COMPOSITIO MATHEMATICA

JIU-KANG YU

On the moduli of quasi-canonical liftings

Compositio Mathematica, tome 96, nº 3 (1995), p. 293-321
<http://www.numdam.org/item?id=CM_1995__96_3_293_0>

Compositio Mathematica **96:** 293–321, 1995.

On the moduli of quasi-canonical liftings

JIU-KANG YU
Department of Mathematics, Harvard University

Received 11 March 1993; accepted in final form 27 May 1994

0. Introduction

In [11], Lubin and Tate established a version of explicit class field theory over a local field K_0: the ray class fields are generated by torsion points of the Lubin–Tate formal A_0-module, where A_0 is the ring of integers in K_0. This is an analogue of the Kronecker–Weber theorem that the ray class fields of $\mathbf{Q}$ are generated by roots of unity.

In this paper, we will derive an analogue of another classical theorem [15, Theorem 5.7] which asserts that the ring class field of an order in an imaginary quadratic field is generated by the moduli of elliptic curves with complex multiplications by that order. In fact, our theory (Section 4) describes the ring class field of any A_0-order $\mathcal{O}$ in an arbitrary separable extension K of K_0. The moduli space here is the Lubin–Tate moduli space (Section 2) that parametrizes liftings of a formal A_0-module. The role of elliptic curves with complex multiplications will be played by liftings with endomorphism action by $\mathcal{O}$. These objects are first introduced by Gross [4] in case K is a quadratic extension of K_0. Following his terminology, such liftings are called *quasi-canonical liftings*.

Some properties of these quasi-canonical liftings will be studied. In particular, we will compute the Newton polygon of the multiplication-by-π_0 map (π_0 is a prime element of K_0) of a quasi-canonical lifting (Section 6). From this computation, the valuations of the moduli (in a suitably normalized coordinate system) can be derived. In particular, we characterize the situations where the moduli are prime elements of the ring class field. When K/K_0 is quadratic, this has been done by Gross [4] and Fujiwara [3]. The result is fundamental in the non-archimedean local height computation of Heegner points by Gross–Zagier. For other applications, see [3], [8].

In Sections 11–13, we study the Gross–Hopkins period map (see [5], [6], and Sect. 11) from the Lubin–Tate moduli space to a projective space. We present an explicit form of the period map and study its valuational properties, which are contained in its valuation function (Section 7). It turns out (Section 13) that the exceptional set of its valuation function looks like walls in (part of) the apartment of the Bruhat–Tits building of $\mathrm{SL}_n(K_0)$, and the vertices are exactly the valuations of moduli of quasi-canonical liftings.

Finally, in Section 14 we determine the endomorphisms of the canonical lifting, which is defined to be a lifting with endomorphism action by the maximal order. Thus all results in Gross [4] in the case of height 2 are generalized to the case of arbitrary finite height.

1. Notations and conventions

Let K_0 be a non-archimedean local field, A_0 its ring of integers, π_0 a fixed prime element, and $k_0 \simeq \mathbf{F}_q$ its residue field. We use $\bar{K}_0$ to denote the completion of the algebraic closure of K_0, and $\bar{A}_0$ its ring of integers, $\bar{k}_0$ its residue field.

Let K be a finite separable extension of K_0 and let A, π, $k \simeq \mathbf{F}_{q^f}$ be the corresponding constructs for K. The valuation on $\bar{K}_0$ is normalized so that $\mathrm{ord}(K^*) = \mathbf{Z}$. Therefore, $\mathrm{ord}(K_0^*) = e\mathbf{Z}$, where e is the ramification index of K/K_0. Finally, we use $n = ef$ to denote the extension degree $[K : K_0]$.

An A_0-*lattice* in a finite-dimensional K_0-vector space V is a free A_0-submodule of V of rank equal to $\dim V$. An A_0-*order* in K is an A_0-subalgebra of K which is an A_0-lattice. In what follows, we will say simply "lattice" and "order" instead of "A_0-lattice" and "A_0-order".

All formal modules are assumed to be 1-dimensional, commutative, and of finite height. If G is a formal A_0-module, then the multiplication-by-a map on G $(a \in A_0)$ is denoted by $[a]_G$. The group of a-torsion points is denoted by $G[a]$.

If x, m are integers, $m > 0$, we use (x mod m) to denote the unique integer k such that $0 \leqslant k \leqslant m - 1$ and $k \equiv x \pmod m$.

2. Liftings and the Lubin–Tate moduli space

Let k' be an extension of k_0, regarded as an A_0-algebra. We denote by $\mathcal{C}_{k'}$ the category of complete, noetherian, local A_0-algebras whose residue fields are extensions of k'. This category has an initial object $W_{A_0}(k')$ (see [2] and also [14, II. Sect. 5]). In particular, every $R \in \mathcal{C}_{k'}$ has a canonical structure of a $W_{A_0}(k')$-algebra.

Let $\bar{G}$ be a formal A_0-module over k' and let $(R, \mathfrak{m}_R) \in \mathcal{C}_{k'}$. We define a *lifting* of $\bar{G}$ over R to be a formal A_0-module G over R such that $G \otimes (R/\mathfrak{m}_R) = \bar{G}$. Two liftings G, G' are considered *isomorphic* if there is an isomorphism $f: G \to G'$ of formal A_0-modules over R such that $f \otimes (R/\mathfrak{m}_R)$ is the identity automorphism of $\bar{G}$.

Let $X_{\bar{G}}(R)$ be the set of isomorphism classes of liftings of $\bar{G}$ over R. This is a co-variant functor on the category $\mathcal{C}_{k'}$. A fundamental theorem due to Lubin and Tate [12, Theorem 3.1] (see also [1, Proposition 4.2], [7, Theorem 22.4.4]) asserts that when $\bar{G}$ is of finite height n, the functor $X_{\bar{G}}$ is representable by $W_{A_0}(k')[[t_1, \ldots, t_{n-1}]]$, i.e. $X_{\bar{G}} \simeq \mathrm{Spf}\, W_{A_0}(k')[[t_1, \ldots, t_{n-1}]]$. More precisely, THEOREM. *Assume that $\bar{G}$ is a formal A_0-module of finite height n over an extension k' of k_0. There is a lifting $\mathcal{G}$* of $\bar{G}$ over $W_{A_0}(k')[[t_1, \ldots, t_{n-1}]]$ *with the following property: for any lifting G over $(R, \mathfrak{m}_R) \in \mathcal{C}$, there is a unique element $m \in \mathfrak{m}_R^{n-1}$ such that the lifting obtained from $\mathcal{G}$ by specializing t_i to m_i is isomorphic to G.*

The lifting $\mathcal{G}$ is called a *universal lifting* of $\bar{G}$. It is not unique though any two such are isomorphic. To fix a choice of $\mathcal{G}$ is to choose a coordinate system on $X_{\bar{G}}$, i.e. to attach an element $m \in \mathfrak{m}_R^{n-1}$ to every lifting $G \in X_{\bar{G}}(R)$. We call m the *modulus* of G.

When $(R, \mathfrak{m}_R)$ is a discrete valuation ring, it is interesting to study the valuations of the moduli of liftings. For example, if G, G' are liftings with moduli m, m', then

$$N = \min_{i=1}^{n-1} \operatorname{ord}_R(m_i - m_i')$$

has the following meaning: the identity automorphism of $G \otimes (R/\mathfrak{m}_R) = G' \otimes (R/\mathfrak{m}_R)$ can be lifted to an isomorphism $G \to G'$ over $R/\mathfrak{m}_R^N$ but cannot be lifted to one over $R/\mathfrak{m}_R^{N+1}$.

3. The isogeny construction

Now asume that R is the ring of integers in some finite extension of K_0 and that G is a lifting over R of $\bar{G}$, which is defined over $R/\mathfrak{m}_R$ and is of height n. The Tate module $T(G)$ is defined to be

$$\varprojlim_m G[\pi_0^m],$$

where the map $G[\pi_0^{m+1}] \to G[\pi_0^m]$ is $[\pi_0]_G$. It is a free A_0-module of rank n. Specifying a lattice L in $T(G) \otimes K_0$ containing $T(G)$ is equivalent to specifying a finite A_0-invariant subgroup scheme C_L of G. We then can form the quotient G/C_L. This formal A_0-module can be given a canonical structure of a lifting of $\bar{G}^{(q^N)}$ ($q^N = \#C_L(\bar{A}_0)$, $\bar{G}^{(q^N)}$ being the formal A_0-module obtained by applying the base change $x \mapsto x^{q^N}$ to $\bar{G}$), which we now describe:

We can find a formal A_0-module G' and an isogeny $g: G \to G'$ such that the kernel of g is C_L and $g \otimes (R/\mathfrak{m}_R)$ is the Nth power of Frobenius: $X \mapsto X^{q^N}$. In fact, such a pair (g, G') is furnished by Serre's formula [10, Theorem 1.4]:

$$g(X) = \prod_{c \in C_L(\bar{A}_0)} G(X, c),$$

and G' is such that $G'(g(X), g(Y)) = g(G(X, Y))$ and $[a]_{G'}(g(X)) = g([a]_G(X))$ for all $a \in A_0$. The condition that $g \otimes (R/\mathfrak{m}_R)$ is the Nth power of Frobenius implies that the reduction of G' is $\bar{G}^{(q^N)}$. Therefore, G' is a lifting of $\bar{G}^{(q^N)}$. The isomorphism class of this lifting does not depend on the choice of (g, G'). We will denote this lifting by G_L and denote the isogeny $g: G \to G_L$ by g_L. It is immediate from Serre's formula that G_L can be defined over $R[C_L(\bar{A}_0)]$.

Let $K' = \mathrm{End}(G) \otimes K_0$. This is an extension of K_0 of degree $\leqslant n$. For any two lattices $L_1, L_2 \supseteq T(G)$, we can identify $\mathrm{Hom}(G_{L_1}, G_{L_2}) \otimes K_0$ with K' by the correspondence

$$\phi \mapsto g_{L_2}^{-1} \circ \phi \circ g_{L_1}.$$

Here $g_{L_2}^{-1}$ means $h \otimes b^{-1} \in \mathrm{Hom}(G_{L_2}, G) \otimes K_0$, if $b \in A_0$, and $h: G_{L_2} \to G$ is an isogeny such that $h \circ g_{L_2} = [b]_G$ ([10], 1.6). We claim: under this correspondence, $\mathrm{Hom}(G_{L_1}, G_{L_2})$ is identified with

$$\mathrm{Hom}(L_1, L_2) = \{\psi \in K' \mid \psi . L_1 \subseteq L_2\}.$$

To see this, assume that ϕ is an isogeny and put $\psi = g_{L_2}^{-1} \circ \phi \circ g_{L_1}$. Choose $b \in A_0$ such that $[b]_G \circ g_{L_2}^{-1}$ is an isogeny. It is easily checked that $\psi \otimes b$ is an isogeny and $(\psi \otimes b)([b]_G^{-1} C_{L_1}) \subseteq C_{L_2}$. That is, $(\psi \otimes b) . (b^{-1} L_1) \subseteq L_2$.

Conversely, if $\psi = g_{L_2}^{-1} \circ \phi \circ g_{L_1}$ is such that $\psi . L_1 \subseteq L_2$, we can choose $b \in A_0$ such that $\psi \otimes b$, $\phi \otimes b$ are both isogenies. For any $y \in G_{L_1}[b]$, write $y = g_{L_1}(x)$ with $x \in [b]_G^{-1}(C_{L_1})$. We then have $(\phi \otimes b)(y) = g_{L_2} \circ (\psi \otimes b)(x) = 0$ since $(\psi \otimes b)(x) \in C_{L_2}$ by assumption. Thus we have proved that $G_{L_1}[b] \subseteq \ker(\phi \otimes b)$. Therefore, ϕ is an isogeny ([10], 1.5).

4. Quasi-canonical liftings

Let F be the Lubin–Tate A-module associated to (K, π) (i.e. the unique formal A-module over A such that $[\pi]_{F \otimes k}(X) = X^{q^f}$, see [12]), considered as a formal A_0-module of height n over A. Let $\bar{F} = F \otimes k$, so that F can be regarded as a lifting of $\bar{F}$. We call F the *canonical lifting* of $\bar{F}$. A lifting of the form F_L (for some lattice L in $T(F) \otimes K_0$ containing $T(F)$) is called a *quasi-canonical lifting* (of $\bar{F}^{(q^N)}$, where $q^N = [L : T(F)]$). The modulus of F_L will be denoted by m_L.

Since the endomorphism $[\pi]_F$ of F satisfies $([\pi]_F \otimes k)(X) = X^{q^f}$ and $q^f = \#F[\pi]$, we see that $F_L = F_{\pi^{-1}L}$ for any L. Thus we are led to the action of $\pi^{\mathbf{Z}}$ on the set of all lattices in $T(F) \otimes K_0$. The orbits of this action are called *lattice classes* and the lattice class of a lattice L is denoted by $[L]$. From preceding discussions, F_L depends on $[L]$ only. Thus we can define F_L for any L by $F_L = F_{\pi^{-m}L}$ for $m \gg 0$.

