ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 42, Number 6, 2012

BI-GENIC HOPF ALGEBRAS IN CHARACTERISTIC p

ALAN KOCH

ABSTRACT. For k a perfect field of characteristic $p > 0$, we construct finite abelian local k-Hopf algebras with local linear duals which are generated as k-algebras by at most two elements. We describe these Hopf algebras using extensions of the Dieudonné modules representing monogenic Hopf algebras.

1. Introduction. Let k be a perfect field, $\operatorname{char} k = p > 0$, and let $\overline{k}$ denote its algebraic closure. It is well known that every finite abelian (i.e., commutative, cocommutative) k-Hopf algebra H decomposes as $H_r \otimes_k H_{\ell r} \otimes_k H_{\ell\ell}$ where H_r is reduced, $H_{\ell r}$ is local with reduced linear dual and $H_{\ell\ell}$ is local with local linear dual. For H a rank n reduced k-Hopf algebra, a finite group Γ exists of order n such that $H \otimes_k \overline{k} \cong k\Gamma$. Through descent, this classifies all reduced Hopf algebras, and using duality we can classify the Hopf algebras with reduced dual as well.

Thus, the trickiest finite abelian k-Hopf algebras to classify are the ones which are local with local dual, hereafter referred to as *local-local*. Any such Hopf algebra must necessarily be of p-power rank and have a truncated polynomial ring as its algebra structure. These Hopf algebras correspond to affine finite commutative k-group schemes which are connected and unipotent, and hence the Dieudonné module theory for such group schemes can be used to classify them. In [**9**] we construct the Dieudonné module for each (finite local-local) k-Hopf algebra which is monogenic, i.e., generated as a k-algebra by a single element; additionally, the ones that are killed by p can be found in [**10**]. We use this classification in [**12**] to construct liftings of a given Hopf algebra H to extensions of $W(k)$ which are *peu ramifeé* using Conrad's finite Honda systems as in [**2**]; and in the case the H is killed by $[p]$ in [**8**] we lift it to discrete valuation rings regardless of ramification using Breuil modules as in [**1**].

It would therefore seem logical to focus next on "bi-genic" Hopf algebras, that is, Hopf algebras which require two generators as a k-algebra.

Received by the editors on August 13, 2009, and in revised form on March 18, 2010.

DOI:10.1216/RMJ-2012-42-6-1919 Copyright ©2012 Rocky Mountain Mathematics Consortium

One way to obtain bi-genic Hopf algebras is through extensions. Given H_1 and H_2 monogenic Hopf algebras, any H appearing in a short exact sequence

$$H_1 \hookrightarrow H \twoheadrightarrow H_2$$

of Hopf algebras must be generated by at most two elements. Recall that $f : H_1 \to H$, $g : H \to H_2$ give a short exact sequence of commutative k-Hopf algebras if f is injective, g is surjective and $\ker g = f(H_1^+)H$, where H_1^+ is the augmentation ideal of H_1.

In this paper we will compute $\mathrm{Ext}^1(M, M')$ in the category of modules over the Dieudonné ring E, where M, M' are Dieudonné modules which correspond to monogenic Hopf algebras H, H'. By [**3**, V, 1.5.1] this extension group is the same as $\mathrm{Ext}^1(\mathrm{Spec}\, H, \mathrm{Spec}\, H')$, in the category of affine commutative connected unipotent group schemes, which in turn will provide Hopf algebras with at most two generators. The relative simplicity of the Dieudonné module structure for M will greatly facilitate the computations: as M is a cyclic E-module, it admits a simple projective resolution, and the elements of the groups $\mathrm{Hom}_E(E, M')$ and $\mathrm{Hom}_E(M, M')$ correspond in a natural way to elements of M'. The simplicity of M' aids in the calculation of $\mathrm{Hom}_E(I, M')$, where $M = E/I$: it corresponds in a natural way to certain elements of $M' \times M'$.

We start with the necessary background on Dieudonné modules and their relationship with finite abelian local-local Hopf algebras, particularly in the monogenic case. Next we compute the extension group, expressing it as a factor group of a certain subgroup of $M' \times M'$. Then, we explicitly describe the Dieudonné modules that arise as extensions of M by M', giving a 2-element generating set (as an E-module) subject to four relations. Neither the number of generators nor relators need be minimal. In the case where M and M' are Dieudonné modules corresponding to Frobenius kernels of $\mathbf{G}_a$, we can quickly compute $\mathrm{Ext}^1(M, M')$ using the long exact Hom-Ext sequence. In this case we describe the extension group using this technique and show how it agrees with our classification. We then give a simple criterion for a Dieudonné module in such an extension to correspond to a monogenic Hopf algebra–the modules that fail to satisfy this criterion give the ones corresponding to bi-genic Hopf algebras. Finally, we determine the algebra structure of a bi-genic Hopf algebra from its Dieudonné

module and give an explicit example of the coalgebra structure for a simple but nontrivial class of Hopf algebras.

It is the hope that future work will examine the lifting questions as in the monogenic case. Also, it should be pointed out that the technique needed to compute $\mathrm{Ext}^1(M, M')$ relies on the relative simplicity of the E-module structure of M but less so on M'. Thus, it may be possible to use the ideas here to construct "tri-genic" Hopf algebras (and beyond) by replacing M' with Dieudonné modules corresponding to bi-genic (and beyond) Hopf algebras. Additionally, the techniques below may help classify cyclic Dieudonné modules killed by p^2, thereby building on the results of [**10**].

