ℓ-RANKS OF CLASS GROUPS OF FUNCTION FIELDS

SUNGHAN BAE AND HWANYUP JUNG*

ABSTRACT. In this paper we give asymptotic formulas for the number of ℓ-cyclic extensions of the rational function field $\mathrm{k} = \mathbb{F}_q(T)$ with prescribed ℓ-class numbers inside some cyclotomic function fields, and density results for ℓ-cyclic extensions of k with certain properties on the ideal class groups.

0. INTRODUCTION

Let $\mathbb{Q}$ be the field of rational numbers and ℓ a prime number. In 1980's F. Gerth studied extensively the asymptotic behavior of ℓ-cyclic extensions of $\mathbb{Q}$ with certain conditions on the ideal class groups and ramified primes. Let us recall Gerth's results more precisely. Write $N_{s,x}$ for the number of ℓ-cyclic extensions of $\mathbb{Q}$ with conductor $\leq x$ and ℓ-class number ℓ^s. In [G2], it is shown that to obtain an asymptotic formula for $N_{s,x}$, it suffices to count the number $M_{s+1,x}$ of ℓ-cyclic extensions of $\mathbb{Q}$ whose conductor is $\leq x$ and divisible by exactly $s+1$ distinct primes, and whose ℓ-class number is ℓ^s. In [G3], a matrix M over $\mathbb{F}_\ell$ is associated to each ℓ-cyclic extension F of $\mathbb{Q}$ with $s+1$ ramified primes such that the ℓ-class number of F is ℓ^n precisely when $\mathrm{rank}(M) = s$, and an asymptotic formula for $N_{s,x}$ is given by studying the asymptotic behavior of the number of such matrices. In [G5], for $\ell = 2$, an effective algorithm for computing the density $d_{t,e}$ (resp. $d'_{t,e}$) of the quadratic fields with 4-class rank e (in the narrow sense) in the set of imaginary (resp. real) quadratic fields with t ramified primes, and explicit formulas for their limiting densities $d_{\infty,e} = \lim_{t\to\infty} d_{t,e}$ and $d'_{\infty,e} = \lim_{t\to\infty} d'_{t,e}$ are given. An explicit formula for the limiting density $d_{\infty,e}$, which depends only on ℓ and e, is given in [G7] for arbitrary prime number ℓ. Similar results for ℓ^n-cyclic extensions of $\mathbb{Q}$ with prescribed (narrow) genus groups are given in [G6].

Let $\mathrm{k} = \mathbb{F}_q(T)$ be the rational function field over the finite field $\mathbb{F}_q$. Let ℓ be a prime number different from the characteristic of k and r be the smallest positive integer such that $\ell | q^r - 1$. In this article we study analogous problems for ℓ-cyclic extensions of k inside some cyclotomic function fields. The content of this paper is as follows. In §1 we recall several asymptotic formulas in $\mathbb{A} = \mathbb{F}_q[T]$, which can be found in [Kn] and [R]. In §2 we recall the genus theory for function fields [BK] and extend

2000 *Mathematics Subject Classification.* 11R58, 11R29, 11R45.

*Corresponding author.

This work was supported by the Korea Science and Engineering Foundation(KOSEF) grant funded by the Korea government(MOST) (No. R01-2006-000-10320-0).

some results of Wittmann [W] to the narrow case. In §3.1 we give an asymptotic formula for the number $N_{s,rn}$ of ℓ-cyclic extensions F inside some cyclotomic function fields with ℓ-class number ℓ^s and with conductor N of degree rn in the case $r > 1$. Similar results of §3.1 in the case $r = 1$ are given in §3.2. In §4 we give the density for ℓ-ranks in ℓ-cyclic function fields. In §5 we give a generalization of §4 to ℓ^m-cyclic extensions of k inside some cyclotomic function fields.

1. Some asymptotic formulas in $\mathbb{A} = \mathbb{F}_q[T]$

In this section we recall several asymptotic formulas in $\mathbb{A} = \mathbb{F}_q[T]$, which will be used later in this paper. For the details and proofs we refer to [Kn] and [R].

- $P(n)$:= the set of monic irreducible polynomials in $\mathbb{A}$ of degree n, and $p(n) = |P(n)|$. Then

$$p(n) = \frac{q^n}{n} + O\Big(\frac{q^{n/2}}{n}\Big) \quad \text{([Kn, Chap. 8], [R, Theorem 2.2]).} \tag{1.1}$$

- $P(n,k)$:= the set of all square-free monic polynomials of degree n with k-irreducible factors, and $p(n,k) = |P(n,k)|$. Then

$$p(n,k) = \frac{q^n(\log n)^{k-1}}{(k-1)!n} + O\Big(\frac{q^n(\log n)^{k-2}}{n}\Big) \quad \text{([Kn, Theorem 9.9]).} \tag{1.2}$$

- $P_r(rn,k)$:= the set of all square-free monic polynomials of degree rn with k-irreducible factors whose degrees are divisible by r, and $p_r(rn,k) = |P_r(rn,k)|$. Following the method of [Kn, §9],

$$p_r(rn,k) = \frac{q^{rn}(\log n)^{k-1}}{(k-1)!r^k n} + O\Big(\frac{q^{rn}(\log n)^{k-2}}{n}\Big). \tag{1.3}$$

Intuitively, (1.3) follows from (1.2) and that the probability that a prime whose degree is divisible by r is $\frac{1}{r}$. For $A, M \in \mathbb{A}$, relatively prime,

- $P(n,A,M)$:= the set of monic irreducible polynomials of degree n, which are congruent to A modulo M, and $p(n,A,M) = |P(n,A,M)|$. Then

$$p(n,A,M) = \frac{q^n}{\phi(M)n} + O\Big(\frac{q^{n/2}}{n}\Big) \quad \text{([R, Theorem 4.8]).} \tag{1.4}$$

Also, for a nontrivial Dirichlet character χ, we have

$$\sum_{P,\deg P = n} \chi(P) = O\Big(\frac{q^{n/2}}{n}\Big) \quad \text{([R, §4 (4), (5)]).} \tag{1.5}$$

From (1.1), we have

$$\sum_{P, \deg P \le n} \frac{\deg P}{q^{\deg P}} = n + O(1), \tag{1.6}$$

$$\sum_{P,\, r|\deg P \le nr} \frac{\deg P}{q^{\deg P}} = n + O(1), \tag{1.7}$$

$$\sum_{P, \deg P \le n} \frac{1}{q^{\deg P}} = \log n + O(1), \tag{1.8}$$

$$\sum_{P,\, r | \deg P \le nr} \frac{1}{q^{\deg P}} = \frac{\log n}{r} + O(1). \tag{1.9}$$

From (1.2), (1.3) and the partial summation formula, we have

$$\sum_{d=1}^{n} \sum_{P \in P(d,k)} \frac{1}{q^d} \sim \frac{(\log n)^k}{k!}, \tag{1.10}$$

$$\sum_{d=1}^{n} \sum_{P \in P_r(rd,k)} \frac{1}{q^{rd}} \sim \frac{(\log n)^k}{k! r^k}. \tag{1.11}$$

2. Genus theory for function fields

Write ∞ for the place of k associated to $1/T$. Let k_∞ be the completion of k at ∞, i.e., $\mathrm{k}_\infty = \mathrm{k}((1/T))$. Let $\mathrm{C} = \mathrm{k}_\infty(\sqrt[q-1]{-1/T})$. We only consider those function fields which can be embedded into C. For a monic polynomial M of $\mathbb{A}$, k_M denotes the cyclotomic function field of conductor M (see [R, §12]). Any abelian extension F of k inside C is contained in k_M for some M. The smallest such M is called the conductor of F. From now on we always assume that every extension of k is contained in some cyclotomic function field. Let ℓ be a prime number different from the characteristic of k and r be the smallest positive integer such that $\ell \mid q^r - 1$.

Let F be a ℓ-cyclic extension of k, and write $N = N_{\mathrm{F}}$ for the conductor of F. Then N must be square-free and for each prime divisor P of N, $\deg P$ is divisible by r. Write $N = P_1 \cdots P_t$. It is easy to see that the number of such extensions F with conductor $P_1 \cdots P_t$ is $(\ell - 1)^{t-1}$. Write $\mathrm{H_F}$ for the Hilbert class field of F and $\mathrm{G_F}$ for the genus field of F/k. Let $\mathcal{C}l(\mathrm{F})$ be the ideal class group of the integral closure $\mathcal{O}_{\mathrm{F}}$ of $\mathbb{A}$ in F, and $\mathcal{C}l(\mathrm{F})_\ell$ be its ℓ-part. Let σ be a fixed generator of $G = \mathrm{Gal}(\mathrm{F/k})$ and

$$\lambda_i(\mathrm{F}) := \dim_{\mathbb{F}_\ell} \left(\mathcal{C}l(\mathrm{F})_\ell^{(\sigma-1)^{i-1}} / \mathcal{C}l(\mathrm{F})_\ell^{(\sigma-1)^i} \right) \quad \text{for } i \ge 1.$$

It is known that ([BK, §2])

$$\mathcal{C}l(\mathrm{F})_\ell / \mathcal{C}l(\mathrm{F})_\ell^{\sigma-1} \simeq \mathcal{C}l(\mathrm{F}) / \mathcal{C}l(\mathrm{F})^{\sigma-1} \simeq \mathrm{Gal}(\mathrm{G_F/F}).$$

It is well-known that $\mathcal{C}l(\mathrm{F})_\ell^G$ and $\mathcal{C}l(\mathrm{F})_\ell / \mathcal{C}l(\mathrm{F})_\ell^{\sigma-1}$ are elementary abelian group of rank λ_1. Since F is contained in some cyclotomic function field, the inertia degree f_∞ at ∞ should be 1, and the ramification degree e_∞ is 1 if $r > 1$.