By Lubin–Tate theory [11], F_L can be defined over an abelian extension of K. We shall determine the smallest field of definition of F_L. First of all, we note that the group A^* acts on lattice classes in an obvious way. For every N, it also acts on $X_{\bar{F}(q^N)}(R) = \mathfrak{m}_R^{n-1}$ through the Artin symbol whenever R is an abelian extension of A. The relation of these actions is:

$$F_{a^{-1}L} = F_L^{(a,K)}, \quad \text{or equivalently } m_{a^{-1}L} = m_L^{(a,K)}, \quad \text{for any } a \in A^*.$$

Indeed, letting $g_L\colon F \to F_L$ be the morphism given by Serre's formula, we then have $g_L^{(a,K)} = g_{a^{-1}L}$ by Lubin–Tate theory [11] and the above relation follows immediately. Now it is easy to see that F_L can be defined over the class field of $\pi^{\mathbf{Z}} \times \mathcal{O}_L^*$, where

$$\mathcal{O}_L = \{a \in K \mid aL \subset L\} \simeq \mathrm{End}(F_L).$$

This class field is called the *ring class field* of the order $\mathcal{O}_L$ (Note: this depends on π). We are going to show that this is actually the smallest field of definition of F_L.

As we have seen in Section 3, $\mathrm{End}(F_L) \otimes K_0$ can be identified with K.

PROPOSITION 1. *Let L_1, L_2 be lattices in $T(F) \otimes K_0$. The following three statements are equivalent:*

(i) *F_{L_1} is isomorphic to F_{L_2} as formal A_0-modules*;
(ii) *The lattice classes $[L_1]$, $[L_2]$ are in the same A^*-orbit;*
(iii) $\mathrm{End}(F_{L_1})$, $\mathrm{End}(F_{L_2})$ *are the same order $\mathcal{O}$ in K, and L_1, L_2 are isomorphic $\mathcal{O}$-modules.*

Proof. (i) $\Rightarrow$ (iii): First we observe the following: For any L and any non-zero $x \in T(G)$, $\mathrm{Hom}(F_{\mathcal{O}_L.x}, F_L)$ is an $\mathcal{O}_L$-module isomorphic to L by the discussion in the end of Section 2. Now if (i) is fulfilled, clearly $\mathrm{End}(F_{L_1})$ and $\mathrm{End}(F_{L_2})$ are identified with the same order $\mathcal{O}$ in K, and L_1 and L_2 are isomorphic as $\mathcal{O}$-modules by the observation we just made. (ii) $\Rightarrow$ (i): if $L_1 = a^{-1}L_2$, the automorphism $[a]\colon F \to F$ induces an isomorphism $F_{L_1} \to F_{L_2}$. (iii) $\Rightarrow$ (ii): an $\mathcal{O}$-module isomorphism from L_1 to L_2 is multiplication by some element $u\pi^\nu$ of K^*. Clearly u sends $[L_1]$ to $[L_2]$. □

PROPOSITION 2. *Let L_1, L_2 be lattices in $T(F) \otimes K_0$. Then F_{L_1} and F_{L_2} are isomorphic as liftings (of some $\bar{F}^{(q^N)}$) if and only if $[L_1] = [L_2]$.*

Proof. Without loss of generality, we may assume that L_1, L_2 are lattices containing $T(G)$. Let $g_L\colon F \to F_L$ be the isogeny defining F_L (say given by Serre's formula). By the preceding proposition, we may assume that $L_1 = aL_2$ for some $a \in A^*$. Then an isomorphism from F_{L_1} to F_{L_2} is given by $g_{L_2} \circ [a]_F \circ g_{L_1}^{-1}$ (see the discussion at the end of Section 3). Any other isomorphism is obtained by composing an automorphism of F_{L_1}, therefore is of the form $g_{L_2} \circ [ab]_F \circ g_{L_1}^{-1}$, with $b \in \mathcal{O}_{L_1} = \mathcal{O}_{L_2}$. It is easy to see that the reduction of this isomorphism is $[ab]_{\bar{F}^{(q^N)}}$. The latter is identity if and only if $ab = 1$ since $x \in A \mapsto [x]_{\bar{F}^{(q^N)}}$ is injective. Therefore, the isomorphism is an isomorphism of liftings if and only if $ab = 1$ and $L_1 = L_2$. □

THEOREM 1. *The smallest field containing K over which F_L is defined is the class field of $\pi^{\mathbf{Z}} \times \mathcal{O}_L^*$. In other words, $K(m_L)$ is the ring class field of $\mathcal{O}_L$.*

Proof. This is immediate from the relation $m_{a^{-1}L} = m_L^{(a,K)}$ and the preceding proposition. □

COROLLARY. *For any $N > 0$, $K(m_L, F_L[\pi^N])$ is the class field of $\pi^{\mathbf{Z}} \times (1 + \pi^N \mathcal{O}_L)$.*

Proof. Indeed, if $u \in \mathcal{O}_L^*$, $x \in F_L[\pi^N]$, we have $(u, K).x = g_L \circ [u^{-1}]_F \circ g_L^{-1}(x)$ by Lubin–Tate theory. Thus (u, K) fixes $K(m_L, F_L[\pi^N])$ if and only if $uy \equiv y \pmod{L}$ for all $y \in \pi^{-N}L$. Clearly this condition is equivalent to $u \equiv 1 \pmod{\pi^N \mathcal{O}_L}$. □

Let $\mathcal{O}$ be an order in K. It is customary to call a lattice in K a *proper $\mathcal{O}$-lattice* if $\mathrm{End}(L) = \mathcal{O}$. Two proper $\mathcal{O}$-lattices L_1, L_2 are *equivalent* if $L_1 = xL_2$ for some $x \in K^*$.

COROLLARY. *Let $G \simeq A^*/\mathcal{O}^*$ be the Galois group of the ring class field of $\mathcal{O}$. Then G permutes the quasi-canonical liftings F_L with $\mathcal{O}_L = \mathcal{O}$. The action is simply transitive on each orbit, and the orbits correspond bijectively to equivalence classes of proper $\mathcal{O}$-lattices.* □

PROPOSITION 3. *Let G be a lifting of $\bar{F} \otimes_k \bar{k}_0$ over $\bar{A}_0$ such that* $\mathrm{End}(G) \simeq \mathcal{O}$ *is an order in A. Then there is some L such that G is isomorphic to F_L over $\bar{A}_0$ as formal A_0-modules.*

Proof. It is enough to show that G and F are isogenous. For any lattice M in $T(G) \otimes K_0$ containing $T(G)$, the endomorphism ring of G_M is $\{a \in K \mid aM \subseteq M\}$ (note that $T(G) \otimes K_0$ is a 1-dimensional K-vector space by the assumption on $\mathrm{End}(G)$). Therefore we can choose M so that G_M has the structure of a height 1 formal A-module. As a height 1 formal A-module is unique over $\bar{A}_0$, G_M must be isomorphic to F. □

With the hypotheses of the last proposition, choose an isomorphism $f: G \to F_L$. Then $g = f \otimes \bar{k}_0 \in \mathrm{Aut}_{\bar{k}_0}(\bar{F})$. Let the ring homomorphism $\iota: A = \mathrm{End}_{\bar{A}_0}(F) \to D = \mathrm{End}_{\bar{k}_0}(\bar{F})$ be defined by reduction. Then G is a quasi-canonical lifting of the pair $(\bar{F}, g \circ \iota \circ g^{-1})$ in the sense of Gross [4], cf. Section 14.

5. Some numerical invariants of quasi-canonical liftings

Let $T = T(F)$ and let L be a lattice in $T \otimes K_0$. Form the filtration $\{L_i = L \cap \pi^{-i}T\}_{i \in \mathbf{Z}}$ and let $l_i = \dim_{k_0} L_{i+1}/L_i$. We have $l_i \leqslant l_{i-e}$ because the map $\pi_0: L_{i+1} \to L_{i+1-e}$ induces an injection $L_{i+1}/L_i \to L_{i+1-e}/L_{i-e}$.

On the other hand, we clearly have $l_i = 0$ for all i sufficiently large, and $l_i = f$ for all i sufficiently small. Therefore, there is a unique nondecreasing sequence of integers, of length n, $a_0(L) \leqslant \cdots \leqslant a_{n-1}(L)$, with the following property: for every integer i and every natural number m, i appears m times in the sequence if and only if $m = l_{i-e} - l_i$.

EXAMPLE 1. If $L = T$, then the set $\{a_0(T), \ldots, a_{n-1}(T)\}$ consists of $0, 1, \ldots, e-1$, each occurring with multiplicity f.

It is easy to see that in general, for each $r \in \mathbf{Z}/e\mathbf{Z}$, there are exactly f indices $j_1, \ldots, j_f$ such that $a_{j_i}(L) \equiv r \pmod{e}$.

EXAMPLE 2. If K/K_0 is unramified and $L \supseteq T$, then the numbers $\{a_0(L), \ldots, a_{n-1}(L)\}$ are the exponents of the *elementary divisors* of L/T, i.e. $L/T \simeq \oplus_{j=0}^{n-1} A_0/\pi_0^{a_j(L)} A_0$.

In general, the structure of L/T as an A_0-module is $L/T \simeq \oplus_{j=0}^{n-1} A_0/\pi_0^{\lfloor a_j(L)/e \rfloor} A_0$ if $L \supseteq T$. More precisely, there are elements $x_0, \ldots, x_{n-1} \in T \otimes K_0$ such that $Ax_j = \pi^{-(a_j(L)-e+1)}T$ for each j and $L = \oplus_{j=0}^{n-1} A_0 x_j$.

Indeed, if $m_i = l_{i-e} - l_i > 0$, we let $y_{i1}, \ldots, y_{im_i} \in L_{i-e+1}$ be such that they generate the cokernel of $\pi_0 \colon L_{i+1}/L_i \to L_{i-e+1}/L_{i-e}$. Let L' be the A_0-submodule of L generated by the n elements $\{y_{ij}\}_{i, 1 \leqslant j \leqslant m_i}$. Form the filtration $\{L'_i\}_{i \in \mathbf{Z}}$ for L' and define the numbers $\{l'_i\}$. We clearly have $l'_i = l_i = 0$ for large i. We also have $l'_{i-e} - l'_i \geqslant l_{i-e} - l_i = m_i$, since the cokernel of $\pi_0 \colon L'_{i+1}/L'_i \to L'_{i-e+1}/L'_{i-e}$ contains the linearly independent elements $y_{i1}, \ldots, y_{im_i}$. It follows that $\operatorname{length}_{A_0}(L'/T) \geqslant \operatorname{length}_{A_0}(L/T)$. Since $L' \subseteq L$, we must have $L' = L$. Now we can suitably re-label the n elements $\{y_{ij}\}_{i, 1 \leqslant j \leqslant m_i}$ as $x_0, \ldots, x_{n-1}$ to conclude the proof of the above claim.

EXAMPLE 3. If we consider the lattice $\pi^{-t}L$, we will obtain $a_j(\pi^{-t}L) = a_j(L) + t$.

EXAMPLE 4. Let $\langle\, , \rangle$ be a non-degenerate symmetric K_0-bilinear form on $T \otimes K_0$ satisfying $\langle ax, y \rangle = \langle x, ay \rangle$ for all $a \in K$, $x, y \in T \otimes K_0$ Define $L^\vee = \{x \in T \otimes K_0 \mid \langle x, L \rangle \subseteq A_0\}$. This is a lattice with $\mathcal{O}_{L^\vee} = \mathcal{O}_L$. Then $a_j(L^\vee) = d + e - 1 - a_{n-1-j}(L)$, where d is such that $T^\vee = \pi^{-d}T$.

This is clear from the following computation:

$$
\begin{aligned}
l_i^\vee &= \operatorname{length}_{A_0} \frac{L^\vee \cap \pi^{-(i+1)}T}{L^\vee \cap \pi^{-i}T} = \operatorname{length}_{A_0} \frac{L^\vee/(L^\vee \cap \pi^{-i}T)}{L^\vee/(L^\vee \cap \pi^{-(i+1)}T)} \\
&= \operatorname{length}_{A_0} \frac{(L^\vee + \pi^{-i}T)/\pi^{-i}T}{(L^\vee + \pi^{-(i+1)}T)/\pi^{-(i+1)}T} = f - \operatorname{length}_{A_0} \frac{L^\vee + (\pi^{i+1-d}T)^\vee}{L^\vee + (\pi^{i-d}T)^\vee} \\
&= f - \operatorname{length}_{A_0} \frac{(L \cap \pi^{i+1-d}T)^\vee}{(L \cap \pi^{i-d}T)^\vee} \\
&= f - \operatorname{length}_{A_0} \frac{L \cap \pi^{i-d}T}{L \cap \pi^{i+1-d}T} = f - l_{d-1-i}.
\end{aligned}
$$

Now let $0 \leqslant r_0(L) \leqslant \cdots \leqslant r_{n-1}(L)$ be integers such that $a_j(L) \equiv r_j(L) \pmod{e}$ and such that $r_{n-1}(L)$ is minimal with respect to this property. For example, if $e = 3$, $f = 1$, then (r_0, r_1, r_2) is one of the following: (0, 1, 2), (0, 2, 4), (1, 3, 5), (1, 2, 3), (2, 4, 6), (2, 3, 4).