Throughout this paper, k will be a perfect field of characteristic p, all Hopf algebras will be finite, abelian, and local-local, and all unadorned tensors will be over k. Furthermore, when A and B are E-modules we write $\mathrm{Hom}\,(A, B)$ for $\mathrm{Hom}_E(A, B)$.

2. Monogenic Hopf algebras and Dieudonné modules. Let $W = W(k)$ be the ring of Witt vectors with coefficients in k. For each $n \geq 0$, we shall denote by S_n (respectively P_n) the polynomial that gives the formula for the nth component of the Witt vector sum (respectively product). This ring has the Frobenius operator which we shall denote $(-)^\sigma$ given by

$$w^\sigma = (w_0, w_1, w_2, \dots)^\sigma = (w_0^p, w_1^p, w_2^p, \dots)\,.$$

Let $E = W[F, V]$ be the ring of polynomials in two variables subject to the relations $FV = VF = p$, $Fw = w^\sigma F$ and $wV = Vw^\sigma$, $w \in W$. (Clearly E is not commutative unless $k = \mathbf{F}_p$.) Let C be the affine group scheme of Witt covectors as defined in [**6**], and let D be its representing algebra. Then, to each Hopf algebra H, we can associate the E-module $D_*(H) := \mathrm{Hom}_{k\text{-gr}}(\mathrm{Spec}\, H, C) \cong \mathrm{Hom}_{k\text{-Alg}}(D, H)$. This E-module is killed by a power of F and V, i.e., $F^n D_*(H) = 0 = V^m D_*(H)$ for m, n sufficiently large positive integers. This correspondence gives a categorical equivalence between (finite abelian local-local) k-Hopf algebras and E-modules killed by some power of F and V. We will use the term *Dieudonné modules* to describe this collection of modules; however, the term can be applied to more general E-modules which correspond to a larger class of Hopf

algebras, see e.g., [**4, 5, 7**]. We will often view E-modules M as k-modules via $\alpha m = (\alpha, 0, 0, \dots)m$ for $\alpha \in k$, $m \in M$.

Since we use Dieudonné modules to find Hopf algebras, it will be important to discuss the inverse correspondence to the one above. Let M be a Dieudonné module, and pick N a natural number such that $V^{N+1}M = 0$. (The construction below is independent of the choice of N.) Define $\mathcal{H}(M)$ to be the k-algebra $k[T_m \mid m \in M]$ subject to the relations

$$\begin{aligned} T_{Fm} &= (T_m)^p \\ T_{m+m'} &= S_N\left((T_{V^N m}, \dots, T_{Vm}, T_m); (T_{V^N m'}, \dots, T_{Vm'}, T_{m'})\right) \\ T_{wm} &= P_N\left(\left(w_0^{p^{-N}}, \dots, w_N^{p^{-N}}\right); (T_{V^N m}, \dots, T_{Vm}, T_m)\right). \end{aligned}$$

In [**9**] we obtain a classification of the Dieudonné modules which correspond to monogenic Hopf algebras. We shall restate the result here using slightly different notation to facilitate the work to come.

Proposition 2.1 [**9**, Proposition 2.2]. *Let H be a monogenic Hopf algebra. Then*

$$D_*(H) \cong E/E(F^n, \eta F^r - V)$$

for some $\eta \in k^\times$ and integers $1 \le r \le n$.

Conversely, it was shown that any Dieudonné module M of the above form corresponds to a monogenic Hopf algebra–the algebra structure is simply $k[T_x]$ where x is the image of $1 \in E$ under the canonical projection $E \to M$.

Notice that, if $r = n$, then $\operatorname{Spec}(H)$ is the nth Frobenius kernel of the additive group scheme $\mathbf{G}_a$ and that $D_*(H) \cong E/E(F^n, V)$.

Let $M = E/E(F^n, \eta F^r - V)$, and let $x \in M$ be as above. Since $Vx \in F^r M$ and

$$px = FVx = F(\eta F^r x) = \eta^p F^{r+1} x \in F^{r+1}M$$

we see that each $m \in M$ can be expressed as $m = g(F)x$, where $g(F) \in k[F]$, the ring of non-commutative polynomials in a single variable. The choice of $g(F)$ is clearly unique $\bmod F^n$. It will be useful

to think of elements of M via these polynomials. We will often write g instead of $g(F)$.

We define the map $(-)^\sigma$ on $k[F]$ by raising each coefficient to the pth power, i.e.,

$$\left(\sum_{i=0}^{n-1} \gamma_i F^i\right)^\sigma = \sum_{i=0}^{n-1} \gamma_i^p F^i.$$

Note that this use of σ is compatible with the one above: for each $w \in W$, the element $wx \in M$ can be viewed as a polynomial, say $wx = f(F)x$ and $w^\sigma = f^\sigma$. It can also be shown that, if $g(F) \in k[F]$, then

$$Fgx = g^\sigma Fx$$
$$gVx = Vg^{\sigma^{-1}}x.$$

We will call a $g(F) \in k[F]$ *invertible in* M if a polynomial $h(F) \in k[F]$ exists such that $h(F)g(F)x = x$. It is clear that $g(F)$ is invertible in M if and only if $g(F)$ has a nonzero constant term. Through abuse of notation, we will write $g^{-1}(F)$ for the $h(F)$ above and $k[F]^\times$ for the set of all polynomials invertible in M.

