m_k
\]
for \( k = 0, \ldots, n - 1 \) and \( \epsilon_{i,j} \neq 0 \) for all \( j \) for \( \sum_{i=0}^{n-1} m_i + 1 \leq i \leq q + 1 \). Further, if \( \epsilon_{i,j} \neq 0 \) then \( \epsilon_{i,j-1} = (\epsilon_{i,j})^p \). Then

\[
|\{(f_{\alpha}) \in \hat{\mathcal{F}}_{[d(\alpha)]} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q + 1\}| = \prod_{k=0}^{n-1} \left( \frac{(p-1)p^{2n-2k-1}}{q} \right)^{\frac{m_k}{q^{p^k(q+p-1)}}} \left( 1 + O\left( q^{-\min_{d \in \mathbb{Z}}} d(\alpha) \right) \right).
\]

**Proof.**

**Case 1:** \( \epsilon_{q+1,k} \neq 0 \) for all \( 1 \leq k \leq n \).

In this case we get that \( (f_{\alpha}) \in \hat{\mathcal{F}}_{[d(\alpha)]} \). Further the leading coefficient of \( f_1 \) under \( \chi_{p^n} \) must be \( \epsilon_{q+1,n} \). Thus

\[
\frac{q-1}{p^n} |\{(f_{\alpha}) \in \mathcal{F}_{[d(\alpha)]} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q\}| = \frac{q-1}{p^n} L_{p^n-2q\sum_{a \in \mathbb{Z}} d(\alpha)-1} \prod_{j=0}^{n-1} \left( \frac{(p-1)p^{2n-2j-1}}{q} \right)^{m_j} \left( 1 + O\left( q^{-\min_{d \in \mathbb{Z}}} d(\alpha) \right) \right).
\]

**Case 2:** \( \epsilon_{q+1,1}, \ldots, \epsilon_{q+1,k} \neq 0 \) and \( \epsilon_{q+1,k+1}, \ldots, \epsilon_{q+1,n} = 0 \) for some \( k \).

In this case we get \( (f_{\alpha}) \in \hat{\mathcal{F}}_{[d(\alpha)]} \) where \( \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z} \) such that \( \beta_j = 0 \) for all \( j \leq k \) and \( \beta_{k+1} \neq 0 \). There are \( (p-1)p^{n-k-1} \) such \( \beta \). Further \( m_k \) will go to \( m_k - 1 \) and the leading coefficient of \( f_1 \) under \( \chi_{p^n} \) must be \( \epsilon_{q+1}^k \). Then

\[
\frac{q-1}{p^n} \sum_{\beta} |\{(f_{\alpha}) \in \hat{\mathcal{F}}_{[d(\alpha)]} : \chi_{p^j}(F_{p^j}(x_i)) = \epsilon_{i,j}, 1 \leq j \leq n, 1 \leq i \leq q\}| = \frac{q-1}{p^n} L_{p^n-2q\sum_{a \in \mathbb{Z}} d(\alpha)-1} \prod_{j=0}^{n-1} \left( \frac{(p-1)p^{2n-2j-1}}{q} \right)^{m_j} \times \left( \frac{(p-1)p^{2n-2j-1}}{q} \right)^{-1} \left( 1 + O\left( q^{-\min_{d \in \mathbb{Z}}} d(\alpha) \right) \right).
\]

Thus, independent of the behavior at \( x_{q+1} \), we get out result.

\[\square\]

Which leads us to restate and prove Theorem 1.2 for \( r = p^n \).

**Theorem 4.5.** Let \( M_j \in \mathbb{Z}[\zeta_{p^n}] \) for \( j = 1, \ldots, n \). Then

\[
|\{(f_{\alpha}) \in \hat{\mathcal{F}}_{[d(\alpha)]} : S_{p^j}(F_{p^j}) = M_j, 1 \leq j \leq n\}| = \prod_{k=0}^{n-1} \left( \frac{(p-1)p^{2n-2k-1}}{q} \right)^{\frac{m_k}{q^{p^k(q+p-1)}}} \left( 1 + O\left( q^{-\min_{d \in \mathbb{Z}}} d(\alpha) \right) \right).
\]
where the $X_{i,j}$ are random variables that take values in $\mu_p \cup \{0\}$ such that $X_{i,j}$ and $X_{h,k}$ are i.i.d unless $i = h$ and

