New York Journal of Mathematics

New York J. Math. **10** (2004) 295–306.

Height one Hopf algebras in low ramification

Alan Koch

Abstract. Let k be a perfect field of characteristic $p > 0$. We obtain a complete classification of finite abelian local k-Hopf algebras with local dual such that the augmentation ideal is annihilated by the Frobenius map. We then use the theory of finite Honda systems to show that these Hopf algebras lift to extensions R of $W(k)$ with $2 \leq e(R/W(k)) \leq p-1$, and construct all such lifts.

Contents

1. Introduction

Let k be a perfect field of characteristic $p > 0$ with separable closure k_s. Let H be a finite abelian (that is, commutative and cocommutative) k-Hopf algebra. We will denote the dual Hopf algebra to H by H^*, the set of primitive elements by $P(H)$, and the augmentation ideal by H^+. We will say that H is of height one if $x^p = 0$ for all $x \in H^+$. Such a Hopf algebra is necessarily local, and hence

$$H \cong H_m \times H_u$$

where H_m^* is separable and H_u^* is local [15, p. 52, 87]. The notation H_m and H_u arise from the fact that $\mathrm{Spec}(H_m)$ is of multiplicative type and $\mathrm{Spec}(H_u)$ is unipotent. Separable Hopf algebras are well understood: if $\mathcal{G} = \mathrm{Gal}(k_s/k)$ then such k-Hopf algebras are anti-equivalent to finite groups with $\mathcal{G}$ acting continuously as group automorphisms [15, p. 48]. Thus here we focus on the classification of finite abelian height one Hopf algebras with local dual (hereafter referred to as "local-local").

Received September 12, 2003; revised submission November 2, 2004.
Mathematics Subject Classification. 16W, 57T, 14L.
Key words and phrases. Hopf algebras, Honda systems.

ISSN 1076-9803/04

We will obtain a complete classification of such Hopf algebras using Dieudonné modules. In this case (local-local height one) the Dieudonné module can be viewed as a module over a noncommutative (unless $k = \mathbf{F}_p$) polynomial ring $k[V]$. A skew polynomial ring is an example of a "noncommutative principal ideal domain" and there is an analogue to the classification given in the Fundamental Theorem of Finitely Generated Modules over a Principal Ideal Domain. Once this gives us all of the relevant Dieudonné modules, we will show a one-to-one correspondence between them and the Hopf algebras of height one. These Hopf algebras, which clearly have a nice algebra structure, also have a simple coalgebra structure which can be described using Witt vector addition. We will see that the number of height one local-local (that is, local with local dual) Hopf algebras of rank p^n is equal to the number of partitions of n. The simplicity of this formula is interesting, although not surprising since the structure theorem of nilpotent matrices implies the same result when looking at the commutative ring $k[x]$. However, it is interesting to note that the number of such Hopf algebras is independent of the choice of k (or p, for that matter) — the classification of other classes of finite abelian connected local-local Hopf algebras such as monogenic Hopf algebras, Hopf algebras that represent uniserial groups, and representing algebras of Witt subgroups have all depended on k ([10], [11], and [9] respectively).

Once the characteristic p results are obtained, we will then look at lifting height one Hopf algebras to characteristic zero. Given a k-Hopf algebra H and a discrete valuation ring R with residue field k, to "lift" H to R is to find an R-Hopf algebra $\widetilde{H}$ such that $\widetilde{H} \otimes_R k \cong H$. This cannot always be done: the simplest example being where H is the unique finite abelian local k-Hopf algebra with local dual of rank p with $R = W(k)$ [14, p. 21]. In fact, we will see that none of the height one Hopf algebras lift to $W(k)$.

However, if R has some ramification, i.e., $e = e(R/W(k)) > 1$, the Hopf algebra H above does lift to R. In the case of height one Hopf algebras, we will see the same thing in general: if H is a Hopf algebra on height one, and $1 < e \leq p-1$, then H lifts to R. Any R for which $e \leq p-1$ will be said to have *low ramification*. The technique we will use will be the theory of finite R-Honda systems as constructed by Conrad in [3]. The procedure will be similar to that found in [9] where liftings of monogenic Hopf algebras are considered. It should be pointed out that other theories of finite R-Honda systems exist, e.g., [1] and [13]. (In the latter work it is proved that any affine finite group scheme over k lifts to R with $1 < e \leq p-1$ and $p \geq 5$. Our results will deviate from these in two ways. First, our results will also hold for $p = 3$. Second, we will construct all lifts.) We will use Conrad's theory because we feel it is the easier to compute, most closely resembles the original theory of finite Honda systems developed by Fontaine in [5], and mimics the free Honda systems in the ramified case as in [6]. One drawback to this theory (as well as the one in [13]) is the low ramification condition. It would be interesting to apply the techniques of [1] to lift H to any discrete valuation ring with ramification, if possible.

We start by recalling the connection between Dieudonné modules and Hopf algebras. Then, we will show that the Dieudonné modules corresponding to height one Hopf algebras may be viewed as certain modules over the skew polynomial ring $k[V]$. We will invoke the structure theorem for modules over such rings to give a

complete classification of height one local-local Hopf algebras. Then, we introduce the notion of finite R-Honda systems, and compute the lifts for any height one Hopf algebra.