It is easy to see that the sequence $r(L) = (r_0(L), \ldots, r_{n-1}(L))$ is determined by $\bar{r}(L) = (r(L) \bmod e)$. Therefore, there are $n!/(f!)^e$ possible values of $r(L)$.

The sequence of integers $a_0(L) - r_0(L), \ldots, a_{n-1}(L) - r_{n-1}(L)$ is still a non-decreasing sequence, with all elements divisible by e. Therefore, we can write

$$a_j(L) = r_j(L) + e(s_0(L) + \cdots + s_j(L)),$$

where $s_0(L), \ldots, s_{n-1}(L)$ are non-negative integers.

In the lattice class $[L]$, we can choose a unique representative L_0 satisfying $L_0 \supset T$, $L_0 \not\supset \pi^{-1}T$. This L_0 is also characterized by $a_0(L_0) = 0$. The numbers $a(L_0)$, $r(L_0)$, $\bar{r}(L_0)$, $s(L_0)$ are canonically associated to the lattice class $[L]$. We denote them by $a[L]$, $r[L]$, $\bar{r}[L]$, $s[L]$ respectively.

The above constructions can be applied to any rank 1 free A-module T. For the rest of this section, take $T = A$ and $\langle x, y\rangle = \mathrm{Tr}_{K/K_0}(xy)$. Let $\mathcal{O}$ be an order in K.

PROPOSITION 4. *The following statements are equivalent:*

(i) *Every proper $\mathcal{O}$-lattice is free over $\mathcal{O}$.*
(ii) *The Galois group of the ring class field of $\mathcal{O}$ acts simply transitively on quasi-canonical liftings F_L with $\mathcal{O}_L = \mathcal{O}$.*
(iii) *$\mathcal{O}^\vee$ is a free $\mathcal{O}$-module.*
(iv) *$a_i(\mathcal{O}) + a_{n-1-i}(\mathcal{O})$ is a number independent of i.*

Proof. The equivalence of (i) and (ii) is clear from the second corollary to Theorem 1. It is obvious that (iii) implies (iv). Conversely, if (iv) holds, put $\mathcal{O}^\vee = xL$, where $x \in \mathcal{O}^\vee \backslash \{0\}$ is such that $\mathrm{ord}(x)$ is minimal. Then $1 \in L$ and $\mathcal{O} \subseteq L \subseteq A$. But one can easily see that $a(\mathcal{O}) = a(L)$ by assumption and therefore $\#(A/\mathcal{O}) = \#(A/L)$. Thus $\mathcal{O} = L$ and $\mathcal{O}^\vee$ is free.

Since (i) clearly implies (iii), it remains to show that (iii) implies (i). Let L be a proper $\mathcal{O}$-lattice. We claim that $L^\vee L = \mathcal{O}^\vee$. One direction is easy: $\langle L^\vee L, \mathcal{O}\rangle = \mathrm{Tr}(L^\vee L\mathcal{O}) \subseteq A_0$, so $L^\vee L \subseteq \mathcal{O}^\vee$. To show the other inclusion, it is enough to show that $(L^\vee L)^\vee \subseteq \mathcal{O}$. We have $x \in (L^\vee L)^\vee \Rightarrow \mathrm{Tr}(xL^\vee L) \subseteq A_0 \Rightarrow xL^\vee \subseteq (L^\vee)^\vee = L \Rightarrow x \in \mathcal{O}_L = \mathcal{O}$. Now since $\mathcal{O}^\vee$ is a free $\mathcal{O}$-module, $L^\vee L = \mathcal{O}^\vee$ implies that L is an invertible module over the local ring $\mathcal{O}$. Therefore, L is free. □

Let $A^\vee = \pi^{-d}A$ be the inverse different of K/K_0.

LEMMA 1. *Suppose that the residue field of $\mathcal{O}$ is of order $q^{f'}$, then*

$$\begin{cases} \#(A/\mathcal{O}) = q^{-df+\Sigma\lfloor a_j(\mathcal{O}^\vee)/e\rfloor} = q^{\Sigma\lfloor a_j[\mathcal{O}^\vee]/e\rfloor}, \\ \#(A^*/\mathcal{O}^*) = \dfrac{q^f - 1}{q^{f'} - 1} q^{-(f-f')+\Sigma\lfloor a_j[\mathcal{O}^\vee]/e\rfloor}. \end{cases}$$

Proof. We have $\#(A/\mathcal{O}) = \#(\mathcal{O}^\vee/A^\vee) = \#(\mathcal{O}^\vee/A)q^{-df}$, and $a_0(\mathcal{O}^\vee) = d$, $a[\mathcal{O}^\vee] = a(\mathcal{O}^\vee) - d$. So the first formula follows from the discussion after

Example 2. The second formula follows easily from the first. □

6. The Newton polygon of $[\pi_0]_{F_L}$

As a shorthand we use q_j to denote $(q^j - 1)/(q - 1)$.

THEOREM 2. *Let F_L be a quasi-canonical lifting and let the Newton polygon of $[\pi_0]_{F_L}$ be the polygonal line joining $(1, e)$, $(q, w_1), \ldots, (q^{n-1}, w_{n-1})$, to $(q^n, w_n = 0)$. Then*

$$\frac{w_j}{q_j} - \frac{w_{j+1}}{q_{j+1}} = f_{j,\bar{r}[L]}(q)\frac{q^j}{q_j q_{j+1}} \cdot q^{-(s_1[L]+2s_2[L]+\cdots+js_j[L])}, \quad 1 \leqslant j \leqslant n-1,$$

where $f_{j,\bar{r}[L]}(q) \in \mathbf{Z}[q, q^{-1}]$ is a polynomial depending on j and $\bar{r}[L]$ only.

Note that in the statement of the theorem, we do not assume that (q^j, w_j) is a break on the Newton polygon. We only assume that it lies on the Newton polygon. The proof of the theorem will be given in Sections 9 and 10. An explicit formula for $f_{j,\bar{r}[L]}$ will be given in Section 10, and we will see:

COROLLARY. *The point (q^j, w_j) is a break of the Newton polygon of $[\pi_0]_{F_L}$ if and only if $a_j[L] \neq a_{j-1}[L]$. In particular, if K/K_0 is unramified, (q^j, w_j) is a break if and only if $s_j \neq 0$; if K/K_0 is totally ramified, (q^j, w_j) is always a break.*

Hazewinkel [7] (cf. Sect. 11) shows that a universal lifting $\mathcal{F}$ over $W_{A_0}(k)[[t_1, \ldots, t_{n-1}]]$ can be chosen in a way such that

$$[\pi_0]_{\mathcal{F}}(X) \equiv t_k X^{q^k}, \quad (\operatorname{mod} \pi_0, t_1, \ldots, t_{k-1}) \quad (\operatorname{mod} \deg q^k + 1).$$

Choosing this particular universal lifting means choosing a particular coordinate system on the Lubin–Tate moduli space $X_{\bar{F}}$. Now we can reformulate Theorem 2 as follows:

THEOREM 2′. *Let $w_1, \ldots, w_{n-1}$, $w_n = 0$ be given by the formula in Theorem 2. Assume that $a_j[L] \neq a_{j-1}[L]$. Then*

$$\operatorname{ord}((m_L)_j) = w_j. \qquad \square$$

COROLLARY. *Let $\mathcal{O}$ be an order in K such that $a_{n-1}[\mathcal{O}^\vee] \neq a_{n-2}[\mathcal{O}^\vee]$. Put $r = r[\mathcal{O}^\vee]$. Then $(m_{\mathcal{O}^\vee})_{n-1}$ is a prime element in the ring class field of $\mathcal{O}$ if and only if the following two conditions are satisfied:* (i) *the residue field of $\mathcal{O}$ is k_0;* (ii) *we have the relation*

$$\sum_{i=0}^{n-1}\left(\left\lceil\frac{r_{n-1}+1-r_i}{e}\right\rceil - \left\lfloor\frac{r_i}{e}\right\rfloor\right) = n.$$

REMARK. The proof will be given in Section 10. The condition on r is satisfied in particular when $\bar{r}_i + \bar{r}_{n-1-i}$ is independent of i.

EXAMPLE. The Newton polygon of $[\pi_0]_F$, where F is the canonical lifting, is easily seen to be the polygonal line joining $(1, e)$, $(q^f, e-1), \ldots, (q^{(e-1)f}, 1)$, to $(q^n, 0)$. This is the case $\bar{r} = \bar{r}_{\mathrm{can}} = (0, \ldots, 0, 1, \ldots, 1, \ldots, e-1, \ldots, e-1)$ (each number occurs f times). So we obtain for $j = if + k$, $0 \leqslant k \leqslant f-1$

$$f_{j,\bar{r}_{\mathrm{can}}}(q) = q^{-j}\left(q_{j+1}\left((e-i) - \frac{q^k - 1}{q^f - 1}\right) - q_j\left((e-i) - \frac{q^{k+1} - 1}{q^f - 1}\right)\right)$$

$$= (e-i) + \frac{1 - q^{-if}}{q^f - 1}.$$

We can use this to compute the valuations of the moduli of any quasi-canonical liftings with $\bar{r} = \bar{r}_{\mathrm{can}}$ (e.g. when K/K_0 is unramified, we always have $\bar{r} = \bar{r}_{\mathrm{can}} = 0$ and $f_j = 1$ for all j). This generalizes Keating [8, Prop. 7], where the case $\bar{r} = \bar{r}_{\mathrm{can}}$, $s = (0, \ldots, 0, s_{n-1})$, $\mathcal{O} = A_0 + \pi^{s_{n-1}}A$ is treated.

If $\mathcal{O}$ is an order with $\bar{r}[\mathcal{O}] = \bar{r}_{\mathrm{can}}$ and residue field k_0, then $(m_{\mathcal{O}^\vee})_{n-1}$ is a prime element of its ring class field.

Let $n = 2$. We obtain Gross' formula [4, Prop. 5.3]:

$$\mathrm{ord}(m_L) = \begin{cases} 1/(q+1)q^{s-1}, & \text{if } K/K_0 \text{ is unramified;} \\ 1/q^s, & \text{if } K/K_0 \text{ is ramified.} \end{cases}$$

Note that in this case, every quasi-canonical lifting has $\bar{r} = \bar{r}_{\mathrm{can}}$ so this gives the valuations of the moduli of all quasi-canonical liftings, and it depends only on the single number $s = s_1[L]$, called the "level" of the quasi-canonical lifting. In this case m_L is always a prime element of the ring class field. See also Fujiwara [3, Prop. 2].

7. Valuation functions

Let f be a non-zero rigid analytic function on $\{u \in \bar{K} \mid \mathrm{ord}(u) > 0\}$. There is a unique piecewise linear continuous function $V_f \colon \mathbf{R}_{>0} \to \mathbf{R}$ such that $V_f(\mathrm{ord}(u)) = \mathrm{ord}(f(u))$ for all u whose valuation $\mathrm{ord}(u)$ lies in a dense open subset of $\mathbf{R}_{>0}$. The function V_f is called the *valuation function* of f. It follows immediately from the definition that $V_{fg} = V_f + V_g$, and we expect to have the relation $V_{f\circ g} = V_f \circ V_g$ in general.

Explicitly, take coordinates and write $f(X) = \Sigma a_k X^k$, then

$$V_f(x) = \min_k\{\mathrm{ord}(a_k) + kx\}.$$

The set E_f of all x such that $\min_k\{\mathrm{ord}(a_k) + kx\}$ is achieved at more than one value of k is called the *exceptional set* of f. For any u such that $\mathrm{ord}(u) \notin E_f$ we have $V_f(\mathrm{ord}(u)) = \mathrm{ord}(f(u))$.

The formula $V_f(x) = \min_k\{\mathrm{ord}(a_k) + kx\}$ enables us to define valuation functions for more general power series (non-convergent, with negative or fractional powers, etc) and extend the domain of V_f to a larger subset of $\mathbf{R}$. The identity $V_{f\circ g} = V_f \circ V_g$ holds provided that $V_g^{-1}(E_f)$ contains no open set.

It is well known that V_f and the *Newton polygon* of f contain the same information about f. The latter is defined to be the boundary of the convex hull of

$$\bigcup_k \{(x, y) \in \mathbf{R}^2 \mid x \geqslant k,\ y \geqslant \mathrm{ord}(a_k)\}.$$

The graph of V_f is sometimes called the *Newton copolygon* of f.

All these can be generalized to power series of several variables. For more details, see Lubin [9, Sect. 3].

8. Special subgroups

Now let G be an arbitrary formal A_0-module over $\bar{A}_0$ of height n. Let the Newton polygon of $[\pi_0]_G$ be the polygonal line joining $(1, w_0(G))$, $(q, w_1(G)), \dots, (q^{n-1}, w_{n-1}(G))$, to $(q^n, w_n(G))$. We have $w_0(G) = e$ and $w_n(G) = 0$. Again, we do *not* assume that every $(q^i, w_i(G))$ is a break of the Newton polygon.