Now we consider the narrow case. We define the narrow Hilbert class field $\mathrm{H_F^+}$ of F to be the maximal abelian extension of F in C, unramified outside the places over ∞. For each place v of F over ∞ we write F_v to denote the completion of F at v and N_v be the norm map from F_v to k_∞. We define a sign map $sgn_v : \mathrm{F}_v \to \mathbb{F}_q$ by $sgn_v(x) = sgn(N_v(x))$, where sgn is the usaul sign map on k_∞. An element $x \in \mathrm{F}$ is called *totally positive* if $sgn_v(x) = 1$ for any v lying over ∞. The narrow ideal class group $\mathcal{C}l^+(\mathrm{F})$ of F is defined to be the quotient group of fractional ideals modulo principal fractional ideals generated by totally positive elements of F. The *narrow genus field* G_F^+ of F/k is defined to be the maximal extension of F in H_F^+ which is the compositum of F and some abelian extension of k. See [BK] for details on the genus theory of function fields. Let

$$\lambda_i^+(\mathrm{F}) := \dim_{\mathbb{F}_\ell}\left(\mathcal{C}l^+(\mathrm{F})_\ell^{(\sigma-1)^{i-1}}/\mathcal{C}l^+(\mathrm{F})_\ell^{(\sigma-1)^{i}}\right) \quad \text{for } i \geq 1.$$

Note that if $r > 1$, then $\mathcal{C}l^+(\mathrm{F})_\ell = \mathcal{C}l(\mathrm{F})_\ell$ and so $\lambda_i^+(\mathrm{F}) = \lambda_i(\mathrm{F})$. We will use the following lemmas in [W]. The narrow case can be proved by the similar method as in [W].

Lemma 2.1. ([W, Theorem 2.1]) Let F be as above.

(i) If $r > 1$, or $r = 1$ and $\ell \mid \deg P_i$ for any i, then $\lambda_1(\mathrm{F}) = t - 1$.
(ii) In all other cases, $\lambda_1(\mathrm{F}) = t - 2 + \log_\ell(e_\infty f_\infty)$.
(iii) $\lambda_1^+(\mathrm{F}) = t - 1$.

Let $\mathfrak{p}_i$ be the unique prime ideal of F lying above P_i.

Lemma 2.2. ([W, Corollary 2.3, 2.4]) Let F be as above.

(i) If $r > 1$, then $\mathcal{C}l(\mathrm{F})_\ell^G$ is generated by the classes $[\mathfrak{p}_1], \ldots, [\mathfrak{p}_t]$.
(ii) If $r = 1$, then

$$\mathcal{C}l(\mathrm{F})_\ell^G = \langle[\mathfrak{p}_1], \ldots, [\mathfrak{p}_t]\rangle,$$

except the case that $\ell \mid \deg P_i$ for any i and $N_{\mathrm{F}/\mathrm{k}}(\mathcal{O}_\mathrm{F}^*) = (\mathbb{F}_q^*)^\ell$. In this case,

$$\mathcal{C}l(\mathrm{F})_\ell^G = \langle[\mathfrak{p}_1], \ldots, [\mathfrak{p}_t], [\mathfrak{a}]\rangle,$$

where $\mathfrak{a}^{\sigma-1} = \alpha\mathcal{O}_\mathrm{F}$ and $N_{\mathrm{F}/\mathrm{k}}(\alpha) \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^\ell$.
(iii) $\mathcal{C}l^+(\mathrm{F})_\ell^G$ is generated by the classes $[\mathfrak{p}_1], \ldots, [\mathfrak{p}_t]$.

Suppose first that $r = 1$. In this case $\mathrm{F} = \mathrm{k}(\sqrt[\ell]{D})$, where $D = aP_1^{e_1}\cdots P_t^{e_t}$ with $1 \leq e_i < \ell$ and $a \in \mathbb{F}_q^*$. We will determine a. From [A, Lemma 3.2], it is known that if $\ell \mid \deg P_i$, then $\mathrm{k}(\sqrt[\ell]{P_i}) \subseteq \mathrm{k}_{P_i}$, and that if $\ell \nmid \deg P_i$, then $\mathrm{k}(\sqrt[\ell]{-P_i^{d_i}}) \subseteq \mathrm{k}_{P_i}$, where d_i is a positive integer such that $d_i \deg P_i \equiv 1 \bmod \ell$. Thus we see that a can be taken to be $(-1)^m$, where $m = \sum_{\ell\nmid\deg P_i}\nu_i$ and $d_i\nu_i \equiv e_i \bmod \ell$. When $\ell \neq 2$, or $q \equiv 1 \bmod 4$ and $\ell = 2$, -1 is an ℓ-th power in $\mathbb{F}_q^*$. Thus one may take a to be 1 in these cases. If $q \equiv 3 \bmod 4$ and $\ell = 2$, then we take $a = (-1)^s$, where s is the number of odd degree P_i's.

Proposition 2.3. ([W, Theorem 2.5]) Let $\mathrm{F} = \mathrm{k}(\sqrt[\ell]{D})$ be as above.

(i) $\mathrm{G}_\mathrm{F}^+ = \mathrm{k}(\sqrt[\ell]{(-1)^{\deg P_1}P_1}, \ldots, \sqrt[\ell]{(-1)^{\deg P_t}P_t})$.
(ii) If $\ell \nmid \deg D$ or $\ell \mid \deg P_i$ for any i, then

$$\mathrm{G}_\mathrm{F} = \mathrm{G}_\mathrm{F}^+ = \mathrm{k}(\sqrt[\ell]{(-1)^{\deg P_i}P_1}, \ldots, \sqrt[\ell]{(-1)^{\deg P_t}P_t}).$$

(iii) If $\ell \mid \deg D$ but $\ell \nmid \deg P_i$ for $1 \le i \le s$ and $\ell \mid \deg P_j$ for $s+1 \le j \le t$, then

$$\mathrm{G_F} = \mathrm{k}(\sqrt[\ell]{P_1 P_2^{u_2}}, \ldots, \sqrt[\ell]{P_1 P_s^{u_s}}, \sqrt[\ell]{P_{s+1}}, \ldots, \sqrt[\ell]{P_t}),$$

where $\deg P_1 + u_i \deg P_i \equiv 0 \bmod \ell$.

Let η be a fixed primitive ℓ-th root of unity in $\mathbb{F}_q$. Let $(\frac{A}{P})_\ell$ be the ℓ-th power residue symbol. For a field F as above, we define a $t \times t$ matrix $M_{\mathrm{F}} = (m_{ij})$ over $\mathbb{F}_\ell$ by, for $i \ne j$,

$$\eta^{m_{ij}} = \left(\frac{\bar{P}_i}{P_j}\right)_\ell,$$

where $\bar{P}_i = (-1)^{\deg P_i} P_i$ and m_{ii} is defined to satisfy

$$\sum_{i=1}^{t} e_i m_{ij} = 0.$$

Then it can be shown (cf, [W, §3]) that

$$\lambda_2(\mathrm{F}) = t - 1 - \mathrm{rank}(M_{\mathrm{F}}), \text{ when } \infty \text{ ramifies in F}$$

and

$$\lambda_2^+(\mathrm{F}) = t - 1 - \mathrm{rank}(M_{\mathrm{F}}), \text{ when } \infty \text{ splits in F}.$$

Note that, if $\ell | \deg P_i$ for every i, then $\lambda_2^+(\mathrm{F}) = \lambda_2(\mathrm{F})$. In the case (iii) of Proposition 2.3, a $(t-1) \times t$ matrix M'_{F} is defined in [W, §3] and was shown that

$$\lambda_2(\mathrm{F}) = t - 2 - \mathrm{rank}(M'_{\mathrm{F}}).$$

Now suppose that $r > 1$. Let

$$w = \sum_{i=1}^{t} (\deg P_i, r),$$

where (a, b) denotes the greatest common divisor of a and b. A $t \times w$ matrix $\tilde{M}_{\mathrm{F}}$ over $\mathbb{F}_\ell$ is defined in [W, §4] and it is shown that

$$\lambda_2(\mathrm{F}) = t - 2 - \mathrm{rank}(\tilde{M}_{\mathrm{F}}).$$

In fact, this matrix $\tilde{M}_{\mathrm{F}}$ is essentially the same as the matrix $M = M_{\mathrm{F}}$ defined in [G3, §2].

