J. Korean Math. Soc. **49** (2012), No. 1, pp. 49–67
http://dx.doi.org/10.4134/JKMS.2012.49.1.049

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 be a prime number. In the 1980s 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 [5], 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 [6], 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^s 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 [8], 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 [10] for an arbitrary prime number ℓ. Similar results for ℓ^n-cyclic extensions of $\mathbb{Q}$ with prescribed (narrow) genus groups are given in [9].

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

Received August 10, 2010; Revised July 11, 2011.
2010 *Mathematics Subject Classification.* 11R58, 11R29, 11R45.
Key words and phrases. class groups, function fields.
The first author was supported by SRC program (ASARC R11-2007-035-01001-0).
The second author was supported by the Korea Science and Engineering Foundation(KOSEF) grant funded by the Korea government(MEST) (No. 2009-0071789).

positive integer such that $\ell \mid q^r - 1$. 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 [11] and [12]. In §2 we recall the genus theory for function fields [2] and extend some results of Wittmann [13] 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 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 [11] and [12].

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

$$p(n) = \frac{q^n}{n} + O\Big(\frac{q^{n/2}}{n}\Big) \quad \text{([11, Chap. 8], [12, Theorem 2.2])}. \tag{1.1}$$

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

$$p(n,k) = \frac{q^n(\log n)^{k-1}}{(k-1)!n} + O\Big(\frac{q^n(\log n)^{k-2}}{n}\Big) \quad \text{([11, Theorem 9.9])}. \tag{1.2}$$

- $P_r(rn,k)$:= 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 [11, §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

$$p(n,A,M) = \frac{q^n}{\phi(M)n} + O\Big(\frac{q^{n/2}}{n}\Big) \quad \text{([12, Theorem 4.8])}, \tag{1.4}$$

  where $\phi(M) = |(\mathbb{A}/M\mathbb{A})^\times|$.

Also, for a nontrivial Dirichlet character χ, we have

$$\sum_{P,\,\deg P=n} \chi(P) = O\Big(\frac{q^{n/2}}{n}\Big) \quad ([12, \S4\ (4), (5)]). \tag{1.5}$$

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

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

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

One more asymptotic formula which will be used later is

$$\sum_{m_1+\cdots+m_k=n} \frac{1}{m_1\cdots m_k} \sim \frac{k(\log n)^{k-1}}{n}. \tag{1.12}$$

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 $\Omega = \mathrm{k}_\infty(\sqrt[q-1]{-1/T})$. We only consider those function fields which can be embedded into Ω. For a monic polynomial M of $\mathbb{A}$, k_M denotes the cyclotomic function field of conductor M (see [12, §12]). Any abelian extension F of k inside Ω 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 $N = N_F$ for the conductor of F. Then N must be square-free since F/k is tamely ramified and for each prime divisor P of N, $\deg P$ is divisible by r, since the ramification index ℓ

divides $q^{\deg P} - 1$, the order of the multiplicative group of the residue field of P. 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 H_F for the Hilbert class field of F. Then the 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. Let $\mathcal{C}l(F)$ be the ideal class group of the integral closure $\mathcal{O}_F$ of $\mathbb{A}$ in F, and $\mathcal{C}l(F)_\ell$ be its Sylow ℓ-subgroup. Let σ be a fixed generator of $G = \mathrm{Gal}(F/\mathrm{k})$ and

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

It is known that ([2, §2])

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

It is well-known that $\mathcal{C}l(F)_\ell^G$ and $\mathcal{C}l(F)_\ell/\mathcal{C}l(F)_\ell^{\sigma-1}$ are elementary abelian groups 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 H_F^+ of F to be the maximal abelian extension of F in Ω, 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 $sgn_v : F_v \to \mathbb{F}_q$ by $sgn_v(x) = sgn(N_v(x))$, where sgn is the usual sign map on k_∞. An element $x \in F$ is called *totally positive* if $sgn_v(x) = 1$ for any v lying over ∞. Denote by F_+ the set of all totally positive elements of F. The narrow ideal class group $\mathcal{C}l^+(F)$ of F is defined to be the quotient group of fractional ideals modulo principal fractional ideals generated by 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 [2] for details on the genus theory of function fields. Let

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

Note that if $r > 1$, then $\mathcal{C}l^+(F)_\ell = \mathcal{C}l(F)_\ell$ and so $\lambda_i^+(F) = \lambda_i(F)$. We will use the following lemmas proved in [13]. The narrow case can be proved by a similar method as in [13].