\[
\begin{align*}
\text{Prob}(X_{i,j} = 0) &= \frac{p^n - p^{n-j}}{q + p^n - 1} \\
\text{Prob}(X_{i,j+1} = 0, X_{i,j} = 0) &= 1 \\
\text{Prob}(X_{i,j} = \epsilon_{i,j}, X_{i,j+1} = \epsilon_{i,j+1}, \ldots, X_{i,n} = 0) &= \begin{cases} (p-1)p^{n-2j-1} & \text{if } \epsilon_{i,k-1} = (\epsilon_{i,k})^p, k = 2, \ldots, j \\ 0 & \text{otherwise} \end{cases} \\
\text{Prob}(X_{i,n} = \epsilon_{i,n}) &= \begin{cases} \frac{q}{p^n(q + p^n)} & \text{if } \epsilon_{i,k-1} = (\epsilon_{i,k})^p, k = 2, \ldots, n \\ 0 & \text{otherwise} \end{cases}
\end{align*}
\]

Proof.

\[
\begin{align*}
&\left|\{(f_{i,j}) \in \hat{F}_{[\bar{d}(\bar{a})]}: S_p(F_{p,i}) = M_j, 1 \leq j \leq n}\right| \\
&= \sum_{(E_{i,j}, \ldots, E_{i+n-1}) \in \mu_p \cup \{0\}} \prod_{k=0}^{n-1} \frac{(p-1)p^{2n-2k-1}}{q} m_k \left(\frac{q}{p^n(q + p^n - 1)}\right)^{q + 1 - \sum_{k=0}^{n-1} m_k} \left(1 + O\left(q^{-\min_{d \in \mathbb{Z}} d(\bar{a})}\right)\right)
\end{align*}
\]

where the $X_i$ have the desired properties. \(\square\)

5. General $r$

Suppose now that $r = r_1 r_2$ with $(r_1, r_2) = 1$. Then, relabeling the $f_i$ as $f_{i,j}$ we can write

\[
F(X) = \prod_{i=0, \ldots, r_1-1 \atop j=0, \ldots, r_2-1 \atop (i,j) \neq (0,0)} f_{i,j}(X)^{s_2 r_2 i + s_1 r_1 j} \mod r
\]

where $s_1 \equiv r_1^{-1} \mod r_2$ and $s_2 \equiv r_2^{-1} \mod r_1$. With this notation we now get

\[
\begin{align*}
F_{r_1} &= \prod_{i=0, \ldots, r_1-1 \atop j=0, \ldots, r_2-1 \atop (i,j) \neq (0,0)} f_{i,j}^{i} \mod r_1 \\
F_{r_2} &= \prod_{i=0, \ldots, r_1-1 \atop j=0, \ldots, r_2-1 \atop (i,j) \neq (0,0)} f_{i,j}^{j} \mod r_2.
\end{align*}
\]
Therefore

\[ F_{r_1}(X)^{s_2 r_2} F_{r_2}(X)^{s_1 r_1} = F(X) \left( \prod_{i,j} f_{i,j}(X)^{n_{i,j}} \right)^r \]

for some, potentially 0, exponents \( n_{i,j} \). Further we see that \( F(x) = 0 \) if and only if \( F_{r_1} F_{r_2}(x) = 0 \) as all the factors that appear in \( F \) appear in \( F_{r_1} F_{r_2} \). Therefore the values of \( F_d(x) \) for all \( d \mid r \) are determined by the values of \( F_{p^n}(x) \) where \( p \) is a prime such that \( p^n \mid r \). That is,

\[
\left| \{ F \in \mathcal{F}(d_1, \ldots, d_\ell) : \chi_d(F_d(x_i)) = \epsilon_{d,i}, \text{ for all } d \mid r, 1 \leq i \leq \ell \} \right|
\]

\[
= \left| \{ F \in \mathcal{F}(d_1, \ldots, d_\ell) : \chi_d(F_d(x_i)) = \epsilon_{d,i}, d = p^n | r, p \text{ a prime}, 1 \leq i \leq \ell \} \right|
\]

Now, suppose \( r = p_1^{t_1} \cdots p_n^{t_n} \). Define

\[
\mathcal{R}' = [0, \ldots, p_1^{t_1} - 1] \times \cdots \times [0, \ldots, p_n^{t_n} - 1] \setminus \{(0, \ldots, 0)\}
\]