3. Asymptotic behavior of ℓ-cyclic extensions with prescribed ℓ-class numbers

3.1. $r > 1$ **case.** In this subsection we assume that $r > 1$. Let

- $N_{s,n}$:= the number of ℓ-cyclic extensions F of k with $|\mathcal{C}l(\mathrm{F})_\ell| = \ell^s$ and with conductor N of degree n,
- $M_{s,n}$:= the number of ℓ-cyclic extensions F of k with $|\mathcal{C}l(\mathrm{F})_\ell| = \ell^{s-1}$ and with conductor N of degree n such that N has exactly s distinct prime factors,

- $G_{s,n}$:= the number of ℓ-cyclic extensions F of k with conductor $N = P_1 \cdots P_s$ of degree n such that P_m is an ℓ-th power residue modulo $P_1, \dots, P_{m-2}$ but an ℓ-th power nonresidue modulo P_{m-1}.

Since we know that r must divide the degrees of prime factors of N, we replace n by rn and write $\deg P_i = rk_i$.

Let χ_{P_i} be a Dirichlet charater of exponent ℓ of conductor P_i, that is, a character of $\mathrm{Gal}(\mathrm{k}_{P_i}/\mathrm{k})$. For a prime $P_m \neq P_1, ..., P_{m-1}$, let

$$W_m := \frac{1}{\ell^{m-1}}\Big(\sum_{j_1=0}^{\ell-1} \chi_{P_1}^{j_1}(P_m)\Big) \cdots \Big(\sum_{j_{m-2}=0}^{\ell-1} \chi_{P_{m-2}}^{j_{m-2}}(P_m)\Big)\Big(\sum_{j_{m-1}=0}^{\ell-1} \zeta^{j_{m-1}} \chi_{P_{m-1}}^{j_{m-1}}(P_m)\Big), \tag{3.1}$$

where ζ is a primtive ℓ-th root of unity. Then we have

$$M_{t,rn} \geq G_{t,rn} \geq \sum W_2 \cdots W_t,$$

where the sum is over the distinct primes $P_1, ..., P_t$ with $\deg(P_1 \cdots P_t) = rn$ and $r \mid \deg P_i$. Let $y_i := 2^i\sqrt{n}$. Then $y_1 + \cdots + y_{t-1} < y_t = y$. Let

$$A_{t,rn} := \sum W_2 \cdots W_{t-1} \sum_{P_t,\, \deg P_t = rn - \deg P_1 - \cdots - \deg P_{t-1}} W_t,$$

where the first sum is over distinct P_i, $1 \leq i \leq t-1$ with $\deg P_{i-1} \leq \deg P_i \leq y_i$. Write

$$W_t = \frac{1}{\ell^{t-1}}\Big(1 + \sum_J \zeta^{j_{t-1}} \chi_{P_1}^{j_1} \cdots \chi_{P_{t-1}}^{j_{t-1}}(P_t)\Big),$$

where $J = (j_1, ..., j_{t-1}) \neq (0, ..., 0)$. Then, by (1.1) and (1.5),

$$\sum_{\deg P_t = r(n-k_1-\cdots-k_{t-1})} W_t = \frac{q^{r(n-k_1-\cdots-k_{t-1})}}{\ell^{t-1} r(n-k_1-\cdots-k_{t-1})} + O\Big(\frac{q^{r(n-k_1-\cdots-k_{t-1})/2}}{n-k_1-\cdots-k_{t-1}}\Big).$$

For $k_i \leq y_i$, since $n - y = n - 2^t\sqrt{n} > n/2$ for large n,

$$\begin{aligned}\frac{q^{r(n-k_1-\cdots-k_{t-1})}}{r(n-k_1-\cdots-k_{t-1})} &= \frac{q^{r(n-k_1-\cdots-k_{t-1})}}{rn} + \frac{q^{r(n-k_1-\cdots-k_{t-1})}(k_1+\cdots+k_{t-1})}{rn(n-k_1-\cdots-k_{t-1})} \\ &= \frac{q^{r(n-k_1-\cdots-k_{t-1})}}{rn} + O\Big(\frac{(k_1+\cdots+k_{t-1})q^{r(n-k_1-\cdots-k_{t-1})}}{n^2}\Big)\end{aligned}$$

and

$$\frac{q^{r(n-k_1-\cdots-k_{t-1})/2}}{(n-k_1-\cdots-k_{t-1})} = O\Big(\frac{q^{r(n-k_1-\cdots-k_{t-1})}}{n^2}\Big).$$

Thus

$$\sum_{\deg P_t = r(n-k_1-\cdots-k_{t-1})} W_t = \frac{q^{r(n-k_1-\cdots-k_{t-1})}}{\ell^{t-1} rn} + O\Big(\frac{(k_1+\cdots+k_{t-1})q^{r(n-k_1-\cdots-k_{t-1})}}{n^2}\Big).$$

From (1.7) and (1.9) we have, for $y = y_t = 2^t\sqrt{n}$,

$$\sum_{\substack{P_1,\dots,P_{t-1} \\ r \mid \deg P_i \leq ry_i}} \frac{q^{rn}(\deg P_1 + \cdots + \deg P_{t-1})}{n^2 q^{\deg P_1} \cdots q^{\deg P_{t-1}}} = O\Big(\frac{y(\log y)^{t-2} q^{rn}}{n^2}\Big) = O\Big(\frac{q^{rn}}{n}\Big).$$

Therefore

$$A_{t,rn} = \frac{1}{\ell^{t-1}} \sum_{\substack{P_1,\dots,P_{t-1}:\ \text{distinct} \\ r|\deg P_i \le r y_i}} W_2 \cdots W_{t-1} \frac{q^{nr}}{rnq^{\deg P_1} \cdots q^{\deg P_{t-1}}} + O\Big(\frac{q^{rn}}{n}\Big).$$

Now

$$W_{t-1} = \frac{1}{\ell^{t-2}} \Big(1 + \sum_J \zeta^{j_{t-1}} \chi_{P_1}^{j_1} \cdots \chi_{P_{t-2}}^{j_{t-2}}(P_{t-1})\Big).$$

Let χ_Q be a nontrivial character with exponent ℓ and conductor $Q \mid P_1 \cdots P_{t-2}$. Let

$$S_Q(u) := \sum_{\deg P_{t-1} = ru} \chi_Q(P_{t-1}).$$

Then, by (1.5)

$$\sum_{u=\frac{\deg P_{t-2}}{r}}^{[y_{t-1}]} \frac{S_Q(u)}{q^{ru}} = \sum_{u=\frac{\deg P_{t-2}}{r}}^{[y_{t-1}]} O\Big(\frac{1}{uq^{\frac{ru}{2}}}\Big) = O(1).$$

Continuing the same process, we have

$$A_{t,rn} = \frac{1}{\ell^{t(t-1)/2}} \sum_{P_1,\dots,P_{t-1}} \frac{q^{rn}}{rnq^{\deg P_1} \cdots q^{\deg P_{t-1}}} + O\Big(\frac{q^{rn}}{n} (\log y)^{t-2}\Big).$$

Thus

$$A_{t,rn} = c\frac{q^{rn}(\log n)^{t-1}}{rn} + O\Big(\frac{q^{rn}(\log n)^{t-2}}{n}\Big).$$

From (1.2), we have

$$M_{s,rn} = O\Big(\frac{q^{rn}}{n}(\log n)^{s-1}\Big).$$

We finally get

$$N_{s,rn} = M_{s+1,rn} + O\Big(\frac{M_{s+1,rn}}{\log n}\Big).$$

We will compute $M_{s+1,rn}$. As in [G3, §2,§3], one can see easily that the ℓ-cyclic extension F has ℓ-class number ℓ^s precisely when $\text{rank}(M_{\text{F}}) = s$, and that the number of distinct $(s+1) \times (s+1)$ matrices Γ over $\mathbb{F}_\ell$ such that $\text{rank}(\Gamma) = s$ and such that $\Gamma = M_F$ for some field F is

$$\ell^{\frac{s(s-1)}{2}} (\ell-1)^s \prod_{i=1}^{s} (\ell^i + \cdots + \ell + 1). \tag{3.2}$$