Lemma 2.1 ([13, Theorem 2.1])**.** *Let F be as above.*

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

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

Lemma 2.2 ([13, Corollary 2.3, 2.4])**.** *Let F be as above.*

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

(ii) *If $r = 1$, then*

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

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

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

where $\mathfrak{a}^{\sigma-1} = \alpha \mathcal{O}_F$ and $N_{F/\mathrm{k}}(\alpha) \in \mathbb{F}_q^* \setminus (\mathbb{F}_q^*)^\ell$.

(iii) *If $r = 1$ and ∞ splits completely, then $\mathcal{C}l^+(F)_\ell^G$ is generated by $[\mathfrak{p}_1]_+$, $\ldots, [\mathfrak{p}_t]_+$ and $[\mathfrak{a}]_+$, where $\mathfrak{a}^{\sigma-1} = \alpha\mathcal{O}_F$ and $N_{F/\mathrm{k}}(\alpha) \in \mathbb{F}_q^{*\ell} \setminus \mathbb{F}_q^{*\ell^2}$. In particular, if $\ell || (q-1)$, then $\mathcal{C}l^+(F)_\ell^G$ is generated by $[\mathfrak{p}_1]_+, \ldots, [\mathfrak{p}_t]_+$.*

Proof. We only need to prove (iii). Recall that a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_F$ is said to be ambiguous if it is invariant under the G-action, i.e., $\mathfrak{a}^\sigma = \mathfrak{a}$. Any ideal class in $\mathcal{C}l(F)^G$ or $\mathcal{C}l^+(F)^G$ is called an ambiguous ideal class. Let $\mathfrak{a}$ be an ideal representing an ambiguous ideal class. Then $\mathfrak{a}^{\sigma-1} = \alpha\mathcal{O}_F$ with $\alpha \in F_+$. Then $N_{F/\mathrm{k}}(\alpha) \in \mathbb{F}_q^{*\ell}$, that is, $N_{F/\mathrm{k}}(\alpha) = \eta^{-\ell}$, and so $N_{F/\mathrm{k}}(\alpha\eta) = 1$ for some $\eta \in \mathbb{F}_q^*$. By Hilbert Theorem 90, there exists $\beta \in F$ such that $\alpha\eta = \beta^\sigma/\beta$. Then, since

$$\mathfrak{a}^{\sigma-1} = (\alpha\eta) = (\beta^\sigma/\beta),$$

$\beta^{-1}\mathfrak{a}$ is an ambiguous ideal. Therefore, $[\mathfrak{a}]_+ \in \langle [\mathfrak{p}_1]_+, \ldots, [\mathfrak{p}_t]_+ \rangle$ if and only if $\beta \in F_+$, which is equivalent to $\alpha\eta \in F_+$. But since $\alpha \in F_+$, this is equivalent to $\eta \in \mathbb{F}_q^{*\ell}$.

We know from [13, §2] that

$$\langle [\mathfrak{p}_1], \ldots, [\mathfrak{p}_t] \rangle = I(F)^G P(F)/P(F) = I(F)^G / I(F)^G \cap P(F)$$

has ℓ-rank at least $t-2$. Thus $\langle [\mathfrak{p}_1]_+, \ldots, [\mathfrak{p}_t]_+ \rangle = I(F)^G P(F_+)/P(F_+) = I(F)^G/I(F)^G \cap P(F_+)$ has ℓ-rank at least $t-2$. It is not hard to see that the ℓ-rank of $\mathcal{C}l^+(F)_\ell^G$ is $t-1$, thus we get the result. □

Remark 2.3. In the number field case, since the size of the group of units in $\mathbb{Z}$ is 2, there does not exist such an ideal $\mathfrak{a}$ as in Lemma 2.2(iii).