Finally, we let $v : k[F] \to \mathbf{Z} \cup \{\infty\}$ be the degree valuation. Thus, $g(F)$ is invertible in M if and only if $v(g) = 0$, and $g_1 x = g_2 x$ if and only if $v(g_1 - g_2) \geq n$. The following shows the importance of the lowest degree term in a polynomial.

Lemma 2.2. *Let $m \in M$, and suppose $gm = 0$ for some $g \in k[F]$. Then $F^{v(g)}m = 0$.*

Proof. Pick n such that $F^n M = 0$, and let $v = v(g)$. Write $g = g'F^v$, $g' \in k[F]^\times$. Then

$$0 = gm = g'F^v m,$$

and applying $(g')^{-1}$ to both sides shows $F^v m = 0$. □

We conclude this section by giving a criterion which we will need later to isolate the extensions which give monogenic Hopf algebras from the extensions which give bi-genic ones.

Lemma 2.3. *The k-Hopf algebra $\mathcal{H}(M)$ is monogenic if and only if M/FM is a k-vector space of dimension one.*

Proof. If $\mathcal{H}(M)$ is monogenic, then by Proposition 2.1, we have

$$M/FM \cong E/E\left(F^n, \eta F^r - V, F\right) \cong E/E\left(F, V\right) \cong k.$$

Now suppose $\dim_k M/FM = 1$. By [**13**, page 112], we may write $\mathcal{H}(M) = k[t_1, \ldots, t_s]/(t_1^{p^{n_1}}, \ldots, t_s^{p^{n_s}})$ for some $s \geq 1$. We have a sequence

$$0 \longrightarrow FM \longrightarrow M \longrightarrow M/FM \longrightarrow 0$$

of Dieudonné modules. Applying D_*, and observing $\mathcal{H}(FM) = k[t_1^p, \ldots, t_s^p]/(t_1^{p^{n_1}}, \ldots, t_s^{p^{n_s}})$ and $\mathcal{H}(k) = k[t]/(t^p)$ gives us

$$0 \longrightarrow k\left[t_1^p, \ldots, t_s^p\right] / \left(t_1^{p^{n_1}}, \ldots, t_s^{p^{n_s}}\right) \longrightarrow k\left[t_1, \ldots, t_s\right] / \left(t_1^{p^{n_1}}, \ldots, t_s^{p^{n_s}}\right) \longrightarrow k\left[t\right] / \left(t^p\right) \longrightarrow 0,$$

which can only happen if $s = 1$. □

3. Dieudonné module extensions. For the next two sections, we shall let $M = E/E(F^n, \eta F^r - V)$ and $M' = E/E(F^{n'}, \eta' F^{r'} - V)$. Let $z \in M'$ be the image of $1 \in E$ under the canonical projection $E \to M'$. Here we compute $\mathrm{Ext}^1(M, M')$ in the category of E-modules, from which we will determine the bi-genic Hopf algebras. Note that

$$0 \longrightarrow \left(EF^n + E\left(\eta F^r - V\right)\right) \longrightarrow E \longrightarrow M \longrightarrow 0$$

is a projective presentation for M. This gives rise to the exact sequence

$$\mathrm{Hom}\left(E, M'\right) \longrightarrow \mathrm{Hom}\left(EF^n + E\left(\eta F^r - V\right), M'\right) \longrightarrow \mathrm{Ext}^1\left(M, M'\right) \longrightarrow 0.$$

Quite clearly, $\mathrm{Hom}\left(E, M'\right) \cong M'$; thus, the work in computing $\mathrm{Ext}^1(M, M')$ lies in the second group above.

Lemma 3.1. *Let*

$$S = \left\{(gz, hz) \in M' \times M' \mid h^{\sigma^n} F^n z = \eta^{p^n} g^{\sigma^r} F^r z - g^{\sigma^{-1}} \eta' F^{r'} z\right\} \subset M' \times M'.$$

Then S is a subgroup of $M' \times M'$ and $\mathrm{Hom}\left(EF^n + E(\eta F^r - V), M'\right) \cong S$.

Proof. That S is in fact a subgroup is an easy calculation which we omit. Let $\phi : EF^n + E(\eta F^r - V) \to M'$ be an E-module map. Then $\phi \mapsto (\phi(F^n), \phi(\eta F^r - V))$ defines a map $\mathrm{Hom}\,(EF^n + E(\eta F^r - V), M') \to M' \times M'$ which is readily seen to be an injective group homomorphism. Now suppose (gz, hz) is in the image of this map. Then an E-module map $\phi : EF^n + E(\eta F^r - V) \to M'$ exists with $\phi(F^n) = gz$ and $\phi(\eta F^r - V) = hz$. We need to ensure that ϕ is well defined by checking its image on $EF^n \cap E(\eta F^r - V) = EF^n(\eta F^r - V)$. We have

$$\phi\left(F^n\left(\eta F^r - V\right)\right) = F^n \phi\left(\eta F^r - V\right) = F^n hz = h^{\sigma^n} F^n z,$$

and

$$\begin{aligned}\phi\left(F^n\left(\eta F^r - V\right)\right) &= \phi\left(\left(\eta^{p^n} F^r - V\right) F^n\right) = \left(\eta^{p^n} F^r - V\right) \phi\left(F^n\right) \\ &= \left(\eta^{p^n} F^r - V\right) gz = \eta^{p^n} g^{\sigma^r} F^r z - g^{\sigma^{-1}} \eta' F^{r'} z,\end{aligned}$$

and so the restrictions on gz and hz are precisely as stated above. □

Notice that the map $\mathrm{Hom}\,(E, M') \to \mathrm{Hom}\,(EF^n + E(\eta F^r - V), M')$ gives rise to a map $M' \to S$ given by

$$fz \longmapsto \left(F^n fz, \left(\eta F^r - V\right) fz\right) = \left(f^{\sigma^n} F^n z, \left(\eta f^{\sigma^r} F^r - f^{\sigma^{-1}} \eta' F^{r'}\right) z\right).$$