The following data clearly all convey the same amount of information about G:

- The Newton polygon of $[\pi_0]_G$;
- The valuation function of $[\pi_0]_G$;
- The decreasing sequence $w(G) = (w_1(G), \dots, w_{n-1}(G))$;
- The sequence $u(G) = (u_1(G), \dots, u_{n-1}(G))$, where (recall that $q_j = (q^j - 1)/(q-1)$)

$$u_j(G) = \frac{w_j(G)}{q_j} - \frac{w_{j+1}(G)}{q_{j+1}};$$

- The decreasing sequence $v(G) = (v_1(G), \dots, v_n(G))$, where

$$v_j(G) = \frac{w_{j-1}(G) - w_j(G)}{q^j - q^{j-1}}.$$

The numbers $v_j(G)$ are simply the slopes of the Newton polygon, and we have the following interpretation: $v_j(G)$ is the largest number t having the following property:

> there is an A_0-invariant subgroup scheme C of $G[\pi_0]$, of order q^j, such that $\mathrm{ord}(x) \geqslant t$ for all $x \in C$

(here and elsewhere, we identify a finite group scheme with its $\bar{A}_0$-points).

An A_0-invariant subgroup scheme C of $G[\pi_0]$ of order q^d is called *special* if

$$\min\{\mathrm{ord}(x) \mid x \in C\} = v_d(G) \quad \text{and} \quad C \supset \{x \in G[\pi_0] \mid \mathrm{ord}(x) > v_d(G)\}.$$

Clearly, a special subgroup of order q^d exists for $d = 0, 1, \ldots, n$. And it is unique if and only if $(q^d, w_d(G))$ is a break on the Newton polygon of $[\pi_0]_G$. When $(q, w_1(G))$ is a break, the unique special subgroup of order q is studied in [9], where it is called *the canonical subgroup.*

As suggested by K. Keating to me, when $(q^d, w_d(G))$ is a break, the subgroup $\{x \in G[\pi_0] \mid \mathrm{ord}(x) \geqslant w_d(G)\}$ can be called a *generalized canonical subgroup.* So the generalized canonical subgroups form a filtration of $G[\pi_0]$, indexed by the breaks. Then a special subgroup can be characterized as an A_0-invariant subgroup that lies between two successive generalized canonical subgroups.

We do not have an interpretation of the number $u_j(G)$. But it turns out that for $G = F_L$, $u_j(G)$ can be expressed by a particularly nice formula (Theorem 2). Proposition 5 below partially explains why: when G' is isogenous to G and the kernel of the isogeny is a special subgroup, $u(G')$ is related to $u(G)$ is a very elegant way.

The following lemma can be verified by straightforward computations.

LEMMA 2. *For any positive integer $d < n$, the following are equivalent:*

(i) *The polygonal line joining* $(1, w'_0)$, $(q, w'_1), \ldots, (q^{n-1}, w'_{n-1})$ *to* (q^n, w'_n) *is a convex polygonal line, where* $w'_i = w_i(G) + (q^i - 1)w_d(G)$ *for* $i \leqslant d$, $w'_i = q^d w_i(G)$ *for* $i \geqslant d$;

(ii) $(1 + q^d)w_d(G) \geqslant w_{d-1}(G) + q^{d-1}w_{d+1}(G)$;

(iii) $u_d(G) \leqslant u_{d-1}(G)q_{d-1}/(q_{d+1}q^{d-1})$;

(iv) $v_d(G) - w_d(G) \geqslant q^d v_{d+1}(G)$. □

PROPOSITION 5. *For any positive integer $d < n$, if one of the equivalent conditions in the preceding lemma holds, and C is any special subgroup of $G[\pi_0]$ of order q^d, $G' = G/C$, then we have*

(i) $w_i(G') = w'_i$, *where w'_i is given in* (i) *of the preceding lemma;*

(ii) $u(G') = (u_1(G), \ldots, u_{d-1}(G), q^d u_d(G), \ldots, q^d u_{n-1}(G))$;

(iii) $v(G') = (v_1(G) - w_d(G), \ldots, v_d(G) - w_d(G), q^d v_{d+1}(G), \ldots, q^d v_n(G))$.

Proof. It is routine to verify the equivalence of the statements (i), (ii), (iii), so it is enough to give a proof of (i). This can be done by the same method for proving Theorem B of Lubin [9], which is the special case $d = 1$, $q = p$ of our proposition. The idea is to calculate $V_{[\pi_0]_{G'}}$ as $V_g \circ V_{[\pi_0]_G} \circ V_g^{-1}$, where $g\colon G \to G'$ is an isogeny with kernel C. Because C is special, we can determine V_g by Serre's formula. We omit the details. □

This proposition is of independent interest. But it is not absolutely necessary in the sequel.

9. Proof of Theorem 2

Now consider the quasi-canonical lifting $G = F_L$. We assume that L is such that $a(L) = a[L]$, i.e. $L \supset T$ and $L \not\supset \pi^{-1}T$. We can find elements $x_0, \ldots, x_{n-1} \in T \otimes K_0$ such that $Ax_j = \pi^{-(a_j(L)-e+1)}T$ for each j and $L = \oplus_{j=0}^{n-1} A_0 x_j$.

Let $g_L\colon F \to F_L$ be the isogeny defining F_L, with kernel C_L, which we identify with L/T. Let $q^{c(i)} = \#(C_L \cap F[\pi^i])$. The following lemma is immediate from Serre's formula and Lubin–Tate theory.

LEMMA 3. *For any torsion point $x \in F_L(A_0)$, let $o(x)$ be the smallest integer t such that $x \in F[\pi^t] + C_L$. The valuation* $\mathrm{ord}(g_L(x))$ *depends on $o(x)$ only and is a strictly decreasing function of $o(x)$. Explicitly, let $t = o(x)$, then*

$$\mathrm{ord}(g_L(x)) = \frac{q^{c(t)}}{(q^f - 1)q^{(t-1)f}} + \sum_{i>t} \frac{q^{c(i)} - q^{c(i-1)}}{(q^f - 1)q^{(i-1)f}}. \qquad \square$$

Lemma 3 is the key to compute the Newton polygon of $[\pi_0]_{F_L}$. From it we see that the valuations of the torsion points of F_L are computable, and these are just the slopes of the Newton polygon (see Lemma 4 (i) below). All we need is some patience to unravel the formula.

Let φ be the function such that $\mathrm{ord}(g_L(x)) = \varphi(o(x))$.

LEMMA. 4.

(i) $v_j(F_L) = \varphi(a_{j-1}(L) + 1)$.
(ii) *Let $L_d = \oplus_{j=0}^{d-1} A_0 \pi_0^{-1} x_j + L$. Then S_d, the subgroup of $F_L[\pi_0]$ identified with L_d/L, is special of order q^d.*
(iii) *F_{L_d} is isomorphic to F_L/S_d.*
(iv) *If moreover we have $s_d(L) > 0$, then*

$$\begin{aligned} a[L_d] &= a(\pi_0 L_d) \\ &= (a_0(L), \ldots, a_{d-1}(L),\ a_d(L) - e, \ldots, a_{n-1}(L) - e). \end{aligned}$$

Proof. (i) is immediate from Lemma 3 because the numbers $v_j(G)$ are the valuations of elements in $F_L[\pi_0] = g_L([\pi_0]_F^{-1}(C_L))$. (ii) and (iii) are obvious. In (iv), we need the assumption that $s_d(L) > 0$ only to ensure that $(a_0(L), \ldots, a_{d-1}(L), a_d(L) - e, \ldots, a_{n-1}(L) - e)$ is non-decreasing. $\square$

Fix some d and assume that $s_d(L) > 0$. Let $G' = F_{\pi_0 L_d}$, $q^{c'(i)} = \#(C_{\pi_0 L_d} \cap F[\pi^i])$.

LEMMA 5.

(i) $c(i) = c(i - e) + \#\{j \mid a_j \geqslant i\}$ *for all $i \in \mathbf{Z}$, if we put $c(i) = i$ for $i < 0$.*
(ii) $c'(i) = c(i) - \#\{j \mid j \geqslant d,\ a_j(L) - e + 1 \leqslant i\}$.
(iii) *For $i \leqslant a_d(L) - e$, $c'(i) = c(i)$.*
(iv) *For $i > 0$, $c'(a_d[L_d] + i) = c(a_d[L] + i) + (n - d)$.*

(v) $c(i) = c(i-1)$ *if* $i > a_{n-1}(L) - e + 1$.

Proof. (i) Observe that $c(i+1) - c(i) = l_i$, where l_i is defined in Section 5. By definition, $l_{i-e} - l_i = \#\{j \mid a_j(L) = i\}$. Now the formula can be proved by an easy induction. (ii) is obvious and (iii) is an easy consequence of (ii). (iv) is deduced using (i), (ii) and the fact $a_d[L_d] = a_d[L] - e$. (v) is easily seen from the remark after Example 2 of Section 5. □

LEMMA 6. *Assume that* $s_d(L) > 0$. *We have* (i) $v_d(G') = v_d(G) - w_d(G)$, (ii) $v_{d+1}(G') = q^d v_{d+1}(G)$. *Consequently,* $v_d(G) - w_d(G) \geqslant q^d v_{d+1}(G)$.

Proof. (ii) can be easily deduced using Lemma 5(iv). In fact we see that $v_j(G') = q^d v_j(G)$ for all $j \geqslant d+1$. Similarly, using Lemma 5(iii) and the fact that $a_d(L) - e \geqslant a_{d-1}(L)$, we can show that $v_j(G') - v_j(G) = x$ is the same for $j = 1, \ldots, d$. Since we have $\Sigma_{j=1}^{n}(q^j - q^{j-1})v_j(G') = w_0 - w_n = e$, we can compute and get $x = -w_d$. □

By Lemma 3, Lemma 4(i), and Lemma 5(i), $u(F_L)$ depends on $a[L]$ only. Thus we can define $f_{j,\bar{r}}(q)$ to be such that $u_j(F_L) = f_{j,\bar{r}}(q)q^j/(q_j q_{j+1})$ for any F_L such that $a[L] = r$. We will compute $f_{j,\bar{r}}(q)$ in the next section and show that it is a polynomial function $\in \mathbf{Z}[q, q^{-1}]$. Assuming this, we can prove Theorem 2 now. Use an induction on $\Sigma s_j[L]$. We have assumed that the theorem is true when $s[L] = 0$, i.e. $\Sigma s_j[L] = 0$. If $\Sigma s_j[L] > 0$, choose any d such that $s_d[L] > 0$. Note that $r[L_d] = r[L]$ and $s_d[L_d] = s_d[L] - 1$, $s_j[L_d] = s_j[L]$ if $j \neq d$. By Lemma 6 and Proposition 5 (or rather, the proof of Lemma 6), we have

$$u(F_L) = (u_1(F_{L_d}), \ldots, u_{d-1}(F_{L_d}), q^{-d}u_d(F_{L_d}), \ldots, q^{-d}u_{n-1}(F_{L_d})).$$

Now we can apply the induction hypothesis to F_{L_d} to conclude the proof.

10. Computation of $f_{j,\bar{r}}(L)$

We maintain the notations and assumptions of the preceding section. Moreover, until the end of this section, we assume that $a(L) = a[L] = r(L)$, so $s(L) = 0$. We are going to derive a formula for $u_j(F_L) = f_{j,\bar{r}[L]}(q)q^j/(q_j q_{j+1})$. We shall omit the reference to F_L or L in notations because this causes no ambiguity. For example, r_j is $r_j(L)$; u_j is $u_j(F_L)$.

One more definition is in order. For $x \in \mathbf{Z}/e\mathbf{Z}$, we use $\tilde{x}$ to denote the unique representative $\tilde{x} \in \mathbf{Z}$ of x such that $0 \leqslant \tilde{x} \leqslant e-1$. If $x_0, \ldots, x_k \in \mathbf{Z}/e\mathbf{Z}$, we write

$$x_0 \preccurlyeq \cdots \preccurlyeq x_k$$

if $0 \leqslant (x_1 - x_0)\tilde{} \leqslant \cdots \leqslant (x_k - x_0)\tilde{}$. If $x, y, z \in \mathbf{Z}/e\mathbf{Z}$ and $x \preccurlyeq y \preccurlyeq z$, we say that y is *between* x and z. For example, if $e = 10$, we have $2 \preccurlyeq 5 \preccurlyeq 6 \preccurlyeq 8$, and $7 \preccurlyeq 9 \preccurlyeq 0 \preccurlyeq 4$.