Suppose first that $r = 1$. In this case $F = \mathrm{k}(\sqrt[\ell]{D})$, where $D = aP_1^{e_1} \cdots P_t^{e_t}$ with $1 \le e_i < \ell$ and $a \in \mathbb{F}_q^*$. We will determine a. From [1, 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 2.4 ([13, Theorem 2.5])**.** *Let $F = \mathrm{k}(\sqrt[\ell]{D})$ be as above.*

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

(ii) *If* $\ell \nmid \deg D$ *or* $\ell \mid \deg P_i$ *for all* i, *then*

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

(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*

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

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 $M_F = (m_{ij})$ 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

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

If $\mathfrak{a}$ is as in Lemma 2.2(ii) or (iii), let $N_{F/\mathrm{k}}(\mathfrak{a}) = (A)$ for some $A \in \mathbb{A}$. Then m_{i0} is defined to be

$$\eta^{m_{i0}} = \left(\frac{P_i}{A}\right)_\ell.$$

Let $M_F := (m_{ij})$, which is a $t \times t$ or $t \times (t+1)$ matrix with entries in $\mathbb{F}_\ell$ according to the existence of $\mathfrak{a}$ as in Lemma 2.2. Then it can be shown (cf. [13, §3]) that

$$\lambda_2(F) = \lambda_1(F) - \mathrm{rank}(M_F), \text{ when } \infty \text{ ramifies in } F$$

and

$$\lambda_2^+(F) = \lambda_1^+(F) - \mathrm{rank}(M_F), \text{ when } \infty \text{ splits in } F.$$

In the case (iii) of Proposition 2.4, a $(t-1) \times t$ matrix M'_F is defined in [13, §3] and it was shown that

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

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 $\tilde{M}_F$ over $\mathbb{F}_\ell$ is defined in [13, §4] and it is shown that

$$\lambda_2(F) = t - 1 - \mathrm{rank}(\tilde{M}_F).$$

Let $\mathrm{k}' = \mathbb{F}_{q^r} \cdot \mathrm{k}$ and $F' = \mathbb{F}_{q^r} \cdot F$. Let the notations be as in [13, §4]. By identifying $\mathrm{Gal}(F'/\mathrm{k}') \cong \mathrm{Gal}(F/\mathrm{k}) \cong \mathbb{F}_\ell$, we have

$$\Big(\frac{Q_i}{P_j}\Big)_\ell = \Big(\frac{Q_i, F'/\mathrm{k}'}{(P_j)}\Big)$$

and

$$\Big(\frac{Q_i, F'/\mathrm{k}'}{(P_j)}\Big)\Big|_F = \Big(\frac{P_i, F/\mathrm{k}}{(P_j)}\Big).$$

Thus the matrix $\tilde{M}_F$ is essentially the same as the matrix M_3 defined in [6, §2]. We let M_F be M_3. The product formula for norm residue symbol implies that the sum of each column of M_F is zero.

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

Let F be a cyclic extension of k of degree ℓ with conductor $N = P_1 \cdots P_s$. Let H_i be the unique cyclic extension of k of degree ℓ with conductor P_i. Let $\mathrm{K}_i = F \cdot \mathrm{H}_i$ and $\mathrm{K} = \mathrm{K}_1 \cdots \mathrm{K}_t$.

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 $|\mathcal{C}l(F)_\ell| = \ell^s$ and with conductor N of degree n,
- $M_{s,n}$:= the number of ℓ-cyclic extensions F of k with $|\mathcal{C}l(F)_\ell| = \ell^{s-1}$ 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 $P_1, \ldots, P_{m-2}$ but an ℓ-th power nonresidue modulo P_{m-1}.

It can be shown, as in Theorem 1 of [4], that if F is an ℓ-cyclic extension of k satisfying the conditions to define $G_{s,n}$, then the ℓ-class group of F is an elementary abelian ℓ-group of rank $s-1$. Hence $M_{s,n} \geq G_{s,n}$.

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

(3.1)

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

where ζ is a primitive ℓ-th root of unity. Since $\sum_{k=0}^{\ell-1} \chi_{P_j}^k(P_m) = \ell$ or 0, depending on P_m is ℓ-th power residue modulo P_j or not, we have

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

where the sum is over the distinct primes $P_1,\dots,P_t$ 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, $1\le i\le t-1$ with $\deg P_{i-1}\le\deg P_i\le y_i$ and $r\mid\deg P_i$. Then

$$M_{t,rn}\ge G_{t,rn}\ge A_{t,rn}. \tag{3.2}$$

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 $J=(j_1,\dots,j_{t-1})\ne(0,\dots,0)$. 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 $k_i\le y_i$, 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 $y=y_t=2^t\sqrt{n}$,

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

Therefore

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

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

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

Since $M_{s,rn} = O(p_r(rn,s))$, we have, from (1.4) and (3.2),

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

If an ℓ-extension F of k has $|\mathcal{C}l(F)_\ell| = \ell^s$, then at most $s+1$ primes can be ramified. Now the rest of the argument to prove Theorem 1 in [5] works here and we get

Theorem 3.1.