Throughout this paper, all Hopf algebras (unless otherwise specified) are finite, abelian, and local-local. Also, all group schemes will be affine, finite, commutative, connected, and unipotent.

2. The Dieudonné module of a Hopf algebra

In this section we will describe the correspondence between Hopf algebras and Dieudonné modules. It is common to describe Dieudonné modules in terms of their anti-equivalence with group schemes, however we will focus on the relationship between the Dieudonné module and the Hopf algebra which represents the corresponding group scheme.

Let $W = W(k)$ be the ring of Witt vectors with coefficients in k. Recall that W is the collection of infinite-length vectors with addition and multiplication determined by collections of polynomials $S_1, S_2, \dots$ and $P_1, P_2, \dots$ respectively. A recursive description of the S_n's and P_n's can be found in [8, p. 128], the first term of each being $S_0(x;y) = x + y$ and $P_0(x;y) = xy$.

Let E be the noncommutative ring of polynomials $E = W[F, V]$ with the relations $FV = VF = p,\ Fw = w^\sigma F,\ wV = Vw^\sigma$, where $w \in W$ and

$$w^\sigma = (w_0, w_1, \dots)^\sigma = (w_0^p, w_1^p, \dots).$$

We will call a finite-length E-module killed by a power of F and V a *Dieudonné module*. It should be pointed out that this is not the most general definition of this term — for example generalizations to formal groups and arbitrary group schemes appear in [4].

Given a Dieudonné module M we shall define $\mathcal{H}(M)$ to be the k-Hopf algebra $k[T_x \mid x \in M]$ with the following relations:

$$\begin{aligned} T_{F_x} &= (T_x)^p \\ T_{x+y} &= S_N((T_{V^N x}, T_{V^{N-1}x}, \dots, T_x); (T_{V^N y}, T_{V^{N-1}y}, \dots, T_y)) \\ T_{wx} &= P_N\Big(\Big(w_0^{p^{-N}}, w_1^{p^{-N}}, \dots, w_N^{p^{-N}}\Big); (T_{V^N x}, T_{V^{N-1}x}, \dots, T_x)\Big) \end{aligned}$$

where $x, y \in M,\ w = (w_0, w_1, \dots) \in W(k)$, and N is any nonnegative integer so that $V^{N+1}M = 0$. The comultiplication is given by

$$\begin{aligned} &\Delta(T_x) \\ &= S_N((T_{V^N x} \otimes 1, T_{V^{N-1}x} \otimes 1, \dots, T_x \otimes 1); (1 \otimes T_{V^N x}, 1 \otimes T_{V^{N-1}x}, \dots, 1 \otimes T_x)). \end{aligned}$$

Notice that when $N = 1$ we get $\Delta(T_x) = T_x \otimes T_x$, i.e., T_x is a primitive element of $\mathcal{H}(M)$. It turns out that $\mathcal{H}(M)$ is a finite abelian local Hopf algebra with local dual, and this gives an equivalence between Dieudonné modules and our class of Hopf algebras [7, II, Sec. 5].

A simple but important result concerning this correspondence is given below.

Lemma 2.1 (Zero Lemma)**.** *Let M be a Dieudonné module, and let*

$$H = \mathcal{H}(M) = k[T_m \,|\, m \in M].$$

For any $m \in M$, $T_m = 0$ if and only if $m = 0$.

Proof. Let N be any integer such that $V^N M = 0$. Then

$$T_0 = T_{0\cdot 0} = P_N((0,0,\ldots,0);(T_0,T_0,\ldots,T_0))$$

from which it follows that $T_0 = 0$.

Conversely, suppose $T_m = 0$. Let $M' = Em \subset M$. Clearly $T_{m'} = 0$ for all $m' \in M'$. Thus $\mathcal{H}(M) = \mathcal{H}(M/M')$ which implies that $M = M/M'$, i.e., $m = 0$. □

3. Height one Hopf algebras in characteristic p

We now focus on height one Hopf algebras. The first result shows that the Dieudonné module of such a Hopf algebra is killed by F.

Proposition 3.1. *Let H be a k-Hopf algebra and M its associated Dieudonné module. Then H is height one if and only if $FM = 0$.*

Proof. Suppose $FM = 0$. Let $t \in H^+$. As $t \in H$, we can write

$$t = f(T_{m_1}, T_{m_2}, \ldots, T_{m_s})$$

for some polynomial f in the variables $T_{m_1}, T_{m_2}, \ldots, T_{m_s}$ for some s and $m_i \in M$ such that f has no constant term. Since $(T_{m_i})^p = T_{Fm_i} = T_0 = 0$, we have $(f(T_{m_1}, T_{m_2}, \ldots, T_{m_s}))^p = 0$, hence $t^p = 0$ and one direction is proved.