Let

\[
\phi : \mathcal{R}' \to [1, \ldots, r - 1]
\]

be the isomorphism that comes from the Chinese Remainder Theorem. Then if \( F = \prod_{i=1}^{r-1} f_i \), we can relabel the \( f_i \) to get

\[
F = \prod_{\beta \in \mathcal{R}'} f_{\phi(\beta)}^r.
\]

Notice that \( \phi(\beta) \equiv k \mod p_j^{t_j} \) if and only if \( \beta_j = k \). Therefore

\[
F_{(p_j^{t_j})}(X) = \prod_{\beta \in \mathcal{R}'} f_{\phi(\beta)}^{p_j^{t_j}} \mod p_j^{t_j} = \prod_{k=0}^{p_j^{t_j}-1} \prod_{\beta \in \mathcal{R}'} f_{\beta_k}^k = \prod_{\beta \in \mathcal{R}'} f_{\beta}^{p_j^{t_j}}.
\]

However, we need all powers of the primes. Therefore we define

\[
\mathcal{R} = [0, \ldots, p_1 - 1]^{t_1} \times \cdots \times [0, \ldots, p_n - 1]^{t_n} \setminus \{(0, \ldots, 0)\}.
\]

Let \( T_j = \sum_{i=1}^{t_j} t_i \). As usual, for \( \alpha \in \mathcal{R} \) we write it as \( \alpha = (\alpha_1, \ldots, \alpha_{T_n}) \). Then there is an isomorphism \( \psi : \mathcal{R} \to \mathcal{R}' \) such that

\[
\psi(\alpha) = (\alpha_1 + p_1 \alpha_2 + \cdots + p_1^{t_1-1} \alpha_{T_1}, \ldots, \alpha_{T_{n-1}} + p_n \alpha_{T_{n-1}+1} + \cdots + p_n^{t_n-1} \alpha_{T_n})
\]

Therefore, if we relabel the \( f_{\beta} \) we get

\[
F_{(p_j^{t_j})}(X) = \prod_{\alpha \in \mathcal{R}} f_{\alpha}^{\alpha_{T_{j-1}}+1+p_1 \alpha_{T_{j-1}+2}+\cdots+p_1^{t_j-1} \alpha_{T_j}(X)}
\]

Moreover, for any \( 1 \leq k_j \leq t_j \)

\[
F_{(p_j^{k_j})}(X) = \prod_{\alpha \in \mathcal{R}} f_{\alpha}^{\alpha_{T_{j-1}}+1+p_1 \alpha_{T_{j-1}+2}+\cdots+p_1^{k_j-1} \alpha_{T_j+k_j}}(X)
\]

Then we get

\[
\left| \{ F \in \mathcal{F}(d_1, \ldots, d_{r-1}) : F_{(p_j^{t_j})}(x_i) = \alpha_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell \} \right|
\]

\[
= \left| \{ (f_{\alpha}) \in \mathcal{F}_{d(\alpha)} : F_{(p_j^{t_j})}(x_i) = \alpha_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell \} \right|
\]

where \( d(\alpha) = d_{\phi \psi(\alpha)} \).
Proposition 5.1. Let \( a_{i,j,k_i} \in \mathbb{F}_q^* \) such that \( a_{i,j,k_i} = a_{i,j,k_i-1}(b_{i,j,k_i})^{p^{k_i-1}} \) for some \( b_{i,j,k_i} \in \mathbb{F}_q^* \). Further we let that \( a_{i,j,0} = 1 \) so that \( a_{i,j,1} = b_{i,j,1} \).

\[
|\{(f_\alpha) \in \mathcal{F}_{\mathcal{C}(\alpha)} : F_{(p_j)}(x_i) = a_{i,j,k_i}, 1 \leq j \leq n, 1 \leq k_i \leq t_j, 1 \leq i \leq \ell\}| = \frac{L_{r-2q} \sum_{\sigma \in S(d(\alpha))} \phi_{\sigma}^{(j,k)}(x_i) = \alpha_{i,j,k_i}}{\zeta_q(2)r^{-1}} \left( \frac{q \prod_{j=1}^{n} p_j (t_j - 1)}{(q - 1)t_n(q + r - 1)} \right)^{\ell} \left( 1 + O\left( q^{-\min_{\sigma \in S(d(\alpha))}} \right) \right)
\]

Proof. As we saw in the proof of Proposition 4.1, it will be enough to consider what values the polynomials

\[
F_{(j,k_j)} = \prod_{\alpha \in \mathcal{R}} f_{\alpha}^{m_{(j,k_j)} + k_j}
\]

up to some root of unity. That is,

\[
|\{(f_\alpha) \in \mathcal{F}_{\mathcal{C}(\alpha)} : F_{(p_j)}(x_i) = a_{i,j,k_i}, 1 \leq j \leq n, 1 \leq k_i \leq t_j, 1 \leq i \leq \ell\}|
\]