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

We will compute $M_{s+1,rn}$. As in [6, §2, §3], one can see easily that the ℓ-cyclic extension F has ℓ-class number ℓ^s precisely when $\operatorname{rank}(M_F) = s$, and that the number of distinct $(s+1)\times(s+1)$ matrices Γ over $\mathbb{F}_\ell$ such that $\operatorname{rank}(\Gamma) = s$ and such that $\Gamma = M_F$ for some field F is

$$\ell^{\frac{s(s-1)}{2}}(\ell-1)^s \prod_{i=1}^{s}(\ell^i + \cdots + \ell + 1). \tag{3.3}$$

Note that $\Gamma = M_F$ if and only if the sum of each column of Γ is 0 by the product formula of Hilbert symbols.

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 $\mathrm{k}' = \mathbb{F}_{q^r}\cdot \mathrm{k}$ and $\mathrm{L}_i = \mathrm{k}'\cdot \mathrm{H}_i$, where H_i is the ℓ-cyclic extension of k with conductor P_i. Then L_i/k' is a Kummer extension $\mathrm{L}_i = \mathrm{k}'(\sqrt[\ell]{\mu_i})$ for some $\mu_i \in \mathrm{k}'$. Then $\mathrm{k}\cdot F = \mathrm{k}'(\sqrt[\ell]{\mu})$ with $\mu = \mu_1^{e_1}\cdots\mu_{s+1}^{e_{s+1}}$. Let $\mathrm{L}_i' = \mathrm{k}'(\sqrt[\ell]{P_i})$. Define, for a prime P of degree divisible by r, $\lambda_i(\mathfrak{p}_j)$ and $\omega_i(\mathfrak{p}_j)$ as follows;

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

where $\mathfrak{p}$ is a prime of k' lying over P. Let $\delta_i(j,k;u,v)(P)=1$ if $(\lambda_i(P)^j,\omega_i(P)^k) = (\zeta^u,\zeta^v)$, and 0 otherwise.

Lemma 3.2. *We have, for $j=1,\dots,\ell-1$,*

$$\sum_{\deg P=rm}\sum_{k=1}^{\ell-1}\delta_i(j,k;u,v)(P)\sim\frac{\ell-1}{\ell^2}\frac{q^{rm}}{rm}. \tag{3.4}$$

Proof. We may assume $j=1$. The probability for a prime P to satisfy $(\lambda_i(P),\omega_i(P))=(\zeta^u,\zeta^v)$ is $\frac{1}{\ell^2}$. When $v=0$, then $\omega_i(P)^k=1=\zeta^0$ for any $k=1,\dots,\ell-1$. Hence the probability for a prime P to satisfy $(\lambda_i(P),\omega_i(P)^k)=(\zeta^u,\zeta^0)$ for some $k=1,\dots,\ell-1$ is $\frac{\ell-1}{\ell^2}$. When $v\neq 0$, then, for $\omega_i(P)\neq 1$, there exists a unique $k=1,\dots,\ell-1$ such that $\omega_i(P)^k=\zeta^v$. Thus the probability for a prime P to satisfy $(\lambda_i(P),\omega_i(P)^k)=(\zeta^u,\zeta^v)$ for some $k=1,\dots,\ell-1$ is again $\frac{\ell-1}{\ell^2}$. Then the result follows from the equation (1.1). □

Note the difference of (3.4) from the formula in [6, p. 200]. In the classical case the condition $p\equiv 1 \bmod \ell$ is imposed instead of the condition that $\deg P_i$ is divisible by r, and the probability for a prime to satisfy $p\equiv 1 \bmod \ell$ is $\frac{1}{\ell-1}$ by Dirichlet theorem on arithmetic progression. We repeat the process to get

$$\sum_{\deg P_w=rm}\sum_{k=1}^{\ell-1}\prod_{i=1}^{w-1}\delta_i(j,k;u,v)(P_w)\sim\frac{\ell-1}{\ell^{2(w-1)}}\frac{q^{rm}}{rm}. \tag{3.5}$$