Now we consider the number $N(\Gamma)$ of F with conductor $N = P_1 \cdots P_{s+1}$ of degree rn and the corresponding matrix $M_F = \Gamma$. Let $\mathbf{k} = \mathbb{F}_{q^r}\mathrm{k}$ and H_i be as in §2. Let $\mathrm{L}_i = \mathbf{k}\mathrm{H}_i$. Then $\mathrm{L}_i/\mathbf{k}$ is a Kummer extension $\mathrm{L}_i = \mathbf{k}(\sqrt[\ell]{\mu_i})$ for some $\mu_i \in \mathbf{k}$. Then $\mathbf{k}\mathrm{F} = \mathbf{k}(\sqrt[\ell]{\mu})$ with $\mu = \mu_1^{e_1} \cdots \mu_{s+1}^{e_{s+1}}$. Let $\mathrm{L}_i' = \mathbf{k}(\sqrt[\ell]{P_i})$. Define $\lambda_i(\mathfrak{p}_j)$ and $\omega_i(\mathfrak{p}_j)$ as follows;

$$(\mathfrak{p}_j, \mathrm{L}_i/\mathbf{k})(\sqrt[\ell]{\mu_i}) = \lambda_i(\mathfrak{p}_j)^{-1}\sqrt[\ell]{\mu_i}, \quad (\mathfrak{p}_j, \mathrm{L}_i'/\mathbf{k})(\sqrt[\ell]{P_i}) = \omega_i(\mathfrak{p}_j)^{-1}\sqrt[\ell]{P_i}.$$

Let $\delta(n(i), m(j), u(i,j), v(j,i))$ be defined by 1 if $(\lambda_i^{n(i)}(\mathfrak{p}_j), \omega_i^{m(j)}(\mathfrak{p}_j)) = (\zeta^{u(i,j)}, \zeta^{v(j,i)})$ and by 0 otherwise. Then we have

$$\sum_{\deg P_j = rm} \sum_{m(j)=1}^{\ell-1} \prod_{i=1}^{j-1} \delta(n(i), m(j), u(i,j), v(j,i)) \sim \frac{\ell-1}{\ell^{2(j-1)}} \frac{q^{rm}}{rm}. \tag{3.3}$$

Note the difference of (3.3) from (3) of [G3]. In the classical case the condition $p \equiv 1 \bmod \ell$ is imposed instead of $\deg P_i$ is divisible by r, and the probability for a prime to satisfy $p \equiv 1 \bmod \ell$ is $1/(\ell-1)$ by Dirichlet's theorem on arithmetic progression.

Following the idea of [G3] and adopting the similar method as above, we get

Theorem 3.1. *We have*

$$N(\Gamma) \sim \frac{(\ell-1)^s}{s! r^{s+1} \ell^{s^2+s}} \frac{q^{rn}(\log n)^s}{n},$$

and so

$$N_{s,rn} \sim \frac{(\ell-1)^{2s} \prod_{i=1}^{s} (\ell^i + \cdots + \ell + 1)}{s! r^{s+1} \ell^{(s^2+3s)/2}} \frac{q^{rn}(\log n)^s}{n}.$$

In the proof we need to replace $p_i \equiv 1 \bmod \ell$ by $r | \deg P_i$, which causes to replace the factor $\frac{1}{\ell-1}$ by $\frac{1}{r}$, and $p_i < p_{i+1} \le (\frac{x}{p_1 \cdots p_i})^{\frac{1}{s+1-i}}$ by $\deg P_i \le \deg P_{i+1} \le \frac{1}{s+1-i}(rn - \deg P_1 - \cdots - \deg P_i)$. We use (1.5) to show

$$\sum_{P_1} \cdots \sum_{P_s} \eta(P_{s+1}) = O\Big(\frac{q^{rn}(\log n)^s}{n}\Big),$$

and then use (1.11) to get the formula for $N(\Gamma)$.

3.2. $r = 1$ **case.** Now we assume that $r = 1$, that is $\ell \mid q-1$. We consider ℓ-cyclic extensions F of k with conductor N of degree n and with $|\mathcal{C}l(\mathrm{F})_\ell| = \ell^s$. We have two cases. One is real, that is, ∞ splits completely. The other is imaginary, that is, ∞ ramifies. The case that ∞ is inert cannot happen, since we have assumed that the field is contained in some cyclotomic function field. Let

- $N_{I,s,n}$:= the number of imaginary ℓ-cyclic extensions F of k with conductor N of degree n and $|\mathcal{C}l(\mathrm{F})_\ell| = \ell^s$,
- $N_{R,s,n}$:= the number of real ℓ-cyclic extensions F of k of degree ℓ with conductor N of degree n and $|\mathcal{C}l(\mathrm{F})_\ell| = \ell^s$,
- $M_{I,t,n}$:= the number of imaginary ℓ-cyclic extensions F of k with conductor N of degree n such that N has exactly t distinct prime factors and $|\mathcal{C}l(\mathrm{F})_\ell| = \ell^{t-1}$,
- $M_{R,t,n}$:= the number of real ℓ-cyclic extensions F of k with conductor N of degree n such that N has exactly t distinct prime factors and $|\mathcal{C}l(\mathrm{F})_\ell| = \ell^{t-2}$.

In this case $\mathrm{F} = \mathrm{k}(\sqrt[\ell]{D})$ with $D = \alpha P_1^{e_1} \cdots P_t^{e_t}$, $1 \le e_i \le l-1$. We may assume that $e_1 = 1$. Here $\alpha \in \mathbb{F}_q^*$ is chosen so that $\mathrm{F} \subseteq \mathrm{k}_N$, where $N = P_1 \cdots P_t$. If ℓ divides $\deg D$, then it is real. If ℓ does not divide $\deg D$, then it is imaginary. If $\ell = 2$, then $(e_1, \ldots, e_t) = (1, \ldots, 1)$. In this case whether F is real or imaginary depends only on the parity of $\deg N$. Otherwise, there always exist real fields and imaginary fields with conductor N. One can follow almost the same process as in the case $r > 1$ to get

$$N_{I,s,n} = M_{I,s+1,n} + O\Big(\frac{M_{I,s+1,n}}{\log n}\Big),$$

and

$$N_{R,s,n} = M_{R,s+2,n} + O\Big(\frac{M_{R,s+2,n}}{\log n}\Big).$$

4. Density for ℓ-ranks of ℓ-cyclic function fields

4.1. $r > 1$ **case.** In this subsection we assume $r > 1$, that is $\ell \nmid q-1$. Let $\mathbf{A}_t$ be the set of all ℓ-cyclic extensions F of k such that t finite primes ramify in F/k, and

$$\begin{aligned}\mathbf{A}_{t;n} &:= \{\mathrm{F} \in \mathbf{A}_t : \deg(\mathit{cond}(\mathrm{F})) = n\},\\ \mathbf{A}_{t,e} &:= \{\mathrm{F} \in \mathbf{A}_t : \lambda_2(\mathrm{F}) = e\},\\ \mathbf{A}_{t,e;n} &:= \mathbf{A}_{t,e} \cap \mathbf{A}_{t;n},\end{aligned}$$

where $\mathit{cond}(\mathrm{F})$ denotes the conductor of F. We define the density $d_{t,e}$ by

$$d_{t,e} := \lim_{n\to\infty} \frac{|\mathbf{A}_{t,e;rn}|}{|\mathbf{A}_{t;rn}|}.$$

For any monic irreducible polynomials $P_1, \ldots, P_t$ with $r | \deg P_i$, there are $(\ell-1)^{t-1}$ distinct fields F in $\mathbf{A}_t$ with conductor $N = P_1 \cdots P_t$. So by (1.3), we have

$$|\mathbf{A}_{t;rn}| = (\ell-1)^{t-1} \sum_{\substack{\deg(P_1\cdots P_t)=rn\\ r|\deg P_i}} 1 \sim \frac{(\ell-1)^{t-1}}{(t-1)!r^t}\frac{q^{rn}(\log n)^{t-1}}{n}. \tag{4.1}$$

Let M_F be the $t\times t$ matrix over $\mathbb{F}_\ell$ associated to F as in §2. Following the arguments in [G3, §2, §3], we see that $\lambda_2(\mathrm{F}) = t-1-\mathrm{rank}(M_\mathrm{F})$. Then $|\mathbf{A}_{t,e;rn}|$ can be estimated as

$$|\mathbf{A}_{t,e;rn}| \sim \sum_{\substack{\Gamma\\ \mathrm{rank}(\Gamma)=t-1-e}} \sum_{\substack{\deg(P_1\cdots P_t)=rn\\ r|\deg P_i}} \sum_{\substack{\mathrm{F}\\ \mathit{cond}(\mathrm{F})=P_1\cdots P_t}} \delta_\Gamma, \tag{4.2}$$

where $\delta_\Gamma = 1$ if $M_\mathrm{F} = \Gamma$ and $\delta_\Gamma = 0$ otherwise. Adapting the similar method as in §3.1, we get

$$N(\Gamma) = \sum_{\substack{\deg(P_1\cdots P_t)=rn\\ r|\deg P_i}} \sum_{\substack{\mathrm{F}\\ \mathit{cond}(\mathrm{F})=P_1\cdots P_t}} \delta_\Gamma \sim \frac{(\ell-1)^{t-1}}{(t-1)!r^t\ell^{t(t-1)}}\frac{q^{rn}(\log n)^{t-1}}{n}.$$