= \[|\{(f_\alpha) \in \mathcal{F}_{\mathcal{C}(\alpha)} : F_{(j,k_j)}(x_i) = \epsilon_{i,j,k_i} b_{i,j,k_i}, \epsilon_{i,j,k_i} \in \mu_{p_j^{k_j-1}}, 1 \leq j \leq n, 1 \leq k_i \leq t_j, 1 \leq i \leq \ell\}|
\]

We can define an isomorphism

\[
\phi : \{(j,k_j) : 1 \leq j \leq n, 1 \leq k_j \leq T_j\} \to \{1, \ldots, T_n\}
\]

by

\[
\phi(j,k_j) = T_j - 1 + k_j.
\]

Let \( \epsilon_{i,j} = \epsilon_{i,\phi^{-1}(j)}, \beta_{i,j} = \beta_{i,\phi^{-1}(j)} \) and \( F_j = F_{\phi^{-1}(j)} \), then

\[
F_j = \prod_{\alpha \in \mathcal{R}} f_{\alpha}^{\mu_{(j,k_j)}}.
\]

If we denote \( \mu_m = \mu_{(j,k_j)} \) where \( \phi(j,k_j) = m \) then,

\[
|\{(f_\alpha) \in \mathcal{F}_{\mathcal{C}(\alpha)} : F_{(j,k_j)}(x_i) = \epsilon_{i,j,k_i} b_{i,j,k_i}, \epsilon_{i,j,k_i} \in \mu_{p_j^{k_j-1}}, 1 \leq j \leq n, 1 \leq k_i \leq t_j, 1 \leq i \leq \ell\}|
\]

= \[|\{(f_\alpha) \in \mathcal{F}_{\mathcal{C}(\alpha)} : F_j(x_i) = \epsilon_{i,j,k_i} b_{i,j,k_i}, \epsilon_{i,j} \in \mu_j, 1 \leq j \leq T_n, 1 \leq i \leq \ell\}|
\]

\[
= \frac{L_{r-2q} \sum_{\sigma \in S(d(\alpha))} \phi_{\sigma}^{(j,k)}(x_i) = \alpha_{i,j,k_i}}{\zeta_q(2)r^{-1}} \left( \frac{q \prod_{j=1}^{n} p_j (t_j - 1)}{(q - 1)t_n(q + r - 1)} \right)^{\ell} \left( 1 + O\left( q^{-\min_{\sigma \in S(d(\alpha))}} \right) \right)
\]

where the last equality comes from Proposition 3.4.

\[\square\]

Define

\[
\mathcal{S} = [0, \ldots, t_1] \times \cdots \times [0, \ldots, t_n] \setminus (t_1, \ldots, t_n).
\]

For any \( S \in \mathcal{S} \) we will write \( S = (s_1, \ldots, s_n) \). We will use \( \mathcal{S} \) to count the number of \( 1 \leq i \leq \ell \) such that \( F_{(p_j^{s_j})}(x_i) = 0 \). That is, for every \( S = (s_1, \ldots, s_n) \in \mathcal{S} \) we say that for some \( i \) \( F_{(p_j^{s_j})}(x_i) = 0 \) (and hence \( F_{(p_j^{s_j})}(x_i) = 0 \) for all \( k_j > s_j \)). If \( s_j = t_j \) this will correspond to the case that \( F_{(p_j^{s_j})}(x_i) \neq 0 \) for all \( 1 \leq i \leq \ell \) for all \( k_j \), hence why we exclude the element \( (t_1, \ldots, t_n) \) from \( \mathcal{S} \) as this corresponds to the case that there are no zeros, which we treated in Proposition 5.1. With this motivation we will define \( J_S = \{ j : s_j \neq t_j \} \).
Corollary 5.2. Let $a_{i,j,k_j} \in F_q$ such that for $m_S$ of the $i$ we have

$$a_{i,j,1}, \ldots, a_{i,j,s_j} \neq 0 \text{ and } a_{i,j,s_j+1}, \ldots, a_{i,j,t_j} = 0, \quad 1 \leq j \leq n$$