Theorem 3.3. *We have, for $(s+1)\times(s+1)$ matrix Γ such that the sum of each column is 0,*

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

and so

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

Proof. (Sketch of proof) As in §4 of [6], we have

$$N(\Gamma)=\frac{1}{(s+1)!}\sum_{m_1+\cdots+m_{s+1}=n}\sum_{\deg P_1=rm_1}\sum_{\deg P_2=rm_2}Y_2\cdots\sum_{\deg P_s=rm_s}Y_s\sum_{\deg P_{s+1}=rm_{s+1}}Y_{s+1},$$

where

$$Y_w=\sum_{k=1}^{\ell-1}\prod_{i=1}^{w-1}\delta_i(j,k;u,v)(P_w)$$

for $w=2,\dots,s+1$. Then using the equation (3.5), we have

$$\begin{aligned} N(\Gamma) &\sim \frac{1}{(s+1)!}\frac{(\ell-1)^s}{\ell^{s^2+s}}\frac{q^{rn}}{r^{s+1}}\sum_{m_1+\cdots+m_{s+1}=n}\frac{1}{m_1\cdots m_{s+1}} \\ &\sim \frac{(\ell-1)^s}{s!r^{s+1}\ell^{s^2+s}}\frac{q^{rn}(\log n)^s}{n}, \end{aligned}$$

by the equation (1.12). □

Remark 3.4. (1) One can do the error estimate as in [6] using (1.5) to get the error term $o(\frac{q^{rn}(\log n)^s}{n})$. But it is not necessary for our purpose.

(2) In the proof of [6, Lemma 3], also in our proof here, the condition that Γ has rank s is not necessary to get the estimate $N(\Gamma)$. Thus the asymptotic formula for $N(\Gamma)$ works for any Γ such that the sum of each column is 0. This will be used in the computation in §4.

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 $|\mathcal{C}l(F)_\ell| = \ell^s$. 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 $|\mathcal{C}l(F)_\ell| = \ell^s$,
- $N_{R,s,n}$:= the number of real ℓ-cyclic extensions F of k with conductor N of degree n and $|\mathcal{C}l(F)_\ell| = \ell^s$,
- $M_{I,t,n}$:= 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 $|\mathcal{C}l(F)_\ell| = \ell^{t-1}$,
- $M_{R,t,n}$:= 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 $|\mathcal{C}l(F)_\ell| = \ell^{t-2}$.
- For $\ell|n$, $M'_{t,n}$:= the number of ℓ-cyclic extensions F of conductor N of degree n, such that N has exactly t prime factors, all having degrees divisible by ℓ and $|\mathcal{C}l(F)_\ell| = \ell^{t-1}$.

In this case $F = \mathrm{k}(\sqrt[\ell]{D})$ 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 $F \subseteq \mathrm{k}_N$, 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 $(e_1, \dots, e_t) = (1, \dots, 1)$. In this case whether F is real or imaginary depends only on the parity of $\deg N$. One can follow almost the same process to prove Theorem 3.1 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

$$N_{R,s,n} = \begin{cases} M_{R,s+2,n} + O(\frac{M_{R,s+2,n}}{\log n}) & \text{for } \ell \nmid n, \\ M_{R,s+2,n} + M'_{s+1,n} + O(\frac{M_{R,s+2,n}}{\log n}) + O(\frac{M'_{s+1,n}}{\log n}) & \text{for } \ell|n. \end{cases}$$

But one can show as in the case $r > 1$ that $M_{R,s+2,n} \sim c\frac{q^n(\log n)^{s+1}}{n}$ for some $c > 0$ and $M'_{s+1,n} = O(\frac{q^n(\log n)^s}{n})$. Therefore,

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

Some calculation concerning this will be carried out in §4.2, where we replace $\mathcal{C}l(F)$ by $\mathcal{C}l^+(F)$.

Remark 3.5. From the equations (1.2) and (1.3), it is very likely that $M'_{s+1,n} = o(M_{R,s+2,n})$.