For the other, suppose H is height one and write

$$H = k[t_1, t_2, \ldots, t_n]/(t_1^p, t_2^p, \ldots t_n^p).$$

Let $m \in M$. We will show $Fm = 0$. Now $T_m \in H = k \oplus H^+$, so there exists an $a \in k$ and a $b \in H^+$ such that $T_m = a + b$. We get

$$T_{Fm} = T_m^p = (a+b)^p = a^p + b^p = a^p.$$

Choose an integer s with $F^s M = 0$. This gives

$$a^{p^s} = T_m^{p^s} = T_{F^s m} = T_0 = 0.$$

Of course, this implies that $a = 0$, hence $a^p = 0$. Thus $T_{Fm} = 0$, and by the Zero Lemma we get $Fm = 0$. □

Notice that the above proposition provides an equivalence of height one Hopf algebras and Dieudonné modules killed by F. If H is height one and $H = \mathcal{H}(M)$ then the E-module M can be viewed as a module over $E/E(F) = k[V]$, the non-commutative ring of polynomials with $aV = Va^\sigma$. Thus we are interested in the classification of $k[V]$-modules. The problem of classifying $k[V]$-modules is very easy in the case that $k = \mathbf{F}_p$ as $k[V]$ is a PID. For general k this is a skew polynomial ring, but there is a structure theorem for such rings which behaves like the well-known theorem in the commutative case. This will enable us to prove:

Proposition 3.2. *Let M be a Dieudonné module such that $FM = 0$. Then*

$$M \cong E/E(F, V^{n_1}) \oplus E/E(F, V^{n_2}) \oplus \cdots \oplus E/E(F, V^{n_j})$$

for some choice of $n_1 \geq n_2 \geq \cdots \geq n_j$.

Proof. By [2, 8.2.4], for any finitely generated $k[V]$-module M we get

$$M \cong k[V]/((f_1(V))) \oplus k[V]/((f_2(V))) \oplus \cdots \oplus k[V]/((f_j(V))) \oplus (k[V])^\ell$$

for some choice of polynomials $f_1(V), f_2(V), \ldots, f_j(V)$ with f_i dividing f_{i-1} for all $1 < i \leq j$. Since $V^n M = 0$ for some n it is clear that $\ell = 0$. Thus to prove the

proposition we need to show that we may take each f_i to be some power of V. It suffices to consider the case where j=1.

Suppose $M \cong k[V]/(f(V))$. As $V^n M = 0$ we have

$$(V^n) \subset (f(V))$$

and hence $V^n = gf$ for some $g = g(V) \in k[V]$. But any divisor of V^n is equal to aV^r for some $a \in k$. Thus $f = aV^r$ for some $a \in k$. Thus $((aV)^n) = (V^n) \subset (V^r)$, so $r \leq n$. But $V^r M = 0$, and since n is the smallest positive integer with this property we must have $r = n$. Thus

$$M \cong k[V]/(V^n) = E/E(F, V^n). \qquad \square$$

Define $M(r) = E/E(F, V^r)$ and $H(r)$ to be $\mathcal{H}(M(r))$. To be explicit we have $H(r) = k[t_1, t_2, \ldots, t_r]/(t_1^p, t_2^p, \ldots t_r^p)$ with

$$\Delta(t_i) = S_{r-i}((t_n \otimes 1, t_{n-1} \otimes 1, \ldots t_i \otimes 1); (1 \otimes t_n, 1 \otimes t_{n-1}, \ldots 1 \otimes t_i)).$$

Note that t_n is primitive. We are now able to state the above result in terms of Hopf algebras.

Theorem 3.3. *Let H be a height one Hopf algebra of rank p^n. Then*

$$H = \bigotimes_{i=1}^{k} H(r_i)$$

for some sequence of positive integers $r_1 \geq r_2 \geq \cdots \geq r_k$ whose sum is n.

We now define for such a sequence $r_1 \geq r_2 \geq \cdots \geq r_k$ the Hopf algebra $H(r_1, r_2, \ldots r_k) = H(r_1) \otimes H(r_2) \otimes \cdots \otimes H(r_k)$. This sequence is of course a partition of n so we get:

Corollary 3.4. *There is a one-to-one correspondence between isomorphism classes of height one Hopf algebras of rank p^n and partitions of n.*

For a group scheme description of the results above, let $G(r) = \mathrm{Spec}(H(r))$. Clearly we have $M = \mathrm{coker}\{F : E/E(V^r) \to E/E(V^r)\}$, and therefore we also have $G(r) = \ker\{F : W_r \to W_r\}$. Thus:

Corollary 3.5. *A k-group scheme is of height one if and only if it is isomorphic to the product of Frobenius kernels of truncated rings of Witt vectors.*

4. Finite Honda systems

In [3] the notion of finite Honda systems are generalized to low ramification. We describe this generalization. Let R be an extension of $W(k)$ with maximal ideal $\mathfrak{m}$, fixed uniformizing parameter π, and $e = e\,(R/W(k)) < p - 1$. Let M be any Dieudonné module, and write W in place of $W(k)$. Let $M^{(1)} = W \otimes_W M$, where W is viewed as a W-module via σ, i.e., $w \otimes m = 1 \otimes w^\sigma m$. Let M_R be the R-module given by $\left(R \otimes M \oplus p^{-1}\mathfrak{m} \otimes M^{(1)}\right)/\mathfrak{I}$, where

$$\mathfrak{I} = \left\{ \left(y - (1 \otimes F)\, z, z - \left(p^{-1} \otimes V\right) y\right) \;\middle|\; y \in \mathfrak{m} \otimes M,\ z \in R \otimes M \right\}.$$

We will write expressions of the form $(r \otimes m, s \otimes m_1)$ to denote elements of M_R despite the fact that elements of M_R are equivalence classes. There will be a few times when we wish to consider elements of $(R \otimes M) \oplus \left(R \otimes M^{(1)}\right)$ directly, however no confusion should arise.