for all $S \in S$. Further if $a_{i,j,k_j} \neq 0$ then $a_{i,j,k_j} = a_{i,j,k_j-1} (b_{i,j,k_j})^{p^{k_j-1}}$ for some $b_{i,j,k_j} \in F_q$. Again, we set $a_{i,j,0} = 1$ so that $a_{i,j,1} = b_{i,j,1}$. Then,

$$|\{(f_{\vec{a}}) \in \mathcal{F}_{\vec{d}(\vec{a})} : F_{(p_j)}^{(k_j)}(x_i) = a_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq \ell\}|$$

$$= \frac{L_{\tau-2g} \sum_{\vec{d} \in \mathbb{R}} d(\vec{a}) \prod_{S \in S} \left( \prod_{j \in J_S} (p_j - 1)p_j^{s_j} \prod_{j=1}^n p_j^{x_j(s_j-1)/2} \right)^{m_S}}{\zeta_q(2)^{r-1} \prod_{S \in S} (q + r - 1)\prod_{j=1}^n (q - 1)^{s_j}} \times \left( \frac{q \prod_{j=1}^n \frac{t_j(\ell - 1)}{(q - 1)^{t_j}(q + r - 1)}} {t - \sum_{S \in S} m_S} \right)^{\ell - \sum_{S \in S} m_S} \left( 1 + O\left( q^{-\min_{\vec{d}} d(\vec{a})} \right) \right).$$

Proof. If we replace $f_{\vec{a}}$ by $f_{\vec{a}}'$, the polynomial divided by its roots, and $F_{(p_j)}$ as the corresponding product of $f_{(p_j)}$, $F_{(p_j)}^{(k_j)}(x_i)$ will be determined by $F_{(p_j)}^{(k_j)}(x_i)$ for $k_j \leq s_j$ and $F_{(p_j)}^{(k_j)}(x_i)$ will be determined, up to a $p^{k_j-1}$th root of unity, by $F_{(p_j)}^{(k_j-1)}(x_i)$ for $s_j < k_j \leq t_j$. Summing up over all the necessary partitions of $m_S$ will give the desired result.

\[ \square \]

Note that if we let $d = \prod_{j=1}^n p_j^{x_j}$, then we can write

$$\prod_{j \in J_S} (p_j - 1)p_j^{s_j} = \phi \left( \frac{r}{d} \right).$$

This illustrates why it was important to consider the set $J_S$ for if the left hand product was over all the $j$, we would not get this nice equality.

Let $\vec{1} \in \mathbb{R}$ be the element that has 1 in the $T_j + 1$ position $j = 0, \ldots, n - 1$ and 0 everywhere else. Then set $\mathbb{R}' = \mathbb{R} \setminus \vec{1}$. Define

$$\mathcal{F}_{\vec{d}(\vec{a})} = \{(f_{\vec{1}}, (f_{\vec{a}})) \in \mathcal{F}_{d_{\vec{1}}} \times \prod_{\vec{a} \in \mathbb{R}'} \mathcal{F}_{\vec{a}} : (f_{\vec{a}}, f_{\vec{b}}) = 1 \text{ for all } \vec{a} \neq \vec{b}\}$$

With this definition, define $\mathcal{F}_{\vec{d}(\vec{a})}^{(\vec{b})}$, $\mathcal{F}_{d(\vec{a})}$ and $\mathcal{F}_{d(\vec{a})}$ the same way as in Section 4.

Now, if $x_{q+1}$ is the point at infinity, then

$$F_{(p_j)}^{(k_j)}(x_{q+1}) = \begin{cases} \text{leading coefficient of } f_{\vec{1}}^{(x_{q+1})} & (f_{\vec{a}}) \in \mathcal{F}_{d(\vec{a})}^{(\vec{b})} \\ 0 & \text{otherwise} \end{cases}$$

where $\beta = (\beta_1, \ldots, \beta_{T_n}) \in \mathbb{R}$ is any tuple such that $\beta_{T_j+1}, \ldots, \beta_{T_j+k_j} = 0$.