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

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

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

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

Note that $\mathbf{A}_{t,0;n} = M_{t,n}$ in §3.1. 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 [6, §2, §3], we see that $\lambda_2(F) = t-1-\mathrm{rank}(M_F)$. Then $|\mathbf{A}_{t,e;rn}|$ can be estimated as

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

where $\delta_{\Gamma,F} = 1$ if $M_F = \Gamma$ and $\delta_{\Gamma,F} = 0$ otherwise. It is shown in Theorem 3.3 that, for $t \times t$ matrix Γ such that the sum of each column is 0,

(4.3)

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

It is known ([7, Proposition 2.1]) that the number $N(t,t-1-e)$ of $t\times t$ matrices Γ, where the sum of each column is 0, over $\mathbb{F}_\ell$ with rank $t-1-e$ is

$$N(t,t-1-e)=\left[\prod_{j=1}^{t-1-e}(\ell^t-\ell^{j-1})\right]\sum_{\substack{k_1+\cdots+k_{t-1-e}\le e\\ \text{each } k_i\ge 0}}\Big(\prod_{s=1}^{t-1-e}\ell^{sk_s}\Big). \tag{4.4}$$

So we have, from (4.2), (4.3) and (4.4),

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

Thus

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

for $1\le e\le t-1$ and $d_{t,t-1}=\ell^{-t(t-1)}$. Let

$$d_{\infty,e}:=\lim_{t\to\infty}d_{t,e}.$$

Then we follow almost the same argument as in [10, §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

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

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

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

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

For each $N\in P(n,t)$ and $\mathbf{e}:=(1,e_1,\ldots,e_t)$ with $1\le e_i<\ell$, let

$$N^{\mathbf{e}}:=P_1^{e_1}P_2^{e_2}\cdots P_t^{e_t}.$$

Then any field in $\mathbf{A}_{t;n}$ is of the form

$$F_{N,\mathbf{e}}:=\mathrm{k}\Big(\sqrt[\ell]{(-1)^{\deg N^{\mathbf{e}}}N^{\mathbf{e}}}\Big).$$

Thus $|\mathbf{A}_{t;n}|=(\ell-1)^{t-1}p(n,t)$. Note that if $F_{N,\mathbf{e}}\in\mathbf{A}_{t,e;n}$ for some $\mathbf{e}$, then so in $F_{N,\mathbf{e}'}$ for any $\mathbf{e}'$.

From now on we assume that $\ell || (q-1)$. The general case is very hard to compute the rank of M_F because of ambiguous ideal class without containing ambiguous ideal. Consider first the case that ℓ is odd, so that $a = 1$ (See §2). It is shown in [13] that $M_F = (m_{ij})$ is given by: $m_{ij} = \left(\frac{P_i}{P_j}\right)_\ell$, 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, since $\frac{q-1}{\ell}$ is even or characteristic is 2, from the ℓ-th power reciprocity ([12, Theorem 3.3]), 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*

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

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 $r+2$.*

Suppose that we have given a total order '$<$' on the set of monic irreducible polynomials in $\mathbb{A}$. For $N, N' \in P(n,t)$, we say that N and N' are equivalent if $\left(\frac{P_j}{P_i}\right)_\ell = \left(\frac{P'_j}{P'_i}\right)_\ell$, where $N = P_1 \cdots P_t$, $P_1 < \cdots < P_t$ and $N' = P'_1 \cdots P'_t$, $P'_1 < \cdots < P'_t$. 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)

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

Note that we have $\ell^{-\frac{t^2-t}{2}}$ instead of $\ell^{-\frac{t^2+t}{2}}$ because we don't have any condition on $\deg P_i$, different from the classical case (formula (2.12) of [8]), where the condition $p_i \equiv p'_i \bmod 4$ is imposed.

Let $\tilde{N}(t-1,u)$ be the number of $(t-1)\times(t-1)$ symmetric matrices with rank u. Then one can show as in §2 of [8] that

$$|\mathbf{A}_{t,e;n}| = (\ell-1)^{t-1} \tilde{N}(t-1, t-1-e) |\mathcal{N}(N)|.$$