LEMMA 7. *The following formulas hold:*

(i) $u_j = \dfrac{q^j}{q_j q_{j+1}}(e - ((q-1)(v_1 - v_2) + (q^2-1)(v_2 - v_3)$
$+ \cdots + (q^j - 1)(v_j - v_{j+1})));$

(ii) $v_j - v_{j+1} = \dfrac{q^{c(r_{j-1}+1)}}{(q^f-1)q^{r_{j-1}f}} + \displaystyle\sum_{i=r_{j-1}+2}^{r_j} \dfrac{q^{c(i)} - q^{c(i-1)}}{(q^f-1)q^{(i-1)f}} - \dfrac{q^{c(r_j)}}{(q^f-1)q^{r_j f}};$

(iii) $c(i) = if - \sum_{j\geqslant 0} \max(\lceil (i - r_j)/e\rceil, 0).$

Proof. (i) is trivial. (ii) is direct from Lemma 3. (iii) can be verified for negative i and by an induction based on the relation $c(i) = c(i-e) + \#\{j \mid i \leqslant r_j\}$. □

PROPOSITION 6. *For any j, suppose that $\bar{r}_{u_1}, \ldots, \bar{r}_{u_k}$ are all numbers among $\bar{r}_0, \ldots, \bar{r}_j$ which are between $\bar{r}_{j-1}$, and $\bar{r}_j$, not equal to $\bar{r}_{j-1}$ and such that*

$$\bar{r}_{j-1} \preccurlyeq \bar{r}_{u_1} \preccurlyeq \cdots \preccurlyeq \bar{r}_{u_k} \preccurlyeq \bar{r}_j.$$

Put $u_0 = j-1$. Then we have

$$v_j - v_{j+1} = q^{m_{j-1}} \sum_{t=0}^{k-1} \frac{(r_{u_{t+1}} - r_{u_t} \bmod e)}{q^t},$$

with

$$m_{j-1} = -\sum_{i\geqslant 0} \max(\lceil (r_{j-1} + 1 - r_i)/e\rceil, 0).$$

REMARK. From this proposition we see immediately: $\bar{r}_{j-1} = \bar{r}_j \Leftrightarrow v_j = v_{j+1} \Leftrightarrow f_{j-1,\bar{r}} = f_{j,\bar{r}}$.

Proof. Let $R_0 \leqslant \cdots \leqslant R_k$ be integers such that $r_{j-1} \leqslant R_t \leqslant r_j$ and $R_t \equiv r_{i_t} \pmod e$. Such integers are uniquely determined. Then we have $c(i) = if + m_{j-1} - t$ if $R_t + 1 \leqslant i \leqslant R_{t+1}$. For simplicity, we let $m = m_{j-1}$ in the remaining of this proof.

Therefore, by Lemma 7(ii),

$$\begin{aligned} &v_j - v_{j+1} \\ &\quad = \frac{q^{m+(R_0+1)f}}{(q^f-1)q^{R_0 f}} \\ &\qquad + \sum_{t=0}^{k-2} \left(\sum_{i=R_t+2}^{R_{t+1}} \frac{q^{if+m-t}(1 - 1/q^f)}{(q^f-1)q^{(i-1)f}} \right. \end{aligned}$$

$$+ \frac{q^{(R_{t+1}+1)f+m-(t+1)} - q^{R_{t+1}f+m-t}}{(q^f-1)q^{R_{t+1}f}}\Bigg)$$

$$+ \sum_{i=R_{k-1}+2}^{R_k} \frac{q^{if+m-(k-1)}(1-1/q^f)}{(q^f-1)q^{(i-1)f}} - \frac{q^{R_kf+m-(k-1)}}{(q^f-1)q^{R_kf}}$$

$$= q^m \left(\frac{q^f}{q^f-1} + \sum_{t=0}^{k-2} \left(\frac{R_{t+1}-R_t-1}{q^t} + \frac{q^{f-(t+1)}-q^{-t}}{q^f-1} \right) \right.$$

$$\left. + \frac{R_k - R_{k-1}-1}{q^{k-1}} - \frac{q^{-(k-1)}}{q^f-1} \right)$$

$$= q^m \sum_{t=0}^{k-1} \frac{(r_{u_{t+1}} - r_{u_t} \bmod e)}{q^t}. \qquad \square$$

PROPOSITION 7. *Suppose that $j \geqslant 1$ is such that $\bar{r}_j \neq \bar{r}_{j+1}$ or $j = n-1$. If $r_j = 0$, then $f_{j,\bar{r}} = e$. Otherwise, sort $\bar{r}_0, \ldots, \bar{r}_j$ into a sequence*

$$\bar{r}_{v_0} \preccurlyeq \bar{r}_{v_1} \preccurlyeq \cdots \preccurlyeq \bar{r}_{v_j},$$

with $v_j = j$. Then

$$f_{j,\bar{r}} = q^{m_j+j+1} \left((\bar{r}_{v_0} - \bar{r}_{v_j} \bmod e) + \sum_{t=1}^{j} \frac{(r_{v_t} - r_{v_{t-1}} \bmod e)}{q^t} \right),$$

where m_j is as in Proposition 6.

REMARK. Note that this gives an explicit formula for all $f_{j,\bar{r}}$, for if $\bar{r}_j = \bar{r}_{j+1} = \cdots = \bar{r}_{j+\nu} \neq \bar{r}_{j+\nu+1}$, then $f_{j,\bar{r}} = f_{j+1,\bar{r}} = \cdots = f_{j+\nu,\bar{r}}$ and the above gives the formula for $f_{j+\nu,\bar{r}}$.

Proof. Perform an induction on j. The case $r_j = 0$ is quite easy. Now assume that $r_j > 0$ and $r_j = r_{j-1} = \cdots = r_{j-\nu} \neq r_{j-\nu-1}$. By the induction hypothesis, our formula is valid for $f_{j-\nu-1,\bar{r}}$. It remains to verify that $f_{j,\bar{r}} = f_{j-\nu,\bar{r}} = f_{j-\nu-1,\bar{r}} + (1-q^{j-\nu})(v_{j-\nu} - v_{j-\nu+1})$ is still given by our formula.

To get the expression for $v_{j-\nu} - v_{j-\nu+1}$, we assume that $\bar{r}_{u_1} \preccurlyeq \cdots \preccurlyeq \bar{r}_{u_k}$ are all numbers among $\bar{r}_0, \ldots, \bar{r}_{j-\nu}$ which are between $\bar{r}_{j-\nu-1}$ and $\bar{r}_{j-\nu}$ and not equal to $\bar{r}_{j-\nu-1}$. Then one can express $v_{j-\nu} - v_{j-\nu+1}$ in terms of these numbers and $m_{j-\nu-1}$ by Proposition 6.

To get the expression for $f_{j-\nu-1,\bar{r}}$, we have to sort $\bar{r}_0, \ldots, \bar{r}_{j-\nu-1}$. It is easily seen that we will get

$$\bar{r}_{v_{j-\nu-k+1}} \preccurlyeq \cdots \preccurlyeq \bar{r}_{v_{j-\nu-1}} \preccurlyeq \bar{r}_{v_0} \preccurlyeq \cdots \preccurlyeq \bar{r}_{v_{j-\nu-k}} = \bar{r}_{j-\nu-1},$$

and the sequence $\bar{r}_{u_1}, \ldots, \bar{r}_{u_k}$ is nothing more or less than $\bar{r}_{j-\nu-k+1}, \ldots, \bar{r}_{j-\nu}$.

Now it is routine to verify the result. One will see that every thing matches provided that we have the relation $m_j = m_{j-\nu-1} - k$. This is easy verified. Thus the proof is complete. □

COROLLARY.

$$f_{n-1,\bar{r}} = \frac{q^n - 1}{q^f - 1} q^{m_{n-1}+f},$$

with

$$m_{n-1} = -\sum_{i \geqslant 0} \left\lceil \frac{r_{n-1} + 1 - r_i}{e} \right\rceil .$$

Proof of Corollary to Theorem 2. Now we drop the assumption that $s[L] = 0$ and consider an arbitrary quasi-canonical lifting F_L. The point $(q^j, w_j(F_L))$ is not a break $\Leftrightarrow$ $v_j(F_L) = v_{j+1}(F_L)$ $\Leftrightarrow$ $u_j(F_L) q_j q_{j+1}/q^j = u_{j-1} q_{j-1} q_j / q^{j-1}$ (by Lemma 7(i); in fact LHS $\leqslant$ RHS always holds) $\Leftrightarrow$ $f_{j,\bar{r}[L]} q^{-s_j[L]} = f_{j-1,\bar{r}[L]}$ $\Leftrightarrow$ $s_j[L] = 0$ and $f_{j,\bar{r}[L]} = f_{j-1,\bar{r}[L]}$ $\Leftrightarrow$ $s_j[L] = 0$ and $r_{j-1}[L] = r_j[L]$ $\Leftrightarrow$ $a_j[L] = a_{j-1}[L]$. □

Proof of Corollary to Theorem 2'. The degree of the ring class field of $\mathcal{O}$ is given in Lemma 1. By the corollary to Theorem 2 and our assumption, $\mathrm{ord}((m_{\mathcal{O}^\vee})_{n-1}) = w_{n-1}(F_{\mathcal{O}^\vee})$. It remains to find out when $\#(A^*/\mathcal{O}^*) = w_{n-1}(F_{\mathcal{O}^\vee})^{-1}$ holds. Using the explicit formula for $f_{n-1,\bar{r}}$, we easily get the two conditions. □

11. Explicit parametrizations of Lubin–Tate space and Gross–Hopkins map

Let $A_0[v]$ be the polynomial ring of infinitely many variables $v_1, v_2, \ldots,$ over A_0. Let $f(v)(X)$ be the unique power series with coefficients in $K[v]$ which satisfies

$$f(v)(X) = X + \frac{1}{\pi_0} \sum_{i \geqslant 1} v_i f(v)^{q^i}(X^{q^i}),$$

where $f(v)^{q^i}(X)$ is the series obtained from $f(v)(X)$ by replacing each variable v_j by $v_j^{q^i}$. It can be shown [7] that there is a unique formal A_0-module law $F(v)$ over $A_0[v]$ whose logarithm is $f(v)$. In that case, $[\pi_0]_{F(v)}$ has the following property [6, Prop. 5.8]:

$$[\pi_0]_{F(v)} \equiv v_k X^{q^k}, \quad (\operatorname{mod} \pi_0, v_1, \ldots, v_{k-1}), \ (\operatorname{mod} \deg q^k + 1).$$

Moreover [7],

PROPOSITION. *We can specialize $F(v)$ by setting each v_j to some suitable $\alpha_j \in A$ to get the canonical lifting F over A.*

PROPOSITION. *Specialize $F(v)$ as follows: setting v_i to $t_i \in A[[t]] = A[[t_1, \ldots, t_{n-1}]]$ for $1 \leqslant i \leqslant n-1$, v_i to α_i for $i \geqslant n$, we obtain a formal A_0-module over $A[[t]]$, to be denoted by $\mathcal{F}$ or $\mathcal{F}(t)$. Then $\mathcal{F}$ is a universal lifting of $\bar{F}$.*

REMARK. When K/K_0 is ramified, $\mathcal{F}$ cannot be a universal lifting in the sense of Section 2, for $A \neq W_{A_0}(k)$. Here, we mean that $\mathcal{F}$ furnishes an isomorphism of $X_{\bar{F}} \otimes_{W_{A_0}(k)} A$ with $\operatorname{Spf} A[[t]]$.

From now on *we assume that K/K_0 is unramified and $\pi = \pi_0$*. Moreover, we assume that $[\pi_0]_F \in A_0[[X]]$. By [11], this is possible and it implies that F is actually defined over A_0. Consequently, $\bar{F}^{(q^N)} = \bar{F}$ for all N. All quasi-canonical liftings are liftings of $\bar{F}$, and have $\bar{r} = \bar{r}_{\text{can}} = 0$. We easily get $f_{j,0} = 1$ for all j.

We choose a universal lifting $\mathcal{F}$ of $\bar{F}$ as follows: $\mathcal{F}$ is obtained from $F(v)$ by setting $v_i = t_i$ for $1 \leqslant i \leqslant n-1$, $v_n = 1$, $v_i = 0$ for $i > n$. Then one can show as in [6, Sect. 13] that the modulus of the canonical lifting is 0.

Now we take a closer look at the logarithm $f(v)$ of $F(v)$. Let

$$f(v)(X) = \sum_{m \geqslant 0} b_m(v) X^{q^m}.$$

A recursive expression for the coefficients $b_n(v)$ is immediate from the definition:

$$b_0(v) = 1, \quad b_m(v) = \pi_0^{-1} \sum_{i=0}^{m-1} b_i(v) v_{m-i}^{q^i}.$$

We are going to write down a more explicit formula for $b_m(v)$. It turns out that the monomials in $b_m(v)$ can be indexed by *ordered partitions* of m. An ordered partition of m means a decomposition of m into a sum of positive integers: $m = \Sigma_{j=1}^{s} l_j$. Equivalently, we can say that an ordered partition of m means dividing $\langle 0, 1, \ldots, m-1 \rangle$ into segments $\langle 0, \ldots, l_1 - 1 \rangle, \langle l_1, \ldots, l_1 + l_2 - 1 \rangle, \ldots$. Let S_i $(i \geqslant 1)$ be the set of the first elements in segments of length i. Then the sets $\{S_i\}_{i \geqslant 1}$ are determined by the ordered partition and conversely, determine the ordered partition. For our applications, it is most convenient to refer to the collection of sets $S = \{S_i\}_{i \geqslant 1}$ as an *ordered partition*. Now introduce the following notation: $q(S_i) = \Sigma_{x \in S_i} q^x$. An easy induction yields

LEMMA 8. *For all $m \geqslant 0$,*

$$b_m(v) = \sum_S \prod_i \frac{v_i^{q(S_i)}}{\pi_0^{\# S_i}},$$

where the sum is taken over all ordered partitions $S = \{S_i\}_{i \geqslant 1}$ of m. □

From this formula we can get a similar formula for the coefficients $b_m(t)$ of the logarithm of $\mathcal{F}(t)$.