Similarly to Corollaries 4.3 and 4.4, we get

Corollary 5.3. Let $\epsilon_{i,j,k_j} \in \mu_{p_j} \cup \{0\}$ such that for $m_S$ of the $i$ we have

$$\epsilon_{i,j,1}, \ldots, \epsilon_{i,j,s_j} \neq 0 \text{ and } \epsilon_{i,j,s_j+1}, \ldots, \epsilon_{i,j,t_j} = 0, \quad 1 \leq j \leq n$$
for all $S \in S$. Further if $\epsilon_{i,j,k_j} \neq 0$ then $\epsilon_{i,j,k_j} = (\epsilon_{i,j,k_j-1})^p$.

$$\left| \{(f_{\alpha}) \in \hat{F}_{[d\alpha]} : \chi_{p^j}(F_j(x_i)) = \epsilon_{i,j,k_j}, 1 \leq j \leq n, 1 \leq k_j \leq t_j, 1 \leq i \leq q + 1 \} \right|$$

$$= \prod_{S \in S} \left( \prod_{j \in J_S} (p_j - 1)p_j^{t_j - s_j} \right)^{m_S} \frac{|\hat{F}_{[d\alpha]}|}{q^{\sum_{S \in S} m_S}} \left( 1 + O \left( q^{-\frac{\min_{a \in \mathbb{Z}} d(a)}{2}} \right) \right).$$

Applying this Corollary we obtain

**Proof of Theorem 1.2.**

$$\left| \{(f_{\alpha}) \in \hat{F}_{[d\alpha]} : S_d(F(d)) = M_d, \forall d|r \} \right|$$

$$= \prod_{S \in S} \left( \prod_{j \in J_S} (p_j - 1)p_j^{t_j - s_j} \right)^{m_S} \left( 1 + O \left( q^{-\frac{\min_{a \in \mathbb{Z}} d(a)}{2}} \right) \right).$$

Where in the subscript we have $\sigma_p = p^{-v_p(d)} \mod \frac{d}{p^{v_p(d)}}$. Further, if we let $d = \prod_{j=1}^n p_j^{s_j}$ then factor being raised to the $m_S$ can be rewritten as

$$\frac{\phi \left( \frac{d}{q+r-1} \right)}{d(q+r-1)}$$

and, if $d \neq r$, the $X_{p^{s_j},i}$ satisfy the relationship

$$\text{Prob} \left( X_{p^{s_j},i} = \epsilon_{p^{s_j},i}, 1 \leq s \leq v_p(d) \right) \text{ and } X_{p^{s_j},i} = 0, v_p(d) < s \leq v_p(r) \text{ for all } p|r$$

$$= \begin{cases} \frac{\phi \left( \frac{d}{q+r-1} \right)}{d(q+r-1)} & \text{if } \epsilon_{p^{s_j-1},i} = \epsilon_{p^{s_j},i}^p \text{ for all } p|r, 1 \leq s \leq v_p(d) \\ 0 & \text{otherwise} \end{cases}.$$
If $d = r$, then

$$\text{Prob}(X_{p^*, i} = \epsilon_{p^*, i}, s \leq v_p(r), \text{ for all } p|r) = \begin{cases} \frac{q}{(q + r - 1)} & \text{if } \epsilon_{p^*, i} = \epsilon_{p^*, i}^p, 1 \leq s \leq v_p(r), \text{ for all } p|r, \\ 0 & \text{otherwise} \end{cases}$$

Notice also, since the $\sigma_p$ come from the Chinese Remainder Theorem, if $X_{d,i} \neq 0$ then the value of $X_{p^*(d), i}$ is uniquely determined and hence so are $X_{p^*, i}$ for all $p|r$ and $k \leq v_p(d)$. Moreover, for $k > v_p(d)$, $X_{p^*, i}$ will either be 0 or determined, up to a $p^{k-v_p(d)}$ th root of unity. From here we get

$$\text{Prob}(X_{d,i} = \epsilon_{d,i} \neq 0) = \sum_{d_1} \sum_{d_1 \neq r} \phi\left(\frac{d_1}{d_i}\right) \frac{q}{d_1(q + r - 1)} + \sum_{d_1 = r} \frac{q}{d_1(q + r - 1)}$$

$$= \frac{q + \sum_{d_1 \neq r} \phi\left(\frac{d_1}{d_i}\right)}{d(q + r - 1)} = \frac{q + \phi\left(\frac{r}{d_i}\right) - 1}{d(q + r - 1)} = \frac{q + \frac{r}{d_i} - 1}{d(q + r - 1)}.$$

Therefore

$$\text{Prob}(X_{d,i} = 0) = 1 - \sum_{\epsilon_{d,i} \in \mu_d} \text{Prob}(X_{d,i} = \epsilon_{d,i}) = 1 - \frac{q + \frac{r}{d_i} - 1}{q + r - 1} = \frac{r - \frac{q}{d_i}}{q + r - 1}.$$

\[\Box\]

6. HEURISTIC

In this section we will discuss a heuristic for Corollary 5.2 and consequently Theorem 1.2. First we will need Lemma 8.1 from [2].