Then

$$d_{t,e;n} := \frac{|\mathbf{A}_{t,e;n}|}{|\mathbf{A}_{t;n}|} \sim \ell^{-\frac{t^2-t}{2}} \tilde{N}(t-1, t-1-e),$$

which is just the density $g(t,e)$ of $(t-1)\times(t-1)$ symmetric matrices with rank $t-1-e$ in the set of $(t-1)\times(t-1)$ symmetric matrices. 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 $\ell=2$. Now the rest is 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 reason for this is that the quadratic reciprocity for function field in this case is $(\frac{P_i}{P_j})(\frac{P_j}{P_i})=(-1)^{\deg P_i\deg P_j}$ in contrast with $(\frac{p_i}{p_j})(\frac{p_j}{p_i})=(-1)^{\frac{p_i-1}{2}\frac{p_j-1}{2}}$ in the classical case. Then following the same ideas to get Proposition 2.1 and Proposition 5.1 of [8], we get

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

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

and

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

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

where $N(s,d,r)$ is the number of $s\times s$ matrices $M=(m_{ij})$ over $\mathbb{F}_2$ with $m_{ij}\ne m_{ji}$ 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 $\operatorname{rank}(M)=r$, and $N'(s,d,r)$ is the number of $s\times(s+1)$ 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 $m'_{ij}\ne m'_{ji}$ 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 $\operatorname{rank}(\overline{M'})=r$. Then as in [8, §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

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

and

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

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 [9]: how likely is $\lambda_2^+(F) = 0, \lambda_2^+(F) = 1, \lambda_2^+(F) = 2, \dots$? When $m = 1$, its answer is already obtained in §4. So we assume $m \geq 2$. Assume that we are given integers $m_1, \dots, m_t$ such that $m = m_1 \geq m_2 \geq \cdots \geq m_t \geq 1$. Let Δ be the abelian group of type $(\ell^{m_2}, \dots, \ell^{m_t})$ (When $t = 1$, we let Δ be the trivial group).

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

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

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

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

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 $m_1, \dots, m_t$ and monic irreducible polynomials $P_1, \dots, P_t$ 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 ramification index $\ell^{m_{j_i}}$ in F. So we have

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

where $\sum_{(m_{j_i})}$ denotes a sum over all distinguishable orderings of $m_1, \dots, m_t$, 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 [11, §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 $\mathbf{A}_e(\Delta)_{rn}$. Assume first that $r > 1$, that is $\ell \nmid q-1$. Following the arguments in [3, §5, Theorem 5.3], one can associate a $t\times(t-1)$ matrix $\bar{M}'_F$ to F such that $\lambda_2^+(F) = t-1-\text{rank}(\bar{M}'_F)$. Moreover, as in [9, §2], one can replace the matrix $\bar{M}'_F$ with a $t\times t$ matrix $\bar{M}_F$ such that $\text{rank}(\bar{M}'_F) = \text{rank}(\bar{M}_F)$. Especially, if $F \in \mathbf{A}_e(\Delta)$, then the matrix $\bar{M}_F$ has rank $t-1-e$. Then $|A_e(\Delta)_{rn}|$ can be estimated as

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

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 $F \in \mathbf{A}(\Delta)$ with conductor $P_1\cdots P_t$ such that each P_i has ramification index $\ell^{m_{j_i}}$, and $\delta_\Gamma = 1$ if $\bar{M}_F = \Gamma$ and $\delta_\Gamma = 0$ otherwise. If the ordering (m_{j_i}) has $m_{j_i} = m_i$ for $1 \leq i \leq t$, then $\bar{M}_F$ has the following form:

$$M_F = \begin{pmatrix} M_1 & M_2 \\ O & D \end{pmatrix} \tag{5.9}$$

where M_1 is a $v_m \times v_m$ matrix over $\mathbb{F}_\ell$ in which the sum of entries in each row is zero, 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

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

where $\delta_\Gamma = 1$ if $\bar{M}_F = \Gamma$ and $\delta_\Gamma = 0$ otherwise. Following the idea of [9, §2] and adopting the similar method as in §3.1, we get:

Proposition 5.1. *We have*

$$N(\Gamma) \sim \frac{\prod_{i=2}^{t}(\ell^{m_i} - \ell^{m_i-1})}{(r_{m_1}\cdots r_{m_t})\ell^{v_m(t-1)+t-v_m}} \frac{q^{rn}(\log n)^{t-1}}{(t-1)!n},$$

and so

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

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

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

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

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 [9].

Now suppose that $r = 1$. As before we only consider the case $\ell||(q-1)$. 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

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

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

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

Then as in [9] 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 $d_{\infty,e} := \lim_{t\to\infty} d_{t,e} = 0$.