PROPOSITION 8. *For any* $j \geqslant 0$,

$$\lim_{k\to\infty} \pi_0^k b_{j+nk}(t)$$

exists in $K_0[[t]]$. *The limit is*

$$\sum_{S\in P_j} \frac{\prod_{t=1}^{n-1} t_i^{q(S_i)}}{\pi_0^{(1/n)(j+\Sigma(n-i)\#S_i)}},$$

where P_j *is the set of all ordered partitions* $S = \{S_i\}_{i\geqslant 1}$ *such that* (1) *there is an integer* k *such that* S *is an ordered partition of* $j + nk$; (2) $j + nk - n \notin S_n$; (3) S_i *is empty for all* $i > n$.

Proof. Let $a_k = \pi_0^k b_{j+nk}(t)$. It is clear that if we specialize the expansion of $b_m(v)$ to get the expansion of $b_m(t)$, only terms involving ordered partitions such that S_i is empty for all $i > n$ are left. It is also clear that $a_k - a_{k-1}$ is the sum of terms involving ordered partitions such that $j + nk - n \notin S_n$. Then $j + nk - n$ has to belong to some $S_i + t$ with $1 \leqslant i \leqslant n-1$ and $0 \leqslant t \leqslant i-1$, and the exponent of t_i in such a term is at least $q^{j+nk-n-(i-1)} > q^{j+nk-2n}$. It follows immediately that $\{a_k\}$ is a Cauchy sequence and converges to the claimed limit. □

It is immediate from the above formula that the limit power series converges on the open unit polydisc $(X_{\bar{F}} \otimes K_0)(\bar{K}_0) = \{x \in \bar{K}_0^{n-1} \mid \mathrm{ord}(x) > 0\}$ and hence defines a rigid analytic function there. Gross and Hopkins define the maps

$$\Phi_0(t) = \lim_{k\to\infty} \pi^k b_{nk}(t),$$

$$\Phi_j(t) = \lim_{k\to\infty} \pi^{k+1} b_{j+nk}(t), \quad j = 1, 2, \ldots, n-1,$$

and use them to define the map $\Phi: X_{\bar{F}} \otimes K_0 \to \mathbf{P}^{n-1} \otimes K_0$, $t \mapsto [\Phi_0(t), \ldots, \Phi_{n-1}(t)]$. That this map is well-defined and étale follows from

PROPOSITION 9. *The determinant of* $T(t) = (\Phi(t), D_{t_1}\Phi(t), \ldots, D_{t_{n-1}}\Phi(t))$ *is a unit in* $A_0[[t]]$. *If the characteristic of* K_0 *is positive, we have* $\det T(t) = 1$.

We will give a proof of the second statement. Let

$$T'(t) = (\Phi(t), t_1 D_{t_1}\Phi(t), \ldots, t_{n-1} D_{t_{n-1}}\Phi(t))$$

and we will show $\det T'(t) = t_1 t_2 \ldots t_{n-1}$. Write $\Phi_j(t) = \Sigma_{S\in P_j} t_S^j$, where

$$t_S^j = \pi_0^{-\lfloor(\Sigma(n-i)\#S_i)/n\rfloor} \prod_{i=1}^{n-1} t_i^{q(S_i)}.$$

Then $t_k D_{t_k}\Phi_j(t)$ is given by

$$\sum_{\substack{S\in P_j\\ 0\in S_k}} t_S^j.$$

Now we expand $\det T'(t)$. A typical term in the expansion is $\operatorname{sgn}(\sigma)t_{S(0)}^{\sigma(0)}\cdots t_{S(n-1)}^{\sigma(n-1)}$, where σ is a permutation on $\{0,1,\ldots,n-1\}$ and $t_{S(0)}^{\sigma(0)}$ is a term in the expansion of $\Phi_{\sigma(0)}$, $t_{S(k)}^{\sigma(k)}$ is a term in the expansion of $t_k D_{t_k}\Phi_{\sigma(k)}$ for $1 \leqslant k \leqslant n-1$.

Let $m-1 = \max_k \max_i(S(k)_i + (i-1))$. Assume $m-1 \in S(k_0)+(i_0-1)$. Then (k_0, i_0) is unique and in fact $m \equiv \sigma(k_0) \pmod n$. Suppose $m > i_0$. Let k_1 be such that $\sigma(k_1) \equiv m - i_0 \pmod n$. Define a new permutation: $\sigma'(k_0) = \sigma(k_1)$, $\sigma'(k_1) = \sigma(k_0)$, $\sigma'(k) = \sigma(k)$ if $k \neq k_0, k_1$. Let $S'(k) = S(k)$ if $k \neq k_0, k_1$. Let $S'(k_0)$ be the same as $S(k_0)$ except that $m - i_0$ is removed from $S(k_0)_{i_0}$. Let $S'(k_1)$ be the same as $S(k_1)$ except that $m - i_0$ is added to $S(k_1)_{i_0}$. We may have to remove some numbers from $S'(k_0)_n$ or to add some numbers to $S'(k_1)_n$ so that $t_{S'(0)}^{\sigma'(0)}$ is a term in the expansion of $\Phi_{\sigma'(0)}(t)$, $t_{S'(k)}^{\sigma'(k)}$ is a term in the expansion of $t_k D_{t_k}\Phi_{\sigma(k)}$ for $1 \leqslant k \leqslant n-1$.

Now it is easy to verify that $t_{S(0)}^{\sigma(0)}\cdots t_{S(n-1)}^{\sigma(n-1)} = t_{S'(0)}^{\sigma'(0)}\cdots t_{S'(n-1)}^{\sigma'(n-1)}$. But the signs $\operatorname{sgn}(\sigma)$, $\operatorname{sgn}(\sigma')$ differ. So they are cancelled with each other in the expansion of $\det T'(t)$.

Thus only terms such that $m = i_0$ are left. But there is only one such term, namely $1\cdot t_1\cdot\cdots\cdot t_{n-1}$. This completes the proof of $\det T(t) = 1$. □

Gross and Hopkins define an action of $G = \operatorname{Aut}(\bar F)$ on both $X_{\bar F}$ and $\mathbf{P}^{n-1}$ and show that the map Φ is G-equivariant. In fact, let R be the ring of integers in the division algebra over K_0 of invariant $1/n$, then $\operatorname{End}_{\bar k}(\bar F) = R$ and $G(\bar k) = R^*$ (cf. Sect. 14). The action of $G(\bar k)$ on $\mathbf{P}^{n-1}$ can be extended to the action of the larger group $(R\otimes K_0)^*$ and we have the following wonderful property.

PROPOSITION. *If $t, t' \in X_{\bar F}(\bar A_0)$, $g \in G(\bar k)$, then $\Phi(t)\,.\,g = \Phi(t')$ if and only if there is an element $f \in \operatorname{Hom}_{\bar A_0}(\mathcal{F}(t), \mathcal{F}(t'))\otimes_{A_0} K_0$ such that $f\otimes \bar k_0$ is equal to g.*

Using this proposition, one can show that the inverse image of $[e_i]$ precisely consists of those quasi-canonical liftings F_L such that $\Sigma_{j=0}^{n-1} j s_j(L) \equiv i \pmod n$. Here $e_1 = (1,0,\ldots,0)$, $e_2 = (0,1,0,\ldots,0), \ldots$, are the standard basis of $\mathbf{G}_a^n$ and $x \mapsto [x]$ is the projection $\mathbf{G}_a^n\backslash\{0\} \to \mathbf{P}^{n-1}$.

12. The Bruhat–Tits building for $\mathrm{SL}_n(K_0)$

In the current case (K/K_0 unramified, $\pi = \pi_0$), the $\pi^{\mathbf{Z}}$-orbits of lattices in K are the same as the K_0^*-orbits. This shows that the quasi-canonical liftings correspond bijectively to the vertices of the Bruhat–Tits building for $\mathrm{SL}_n(K_0)$. We find that our next main result (Theorem 3) is best formulated in terms of the apartment $\mathcal{A}$ of this building, which is described below:

Let $p_n \in \mathbf{R}^n$ be the vector $e_1 + \cdots + e_n$, $W = \mathbf{R}^n/\mathbf{R}p_n$, and $\phi\colon \mathbf{R}^n \to W$ be the natural map. The set of vertices in $\mathcal{A}$ is $\phi(\mathbf{Z}^n)$. Let $p_k = \Sigma_{i=1}^k e_i \in \mathbf{R}^n$ $(1 \leqslant k \leqslant n)$. Then for any point $x \in \mathbf{Z}^n$, and any $\sigma \in S_n \subset \mathrm{GL}_n(\mathbf{Z})$, the n points $\phi(x + \sigma . p_i)\,(1 \leqslant i \leqslant n)$ form an $(n-1)$-simplex in $\mathcal{A}$ and any simplex is contained in such an $(n-1)$-simplex. The geometric realization $|\mathcal{A}|$ of $\mathcal{A}$ is an $(n-1)$-dimensional affine space. To see this, we remark that the affine root system Φ of $\mathrm{SL}_n(K)$ consists of the affine functions $e_i^* - e_j^* - m$ $(i \neq j,\ m \in \mathbf{Z},\ \{e_i^*\}$ is the dual basis of $\{e_i\})$ on W and the geometric realization of $(n-1)$-simplices in the apartment are the Weyl chambers of Φ. Therefore, by standard theory of Coxeter groups, $|\mathcal{A}|$ is the $(n-1)$-dimensional space W. The action of S_n on $\mathbf{R}^n$ induces an action on W. A fundamental domain for this action is $\{\phi(x) \mid x_1 \geqslant \cdots \geqslant x_n\}$, which can be considered as a geometric realization $|\mathcal{A}^+|$ for some subcomplex $\mathcal{A}^+$ in an obvious way.

We shall put two coordinates s, l on $|\mathcal{A}|$, which we identify with W. For any point $P = \phi(t_1, \ldots, t_n) \in W$, we set $s_i(P) = t_{i+1} - t_i$, $l_i(P) = s_1(P) + 2s_2(P) + \cdots + is_i(P)$. We also set $l(P) \stackrel{\mathrm{def}}{=} l_{n-1}(P)$. This function has the following remarkable property: for any $(n-1)$-simplex with vertices $P_0, \ldots, P_{n-1}$, the integers $l(P_i)$ are all distinct modulo n. By abuse of notation, we also use $l_i(s)$ to denote $s_1 + 2s_2 + \cdots + is_i$, for any $s \in \mathbf{R}^{n-1}$.

13. Valuation functions of Gross–Hopkins map

To state the following theorem, we shall use $q^{-l(P)}$ to denote the point

$$(q^{-l_1(P)}, \ldots, q^{-l_{n-1}(P)}) \in \mathbf{R}^{n-1},$$

for any $P \in |\mathcal{A}|$. Recall that $q_i = (q^i - 1)/(q-1)$.

THEOREM 3. *Let $t \in X(\bar{A})$,*

$$y_i = \frac{q_i q_{i+1}}{q^i}\left(\frac{\mathrm{ord}(t_i)}{q_i} - \frac{\mathrm{ord}(t_{i+1})}{q_{i+1}}\right),$$

for $1 \leqslant i \leqslant n-1$. Assume $1 \geqslant y_1 \geqslant \cdots \geqslant y_{n-1} > 0$. There is some $(n-1)$-simplex Δ on $\mathcal{A}$ with vertices $P_0, \ldots, P_{n-1}$ such that y is on the geometric simplex in $\mathbf{R}^{n-1}$ spanned by $q^{-l(P_0)}, \ldots, q^{-l(P_{n-1})}$. Arrange the index so that $l(P_j) \equiv j \pmod n$. Then we have

$$\mathrm{ord}(\Phi_j(t)) \geqslant \sum_{i=1}^{n-1} q_{l_i(P_j)} \frac{q^i}{q_i q_{i+1}} y_i - \left\lfloor n^{-1} \sum_{i=1}^{n-1} (n-i) s_i(P_j) \right\rfloor.$$

The equality holds when y is not on the face of Δ opposite to P_j.