**Lemma 6.1.** Let $S_n$ be the set of $n$-tuples $(F_1, \ldots, F_n)$ of nonzero residues of modulo $(X - t)^2$ such that $(X - t)$ divides at most one of the $F_1$. Then

$$|S_n| = q^{n-1}(q - 1)^n(q + n).$$

The set $S$ models the set of $n$ squarefree coprime polynomials. Write $F = f_1 f_2 \cdots f_{r-1}$ with $(f_1, \ldots, f_{r-1}) \in S_{r-1}$. If $r = \prod_{j=1}^n p_j$ then Corollary 5.2 deals with $F_{(p_j)}$ for $1 \leq j \leq n$, $1 \leq k_j \leq t_j$. That is, we want to determine how many $(r-1)$-tuples there are in $S_{r-1}$ that satisfy

$$F_{(p_j)}^{k_j} \equiv a_{j,k_j} \mod (X - t)^2$$

where $a_{j,k_j} = a_{j,k_j-1}(b_{j,k_j})^{p_j-1}$ for some $b_{j,k_j}$.
Suppose \( a_{j,t_j} \neq 0 \mod (X-t) \) for all \( j \). Using the notation \( F_{(p_j^{s_j})} = \prod_{i=1}^{r-1} f_i^{i \mod p_j^{s_j}} \), we will start with \( j = 1 \). The condition of

\[
F_{(p_1)} \equiv a_{1,1} \mod (X-t)^2
\]
says that there are \( (q(q-1))^{r-\frac{r_t}{r_1}}-1 \) choices for \( f_i \) with \( i \neq 1 \) and \( q \) choices for \( f_1 \) which gives a total of \( q^{r-\frac{r_t}{r_1}}(q-1)^{r-\frac{r_t}{r_1}}-1 \) choices of the \( f_i \). Now if we fix one of these choices and look at

\[
F_{(p_1^{s_1})} \equiv a_{1,s_1} \mod (X-t)^2
\]
then there would be \( (q(q-1))^{r-\frac{r_t}{r_1}}-1 \) choices for the \( f_{p_1,i} \) with \( i \neq 1 \) and \( p_1q \) choices for \( f_{p_1} \), which gives a total of \( p_1q^{r-\frac{r_t}{r_1}}(q-1)^{r-\frac{r_t}{r_1}}-2 \). From here we can see that if we consider all the conditions

\[
F_{(p_2^{s_2})} \equiv a_{2,1} \mod (X-t)^2
\]
than all the \( f_i \) appearing in \( F_{(p_2^{s_2})} \) such that \( i \neq 0 \mod p_2^{s_2} \) are already determined.

If we let \( j = p_2^{-t_1} \mod p_2^{s_2} \) then there are \( (q(q-1))^{r-\frac{r_t}{r_1}}-1 \) choices for the \( f_{p_2^{s_2},i} \) such that \( i \neq j \), \( i \neq 0 \mod p_2 \) and \( q \) choices for \( f_{p_2^{s_2},j} \). Therefore we get a total of \( p_1^{t_1} q^{r-\frac{r_t}{r_1}}(q-1)^{r-\frac{r_t}{r_1}}-1 \). From here it is clear what will happen and if we look at all the conditions

\[
F_{(p_j^{s_j})} \equiv a_{j,k_j} \mod (X-t)^2 \quad 1 \leq k_j \leq t_j, \ 1 \leq j \leq n
\]
then we get

\[
(q(q-1))^{r-1} \prod_{j=1}^{n} p_j^{\frac{t_j(t_j-1)}{2}} \frac{p_j^{s_j}}{(q-1)^{k_j}}.
\]

Dividing by \( |S| \), we get

\[
\frac{q}{q+r-1} \prod_{j=1}^{n} p_j^{s_j} \frac{p_j^{\frac{t_j(t_j-1)}{2}}}{(q-1)^{k_j}}
\]
which is consistent with Proposition 5.1.