There are R-linear maps $\mathcal{F} : p^{-1}\mathfrak{m} \otimes M^{(1)} \to M_R$ and $\mathcal{V} : M_R \to R \otimes M$ given by

$$\mathcal{F}(s \otimes m_1) = (0, s \otimes m_1)$$
$$\mathcal{V}(r \otimes m, s \otimes m_1) = r \otimes vm + ps \otimes m_1$$

for $r, s \in R,\ m \in M,\ m_1 \in M^{(1)}$.

A *finite R-Honda system* (or a finite Honda system over R) is a pair (L, M) where M is a finite Dieudonné module and L is an R-submodule of M_R such that:

(1) $L \cap \ker \mathcal{V} = 0$.
(2) The canonical map $L/\mathfrak{m}L \to \operatorname{coker} \mathcal{F}$ is an isomorphism.

In the case where $R = W$ it can be shown that $M^R \cong M$ in an obvious way, and the isomorphism carries $\mathcal{F}$ and $\mathcal{V}$ to F and V respectively, so clearly a finite W-Honda system is simply a finite Honda system in the sense of [5].

There is a one-to-one correspondence between finite R-Honda systems and R-Hopf algebras which we will now describe. For any k-algebra S we shall let the map $w'_S : CW_{k,R}(\bar{S}) \to (S \otimes K)/\mathfrak{m}R$ be as defined in [6, p. 197], where $CW_{k,R}(\bar{S})$ is defined to be $(CW_k(\bar{S}))_R$. (Throughout this explanation, an overbar denotes reduction mod $\mathfrak{m}$.) Given an R-Hopf algebra H, the associated R-Honda system is (L, M), where $M = D^*(\overline{H})$ and $L = \ker w'_H|_M$, M_R viewed as a submodule of $CW_{k,R}(\overline{H})$ (since M can be viewed as a submodule of $CW_k(\overline{H})$. Conversely, given a finite Honda system (L, M) we can describe the associated Hopf algebra H in terms of its group scheme $G = \operatorname{Spec} H$: for any finite flat R-algebra S we have

$$G(S) = \{s \in \overline{G}(\bar{S}) \,|\, CW_{k,R}(s)(L) \subset \ker w'_s\}.$$

A morphism of R-Honda systems $(L, M) \to (L', M')$ is an E-module map $\phi : M \to M'$ such that $\phi_R(L) \subset L'$, where $\phi_R : M_R \to M_R$ is the map induced by ϕ.

5. Lifting in low ramification

Finally, we will construct finite R-Honda systems for our height one Hopf algebras. This will be accomplished by finding all of the systems for $H(n) = \mathcal{H}(M(n)) = \mathcal{H}(E/E(F, V^n))$ for every n. First, we need a lemma to that enables us to better perform calculations in M_R. The following lemma provides a k-basis for M_R:

Lemma 5.1. *Let $M = E/E(F, V^n)$. Let X, Y, Z be the k-subspaces of M_R generated by*

$$S_X = \{(\pi^i \otimes V^j x, 0) \,|\, 0 \le i \le e-1,\ 0 \le j \le n-2\},$$
$$S_Y = \{(0, p^{-1}\pi^i \otimes x) \,|\, 1 \le i \le e-1\},$$
$$S_Z = \{(1 \otimes V^{n-1}x, 0)\},$$

respectively. Then M_R is the internal direct sum of X, Y, and Z, and

$$S := S_X \cup S_Y \cup S_Z$$

is a k-basis for M_R.

Proof. Clearly $X \cup Y \cup Z \subset M_R$, so we need to show that this union is all of M_R, that S_X, S_Y, and S_Z are bases for X, Y, and Z respectively (which is clear in the case of Z), and that these three spaces are pairwise disjoint. Since

$\{x, Vx, \ldots, V^{n-1}x\}$ is a k-basis for M we clearly have that $S_1 \cup S_2$ is a generating set for $M(R)$ over k, where

$$S_1 = \{(\pi^i \otimes V^j x, 0) \,|\, 0 \le i \le e-1,\, 0 \le j \le n-1\}$$
$$S_2 = \{(0, p^{-1}\pi^i \otimes V^j x) \,|\, 1 \le i \le e,\, 0 \le j \le n-1\}.$$

We will show that the elements in the above set that are not in S are multiples of elements of S or are zero. Each element in the above set not in S is one of the following:

$$\begin{array}{ll} (\pi^i \otimes V^{n-1}x, 0) & 1 \le i \le e-1 \\ (0, u \otimes x) & (\text{the case } i = e \text{ in } S_Y) \\ (0, p^{-1}\pi^i \otimes V^j x) & 1 \le i \le e-1,\ 1 \le j \le n-1. \end{array}$$

Here $M_R = ((R \otimes M) \oplus (p^{-1}\mathfrak{m} \otimes M^{(1)}))/\mathfrak{I}$, where

$$\mathfrak{I} = \{(y, z - (p^{-1} \otimes V)y) \,|\, y \in \mathfrak{m} \otimes M,\ z \in R \otimes M\}$$

since here F acts trivially on M. If we set $y = \pi^i \otimes V^{n-1}x$ for $i > 0$ and $z = 0$ we get $(\pi^i \otimes V^{n-1}x, 0) = (0, p^{-1}\pi^i \otimes V^n x) = (0, 0)$. If we let $z = u \otimes x$ and $y = 0$ we have $(0, u \otimes x) = (0, 0)$. Finally, setting $y = \pi^i \otimes V^j x$ for $1 \le i \le e-1, 0 \le j \le n-2$, and $z = 0$ we obtain $(0, p^{-1}\pi^i \otimes V^j x) = (\pi^i \otimes V^j x, 0) \in S_X$. Thus $M_R = X + Y + Z$.