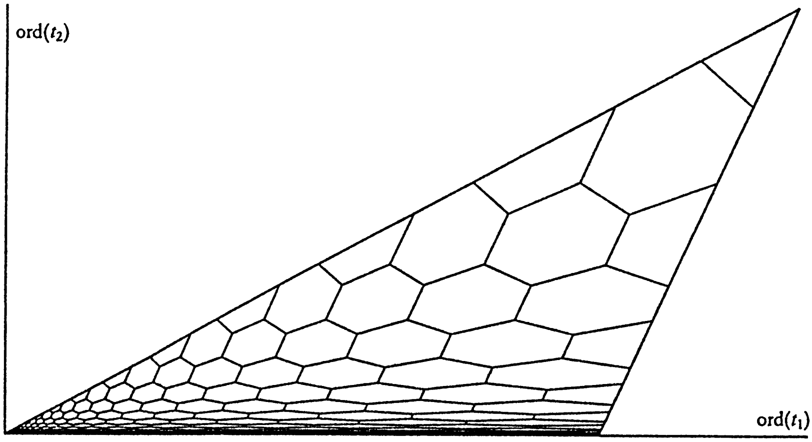

Fig. 1. Exceptional set of Φ_0.

REMARK. Let $t \in X(\bar{A})$ and y_i be given as above. The condition $1 > y_1 > \cdots > y_{n-1} > 0$ is equivalent to that the Newton polygon of the multiplication-by-π morphism on $F(t)$ has a break at $(q^i, \operatorname{ord}(t_i))$ for each $i = 1, \dots, n-1$.

EXAMPLE 1 $(n = 2)$. We have

$$\begin{cases} \operatorname{ord}(\Phi_0(t)) = \frac{q^{2m}-1}{q-1} \operatorname{ord}(t) - m, & \text{if } q^{-(2m+1)} < \frac{q+1}{q} \operatorname{ord}(t) < q^{-(2m-1)}; \\ \operatorname{ord}(\Phi_1(t)) = \frac{q^{2m+1}-1}{q-1} \operatorname{ord}(t) - m, & \text{if } q^{-2(m+1)} < \frac{q+1}{q} \operatorname{ord}(t) < q^{-2m}. \end{cases}$$

Therefore, the exceptional set of Φ_0 (resp. Φ_1) consists of the valuations of the moduli of quasi-canonical liftings of odd (resp. even) levels.

EXAMPLE 2 $(n = 3)$. The exceptional sets of Φ_0, Φ_1, Φ_2 in the region $1 \geqslant y_1 \geqslant y_2 \geqslant 0$ are shown in Figure 1, Figure 2, Figure 3, and Figure 4 is all the three figures overlapped. The vertices in Figure 4 represent the valuations of the moduli of quasi-canonical liftings.

We begin the proof with a few Lemmas.

LEMMA 9. *The valuation function of $\Phi_j(t)$ restricted to*

$$\Omega = \left\{ x \in \mathbf{R}_{\geqslant 0}^{n-1} \;\middle|\; \frac{x_i}{q_i} > \frac{x_{i+1}}{q_{i+1}},\ 1 \leqslant i \leqslant n-2 \right\}$$

is the same as that of

$$\Psi_j(t) = \sum_{s \in F_j} \pi^{-\lfloor n^{-1}\Sigma(n-i)s_i \rfloor} \prod_{i=1}^{n-1} U_i^{q l_i(s)},$$

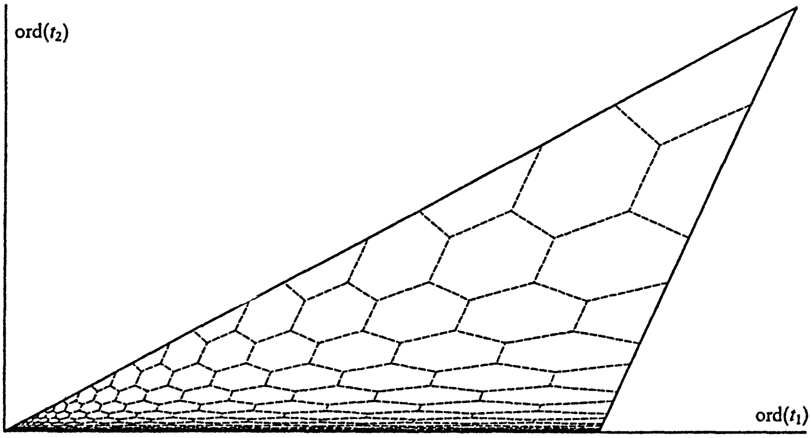

Fig. 2. Exceptional set of Φ_1.

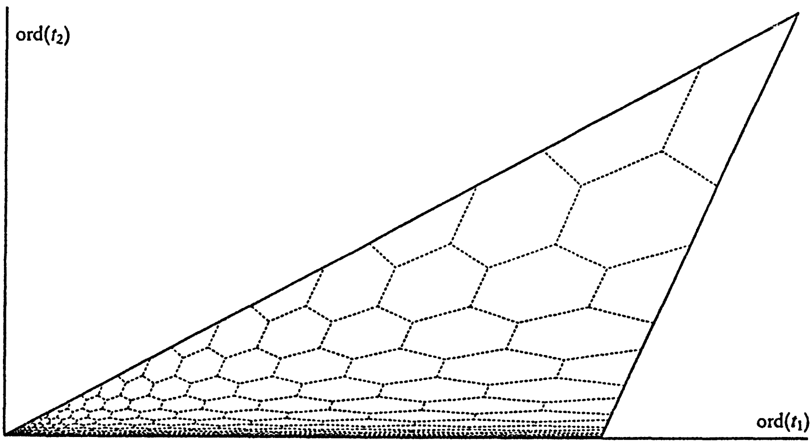

Fig. 3. Exceptional set of Φ_2.

where $U_{n-1} = t_{n-1}^{1/q_{n-1}}$, $U_i = t_i^{1/q_i} t_{i+1}^{-1/q_{i+1}}$, $1 \leqslant i \leqslant n-2$, *and* F_j *is the set of all* $(n-1)$*-tuple* s *of non-negative integers such that* $s_1 + 2s_2 + \cdots + (n-1)s_{n-1} \equiv j \pmod{n}$. *Moreover, the exceptional sets* E_{Φ_j} *and* E_{Ψ_j} *are also the same.*

Proof. Using the notations in the proof of Proposition 9, $\Psi_j(t)$ can be rewritten as follows:

$$\Psi_j(t) = \sum_s t^j_{S(s)},$$

where $S(s)_i = \{l_{i-1}(s) + it \mid t = 0, 1, \ldots, s_i - 1\}$. We make the following claim: *given* $t \in \bar{A}$ *such that* $\mathrm{ord}(t) \in W$, *if* $t^j_S(t)$ *is of minimal order in the expansion of* $\Phi_j(t)$, $s_i = \#S_i$, *then* $S = S(s)$. Both statements of the lemma will follow from this claim.

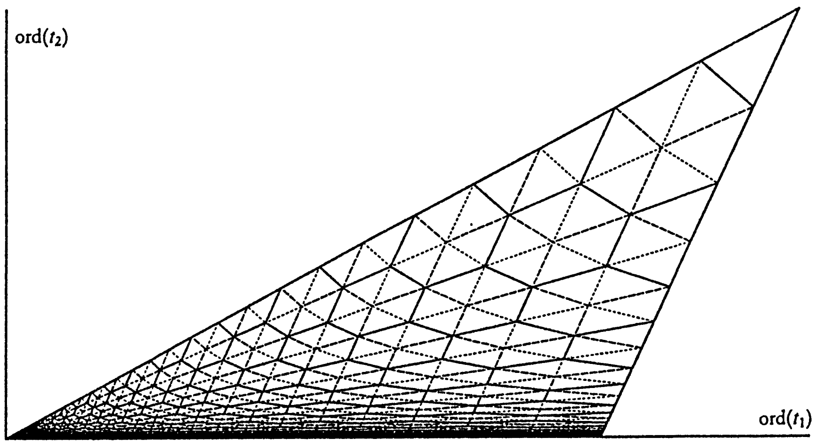

Fig. 4.

To prove the claim, let $x = \mathrm{ord}(t)$. By assumption, the minimum of $\Sigma q(T_i)x_i - n^{-1}\Sigma(n-i)\#T_i\,(T \in P_j)$ occurs when $T = S$. Recall that the ordered partition S of m can be considered as a finite sequence of positive integers (l_j) such that $\Sigma l_j = m$. Our claim is equivalent to: (l_j) is an increasing sequence. But this is easy to verify: if $l_j > l_{j+1}$, exchange l_j and l_{j+1} we get a new ordered partition T and it can be shown that $\Sigma q(T_i)x_i - n^{-1}\Sigma(n-i)\#T_i$ is strictly smaller than $\Sigma q(S_i)x_i - n^{-1}\Sigma(n-i)\#S_i$ using the relation $x_i/q_i > x_{i+1}/q_{i+1}$. This finished the proof of the claim and also of the lemma. □

For any $(n-1)$-simplex Δ with vertices $P_0, \ldots, P_{n-1}$ on $\mathcal{A}$, let $|q^\Delta|$ be the geometric simplex in $\mathbf{R}^{n-1}$ spanned by $q^{-l(P_0)}, \ldots, q^{-l(P_{n-1})}$. This first statement of Theorem 3 is contained in the following, which is basically a consequence of our description of $|\mathcal{A}^+|$.

LEMMA 10. *The subset $\Omega' = \{x \in \mathbf{R}^{n-1}_{>0} \mid 1 \geqslant x_1 \geqslant \cdots \geqslant x_{n-1}\}$ is the union of all $|q^\Delta|$ for all Δ on $\mathcal{A}^+$.* □

LEMMA 11. *Let $f(X) = \Sigma_{k \in \mathbf{Z}^n} a_k X^k$ be a power series in n variables,*

$$V_f(x) = \min_k\{\mathrm{ord}(a_k) + k \,.\, x\}$$

be its valuation function. For any k, the set $\{x \in \mathbf{R}^n \mid V_f(x) = \mathrm{ord}(a_k) + k \,.\, x\}$ is convex. □

From these lemmas, Theorem 3 can be translated into the following statements:

(A) For any vertex P on $\mathcal{A}$, let $j \equiv l(P)$, then the minimal of

$$\sum \frac{q^i}{q_i q_{i+1}} q_{l_i(t)} q^{l_i(P)} - \lfloor n^{-1} \sum (n-i) t_i \rfloor, \quad t \in F_j$$

occurs when and only when $t = s(P)$.

(B) If P' is a vertex adjacent to P, then the minimum of

$$\sum \frac{q^i}{q_i q_{i+1}} q_{l_i(t)} q^{l_i(P')} - \lfloor n^{-1} \sum (n-i) t_i \rfloor, \quad t \in F_j$$

occurs when $t = s(P)$ (it may also occur somewhere else).

These statements are further translated into the following lemma:

LEMMA 12. *Let $\epsilon \in \mathbf{Z}^{n-1}$ be such that $\epsilon = 0$ or $\epsilon = s(P) - s(Q)$ for some adjacent vertices P, Q on $\mathcal{A}$. For any $s \in \mathbf{Z}^{n-1}$ such that $l(s) \equiv 0 \pmod{n}$, we have*

$$\sum q^{l_i(\epsilon)}(q^{l_i(s)} - 1)\left(\frac{1}{q^i - 1} - \frac{1}{q^{i+1} - 1}\right) \geqslant n^{-1} \sum (n-i) s_i.$$

In case $\epsilon = 0$, the equality holds if and only if $s = 0$.

Proof. Let $b = n^{-1}\Sigma(n-i)s_i$. Let $z = q^{-1} < 1$. Let $W(q)$ be the LHS of the inequality in question. We are going to expand $W(1/z)/(1-z)$ into a Laurentz series around $z = 0$: $W(z)/(1-z) = \Sigma_{i\in\mathbf{Z}} a_k z^k$ and to show that $a_i \geqslant b$ for all $i \geqslant 0$, and $a_i \geqslant 0$ for all $i \in \mathbf{Z}$.

Let us introduce the following symbol: for any real x, $\{x\}$ is defined to be $\lfloor x \rfloor$ if $x \geqslant 0$, otherwise it is defined to be 0. Then the coefficient a_k of the expansion of $W(z)$ is easily seen to be

$$\begin{aligned} a_k = \sum_{i=1}^{n-1} \Bigg(&\left\{\frac{k + l_i(s+\epsilon)}{i}\right\} - \left\{\frac{k + l_i(\epsilon)}{i}\right\} - \left\{\frac{k + l_i(s+\epsilon)}{i+1}\right\} \\ &+ \left\{\frac{k + l_i(\epsilon)}{i+1}\right\}\Bigg), \qquad (*) \\ = \sum_{i=2}^{n-1} \Bigg(&\left\{\frac{k + l_i(s+\epsilon)}{i}\right\} - \left\{\frac{k + l_i(\epsilon)}{i}\right\} - \left\{\frac{k + l_{i-1}(s+\epsilon)}{i}\right\} \\ &+ \left\{\frac{k + l_{i-1}(\epsilon)}{i}\right\}\Bigg) + \{k + s_1 + \epsilon_1\} - \{k + \epsilon_1\} \\ &- \left\{\frac{k + l(s+\epsilon)}{n}\right\} + \left\{\frac{k + l(\epsilon)}{n}\right\}. \qquad (**) \end{aligned}$$

Now assume $k \geqslant 0$. We claim that if a'_k is defined by the above formula with all $\{\cdot\}$ replaced with $\lfloor\cdot\rfloor$, then $a_k \geqslant a'_k$. To see the claim, we look at $(*)$. Note that $\{x/i\} - \{x/(i+1)\} \geqslant \lfloor x/i \rfloor - \lfloor x/(i+1) \rfloor$ for any real x. This takes care of the terms

$\{k+l_i(s+\epsilon)/i\}-\{k+l_i(s+\epsilon)/i+1\}$. We also note that $|l_i(\epsilon)|$ is always less than or equal to i. Therefore, if $k+l_i(\epsilon)<0$, we have $-\{k+l_i(\epsilon)/i\}+\{k+l_i(\epsilon)/i+1\}=-0+0=-(-1)+(-1)=-\lfloor k+l_i(\epsilon)/i\rfloor+\lfloor k+l_i(\epsilon)/i+1\rfloor$. If $k+l_i(\epsilon)\geqslant 0$, this equality surely holds also. But it is very easy to see from $(**)$ that in fact $a'_k=b$ (using the fact $\lfloor x+n\rfloor-\lfloor x\rfloor=n$ for any $x\in\mathbf{R}$, $n\in\mathbf{Z}$). Thus we have proved $a_k\geqslant b$ for $k\geqslant 0$.