From this, we obtain:

Proposition 3.2. *Let*

$$S_0 = \left\{\left(f^{\sigma^n} F^n z, \left(\eta f^{\sigma^r} F^r - f^{\sigma^{-1}} \eta' F^{r'}\right) z\right) \mid f \in k\left[F\right]\right\} \leq S.$$

Then $\mathrm{Ext}^1(M, M') \cong S/S_0$.

Proof. Obvious by the definition of Ext^1. □

Notice that the choice of $h \in k[F]$ only matters $\mathrm{mod} F^{n'}$, so we may assume $v(h) \leq n'$. We can make a similar statement for g:

Corollary 3.3. *For every $(gz, hz) \in S$ a $(g'z, h'z) \in S$ exists with $v(g') \leq n$ which gives the same extension class.*

Proof. If $v(g) \leq n$ we are done. Otherwise, let

$$g' = g - F^n, \qquad h' = h - \eta F^r + \eta' F^{r'}.$$

Then $g - g' = F^n$, $h - h' = \eta F^r - \eta' F^{r'}$ and $((g - g')z, (h - h')z) \in S_0$ (take $f = 1$). Since $v(g') = n$, the corollary is proved. □

We now give the Dieudonné module description of each extension.

Theorem 3.4. *Every extension of M by M' is of the form $M_{g,h}$, where $M_{g,h}$ is generated as an E-module by two elements x and y subject to the relations*

$$F^n x = gy, \quad (\eta F^r - V)\, x = hy, \quad F^{n'} y = 0, \quad \left(\eta' F^{r'} - V\right) y = 0$$

and $h^{\sigma^n} F^n z = \eta^{p^n} g^{\sigma^r} F^r z - g^{\sigma^{-1}} \eta' F^{r'} z$. Furthermore, the set

$$\left\{x, Fx, \ldots, F^{n-1}x, y, Fy, \ldots F^{n'-1}y\right\}$$

is a k-basis for $M_{g,h}$.

Proof. Let $[\phi]$ be an equivalence class in $\mathrm{Ext}^1(M, M')$, and let $\phi(F^n) = -gz$ and $\phi(\eta F^r - V) = -hz$. Then the extension M_ϕ obtained is the push-out of the diagram

$$\begin{array}{ccc} E(F^n) + E(\eta F^r - V) & \longrightarrow & M' \\ \downarrow & & \downarrow \\ E & \longrightarrow & M_\phi. \end{array}$$

In other words, $M_\phi \cong (E \times M')/\mathcal{I}$, where

$$\mathcal{I} = \{(i, \phi(i)) \mid i \in EF^n + E(\eta F^r - V)\}.$$

Now, since $EF^n + E(\eta F^r - V)$ is generated by F^n and $\eta F^r - V$, we see that $\mathcal{I}$ is generated by $(F^n, \phi(F^n))$ and $(\eta F^r - V, \phi(\eta F^r - V))$. Let $x \in M_\phi$ be the element corresponding to $(1,0) \in E \times M'$, and let $y \in M_\phi$ correspond to $(0,z)$. Then $F^{n'}y = (\eta' F^{r'} - V)y = 0$. Since $(F^n, -gz)$ and $(\eta F^r - V, -hz)$ generate $\mathcal{I}$, it follows that $F^n x = gy$ and $(\eta F^r - V)x = hy$ are the only other necessary relations. Writing $M_{g,h}$ for M_ϕ completes the first statement of the theorem.

For the second statement, since $Vx = \eta F^r x - hy$ and $Vy = \eta' F^{r'} y$, clearly any element in $M_{g,h}$ can be expressed as $f_1 x + f_2 y$, $f_1, f_2 \in k[F]$. Moreover, if $v(f_1) \geq n$, then $f_1 x = f_1' y$ for some $f_1' \in k[F]$ and, since $f_2 y = 0$ or $v(f_2) \leq n'$, the set $\{x, Fx, \ldots, F^{n-1}x, y, Fy, \ldots, F^{n'-1}y\}$ spans $M_{g,h}$ over k. As $\dim_k M_{g,h} = \dim_k M + \dim_k M' = n + n'$, this set is also k-linearly independent, and we are done. □

The group $\mathrm{Ext}^1(M, M')$ provides the equivalence classes of extensions

$$0 \longrightarrow M' \longrightarrow M_{g,h} \longrightarrow M \longrightarrow 0$$

of E-modules, not necessarily Dieudonné modules. However, given the generators and relations described above, it is clear that $M_{g,h}$ is killed by a power of F and V; hence, each $M_{g,h}$ is a Dieudonné module, corresponding to a Hopf algebra with at most two generators.