We now show that S_X is a basis for X. To show that S_X is linearly independent, if

$$\sum_{i=0}^{e-1} \sum_{j=0}^{n-2} \lambda_{i,j}(\pi^i \otimes V^j x, 0) = (0, 0)$$

then

$$\sum_{i,j} \lambda_{i,j}(\pi^i \otimes V^j x, 0) = \left(\sum_{i,j} \lambda_{i,j}(\pi^i \otimes V^j x), 0 \right)$$

which is an element of $\mathfrak{I} \subset ((R \otimes M) \oplus (R \otimes M^{(1)}))$, so it follows that there exists a $y \in \mathfrak{m} \otimes M,\ z \in R \otimes M$ such that

$$\left(\sum_{i,j} \lambda_{i,j}(\pi^i \otimes V^j x), 0 \right) = (y, z - (p^{-1} \otimes V)y).$$

Clearly $y = \sum_{i,j} \lambda_{i,j}(\pi^i \otimes V^j x)$ and

$$z = (p^{-1} \otimes V)y = \sum_{i,j} \lambda_{i,j}(p^{-1}\pi^i \otimes V^{j+1}x, 0).$$

In order for $z \in R \otimes M$ we need $\lambda_{i,j} = 0$ whenever $i < e$, which here is all i. Thus $\lambda_{i,j} = 0$ for all i and j, hence S_X is linearly independent in X. That S_X spans is obvious from the definition of X, of course.

For S_Y, suppose

$$\sum_{i=1}^{e-1} \lambda_i(0, p^{-1}\pi^i \otimes x) = (0, 0).$$

Then

$$\sum \lambda_i(0, p^{-1}\pi^i \otimes x) = \left(0, \sum \lambda_i(p^{-1}\pi^i \otimes x)\right) \in \mathfrak{I} \subset ((R \otimes M) \oplus (R \otimes M^{(1)}))$$

so, as above, there exist a $y \in \mathfrak{m} \otimes M$, $z \in R \otimes M$ such that

$$\left(0, \sum \lambda_i (p^{-1}\pi^i \otimes x)\right) = (y, z - (p^{-1} \otimes V)y).$$

Clearly $y = 0$. In order to have equality we must have $z = \sum \lambda_i (p^{-1}\pi^i \otimes x)$. But this sum is in $R \otimes M$ if and only if $\lambda_i = 0$ for all i.

It remains to show that X, Y, and Z are pairwise disjoint. It is easy to see that Z is disjoint from the other two: if not then $Z \subset X$ or $Z \subset Y$, i.e., $(1 \otimes V^{n-1}x, 0) \in X \cup Y$. If $(1 \otimes V^{n-1}x, 0) \in Y$ then $(1 \otimes V^{n-1}x, 0)$ has an additive inverse in Y, so $(1 \otimes V^{n-1}x, y) \in \mathfrak{I} \subset ((R \otimes M) \oplus (p^{-1}\mathfrak{m} \otimes M^{(1)}))$ for some $y \in Y$, which implies $1 \otimes V^{n-1}x \in \mathfrak{m} \otimes M$, which is a not true. Similarly, if $(1 \otimes V^{n-1}x, 0) \in X$ then there is a $y' \in X$ such that $(y' + 1 \otimes V^{n-1}x, 0) \in \mathfrak{I}$, which says that $y' + 1 \otimes V^{n-1}x \in \mathfrak{m} \otimes M$, which is impossible since y' is a linear combination of elements of the form $\pi^i \otimes V^j x$ with $j < n-1$. Thus $X \cap Z = Y \cap Z = 0$. Finally, any element $y' \in X \cap Y$ can be written two different ways:

$$\begin{aligned} y' &= \left(\sum_{i=0}^{e-1} \sum_{j=0}^{n-2} \lambda_{i,j} (\pi^i \otimes V^j x), 0 \right) \\ &= \left(0, \sum_{i=1}^{e-1} \lambda'_i (p^{-1}\pi^i \otimes x) \right) \end{aligned}$$

for some $\lambda_{ij}, \lambda'_i \in k$. Thus

$$\left(\sum_{i=0}^{e-1} \sum_{j=0}^{n-2} \lambda_{i,j} (\pi^i \otimes V^j x), \sum_{i=1}^{e-1} -\lambda'_i (p^{-1}\pi^i \otimes x) \right) \in \mathfrak{I}$$

and thus there exists a $z \in R \otimes M$ such that

$$z - \sum_{i=0}^{e-1} \sum_{j=0}^{n-2} \lambda_{i,j} (p^{-1}\pi^i \otimes V^{j+1} x) = \sum_{i=1}^{e-1} -\lambda'_i (p^{-1}\pi^i \otimes x)$$

which can only happen if $\lambda'_i = 0$ for all i. But then

$$z = \sum_{i=0}^{e-1} \sum_{j=0}^{n-2} \lambda_{i,j} (p^{-1}\pi^i \otimes V^{j+1} x),$$

which cannot happen unless $\lambda_{i,j} = 0$ for all i, j since otherwise

$$\sum_{i=0}^{e-1} \sum_{j=0}^{n-2} \lambda_{i,j} (p^{-1}\pi^i \otimes V^{j+1} x) \notin R \otimes M.$$

Thus $X \cap Y = 0$ and we are done. □

Corollary 5.2. *With M as above we have $\dim_k M_R = en$ and the set*

$$\{(1 \otimes V^j x, 0) \,|\, 0 \le j \le n-1\} \cup \{(0, p^{-1}\pi \otimes x)\}$$

generates M_R as an R-module.