If $k<0$, then all the terms of the form $\{k+l_i(\epsilon)/i\}$ or $\{k+l_i(\epsilon)/i+1\}$ vanish. Thus the inequality $\{x/i\}-\{x/(i+1)\}\geqslant 0$ implies that a_k is non-negative (look at $(*)$).

Finally, if $\epsilon=0$ and the equality holds, we will show that $s=0$. Examining the above arguments, we find that the equality holds precisely when $|l_i(s)|\leqslant i$ for all i. But $l_{n-1}(s)$ is divisible by n, so it must be equal to 0. Moreover, $l_{n-2}(s)\equiv l_{n-1}(s)=0\ (\operatorname{mod} n-1)$, so $l_{n-2}(s)$ must vanish also. Inductively we then show that all $l_i(s)$ are zero. It follows $s=0$. □

The proof of Theorem 3 is now completed.

14. Endomorphisms of reductions of the canonical lifting

Let W be the ring of integers in the completion of the maximal unramified extension of K. We shall determine the endomorphism ring of $F\otimes_A(W/\pi^N W)$ for all $N\geqslant 1$. This result is due to Gross [4] when $n=2$ and to Tatevossian [16] when K/K_0 is unramified. Our proof of the general case is based on Gross' method. Thus we want to re-normalize our constructions, following Gross [4] (cf. discussions at the end of Sect. 4).

Let L be the unramified extension of K_0 of degree n and B its ring of integers. Let G_B be the special model of the Lubin–Tate B-module over B attached to (L,π_0) such that $[\pi_0]_{G_B}(X)=\pi_0X+X^{q^n}$. Let $\bar{G}_B$ be $G_B\otimes_B\bar{k}_0$. Considering $\bar{G}_B$ only as an A_0-module, we get a formal A_0-module $\bar{G}_{A_0}$ of height n. By our choice of $[\pi_0]_{G_B}$, it follows that $\bar{G}_{A_0}$ is actually defined over k_0. In particular, the Frobenius $\varphi\colon X\mapsto X^q$ is an endomorphism of $\bar{G}_{A_0}$. In fact

$$R=\operatorname{End}_{\bar{k}_0}(\bar{G}_{A_0})=\bigoplus_{i=0}^{n-1}B\varphi^i,$$

where B acts on $\bar{G}_{A_0}$ by $b\mapsto[b]_{\bar{G}_B}$. We have $\varphi^n=[\pi_0]_{\bar{G}_B}$, $\varphi\circ[b]_{\bar{G}_B}=[b^\sigma]_{\bar{G}_B}\circ\varphi$, where σ is the Frobenius automorphism of L/K_0. This shows that R is the ring of integers in the division algebra over K_0 of invariant $1/n$.

Now fixing an A_0-embedding $\iota\colon A\to R$. Then $\bar{G}_{A_0}$ can be given a formal A-module structure via ι, to be denoted by $\bar{G}_A$. Clearly $\bar{G}_A$ is of height 1. Therefore it lifts uniquely to W. This unique lifting, when considered as an A_0-module, is denoted by F and is called the canonical lifting of $(\bar{G}_{A_0},\iota)$. Let $F_{N-1}=F\otimes W/\pi^N W$,

$$R_{N-1}=\operatorname{End}_{W/\pi^N W}(F_{N-1}).$$

Reductions of homomorphisms give embeddings

$$R_N \to R_{N-1} \to \cdots \to R_1 \to R_0.$$

Identifying each R_N with its image in $R_0 = R$, we have $\cap_{N \geqslant 0} R_N = A$, which is identified with $\iota(A)$.

THEOREM 4. *For all* $N \geqslant 0$,

$$R_N = A + \pi^N R.$$

Proof. Using formal cohomology, Gross [4] showed that the A-module R_0/R_1 is annihilated by π and reduced the theorem to the following statement: $\dim_k(R_0/R_1) = n - 1$. We observe that Gross' result in particular implies $A + \pi R \subseteq R_1$.

LEMMA 13. *Let* $f \in \mathrm{End}_{W/\pi^2 W}(F_1)$, $g \in (W/\pi^2 W)[[X]]$ *be such that* $g(0) = 0$. *Then*

$$(f + \pi g) \circ [\pi_0]_{F_1} - [\pi_0]_{F_1} \circ (f + \pi g) \equiv 0, \ (\mathrm{mod}\, \pi^2, X^{q^n}).$$

Proof. Since $[\pi_0]_{F_1}(X) \equiv X^{q^n} \ (\mathrm{mod}\, \pi)$, we can write $[\pi_0]_{F_1}(X) = \pi h(X) + X^{q^n}$, with $h(X) \in (W/\pi^2 W)[[X]]$. So

$$\begin{aligned} &[\pi_0]_{F_1} \circ (f + \pi g) - [\pi_0]_{F_1} \circ f \\ &\quad = \pi(h(f + \pi g) - h(f)) + (f + \pi g)^{q^n} - f^{q^n} = 0, \quad (\mathrm{mod}\, \pi^2). \end{aligned}$$

Therefore,

$$\begin{aligned} &(f + \pi g) \circ [\pi_0]_{F_1} - [\pi_0]_{F_1} \circ (f + \pi g) \\ &\quad = f \circ [\pi_0]_{F_1} + \pi g \circ [\pi_0]_{F_1} - [\pi_0]_{F_1} \circ f \\ &\quad = \pi g(\pi h(X) + X^{q^n}) = 0, \quad (\mathrm{mod}\, \pi^2, X^{q^n}). \end{aligned}$$

□

LEMMA 13′. *Let* $f \in R_1$. *Lift* f *arbitrarily to a power series* $f' \in W[[X]]$ *with* $f'(0) = 0$. *Then* $f' \circ [\pi_0]_{F_1} - [\pi_0]_{F_1} \circ f' \equiv 0 \ (\mathrm{mod}\, \pi^2, X^{q^n})$.

Proof. This is a restatement of last lemma. □

LEMMA 14. *There is some* $u \in W^*$ *and some* $g \in W[[X]]$ *with* $g(0) = 1$ *such that*

$$[\pi_0]_{F_1}(X) = u\pi X^{q^{n-f}} g(X), \quad (\mathrm{mod}\, \pi^2, X^{q^n}).$$

Proof. This is clear from the Newton polygon of $[\pi_0]_F$, see the example in Section 6. □

We can replace ι by any $\alpha\iota\alpha^{-1}(\alpha \in \mathrm{Aut}_{\bar{k}}(\bar{G}_{A_0}))$. Therefore, by the theorem of Skolem–Noether, we may assume that the maximal unramified subextension A' of A/A_0 is contained in B (both A and B are now considered as subrings of $R = \mathrm{End}_{\bar{k}}(\bar{G}_{A_0})$).

LEMMA 15. (i) $A'+\pi R = A+\pi R$. (ii) $A'+\varphi R = A+\varphi R$. (iii) $R_1 \subseteq A+\varphi R$.

Proof. To see (i), note that the inclusion $A' + \pi R \subseteq A + \pi R$ is obvious, and that their quotient modulo πR are both of order q^f. (ii) follows from (i). To prove (iii), let $f \in R_1$. Write $f = \Sigma_{i=0}^{n-1}[b_i]_{\bar{G}_B}\varphi^i$, with $b_i \in B$. Lift f to $f' \in W[[X]]$ as

$$f'(X) = \sum_{i=0}^{n-1}[b_i]_{G_B}(X^{q^i}) = b_0X + \text{ higher terms.}$$

An easy computation using Lemma 14 shows that $f' \circ [\pi_0]_{F_1} - [\pi_0]_{F_1} \circ f'$ is of $\mathrm{ord}_X \geqslant q^{n-f}$, and the coefficient of $X^{q^{n-f}}$ is $u\pi(b_0 - b_0^{q^{n-f}}) \pmod{\pi^2}$. By Lemma 13$'$, this implies that $b_0 \in A' + \pi_0 B$. It follows that $f \in A' + \varphi R = A + \varphi R$. □

LEMMA 16. *For any integer j such that $0 \leqslant j \leqslant f - 1$, we have*

$$\text{(i)} \quad \varphi^j R = \bigoplus_{i=0}^{j-1} \pi_0 B\varphi^i + \bigoplus_{i=j}^{n-1} B\varphi^i;$$

$$\text{(ii)} \quad A + \varphi^j R = (A + \pi R) + \bigoplus_{i=j}^{n-1} B\varphi^i. \qquad \square$$

LEMMA 17. $R_1 \subseteq A + \pi R$.

Proof. Given $f \in R_1$, write $f = \Sigma_{i=0}^{n-1}[b_i]_{\bar{G}_B}\varphi^i$. By Lemma 15, $f \in A+\varphi R$. By Lemma 16, we can adjust f by adding an element of $A+\pi R$ (which is known to be contained in R_1) and assume that $b_0 = 0$. Lift f to $f'(X) = \Sigma_{i=1}^{n-1}[b_i]_{G_B}(X^{q^i}) = b_1X^q +$ higher terms. Compute $f' \circ [\pi_0]_{F_1} - [\pi_0]_{F_1} \circ f'$. We find that it is of $\mathrm{ord}_X \geqslant q^{n-f+1}$ and the coefficient of $X^{q^{n-f+1}}$ is $-u\pi b_1^{q^{n-f}} \pmod{\pi^2}$. This implies that $b_1 \in \pi_0 B$ and therefore, $f \in \phi^2 R$.

Thus we have established $R_1 \subseteq A + \phi^2 R$. Repeat the argument inductively. We finally obtain $R_1 \subseteq A + \phi^f R = A + \pi R$. □

Now we have proved $R_1 = A + \pi R$. It follows that $\dim_k(R/R_1) = n - 1$. By Gross' result, this completes the proof of Theorem 4. □

Acknowledgement

I would like to thank Professor Gross for inspiring discussions and encouragements.

References

1. Drinfeld, V. G.: Elliptic modules, *Math. USSR, Sb.* (1974) 23, 561–592.
2. Drinfeld, V. G.: Coverings of p-adic symmetric regions, *Func. Anal. and Appl.* 10 (1976) 29–40.
3. Fujiwara, Y.: On Divisibilities of special values of real analytic Eisenstein series, *J. Fac. Sci. Univ.* Tokyo 35 (1988) 393–410.
4. Gross, B.: On canonical and quasi-canonical liftings, *Invent. Math.* 84 (1986) 321–326.
5. Gross, B. and Hopkins, M.: The rigid analytic period mapping, Lubin–Tate space, and stable homotopy theory (to appear).
6. Gross, B. and Hopkins, M.: Equivariant vector bundles on the Lubin–Tate moduli space (to appear).
7. Hazewinkel, M.: *Formal groups and applications*, Academic Press, 1978.
8. Keating, K.: Galois extensions associated to deformations of formal A-modules, *J. Fac. Sci. Univ.* Tokyo 37 (1990) 151–170.
9. Lubin, J.: Canonical subgroups of formal groups, *Trans. Ann. Math. Soc.* 251 (1979) 103–127.
10. Lubin, J.: Finite subgroups and isogenies of one-parameter formal lie groups, *Ann. Math.* 85 (1967) 296–302.
11. Lubin, J. and Tate, J.: Formal complex multiplication in local fields, *Ann. Math.* 81 (1965) 380–387.
12. Lubin, J. and Tate, J.: Formal moduli for one-parameter formal Lie groups, *Bull. Soc. Math. Fr.* 94 (1966) 49–60.
13. Lubin, J., Serre, J.-P. and Tate, J.: *Elliptic curves and formal groups*, Seminar at Woods Hole Institute on algebraic geometry 1964.
14. Serre, J.: *Local field*, GTM 67, Springer-Verlag (1979).
15. Shimura, G.: Introduction to the arithmetic theory of automorphic functions, *Publ. of the Math. Soc. of Japan* 11 (1971).
16. Tatevossian, L.: *Canonical liftings of formal modules*, Proceedings of the 1985 Montreal Conference on Number Theory, *CMS Conference Proceedings* 7 (1987) 457–483.