4. A special case. In the following section we will give a more explicit description of S. However, we first wish to look at the case $n = r$, $n' = r'$. Recall that the Dieudonné modules are in fact $E/E(F^n, V)$ and $E/E(F^{n'}, V)$, and this simpler description allows for a faster calculation of $\mathrm{Ext}^1(M, M')$. We could have looked at the cases where $n = r$ and $n' = r'$, separately, but we chose not to in order to present one Ext group calculation. However, here we will show how our work can be simplified when we are in this special case.

We start by describing a faster way to compute $\mathrm{Ext}^1(M, M')$. First, note that M arises in a short exact sequence

$$0 \longrightarrow E/E(V) \xrightarrow{\cdot F^n} E/E(V) \longrightarrow M \longrightarrow 0$$

of E-modules killed by V. These are not "Dieudonné modules" in our sense since F acts injectively on $E/E(V) \cong k[F]$. This gives a long

exact sequence

$$\begin{aligned}0 &\longrightarrow \operatorname{Hom}(M, M') \longrightarrow \operatorname{Hom}(k[F], M') \longrightarrow \operatorname{Hom}(k[F], M') \\ &\longrightarrow \operatorname{Ext}^1(M, M') \longrightarrow \operatorname{Ext}^1(k[F], M') \longrightarrow \operatorname{Ext}^1(k[F], M') \\ &\longrightarrow \operatorname{Ext}^2(M, M') \longrightarrow \operatorname{Ext}^2(k[F], M').\end{aligned}$$

Now clearly $\operatorname{Hom}(k[F], M') \cong M'$ and by [**3**, V, 5.1], we know that $\operatorname{Ext}^1(k[F], M') \cong M'/FM'$ and $\operatorname{Ext}^2(k[F], M') = 0$. Thus, the sequence is transformed into

$$\begin{aligned}0 &\longrightarrow \operatorname{Hom}(M, M') \longrightarrow M' \xrightarrow{\cdot F^n} M' \\ &\longrightarrow \operatorname{Ext}^1(M, M') \longrightarrow M'/F^nM' \xrightarrow{\cdot F^n} M'/F^nM' \\ &\longrightarrow M'/F^nM' \longrightarrow 0.\end{aligned}$$

In the case where $n \geq n'$, the two maps "$\cdot F^n$" are trivial, thereby giving an exact sequence

$$0 \longrightarrow M' \longrightarrow \operatorname{Ext}^1(M, M') \longrightarrow M' \longrightarrow 0$$

and, as there is a natural inclusion $\operatorname{Ext}^1(M, M') \hookrightarrow M' \times M'$, it is easy to see that $\operatorname{Ext}^1(M, M') \cong M' \times M'$. On the other hand, if $n' > n$, then $\operatorname{Hom}(M, M') \cong F^{n'-n}M' \cong M$ and $M'/F^nM' \cong E/E(F^n, V) \cong M$ and, as $\cdot F^n$ is trivial on M, we get

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M' \longrightarrow \operatorname{Ext}^1(M, M') \longrightarrow M \longrightarrow 0$$

and, after some computations, it can be shown that $\operatorname{Ext}^1(M, M') \cong M \times M$.

Let us demonstrate how Theorem 3.4 produces the same results. Let $(gz, hz) \in S$. Then

$$h^{\sigma^n} F^n z = \eta^{p^n} g^{\sigma^r} F^n z - g^{\sigma^{-1}} \eta' F^{n'} z = \eta^{p^n} g^{\sigma^r} F^n z,$$

and so

$$h^{\sigma^n} \equiv \eta^{p^n} g^{\sigma^r} \bmod F^d,$$

where $d = \min\{n' - n, 0\}$. Here the $M_{g,h}$ obtained is generated by x and y, subject to the relations

$$F^n x = gy, \quad (\eta F^n - V)\, x = hy, \quad F^{n'} y = 0, \quad Vy = 0.$$

Let $h' = \eta g - h \in k[F]$. Then

$$(\eta F^n - V)\, x = hy = (\eta g - h')\, y = \eta F^n x - h' y,$$

and hence $Vx = h'y$. Our relations can now be simplified to

$$F^n x = gy, \qquad Vx = h'y, \qquad F^{n'} y = 0, \qquad Vy = 0.$$

We have

$$\eta^{p^n} g^{\sigma^r} \equiv h^{\sigma^n} = (\eta g - h')^{\sigma^n} = \eta^{p^n} g^{\sigma^n} - (h')^{\sigma^n} \bmod F^d,$$

and hence $v(h') \geq d$. Conversely, any h' with $v(h') \geq d$ gives the element $(gz, (\eta g - h')z)$ of S. Thus,

$$S \cong \{(gz, h'z) \mid v\,(h') \geq d\} \cong M' \times F^d M'.$$

Now suppose $(gz, hz) \in S_0$. This is true if and only if, for some $f \in k[F]$, we have $gz = f^{\sigma^n} F^n z$ (hence $v(g) \geq n$) and

$$\begin{aligned} hz &= \left(\eta f^{\sigma^r} F^r - f^{\sigma^{-1}} \eta' F^{r'}\right) z \\ &= \left(\eta f^{\sigma^r} F^n - f^{\sigma^{-1}} \eta' F^{n'}\right) z = \eta f^{\sigma^n} F^n z = \eta g z. \end{aligned}$$