It is known ([G4, Proposition 2.1]) that the number $N(t, t-1-e)$ of $t\times t$ matrices Γ over $\mathbb{F}_\ell$ with rank $t-1-e$ is

$$N(t, t-1-e) = \left[\prod_{j=1}^{t-1-e} (\ell^t - \ell^{j-1})\right] \sum_{\substack{k_1+\cdots+k_{t-1-e}\le e+1\\ \text{each } k_i\ge 0}} \Big(\prod_{s=1}^{t-1-e} \ell^{sk_s}\Big).$$

So we have

$$|\mathbf{A}_{t,e;rn}| \sim \frac{(\ell-1)^{t-1}}{(t-1)!r^t\ell^{t(t-1)}}\frac{q^{rn}(\log n)^{t-1}}{n}\left[\prod_{j=1}^{t-1-e}(\ell^t-\ell^{j-1})\right]\sum_{\substack{k_1+\cdots+k_{t-1-e}\le e+1\\ \text{each } k_i\ge 0}}\Big(\prod_{s=1}^{t-1-e}\ell^{sk_s}\Big),$$

and

$$d_{t,e} = \frac{1}{\ell^{te}}\left[\prod_{j=1}^{t-1-e}\Big(1-\frac{1}{\ell^{t+1-j}}\Big)\right]\sum_{\substack{k_1+\cdots+k_{t-1-e}\le e+1\\ \text{each } k_i\ge 0}}\Big(\prod_{s=1}^{t-1-e}\ell^{sk_s}\Big).$$

Let $d_{\infty,e} := \lim_{t\to\infty} d_{t,e}$. Then we follow almost the same argument as in [G7, §3] to get

$$d_{\infty,e} = \frac{\ell^{-e(e+1)}\prod_{k=1}^{\infty}(1-\ell^{-k})}{\prod_{k=1}^{e}(1-\ell^{-k})\prod_{k=1}^{e+1}(1-\ell^{-k})} \qquad \text{for } e=0,1,2,\ldots.$$

4.2. $r=1$ **case.** Now we assume $r=1$. Let $\mathbf{A}_t$ be the set of all ℓ-cyclic extensions F such that t finite primes and ∞ ramify in F/k, and

$$\begin{aligned}\mathbf{A}_{t;n} &:= \{\mathrm{F}\in\mathbf{A}_t : \deg(\mathit{cond}(\mathrm{F}))=n\},\\ \mathbf{A}_{t,e} &:= \{\mathrm{F}\in\mathbf{A}_t : \lambda_2(\mathrm{F})=e\},\\ \mathbf{A}_{t,e;n} &:= \mathbf{A}_{t,e}\cap\mathbf{A}_{t;n}.\end{aligned}$$

Let $\mathbf{B}_t$ be the set of all F as above such that t finite primes ramify and ∞ splits in F/k, and

$$\begin{aligned}\mathbf{B}_{t;n} &:= \{\mathrm{F}\in\mathbf{B}_t : \deg(\mathit{cond}(\mathrm{F}))=n\},\\ \mathbf{B}_{t,e} &:= \{\mathrm{F}\in\mathbf{B}_t : \lambda_2^+(\mathrm{F})=e\},\\ \mathbf{B}_{t,e;n} &:= \mathbf{B}_{t,e}\cap\mathbf{B}_{t;n}.\end{aligned}$$

Note that $\lambda_2(\mathrm{F}) = t-1-\mathrm{rank}(M_\mathrm{F})$ (resp. $\lambda_2^+(\mathrm{F}) = t-1-\mathrm{rank}(M_\mathrm{F})$) for $\mathrm{F}\in\mathbf{A}_t$ (resp. $\mathrm{F}\in\mathbf{B}_t$).

Consider first the case that $q \not\equiv 3 \bmod 4$ or $\ell\neq 2$, that is, $a=1$ (See §2). It is shown in [W] that $M_\mathrm{F}=(m_{ij})$ is given by; $m_{ij} = \big(\frac{P_i}{P_j}\big)_\ell$, for $i\neq j$, where $(-)_\ell$ is the ℓ-th power residue, and m_{jj} is defined by the relation $\sum_i e_i m_{ij}=0$. Then from the ℓ-th power reciprocity, M_F is symmetric. There is an algorithm to determine the number of $s\times s$ symmetric matrices with rank r over $\mathbb{F}_\ell$ from the following proposition.

Proposition 4.1. *Let M be a symmetric $u\times u$ matrix of rank r over $\mathbb{F}_\ell$. Let*

$$M_1 = \begin{bmatrix} M & V\\ V^T & v\end{bmatrix},$$

with $V\in\mathbb{F}_\ell^u$, $v\in\mathbb{F}_\ell$. Then among all possible M_1,

(i) *ℓ^r of them have rank r.*
(ii) *$\ell^r(\ell-1)$ of them have rank $r+1$.*
(iii) *$\ell^{u+1}-\ell^{r+1}$ of them have rank $r+2$.*

Let $\mathbf{e} = (1, e_2, \ldots, e_t)$ with $1 \le e_i < \ell$ and E the set of all such $\mathbf{e}$'s. Let

$$\mathbf{I}_{t,\mathbf{e},n} := \{\mathrm{F} = \mathrm{k}(\sqrt[\ell]{D}) : D = P_1 P_2^{e_2} \cdots P_t^{e_t},\ \deg P_1 + \cdots + \deg P_t = n,\ \ell \nmid \deg D\},$$

$$\mathbf{R}_{t,\mathbf{e},n} := \{\mathrm{F} = \mathrm{k}(\sqrt[\ell]{D}) : D = P_1 P_2^{e_2} \cdots P_t^{e_t},\ \deg P_1 + \cdots + \deg P_t = n,\ \ell \mid \deg D\},$$

$$\mathbf{I}_{t,\mathbf{e},u,n} := \{\mathrm{F} \in \mathbf{I}_{t,\mathbf{e},n} : \mathrm{rank}(M_{\mathrm{F}}) = u\},$$

$$\mathbf{R}_{t,\mathbf{e},u,n} := \{F \in \mathbf{R}_{t,\mathbf{e},n} : \mathrm{rank}(M_{\mathrm{F}}) = u\}.$$

Here '**I**' (resp. '**R**') means imaginary (resp. real). Then

$$|\mathbf{A}_{t;n}| \sim \sum_{\mathbf{e}\in E} |\mathbf{I}_{t,\mathbf{e},n}|, \quad |\mathbf{B}_{t;n}| \sim \sum_{\mathbf{e}\in E} |\mathbf{R}_{t,\mathbf{e},n}|,$$

and

$$|\mathbf{A}_{t,e;n}| \sim \sum_{\mathbf{e}\in E} |\mathbf{I}_{t,\mathbf{e},t-1-e,n}|, \quad |\mathbf{B}_{t,e;n}| \sim \sum_{\mathbf{e}\in E} |\mathbf{R}_{t,\mathbf{e},t-1-e,n}|.$$

When $\mathbf{e} \neq (1, 1, \ldots, 1)$, then the linear equations

$$x_1 + e_2 x_2 + \cdots + e_t x_t \equiv a \bmod \ell$$

and

$$x_1 + x_2 + \cdots + x_t = n$$

are not dependent. Thus, for $\mathbf{e} \neq (1, \ldots, 1)$,

$$|\mathbf{I}_{t,\mathbf{e},n}| \sim \frac{\ell-1}{\ell} p(n,t) \quad \text{and} \quad |\mathbf{R}_{t,\mathbf{e},n}| \sim \frac{1}{\ell} p(n,t).$$

If $\mathbf{e} = (1, \ldots, 1)$, then

$$|\mathbf{I}_{t,\mathbf{e},n}| = \begin{cases} p(n,t) & \text{if } \ell \nmid n, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$|\mathbf{R}_{t,\mathbf{e},n}| = \begin{cases} p(n,t) & \text{if } \ell \mid n, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$|\mathbf{A}_{t;n}| \sim \begin{cases} \left(\frac{(\ell-1)}{\ell}((\ell-1)^{t-1} - 1) + 1\right) \frac{q^n (\log n)^{t-1}}{(t-1)!n} & \text{if } \ell \nmid n, \\ \frac{(\ell-1)}{\ell}((\ell-1)^{t-1} - 1) \frac{q^n (\log n)^{t-1}}{(t-1)!n} & \text{if } \ell \mid n, \end{cases}$$

and

$$|\mathbf{B}_{t;n}| \sim \begin{cases} \left(\frac{1}{\ell}((\ell-1)^{t-1} - 1) + 1\right) \frac{q^n (\log n)^{t-1}}{(t-1)!n} & \text{if } \ell \mid n, \\ \frac{1}{\ell}((\ell-1)^{t-1} - 1) \frac{q^n (\log n)^{t-1}}{(t-1)!n} & \text{if } \ell \nmid n. \end{cases}$$

For $N, N' \in P(n,t)$, we say that N and N' are equivalent if $(\frac{P_j}{P_i}) = (\frac{P'_j}{P'_i})$, where $N = P_1 \cdots P_t$ and $N' = P'_1 \cdots P'_t$. Let $\mathcal{N}(N)$ be the set of polynomials in $P(n,t)$, which are equivalent to N. Then it can be shown that (similar to §3.1)

$$|\mathcal{N}(N)| \sim \ell^{-\frac{t^2-t}{2}} \frac{q^n (\log n)^{t-1}}{(t-1)!n}.$$