Now to have finite R-Honda system (L, M) we must have that the canonical map $L/\mathfrak{m}L \to \operatorname{coker} \mathcal{F}$ is an isomorphism. The next result helps to make that cokernel explicit.

Lemma 5.3. *With M as above $\operatorname{Im}\mathcal{F}$ has k-basis*

$$\{(\pi^i \otimes V^j x, 0) \,|\, 1 \leq i \leq e-1, 0 \leq j \leq n-1\} \cup \{(0, p^{-1}\pi^i \otimes x) \,|\, 1 \leq i \leq e-1\}.$$

Proof. Let M' be the k-submodule of M spanned by the set above. Clearly $(0, p^{-1}\pi^i \otimes x) = \mathcal{F}(p^{-1}\pi^i \otimes x) \in \operatorname{Im}\mathcal{F}$. Furthermore, we have that $(\pi^i \otimes V^j x, 0) = (0, p^{-1}\pi^i \otimes V^j x) = \mathcal{F}(0, p^{-1}\pi^i \otimes V^j x) \in \operatorname{Im}\mathcal{F}$, so $M' \subset \operatorname{Im}\mathcal{F}$. That we have equality is a length argument that follows from [3, 2.4]. □

Corollary 5.4. *The cokernel of $\mathcal{F}$ has k-basis $\{(1 \otimes V^j x, 0) \,|\, 0 \leq j \leq n-1\}$.*

We are now ready to describe all of the lifts of a height one Hopf algebra. The main theorem below will show all of the lifts for one summand of a height one Hopf algebra — finding all of the lifts for the height one Hopf algebra in question will follow by lifting each summand.

Theorem 5.5. *Let $M = E/E(F, V^n)$. For $0 \leq r \leq n-1$, let*

$$y_r = \left(\sum_{j=0}^{n-1} a_{j,r} \otimes V^j x, p^{-1}\pi a_{n,r} \otimes x \right)$$

with $a_{j,r} \in R$. Define $z_r = (1 \otimes V^r x, 0) + \pi y_r$. Let L be the R-submodule of M_R generated by $\{z_0, z_1, \ldots, z_{n-1}\}$. Then (L, M_R) is a finite R-Honda system if and only if $v(a_{n,n-1}) < e-2$ or there exists a $j \leq n-2$ such that $v(a_{j,n-1}) < e-1$.

Proof. Since $z_r \equiv (1 \otimes V^r x, 0) \bmod \mathfrak{m}$ it is clear by (5.4) that the canonical map $L/\mathfrak{m}L \to \operatorname{coker}\mathcal{F}$ is an isomorphism regardless of any conditions on the $a_{j,r}$'s. Thus (L, M) is a finite R-Honda system if and only if $L \cap \ker\mathcal{V} = 0$.

For any $r \leq n-1$ let L_r be the R-submodule of L generated by z_r. (For the moment there remain no conditions on the $a_{j,r}$'s.) We claim that, for $r \neq s$ we have $\mathcal{V}(L_r) \cap \mathcal{V}(L_s) \neq 0$. Suppose first that neither r nor s is $n-1$. For $b, c \in R^\times$ and $e_1 \leq e_2 \leq e-1$ we have

$$\mathcal{V}(\pi^{e_1} b z_r) \equiv b\pi^{e_1} \otimes V^{r+1} x \bmod \mathfrak{m}^{e_1+1}$$
$$\mathcal{V}(\pi^{e_2} c z_s) \equiv c\pi^{e_2} \otimes V^{s+1} x \bmod \mathfrak{m}^{e_1+1}$$

and these cannot be equal since the top congruence is nonzero. Suppose $r = n-1$. For $b, c \in R^\times$, and $e_1, e_2 \leq e-1$ we have

$$\mathcal{V}(\pi^{e_1} b z_{n-1}) \equiv b\pi^{e_1} \otimes V^n x \equiv 0 \bmod \mathfrak{m}^{e_2+1}$$
$$\mathcal{V}(\pi^{e_2} c z_s) \equiv c\pi^{e_2} \otimes V^{s+1} x \bmod \mathfrak{m}^{e_2+1}$$

and here the bottom congruence is nonzero and the claim is proved.