Thus,

$$\eta g z = (\eta g - h')\, z,$$

and so $h'z = 0$, i.e., $v(h') \geq n'$. Therefore.

$$S_0 \cong \{(gz, h'z) \in M' \times M' \mid v\,(g) \geq n,\ v\,(h) \geq n'\} \cong F^n M' \times 0.$$

If $n \geq n'$, then S_0 is trivial and $\mathrm{Ext}^1(M, M') \cong M' \times F^d M' = M' \times M'$, as expected. If $n < n'$, then

$$\begin{aligned} \mathrm{Ext}^1\,(M, M') &\cong \left(M' \times F^d M'\right) / \left(F^n M' \times 0\right) \\ &\cong M' / F^n M' \times F^{n'-n} M' \\ &\cong M \times M. \end{aligned}$$

5. A closer look at S. We wish to study S in greater detail to help generate all of the ordered pairs (gz, hz) that are contained in it.

We will see that this will depend on the relationship between n and n', between r and r', as well as properties of the field k.

The first result illustrates the dependence of S on the relative sizes of n, n', r, and r'. It also shows the extent to which the choice of g dictates the choice of h.

Lemma 5.1. *Let $(gz, hz) \in S$. Let $r'' = \min\{r, r'\}$, and set*

$$g_1 = \eta^{p^n} g^{\sigma^r} F^{r-r''} - g^{\sigma^{-1}} \eta' F^{r'-r''}.$$

Then $v(g_1) \geq n - r''$. Let $g_2 \in k[F]$ be given by $g_1 = g_2 F^{n-r''}$.

1. *If $n' > n$, then $h \equiv g_2^{\sigma^{-n}} \bmod F^{n'-n}$. Furthermore, $(gz, (g_2^{\sigma^{-n}} + h_1 F^{n'-n})z) \in S$ for all $h_1 \in k[F]$.*
2. *If $n' \leq n$, then $(gz, h_1 z) \in S$ for every $h_1 \in k[F]$.*

Proof. Since $(gz, hz) \in S$, we have

$$h^{\sigma^n} F^n z = \eta^{p^n} g^{\sigma^r} F^r z - g^{\sigma^{-1}} \eta' F^{r'} z = g_1 F^{r''} z,$$

and so $h^{\sigma^n} F^n z \equiv g_1 F^{r''} z$. Taking the valuation of each side gives

$$v(h) + n = v(g_1) + r''.$$

Since $v(h) \geq 0$, it follows that $v(g_1) \geq n - r''$. If we let g_2 be as in the statement of the lemma, we have

$$h^{\sigma^n} F^n z = g_2 F^n z.$$

Now, if $n' \leq n$, then both sides are zero, and it is easy to see that item 2 is established. If $n' > n$, then $h^{\sigma^n} \equiv g_2 \bmod F^{n'-n}$ and 1 follows. □

At this point it is easier to proceed in two separate cases, depending upon whether r is equal to r'. We will start with the easier case where they are not equal.

Lemma 5.2. *Let $(gz, hz) \in S$, $r'' = \min\{r, r'\}$. Suppose $r \neq r'$. Then $v(g) \geq n - r''$.*

Proof. For $(gz, hz) \in S$ we know from above that $v(g_1) \geq n - r''$, where $g_1 = \eta^{p^n} g^{\sigma^r} F^{r-r''} - g^{\sigma^{-1}} \eta' F^{r'-r''}$. Since $r \neq r''$, we see that exactly one of $r - r''$, $r' - r''$ is zero; hence, $v(g_1) = v(g)$. □

On the other hand, if $r = r'$ it is a little more complicated since it is not necessarily true that $v(g) \geq n - r''$. In this case, S depends on solutions to certain polynomials, and hence to k.

Lemma 5.3. *Suppose $r = r'$, and let $(gz, hz) \in S$. Write $gz = \sum_{i=0}^{n'} \gamma_i F^i z$. Then, for all $i < n - r$, we have that γ_i is a zero of the polynomial*

$$\eta^{p^{n+1}} t^{p^{r+1}} - (\eta')^{p^i} t.$$

Proof. Since $r = r'$, we have

$$h^{\sigma^n} F^n z = \eta^{p^n} g^{\sigma^r} F^r z - g^{\sigma^{-1}} \eta' F^r z = \left(\eta^{p^n} g^{\sigma^r} - g^{\sigma^{-1}} \eta'\right) F^r z.$$

Taking the valuation of each side gives

$$v(h) + n = v(g_1) + r,$$

where again $g_1 = \eta^{p^n} g^{\sigma^r} - g^{\sigma^{-1}} \eta'$. Thus, $v(g_1) \geq n - r$. Since

$$g_1 = \sum_{i=0}^{n'} \eta^{p^n} \gamma_i^{p^r} F^i - \sum_{i=0}^{n'} \gamma_i^{p^{-1}} F^i \eta' = \sum_{i=0}^{n'} \left(\eta^{p^n} \gamma_i^{p^r} - \gamma_i^{p^{-1}} (\eta')^{p^i}\right) F^i,$$

we see that $\eta^{p^n} \gamma_i^{p^r} - \gamma_i^{p^{-1}} (\eta')^{p^i} = 0$ whenever $i < n - r$. Raising both sides to the pth power gives

$$\eta^{p^{n+1}} \gamma_i^{p^{r+1}} - (\eta')^{p^i} \gamma_i = 0,$$

and γ_i is clearly a zero of the polynomial above. □

We summarize the results of this section.