The formula (5.7) also works in this case too. As in the case of $r > 1$, we get the matrix M_F in (5.9). But in this case we need one more step, that is, multiply z_i, which is defined as in (2.12) of [9], to each ith row of M_F with $1 \leq i \leq v_m$. The resulting matrix M_F^* has the same rank as M_F and is of the form

$$M_F^* = \begin{pmatrix} M_1^* & M_2^* \\ O & D \end{pmatrix} \tag{5.16}$$

where M_1^* is a $v_m \times v_m$ symmetric matrix over $\mathbb{F}_\ell$ in which the sum of entries in a row is 0 and M_2^*, O, D are the same as before. When $\ell = 2$ as in the classical case, we do not need this step, since $z_i = 1$ in this case. The reason for the symmetricity of M_1^* follows from the ℓth power reciprocity law ([12], Theorem 3.3) for $\ell > 2$, and from the fact that $m > 1$ for $\ell = 2$. Exactly the same way as in the case $r > 1$, we obtain

$$|\mathbf{A}_e(\Delta)_n| \sim \frac{N_s(t, v_m, t-1-e) \prod_{i=2}^{t} (\ell^{m_i} - \ell^{m_i - 1})}{(r_{m_1} \cdots r_{m_t}) v_1! \cdots v_m! \ell^{\frac{v_m(v_m-1)}{2} + v_m(t-v_m)}} \frac{tq^n (\log n)^{t-1}}{n}, \tag{5.17}$$

where $N_s(t, u, s)$ denotes the number of matrices Γ of the form specified in (5.16) such that $\operatorname{rank}\Gamma = s$. The density $d_e(\Delta)$ and $d_{t,e}$ are given by

$$d_e(\Delta) = \frac{N_s(t, v_m, t-1-e)}{\ell^{\frac{v_m(v_m-1)}{2} + v_m(t-v_m)}}, \tag{5.18}$$

and

$$d_{t,e} = \left[\sum_{u=1}^{t} \frac{N_s(t,u,t-1-e)}{\ell^{\frac{u(u-1)}{2}} + u(t-u)} \binom{t}{u} \frac{(m-1)^{t-u}}{m^t} \right] \Big(1 - \big(\frac{m-1}{m}\big)^t\Big)^{-1}. \tag{5.19}$$

References

[1] B. Angles, *On Hilbert class field towers of global function fields*, Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996), 261–271, World Sci. Publ., River Edge, NJ, 1997.

[2] S. Bae and J. Koo, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60** (1996), no. 3, 301–310.

[3] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*, American Mathematical Society, Providence, RI, 1983.

[4] F. Gerth, *Number fields with prescribed ℓ-class groups*, Proc. Amer. Math. Soc. **49** (1975), 284–288.

[5] ———, *Asymptotic behavior of number fields with prescribed ℓ-class numbers*, J. Number Theory **17** (1983), no. 2, 191–203.

[6] ———, *Counting certain number fields with prescribed ℓ-class numbers*, J. Reine Angew. Math. **337** (1982), 195–207.

[7] ———, *An application of matrices over finite fields to algebraic number theory*, Math. Comp. **41** (1983), no. 163, 229–234.

[8] ———, *The* 4*-class ranks of quadratic fields*, Invent. Math. **77** (1984), no. 3, 489–515.

[9] ———, *Densities for certain ℓ-ranks in cyclic fields of degree* ℓ^n, Compositio Math. **60** (1986), no. 3, 295–322.

[10] ———, *Densities for ranks of certain parts of p-class groups*, Proc. Amer. Math. Soc. **99** (1987), no. 1, 1–8.

[11] J. Knopfmacher, *Analytic Arithmetic of Algebraic Function Fields*, Marcel Decker Inc., New York-Basel, 1979.

[12] M. Rosen, *Number Theory in Function Fields*, GTM vol. 210, Springer, 2002.

[13] C. Wittmann, *ℓ-Class groups of cyclic function fields of degree ℓ*, Finite Fields Appl. **13** (2007), no. 2, 327–347.

Sunghan Bae
Department of Mathematics
Korea Advanced Institute of Science and Technology
Daejeon 305-701, Korea
E-mail address: shbae@kaist.ac.kr

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