For $\mathbf{e} = (1, e_2, \dots, e_t)$ and $N = P_1 \cdots P_t$ we write

$$N^{\mathbf{e}} := P_1 P_2^{e_2} \cdots P_t^{e_t}.$$

Let

$$\mathcal{N}_I^{\mathbf{e}}(N) := \{N_1 \in \mathcal{N}(N) : \ell \nmid \deg N_1^{\mathbf{e}}\}$$

and

$$\mathcal{N}_R^{\mathbf{e}}(N) := \{N_1 \in \mathcal{N}(N) : \ell \mid \deg N_1^{\mathbf{e}}\}.$$

Then

$$|\mathcal{N}_I^{\mathbf{e}}(N)| \sim \frac{\ell - 1}{\ell} |\mathcal{N}(N)|$$

and

$$|\mathcal{N}_R^{\mathbf{e}}(N)| \sim \frac{1}{\ell} |\mathcal{N}(N)|,$$

if $\mathbf{e} \neq (1, \dots, 1)$. If $\mathbf{e} = (1, \dots, 1)$, then

$$|\mathcal{N}_I^{\mathbf{e}}(N)| = \begin{cases} |\mathcal{N}(N)| & \text{if } \ell \nmid \deg N, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$|\mathcal{N}_R^{\mathbf{e}}(N)| = \begin{cases} |\mathcal{N}(N)| & \text{if } \ell \mid \deg N, \\ 0 & \text{otherwise.} \end{cases}$$

Let $N(t-1, u)$ be the number of $(t-1) \times (t-1)$ symmetric matrices with rank u. Then

$$|\mathbf{I}_{t,\mathbf{e},u,n}| \sim N(t-1, u) |\mathcal{N}_I^{\mathbf{e}}(N)|,$$

and

$$|\mathbf{R}_{t,\mathbf{e},u,n}| \sim N(t-1, u) |\mathcal{N}_R^{\mathbf{e}}(N)|.$$

Therefore we have

$$|\mathbf{A}_{t,\nu;n}| \sim \begin{cases} \left(\frac{(\ell-1)}{\ell} ((\ell-1)^{t-1} - 1) + 1 \right) N(t-1, t-1-\nu) |\mathcal{N}(N)| & \text{if } \ell \nmid n, \\ \frac{(\ell-1)}{\ell} ((\ell-1)^{t-1} - 1) N(t-1, t-1-\nu) |\mathcal{N}(N)| & \text{if } \ell \mid n, \end{cases}$$

and

$$|\mathbf{B}_{t,\nu;n}| \sim \begin{cases} \left(\frac{1}{\ell} ((\ell-1)^{t-1} - 1) + 1 \right) N(t-1, t-1-\nu) |\mathcal{N}(N)| & \text{if } \ell \mid n, \\ \frac{1}{\ell} ((\ell-1)^{t-1} - 1) N(t-1, t-1-\nu) |\mathcal{N}(N)| & \text{if } \ell \nmid n. \end{cases}$$

Then the densities $d_{t,e,n} = \frac{|\mathbf{A}_{t,e;n}|}{|\mathbf{A}_{t;n}|}$ and $d'_{t,e,n} = \frac{|\mathbf{B}_{t,e;n}|}{|\mathbf{B}_{t;n}|}$ are

$$d_{t,e,n} \sim d'_{t,e,n} \sim N(t-1, t-1-e) \ell^{-\frac{t^2-t}{2}}. \tag{4.3}$$

The right hand side of (4.3) is just the density $g(t, e)$ of $(t-1) \times (t-1)$ symmetric matrices which have rank $t-1-e$. We will compute the limit $\lim_{t \to \infty} g(t, e)$. From Proposition 4.1, we see that

$$g(t+1, e) = \frac{1}{\ell^e} g(t, e-1) + \frac{\ell - 1}{\ell^{1+e}} g(t, e) + \frac{\ell^{1+e} - 1}{\ell^{1+e}} g(t, e+1), \text{ if } e > 0$$

and

$$g(t+1,0)=\frac{\ell-1}{\ell}g(t,0)+\frac{\ell-1}{\ell}g(t,1).$$

Let $G(t)=(g(t,0),g(t,1),\ldots,g(t,i),\ldots)$. One can show by induction that $G(t)$ converges to, as $t\to\infty$,

$$G=\alpha\Big(1,\frac{1}{\ell-1},\ldots,\frac{1}{\prod_{i=1}^{k}(\ell^i-1)},\ldots\Big),$$

where

$$\alpha^{-1}=1+\frac{1}{\ell-1}+\frac{1}{(\ell-1)(\ell^2-1)}+\cdots.$$

Now assume that $q\equiv 3 \bmod 4$ and $\ell=2$. In order that $\mathbf{A}_{t;n}\neq\emptyset$ (resp. $\mathbf{B}_{t;n}\neq\emptyset$), n must be odd (resp. even). Now the rest are almost the same as the classical case replacing '$p\equiv 1 \bmod 4$' (resp. $p\equiv 3 \bmod 4$) by '$\deg P$ is even' (resp. odd). The result will be;

$$|\mathbf{A}_{t,e;n}|\sim\sum_{\substack{1\le d\le t\\ d\,\mathrm{odd}}}N(t-1,d-1,t-1-e)\binom{t}{d}2^{-\frac{t^2+t}{2}}\frac{q^n(\log n)^{t-1}}{(t-1)!n}\quad\text{for } n \text{ odd},$$

$$|\mathbf{B}_{t,e;n}|\sim\sum_{\substack{1\le d\le t\\ d\,\mathrm{even}}}N(t-1,d-1,t-1-e)\binom{t}{d}2^{-\frac{t^2+t}{2}}\frac{q^n(\log n)^{t-1}}{(t-1)!n}\quad\text{for } n \text{ even},$$

and

$$d_{t,e,n}\sim\sum_{\substack{1\le d\le t\\ d\,\mathrm{odd}}}N(t-1,d-1,t-1-e)\binom{t}{d}2^{-\frac{t^2+t}{2}}\quad\text{for } n \text{ odd},$$

$$d'_{t,e,n}\sim\sum_{\substack{1\le d\le t\\ d\,\mathrm{even}}}N'(t-1,d-1,t-1-e)\binom{t}{d}2^{-\frac{t^2+t}{2}}\quad\text{for } n \text{ even},$$

where $N(s,d,r)$ is the number of $s\times s$ matrices $M=(m_{ij})$ over $\mathbb{F}_2$ with $m_{ij}\neq m_{ji}$ for $1\le i<j\le d$ and with $m_{ij}=m_{ji}$ for $d+1\le i\le s$ and $1\le j\le s$ such that $\mathrm{rank}(M)=r$, and $N'(s,d,r)$ is the number of $(s+1)\times s$ matrices $\overline{M'}$ whose first column is the transpose of the vector $(1,\ldots,1,0,\ldots,0)$ with first d entries 1 and the rest part is an $s\times s$ matrix $M'=(m'_{ij})$ over $\mathbb{F}_2$ with $m'_{ij}\neq m'_{ji}$ for $1\le i<j\le d$ and $m'_{ij}=m'_{ji}$ for $d+1\le i\le s$ and $1\le j\le s$ such that $\mathrm{rank}(\overline{M'})=r$. Then as in [G5, §4, §5],

$$G(t):=(d_{t,0,2n+1},d_{t,1,2n+1},\ldots)\quad\text{and}\quad G'(t):=(d'_{t,0,2n},d'_{t,1,2n},\ldots)$$

converge to $\frac{Y}{2}$ and $\frac{Y'}{2}$ as $t\to\infty$, where

$$Y=\Big[\prod_{m=1}^{\infty}(1-2^{-m})\Big]^{-1}\big(1,2,\ldots,2^{-i^2}\prod_{m=1}^{i}(1-2^{-m})^{-2},\ldots\big)$$

and

$$Y'=\Big[\prod_{m=2}^{\infty}(1-2^{-m})\Big]\big(1,2/3,\ldots,2^{-i(i+1)}\prod_{m=1}^{i}(1-2^{-m})^{-1}(1-2^{-m-1})^{-1},\ldots\big).$$

5. Generalization to ℓ^m-cyclic function fields

In this section we consider ℓ^m-cyclic extensions F of k and the following question as in [G6] : how likely is $\lambda_2^+(\mathrm{F}) = 0, \lambda_2^+(\mathrm{F}) = 1, \lambda_2^+(\mathrm{F}) = 2, \ldots$? When $m = 1$, its answer is already obtained in §4. So we assume $m \geq 2$. Assume that we are given integers $m_1, \ldots, m_t$ such that $m = m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$. Let Δ be the abelian group of type $(\ell^{m_2}, \ldots, \ell^{m_t})$. (When $t = 1$, we let Δ be the trivial group.)