Theorem 5.4. *For each $i < n - r$, let*

$$f_i(t) = \eta^{p^{n+1}} t^{p^{r+1}} - (\eta')^{p^i} t,$$

and let Z_i be the zeros of $f_i(t)$ in k. For $g \in k[F]$, define

$$g_2 = \left(\eta^{p^n} g^{\sigma^r} F^{r-r''} - g^{\sigma^{-1}} \eta' F^{r'-r''}\right) F^{n-r''}$$

where $r'' = \min\{r, r'\}$.

1. *If $r \neq r'$, $n < n'$, then*

$$S = \left\{ \left(gz, \left(g_2^{\sigma^{-n}} + h_1 F^{n'-n}\right) z\right) \mid g \in F^{n-r''} k[F],\ h_1 \in k[F] \right\}.$$

2. *If $r \neq r'$, $n \geq n'$, then*

$$S = \left\{ (gz, hz) \mid g \in F^{n-r''} k[F],\ h \in k[F] \right\}.$$

3. *If $r = r'$, $n < n'$, then*

$$S = \left\{ \left(gz, \left(g_2^{\sigma^{-n}} + h_1 F^{n'-n}\right) z\right) \mid g \in \bigoplus_{i=0}^{n-r} Z_i F^i + F^{n-r} k[F],\ h_1 \in k[F] \right\}.$$

4. *If $r = r'$, $n \geq n'$, then*

$$S = \left\{ (gz, hz) \mid g \in \bigoplus_{i=0}^{n-r} Z_i F^i + F^{n-r} k[F],\ h \in k[F] \right\}.$$

6. The Hopf algebra structure of $\mathcal{H}(M_{g,h})$. Throughout this section, we let $M = M_{g,h}$ and $H = \mathcal{H}(M)$. We wish to examine the Hopf algebra structure of H. Since we are interested in identifying the bi-genic Hopf algebras, one approach is to eliminate the monogenic ones from this classification. Determining if H is monogenic is surprisingly straightforward.

Proposition 6.1. *The Hopf algebra H is monogenic if and only if $v(g) = 0$.*

Proof. Recall that H is monogenic if and only if $\dim_k M/FM = 1$. The relations on M induce the following relations on M/FM:

$$g\overline{y} = 0, \quad V\overline{x} = -h\overline{y}, \quad V\overline{y} = 0,$$

where, for $m \in M$, the symbol $\overline{m}$ represents the coset $m + FM$. Now, if $v(g) > 0$, we see that $\{\overline{x}, \overline{y}\}$ forms a k-basis for M/FM, and hence H is not monogenic. On the other hand, if $v(g) = 0$, then $g\overline{y} = 0$ implies that $\overline{y} = 0$; hence, M/FM has k-basis $\{\overline{x}\}$ and H is monogenic. □

Corollary 6.2. *The Hopf algebra H is necessarily bi-genic if $n \neq r''$ and either $r \neq r'$ or $\eta^{p^{n+1}}/\eta' \notin (k^\times)^{p-1}$.*

Proof. In cases 1 and 2 of Theorem 5.4, we have $v(g) \geq n - r''$, and in cases 3 and 4 $v(g) > 0$ if $Z_0 = \{0\}$. Since $0 \neq \gamma \in Z_0$, if and only if $\eta^{p^{n+1}}\gamma^p - \eta'\gamma = 0$, we have

$$\frac{\eta^{p^{n+1}}}{\eta'} = \gamma^{1-p} \in \left(k^\times\right)^{p-1}. \qquad \square$$

While not needed for the remainder of the paper, the following shows how the $v(g) = 0$ case corresponds to the classification in [**9**].

Corollary 6.3. *If $v(g) = 0$, then*

$$M \cong E/E\left(F^{n+n'}, \eta_0 F^r - V\right), \quad \eta_0 \in k,$$

where $\eta_0 = \eta$ if $r < n$ and $\eta_0 \equiv \eta - hg^{-1} \bmod Fk[F]$ if $r = n$.

Proof. Since $y = g^{-1}F^n x$, it is clear that $F^{n'+n}x = 0$ and $F^{n'+n-1}x \neq 0$. Since $(\eta F^r - V)x = hy = hg^{-1}F^n x$, we see that

$$Vx = \eta F^r x - hg^{-1}F^n x.$$

Suppose $r < n$. Then

$$px = FVx = \eta^p F^{r+1}x - \left(hg^{-1}\right)^\sigma F^{n+1}x = \left(\eta^p - \left(hg^{-1}\right)^\sigma F^{n-r}\right)F^{r+1}x,$$

and $v(\eta^p - (hg^{-1})^\sigma F^{n-r}) = 0$; hence, $F^{r+1}x = (\eta^p - (hg^{-1})^\sigma F^{n-r})^{-1}px \in pM$. Thus,

$$M/pM \cong E/E\left(F^{r+1}, \eta F^r - V\right),$$

and the result in this case follows from the proof of [**9**, Proposition 2.2]. On the other hand, if $r = n$, then

$$\begin{aligned} Vx &= \left(\eta - hg^{-1}\right)F^n x \\ px &= \left(\eta^p - \left(hg^{-1}\right)^\sigma\right)F^{n+1}x. \end{aligned}$$

Now, if $v(\eta^p - (hg^{-1})^\sigma) = 0$, then again $F^{r+1}x \in M$, and we get

$$M/pM \cong E/E\left(F^{r+1}, \eta_0 F^r - V\right)$$

where η_0 is as in the statement of the corollary. Using [**9**, Proposition 2.2] again will give the desired result.