Thus $L \cap \ker\mathcal{V} = 0$ if and only if $L_r \cap \ker\mathcal{V} = 0$ for all r. Notice that for any $r < n-1$ we have

$$\pi^{e-1} z_r = (\pi^{e-1} \otimes V^r x, 0) + \pi^e y_r = (\pi^{e-1} \otimes V^r x, 0)$$

and $\mathcal{V}(\pi^{e-1} z_r) = \pi^{e-1} \otimes V^{r+1} x \neq 0$. Since $\pi^e z_r$ is clearly $(0, 0)$ it follows that $\mathcal{V}|_{L_r}$ has trivial kernel. Thus (L, M) is a finite R-Honda system if and only if $L_{n-1} \cap \ker\mathcal{V} = 0$.

For ease of notation, we will write a_j for $a_{j,n-1}$. This should not create any difficulty since for the remainder of the proof we only look at z_{n-1}. Let $e' =$

$\min_{j\leq n-2}\{v(a_j)\}$ and let t be chosen so that $v(a_t)=e'$. Suppose $e'<e-1$. Then we claim $\pi^{e-e'-1}z_{n-1}=0$. We have

$$\pi^{e-e'-1}z_{n-1}=(\pi^{e-e'-1}\otimes V^{n-1}x,0)+\left(\sum_{j=0}^{n-1}\pi^{e-e'}a_j\otimes V^jx,p^{-1}\pi^{e-e'+1}a_n\otimes x\right).$$

Of course, $(\pi^{e-e'-1}\otimes V^{n-1}x,0)=(0,0)$, so we only need to show the sum on the right is zero. Since $v(a_j)\geq e'$ we know $\pi^{e-e'}a_j=ua'_jp$ for some $a'_j\in R$ for all $j\leq n$; hence

$$\pi^{e-e'-1}z_{n-1}=p\left(\sum_{j=0}^{n-1}ua'_j\otimes V^jx,p^{-1}\pi ua'_n\otimes x\right)=(0,0)$$

since M_R is killed by p. However,

$$\begin{aligned}\mathcal{V}(\pi^{e-e'-2}z_{n-1})&=\mathcal{V}\left(\sum_{j=0}^{n-1}\pi^{e-e'-1}a_j\otimes V^jx,p^{-1}\pi^{e-e'}a_n\otimes x\right)\\&=\sum_{j=0}^{n-1}\pi^{e-e'-1}a_j\otimes V^{j+1}x+\pi^{e-e'}a_n\otimes x\\&=\sum_{j=0}^{n-2}\pi^{e-e'-1}a_j\otimes V^{j+1}x+\pi^{e-e'}a_n\otimes x.\end{aligned}$$

Since $t\leq n-2$ we know $\pi^{e-e'-1}a_t\otimes V^{t+1}x\neq 0$, and by the R-linear independence of the set $\{1\otimes V^jx\,|\,j\leq n-1\}$ we have that $\mathcal{V}(\pi^{e-e'-2}z_{n-1})\neq 0$ and hence $L_{n-1}\cap\ker\mathcal{V}=0$, thus (L,M) is a finite R-Honda system.

The above establishes that (L,M) is a finite R-Honda system in the case where there exists a $j\leq n-2$ such that $v(a_{n-1})<e-1$. We now wish to show that the condition $v(a_n)<e-2$ also gives such a system. It suffices to show the result in the case where $v(a_j)\geq e-1$ for all $j\leq n-2$. Then

$$\begin{aligned}z_{n-1}&=(1\otimes V^{n-1}x,0)+\left(\sum_{j=0}^{n-1}\pi a_j\otimes V^jx,p^{-1}\pi^2a_n\otimes x\right)\\&=(1\otimes V^{n-1}x,0)+(\pi a_{n-1}\otimes V^{n-1}x,p^{-1}\pi^2a_n\otimes x)\end{aligned}$$

since $v(\pi a_j)\geq e$ for $j<n-1$. Clearly $z_{n-1}\neq(0,0)$. We have

$$\mathcal{V}(z_{n-1})=1\otimes V^nx+\pi a_{n-1}\otimes V^nx+\pi^2a_n\otimes x=\pi^2a_n\otimes x\neq 0$$

since $v(\pi^2a_n)<e$. Thus $L_{n-1}\cap\ker\mathcal{V}=0$, as desired.

Conversely, suppose $v(a_j)\geq e-1$ for all $j\leq n-2$, and that $v(a_n)\geq e-2$. Then again we have

$$z_{n-1}=(1\otimes V^{n-1}x,0)+(\pi a_{n-1}\otimes V^{n-1}x,p^{-1}\pi^2a_n\otimes x)\neq(0,0)$$

and

$$\mathcal{V}(z_{n-1})=1\otimes V^nx+\pi a_{n-1}\otimes V^nx+\pi^2a_n\otimes x=\pi^2a_n\otimes x.$$

However, since $v(\pi^2a_n)\geq e$ we get $\mathcal{V}(z_{n-1})=0$, thus $z_{n-1}\in L\cap\ker\mathcal{V}$ and (L,M) is not a finite Honda system. □

Remark 5.6. Of course, in the case $R = W(k)$ we have $e = 1$, so it is impossible to choose $a_{j,r} \in R$ to satisfy the conditions in the theorem. While it can also be shown quickly using the "classical" theory of finite Honda systems, an immediate consequence of this theorem is that these Hopf algebras do not lift to $W(k)$. However, they do lift to every extension of $W(k)$ with low ramification.

Remark 5.7. The above provides every lift of H to R, however, different choices of $a_{j,r}$'s can lead to isomorphic finite Honda systems (and hence isomorphic Hopf algebras). For example, it should be clear that if $a_{j,r} \equiv a'_{j,r} \bmod p$ for all j and r then their finite Honda systems will be isomorphic.