Now suppose that not all \( a_{i,j,k_j} \) are non-zero. As with the statement of Corollary 5.2 we have \( s_1, \ldots, s_n \) such that \( 0 \leq s_j \leq t_j \) (but not all \( s_j = t_j \)) and \( a_{j,k_j} \equiv 0 \mod (X-t) \) if and only if \( k_j > s_j, j = 1, \ldots, n \). Let \( d = \prod_{j=1}^{n} p_j^{s_j} \) then, as above, the conditions

\[
F_{(p_j^{s_j})} \equiv a_{j,k_j} \mod (X-t)^2 \quad 1 \leq k_j \leq s_j, \ 1 \leq j \leq n
\]
yields

\[
(q(q-1))^{r-d} \prod_{j=1}^{n} p_j^{\frac{s_j(s_j-1)}{2}} \frac{p_j^{s_j}}{(q-1)^{s_j}}
\]
choices of the $f_i$. Fixing one of these choices, consider the conditions
$$F_{(p_j^{s_j+1})} = a_{j,s_j+1} \mod (X-t)^2 \quad j = 1, \ldots, n \text{ such that } s_j \neq t_j.$$  

The value of $f_i$ is already determined if $i \neq 0 \mod d$. Further there is exactly one $1 \leq i \leq r-1$ such that $v_{p_j}(i) = s_j$ for all $1 \leq j \leq n$ such that $f_i \equiv 0 \mod (X-t)$. Then $f_i$ has $(q-1)$ different choices and the rest of the $f_j$ have $(q(q-1))^{\frac{r-2}{d} - 1}$ different choices where
$$d' = \prod_{j=1 \atop s_j \neq t_j}^{n} p_j^{s_j+1} \prod_{j=1 \atop s_j = t_j}^{n} p_j^{t_j}.$$ 

Moreover, there are $\phi\left(\frac{r}{d}\right) = \prod_{j=1,s_j \neq t_j}^{n} (p_j-1)p_j^{s_j-t_j-1}$ such $i$ that satisfy $v_{p_j}(i) = s_j$ for all $1 \leq j \leq n$. Hence with the new conditions there are
$$q^{r-2} (q-1)^{r-1} \phi\left(\frac{r}{d}\right) \prod_{j=1}^{n} p_j^{s_j(s_j-1)} \prod_{j=1}^{n} (q-1)^{s_j}$$

choices of the $f_i$.

For the remaining $\frac{r}{d} - 1$ of the $f_i$ not accounted for, the conditions
$$F_{(p_j^{k_j})} = a_{j,k_j} \mod (X-t)^2 \quad k_j > s_j + 1, j = 1, \ldots, n \text{ such that } s_j \neq t_j$$

are already satisfied as $a_{j,k_j} \equiv 0 \mod (X-t)$. Therefore, we need only $f_i \neq 0 \mod (X-t)$ giving $(q(q-1))^{\frac{r-2}{d} - 1}$ choices. Therefore our final count will be
$$q^{r-2} (q-1)^{r-1} \phi\left(\frac{r}{d}\right) \prod_{j=1}^{n} p_j^{s_j(s_j-1)} \prod_{j=1}^{n} (q-1)^{s_j}.$$ 

Dividing by $|S|$ gives
$$\frac{\phi\left(\frac{r}{d}\right)}{q^{r-1} + r-1} \prod_{j=1}^{n} p_j^{s_j(s_j-1)} \prod_{j=1}^{n} (q-1)^{s_j}$$

which is consistent with Corollary 5.2.

Acknowledgements: I would like to thank Chantal David for the many discussions we had about this topic and for taking time to make sure the final paper was presentable. I would also like to thank Elisa Lorenzo, Giulio Meleleo and Piermarco Milione for their helpful discussions about their paper.

References

[1] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín, Biased statistics for traces of cyclic p-fold covers over finite fields, WIN–Women in Numbers: Research Directions in Number Theory 60 (2009), 121–143.

[2] Alina Bucur, Chantal David, Brooke Feigon, and Matilde Lalín, Statistics for traces of cyclic trigonal curves over finite fields, International Mathematics Research Notices (2009), rnp162.

[3] Nicholas M Katz and Peter Sarnak, Random matrices, frobenius eigenvalues, and monodromy, vol. 45, American Mathematical Soc., 1999.

[4] Pär Kurlberg and Zeév Rudnick, The fluctuations in the number of points on a hyperelliptic curve over a finite field, Journal of Number Theory 129 (2009), no. 3, 589–587.

[5] Elisa Lorenzo, Giulio Meleleo, and Piermarco Milione, Statistics for biquadratic covers of the projective line over finite fields, arXiv preprint arXiv:1503.03276 (2015).

[6] Michael Rosen, Number theory in function fields, vol. 210, Springer Science & Business Media, 2013.