Assume first that $r > 1$, that is $\ell \nmid q - 1$. Write $\mathbf{A}(\Delta)$ for the set of all F as above such that the narrow genus group $\mathcal{C}l^+(\mathrm{F})_\ell / \mathcal{C}l^+(\mathrm{F})_\ell^{1-\sigma}$ is isomorphic to Δ, and

$$\mathbf{A}(\Delta)_n := \{\mathrm{F} \in \mathbf{A}(\Delta) : \deg(cond(\mathrm{F})) = n\}, \tag{5.1}$$

$$\mathbf{A}_e(\Delta) := \{\mathrm{F} \in \mathbf{A}(\Delta) : \lambda_2^+(\mathrm{F}) = e\}, \tag{5.2}$$

$$\mathbf{A}_e(\Delta)_n := \mathbf{A}_e(\Delta) \cap \mathbf{A}(\Delta)_n. \tag{5.3}$$

Then we define the density $d_e(\Delta)$ of $\mathbf{A}_e(\Delta)$ in $\mathbf{A}(\Delta)$ by

$$d_e(\Delta) := \lim_{n\to\infty} \frac{|\mathbf{A}_e(\Delta)_{rn}|}{|\mathbf{A}(\Delta)_{rn}|}. \tag{5.4}$$

It is easy to see that for any ordering (m_{j_i}) of $m_1, \ldots, m_t$ and monic irreducible polynomials $P_1, \ldots, P_t$ with $q^{\deg P_i} \equiv 1 \bmod \ell^{m_{j_i}}$, there are

$$\frac{\prod_{i=1}^t (\ell^{m_{j_i}} - \ell^{m_{j_i}-1})}{(\ell^m - \ell^{m-1})} = \prod_{i=2}^t (\ell^{m_i} - \ell^{m_i-1})$$

distinct fields F in $\mathbf{A}(\Delta)$ such that the conductor of F is $P_1 \cdots P_t$ and each P_i has the ramification index $\ell^{m_{j_i}}$ in F. So we have

$$|\mathbf{A}(\Delta)_{rn}| \sim \left[\prod_{i=2}^t (\ell^{m_i} - \ell^{m_i-1})\right] \left(\sum_{(m_{j_i})} \sum_{\substack{\deg(P_1\cdots P_t)=rn \\ q^{\deg P_i}\equiv 1 \bmod \ell^{m_{j_i}}}}^{(m_{j_i})} 1\right), \tag{5.5}$$

where $\sum_{(m_{j_i})}$ denotes a sum over all distinguishable orderings of $m_1, \ldots, m_t$, and $\sum^{(m_{j_i})}$ is a sum for a fixed reordering (m_{j_i}). For any positive integer k, write r_k for the smallest positive integer such that $\ell^k | q^{r_k} - 1$. Then for any monic irreducible polynomial P in $\mathbb{A}$, we have $q^{\deg P} \equiv 1 \bmod \ell^k$ if and only if $r_k | \deg P$. Following the method of [Kn, §9], we have

$$\sum_{\substack{\deg(P_1\cdots P_t)=rn \\ q^{\deg P_i}\equiv 1 \bmod \ell^{m_{j_i}}}}^{(m_{j_i})} 1 = \sum_{\substack{\deg(P_1\cdots P_t)=rn \\ r_{m_{j_i}} | \deg P_i}}^{(m_{j_i})} 1 \sim \frac{q^{rn}(\log n)^{t-1}}{(t-1)!(r_{m_1}\cdots r_{m_t})n}. \tag{5.6}$$

Let $v_w = |\{m_i : m_i = w\}|$ for $1 \leq w \leq m$. Since there are $\frac{t!}{(v_1!)\cdots(v_m!)}$ distinguishable orderings (m_{j_i}) of $m_1, \ldots, m_t$, by (5.5) and (5.6), we have

$$|\mathbf{A}(\Delta)_{rn}| \sim \frac{t\prod_{i=2}^t (\ell^{m_i} - \ell^{m_i-1})}{(r_{m_1}\cdots r_{m_t})(v_1!)\cdots(v_m!)} \frac{q^{rn}(\log n)^{t-1}}{n}. \tag{5.7}$$

Now we are going to obtain an asymptotic formula for $\mathbf{A}_e(\Delta)_{rn}$. Following the arguments in [F, §5, Theorem 5.3], one can associate a $t \times (t-1)$ matrix $\bar{M}'_{\mathrm{F}}$ to F such that $\lambda_2^+(\mathrm{F}) = t - 1 - \mathrm{rank}(\bar{M}'_{\mathrm{F}})$. Moreover, as in [G6, §2], one can replace the matrix $\bar{M}'_{\mathrm{F}}$ with a $t \times t$ matrix $\bar{M}_{\mathrm{F}}$ such that $\mathrm{rank}(\bar{M}'_{\mathrm{F}}) = \mathrm{rank}(\bar{M}_{\mathrm{F}})$. Especially, if $\mathrm{F} \in \mathbf{A}_e(\Delta)$, then the matrix $\bar{M}_{\mathrm{F}}$ has rank $t-1-e$. Then $|A_e(\Delta)_{rn}|$ can be estimated as

$$|\mathbf{A}_e(\Delta)_{rn}| \sim \sum_{\substack{\Gamma \\ \mathrm{rank}(\Gamma)=t-1-e}} \sum_{(m_{j_i})} \sum_{\substack{\deg(P_1\cdots P_t)=rn \\ r_{m_{j_i}} \mid \deg P_i}}^{(m_{j_i})} \sum_{\substack{\mathrm{F} \\ cond(\mathrm{F})=P_1\cdots P_t}} \delta_\Gamma, \tag{5.8}$$

where the first sum is over all $t \times t$ matrices Γ over $\mathbb{F}_\ell$ with rank $t-1-e$. The fourth sum runs over all $\mathrm{F} \in \mathbf{A}(\Delta)$ with conductor $P_1 \cdots P_t$ such that each P_i has ramification index $\ell^{m_{j_i}}$, and $\delta_\Gamma = 1$ if $\bar{M}_{\mathrm{F}} = \Gamma$ and $\delta_\Gamma = 0$ otherwise. If the ordering (m_{j_i}) has $m_{j_i} = m_i$ for $1 \le i \le t$, then $\bar{M}_{\mathrm{F}}$ has the following form:

$$M_{\mathrm{F}} = \begin{pmatrix} M_1 & M_2 \\ O & D \end{pmatrix} \tag{5.9}$$

where M_1 is a $v_m \times v_m$ matrix over $\mathbb{F}_\ell$ with zero row sums, M_2 is a $v_m \times (t - v_m)$ matrix over $\mathbb{F}_\ell$, O is the $(t - v_m) \times v_m$ zero matrix and D is a $(t - v_m) \times (t - v_m)$ diagonal matrix.

Let Γ be a $t \times t$ matrix over $\mathbb{F}_\ell$ such that Γ has the same form as the matrix on the right hand side of (5.9), and let

$$N(\Gamma) = \sum_{\substack{\deg(P_1\cdots P_t)=rn \\ r_{m_i} \mid \deg P_i}} \sum_{\substack{\mathrm{F} \\ cond(\mathrm{F})=P_1\cdots P_t}} \delta_\Gamma,$$

where $\delta_\Gamma = 1$ if $\bar{M}_{\mathrm{F}} = \Gamma$ and $\delta_\Gamma = 0$ otherwise. Following the idea of [G6, §2] and adopting the similar method as in §3.1, we get

Proposition 5.1. *We have*

$$N(\Gamma) \sim \frac{(\ell^m - \ell^{m-1})^{v_m - 1} \prod_{i=v_m+1}^{t} (\ell^{m_i} - \ell^{m_i - 1})}{(t-1)!(r_{m_1} \cdots r_{m_t}) \ell^{v_m(t-1)+t-v_m}} \frac{q^{rn}(\log n)^{t-1}}{n},$$

and so

$$|\mathbf{A}_e(\Delta)_{rn}| \sim \frac{tN(t, v_m, t-1-e)(\ell^m - \ell^{m-1})^{v_m-1} \prod_{i=v_m+1}^{t} (\ell^{m_i} - \ell^{m_i-1})}{(r_{m_1} \cdots r_{m_t})(v_1!) \cdots (v_n!) \ell^{v_m(t-1)+t-v_m}} \times \frac{q^{rn}(\log n)^{t-1}}{n}, \tag{5.10}$$

where $N(t, v_m, t-1-e)$ denote the number of Γ's as above with $\mathrm{rank}(\Gamma) = t-1-e$.

Finally, by (5.7) and (5.10), we have

$$d_e(\Delta) = \frac{N(t, v_m, t-1-e)}{\ell^{v_m(t-1)+t-v_m}} \quad \text{for } 0 \le e \le t-1. \tag{5.11}$$

We note that the number $N(t, v_m, t-1-e)$ can be computed as in Lemma 2.4 and the remark following it in [G6].