Since the Dieudonné module of any height one Hopf algebra is a direct sum of modules of the form $E/E(F, V^n)$, we obtain:

Corollary 5.8. *Let H be the height one Hopf algebra defined over k corresponding to the Dieudonné module*

$$E/E(F, V^{n_1}) \oplus E/E(F, V^{n_2}) \oplus \cdots \oplus E/E(F, V^{n_t})$$

with $n_1 \geq n_2 \geq \cdots \geq n_t$. Then H lifts to R if $2 \leq e \leq p-1$. If $e = 1$ then H does not lift to R.

As one can imagine, it can be difficult to explicitly compute the Hopf algebra corresponding to a finite Honda system. Determining reasonable conditions for when two finite Honda systems give the same lift seems like a very complicated problem as well. We will conclude with a very small concrete example.

Example 5.9. Let $M = E/E(F, V)$. Then M corresponds to the unique simple (affine finite abelian local-local) Hopf algebra H. Using (5.5) in the case where $n = 1$ gives

$$z = z_0 = (1 \otimes x, 0) + (a_{0,0} p^{-1} \pi a_{1,0} \otimes x)$$

with $v(a_{1,0}) < e - 2$. We may multiply by the appropriate invertible element of R and assume $z = (1 \otimes x, p^{-1}\pi c \otimes x)$ with $v(c) < e - 2$. Thus the lifts of H correspond to elements $a = \pi c \in R$ with $1 \leq v(a) \leq e - 1$ — of course this is a well-known result of Tate and Oort [14, p. 21]. Let us denote the corresponding R-Hopf algebra by H_c. Letting $e' = v(c)$ and $c = \pi^{e'} c_0$ gives $H_c = R[x]/(x^p - bx)$, where $b = -\pi^{e-e'-1}(uc_0)^{-1}$.

In [14] it is also shown that $H_c \cong H_d$ if and only if $c = dr^{p-1}$ for some $r \in R^\times$. The corresponding map on the finite Honda systems is induced from the endomorphism $\phi : M \to M$ given by $\phi(x) = r^\sigma x$. For explicit calculations of all of the results in this example, see [12, 4.3].

References

[1] C. Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math **152** (2000), 489–549, MR 1804530 (2001k:14087).

[2] P.M. Cohn, *Free rings and their relations* (Second edition), Academic Press, London, 1985, MR 0800091 (87e:16006), Zbl 0659.16001.

[3] B. Conrad, *Finite group schemes over bases with low ramification*, Comp. Math. **119** (1999), 239–320, MR 1727133 (2001c:14071), Zbl 0984.14015.

[4] J.-M. Fontaine, *Sur la construction du module de Dieudonné d'un groupe formel*, C.R. Acad Sci. Paris Paris Sér. A-B **280** (1975), A1273–A1276, MR 0374151 (51 #10351), Zbl 0331.14022.

[5] J.-M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C.R. Acad Sci. Paris Sér. A-B **280** (1975), A1423–A1425, MR 0374153 (51 #10353), Zbl 0331.14023.

[6] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Asterisque 47–48, Soc. Math. de France, 1977, MR 0498610 (58 #16699), Zbl 0377.14009.

[7] A. Grothendieck, *Groupes de Barsotti–Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970), Les Presses de L'Université de Montreal, Montreal, Canada, 1974, MR 0417192 (54 #5250), Zbl 0331.14021.

[8] N. Jacobson, *Lectures in abstract algebra.* III. *Theory of fields and Galois theory*, Graduate Texts in Mathematics, **32**, Springer-Verlag, New York, 1975, MR 0392906 (52 #13719), Zbl 0455.12001.

[9] A. Koch, *Cyclic Dieudonné modules and Witt subgroups killed by p*, Rocky Mountain J. Math. **31** (2001), MR 1877332 (2002j:14051).

[10] A. Koch, *Monogenic bialgebras over finite fields and rings of Witt Vectors*, J. Pure Appl. Algebra **163** (2001), 193–207, MR 1846661 (2002g:14067), Zbl 0988.16026.

[11] A. Koch, *The Hopf algebra of a uniserial group*, Pacific J. Math. **215** (2004), 347–356, MR 2068786.

[12] A. Koch, *Monogenic Hopf algebras over discrete valuation rings with low ramification*, J. Algebra, to appear.

[13] J. Roubaud, *Schémas en groupes finis sur un anneau de valuation discrèt et systèmes de Honda associés*, Publications Mathématiques d'Orsay, **91-01**, Université de Paris-Sud, Département de Mathématiques, Orsay, 1991, MR 1117230 (92m:14059), Zbl 0755.14013.

[14] J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. Éc. Norm. Sup. **3** (1970), 1–21, MR 0265368 (42 #278), Zbl 0195.50801.

[15] W. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, **66**, Springer-Verlag, New York, 1979, MR 0547117 (82e:14003), Zbl 0442.14017.

DEPARTMENT OF MATHEMATICS, AGNES SCOTT COLLEGE, 141 E. COLLEGE AVE., DECATUR, GA 30033

akoch@agnesscott.edu

This paper is available via http://nyjm.albany.edu:8000/j/2004/10-19.html.