Let $\mathbf{B}_t$ be the set of all ℓ^m-cyclic extensions F of k such that t finite primes ramify in F/k, and

$$\mathbf{B}_{t;n} := \{\mathrm{F} \in \mathbf{B}_t : \deg(cond(\mathrm{F})) = n\}, \tag{5.12}$$

$$\mathbf{B}_{t,e} := \{\mathrm{F} \in \mathbf{B}_t : \lambda_2^+(\mathrm{F}) = e\}, \tag{5.13}$$

$$\mathbf{B}_{t,e;n} := \mathbf{B}_{t,e} \cap \mathbf{B}_{t;n}. \tag{5.14}$$

Then as in [G6] we see that the density $d_{t,e} := \lim_{n\to\infty} \frac{|\mathbf{B}_{t,e;rn}|}{|\mathbf{B}_{t;rn}|}$ is given by

$$d_{t,e} = \frac{\sum_{u=1}^{t} \frac{N(t,u,t-1-e)}{\ell^{u(t-1)+t-u}} \binom{t}{u} \frac{(m-1)^{t-u}}{m^t}}{1-(\frac{m-1}{m})^t}, \tag{5.15}$$

and its limit $d_{\infty,e} := \lim_{t\to\infty} d_{t,e} = 0$.

Now suppose that $r = 1$. There are many cases to consider. Let $\ell^a = (\ell^m, q-1)$. For each $b = 0, 1, \ldots, a$, we have to consider ℓ^m-cyclic extensions F whose ramification index at ∞ is ℓ^b. Let p_b be the asymptotic probability of ℓ^m-cyclic extensions F of k with ramification index at ∞ to be ℓ^b.

Write $\mathbf{A}^{(b)}(\Delta)$ for the set of all ℓ^m-cyclic extensions F of k such that the ramification index at ∞ is ℓ^b and the narrow genus group $\mathcal{C}l^+(\mathrm{F})_\ell/\mathcal{C}l^+(\mathrm{F})_\ell^{1-\sigma}$ is isomorphic to Δ. Define $\mathbf{A}^{(b)}(\Delta)_n, \mathbf{A}_e^{(b)}(\Delta)$ and $\mathbf{A}_e^{(b)}(\Delta)_n$ similarly as in (5.1), (5.2) and (5.3), respectively. Then the analog of (5.7) is

$$|\mathbf{A}^{(b)}(\Delta)_n| \sim \frac{p_b t \prod_{i=1}^{t}(\ell^{m_i} - \ell^{m_i-1})}{(r_{m_1}\cdots r_{m_t})(v_1!)\cdots(v_m!)(\ell^m - \ell^{m-1})} \frac{q^n(\log n)^{t-1}}{n}, \tag{5.16}$$

and if $\ell > 2$, the analog of (5.10) is

$$|\mathbf{A}_e^{(b)}(\Delta)_n| \sim \frac{p_b t N(t, v_m, t-1-e)(\ell^m - \ell^{m-1})^{v_m-1} \prod_{i=v_m+1}^{t}(\ell^{m_i} - \ell^{m_i-1})}{(r_{m_1}\cdots r_{m_t})(v_1!)\cdots(v_n!)\ell^{v_m(t-1)+t-v_m}} \times \frac{q^n(\log n)^{t-1}}{n}. \tag{5.17}$$

When $\ell = 2$, as in [G6, §4], the analog of (5.9) is

$$M_\mathrm{F} = \begin{pmatrix} M_1 & M_2 \\ O & D \end{pmatrix} \tag{5.18}$$

where M_1 is a symmetric $v_m \times v_m$ matrix over $\mathbb{F}_2$ with zero row sums, M_2 is a $v_m \times (t - v_m)$ matrix over $\mathbb{F}_2$, O is the $(t - v_m) \times v_m$ zero matrix and D is the $(t - v_m) \times (t - v_m)$ diagonal matrix with each diagonal entry equal to the sum of the entries in the corresponding column of M_2. Let $N'(t, u, s)$ denote the number of matrices Γ of the form specified on the right side of (5.18) such that rank$(\Gamma) = s$, where $0 \le s \le t-1$. Then the analog of (5.10) is

$$|\mathbf{A}_e^{(b)}(\Delta)_n| \sim \frac{p_b t N'(t, u, t-1-e)(\ell^m - \ell^{m-1})^{v_m-1} \prod_{i=v_m+1}^{t}(\ell^{m_i} - \ell^{m_i-1})}{(r_{m_1}\cdots r_{m_t})(v_1!)\cdots(v_n!)\ell^{\frac{v_m(v_m-1)}{2}+v_m(t-v_m)}} \times \frac{q^n(\log n)^{t-1}}{n}. \tag{5.19}$$

Thus the density $d_e^{(b)}(\Delta) := \lim_{n\to\infty} \frac{|\mathbf{A}_e^{(b)}(\Delta)_n|}{|\mathbf{A}^{(b)}(\Delta)_n|}$ is given by the formula (5.11) if $\ell > 2$, and if $\ell = 2$,

$$d_e^{(b)}(\Delta) = \frac{N'(t, v_m, t-1-e)}{\ell^{\frac{v_m(v_m-1)}{2}+v_m(t-v_m)}}.$$

Write $\mathbf{B}_t^{(b)}$ for the set of all ℓ^m-cyclic extensions F of k such that the ramification index at ∞ is ℓ^n and t finite primes ramify in F/k. Define $\mathbf{B}_{t;n}^{(b)}, \mathbf{B}_{t,e}^{(b)}$ and $\mathbf{B}_{t,e;n}^{(b)}$ similarly as in (5.12), (5.13) and (5.14), respectively. Then we see that the density $d_{t,e}^{(b)} := \lim_{n\to\infty} \frac{|\mathbf{B}_{t,e;n}^{(b)}|}{|\mathbf{B}_{t;n}^{(b)}|}$ is given by the formula (5.15) if $\ell > 2$, and if $\ell = 2$,

$$d_{t,e}^{(b)} = \frac{\sum_{u=1}^{t} \frac{N'(t,u,t-1-e)}{\ell^{\frac{u(u-1)}{2}+u(t-u)}} \binom{t}{u} \frac{(m-1)^{t-u}}{m^t}}{1-(\frac{m-1}{m})^t},$$

and its limit $d_{\infty,e}^{(b)} := \lim_{t\to\infty} d_{t,e}^{(b)} = 0$.

Remark 5.2. Since $G = \mathrm{Gal}(\mathrm{F}/\mathrm{k})$ is cyclic of order ℓ^m, there is a unique subgroup H of order ℓ^a, and the inertia group G_∞ at ∞ is contained in H. Let $\mathrm{F}_1 = \mathrm{F}^H$. Then ∞ splits completely in F_1, and F is a cyclic extension of F_1 of order ℓ^a. Then $\mathrm{F} = \mathrm{F}_1(\sqrt[\ell^a]{\alpha})$ for some $\alpha \in \mathcal{O}_{\mathrm{F}_1}$. Thus the asymptotic probability p_b seems to be $\frac{\ell^b-\ell^{b-1}}{\ell^a}$.

References

[A] B. Angles, *Class field towers of global function fields.* Drinfeld modules, modular schemes and applications. World Scientific (1997), 261-271.

[BK] S. Bae and J. Koo, *Genus theory for function fields.* J. Austral. MAth. Soc. (Ser. A) **60** (1996), 301-310.

[F] A. Frohlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields.* American Mathematical Society, Providence, R.I. (1983).

[G1] F. Gerth, *Number fields with prescribed ℓ-class groups.* Proc. AMS **49** (1975), 284-288.

[G2] ———, *Asymptotic behavior of number fields with prescribed ℓ-class numbers.* J. Number Theory **17** (1983), 191-203.

[G3] ———, *Counting certain number fields with prescribed ℓ-class numbers.* J. reine angew. Math. **337** (1982), 195-207.

[G4] ———, *An application of matrices over finite fields to algebraic number theory.* Math. Comp. **41** (1983), 229-234.

[G5] ———, *The 4-class ranks of quadratic fields.* Invent. Math. **77** (1984), 489-515.

[G6] ———, *Densities for certain ℓ-ranks in cyclic fields of degree ℓ^n.* Compos. Math. **60** (1986), 295-322.

[G7] ———, *Densities for ranks of certain parts of p-class groups.* Proc. Amer. Math. Soc. **99** (1987), 1-8.

[Kn] J. Knopfmacher, *Analytic arithmetic of algebraic function fields.* Marcel Decker Inc., New York-Basel (1979).

[R] M. Rosen, *Number theory in function fields.* GTM vol. 210, Springer (2001).

[W] C. Wittman, *ℓ-Class groups of cyclic function fields of degree ℓ.* Finite fields and their applications **13** (2007), 327-347.

Department of Mathematics, KAIST, Taejon 305-701, Korea
E-mail address: `shbae@kaist.ac.kr`

Department of Mathematics Education, Chungbuk National University, Cheongju 361-763, Korea
E-mail address: `hyjung@chungbuk.ac.kr`