Finally, if $r = n$ and $v(\eta^p - (hg^{-1})^\sigma) > 0$, then $Vx \equiv 0 \bmod pM$, and

$$M = M/pM \cong E/E\left(F^{n+n'}, V\right)$$

and we are done. □

The Hopf algebra structure when $v(g) = 0$ can be found in [**11**, Section 4].

We return to the case of interest, namely, $v(g) \neq 0$. The following proposition provides the algebraic structure.

Proposition 6.4. *Let $v = v(g)$, $v(g) \leq n'$. Then*

$$H \cong k[t_1, t_2] \Big/ \left(t_1^{p^{n+n'-v}}, t_2^{p^v}\right).$$

Proof. Let $g_* \in k[F]^\times$ have the property that $gg_* \equiv F^v \bmod F^{n+n'}$. (Such a g_* clearly exists.) Then $gg_*x = F^v x$ and $gg_*y = F^v y$. We get

$$F^{n+n'-v}x = F^{n'-v}gy = F^{n'-v}F^v g_*^{-1}y = \left(g_*^{-1}\right)^{\sigma^{n'}} F^{n'}y = 0.$$

Let $y' = g_*F^{n-v}x - y$. It is clear that $\{x, y'\}$ generate M as an E-module with relations

$$F^n x = g\left(g_*F^{n-v}x - y'\right), \quad (\eta F^r - V)\, x = h\left(g_*F^{n-v}x - y'\right),$$
$$F^{n'}\left(g_*F^{n-v}x - y'\right) = 0, \quad \left(\eta' F^{r'} - V\right)\left(g_*F^{n-v}x - y'\right) = 0.$$

The first relation simplifies as

$$F^n x = g\left(g_*F^{n-v}x - y'\right) = F^n x - gy',$$

and hence $gy' = 0$. By Lemma 2.2, we get $F^v y' = 0$. Since $Vx, Vy \in k[F]x + k[F]y'$, we see that

$$\left\{x, Fx, \ldots, F^{n+n'-v-1}x, y', Fy', \ldots F^{v-1}y'\right\}$$

spans M as a k-module, and since $\dim M = n + n'$ it must also be a basis. Let $t_1 = T_x$ and $t_2 = T_{y'}$. Since $F^{n+n'-v}x = 0$, we have that $t_1^{p^{n+n'-v}} = T_{F^{n+n'-v}x} = 0$, and similarly $t_2^{p^v} = 0$. Thus, we get a surjective map:

$$k\left[t_1, t_2\right] \Big/ \left(t_1^{p^{n+n'-v}}, t_2^{p^v}\right) \longrightarrow H,$$

and, by comparing dimensions, we see it is in fact an isomorphism. □

Remark 6.5. The above proposition does not assume $v \neq 0$. In the case $v = 0$, we get

$$H \cong k\left[t_1, t_2\right] \Big/ \left(t_1^{p^{n+n'}}, t_2\right) \cong k\left[t_1\right] \Big/ \left(t_1^{p^{n+n'}}\right),$$

as expected.

In general, the coalgebra structure is straightforward, but it can be messy depending upon the complexity of g and h. We conclude with a simple example to illustrate how this is done.

Example 6.6. Suppose $n = r$, $n' = r'$, $g = F^i$ and $h = F^j$. We have

$$\begin{aligned} Vx &= F^j y \\ V^2 x &= 0 \end{aligned}$$

since $Vy = 0$. Thus, we may pick $N = 1$. If $i \geq n'$, then

$$\begin{aligned} H &\cong k[t_1, t_2] \Big/ \left(t_1^{p^n}, t_2^{p^{n'}}\right) \\ \Delta(t_1) &= S_1\left(\left(t_2^{p^j} \otimes 1, t_1 \otimes 1\right); \left(1 \otimes t_2^{p^j}, 1 \otimes t_1\right)\right) \\ &= t_1 \otimes 1 + 1 \otimes t_1 + \sum_{\ell=1}^{p-1} \binom{p}{\ell} t_2^{p^{j+\ell}} \otimes t_2^{p^{j+(p-\ell)}} \\ \Delta(t_2) &= S_1\left((0 \otimes 1, t_2 \otimes 1); (1 \otimes 0, 1 \otimes t_2)\right) \\ &= t_2 \otimes 1 + 1 \otimes t_2. \end{aligned}$$

On the other hand, if $i < n'$, then as before we set $y' = F^{n-i}x - y$ and let $t_1 = T_x$, $t_2 = T_{y'}$. Note that $V(F^{n-i}x) = F^{n-i+j}y$, so

$$\begin{aligned} T_{y'} &= T_{F^{n-i}x - y} \\ &= S_1\left(\left(T_{V(F^{n-i}x)}, T_{F^{n-i}x}\right); (T_{-Vy}, T_{-y})\right) \\ &= S_1\left(\left(T_y^{p^{n-i+j}}, T_x^{p^{n-i}}\right); (0, -T_y)\right) = T_x^{p^{n-i}} - T_y. \end{aligned}$$

Thus, $T_y = T_x^{p^{n-i}} - T_{y'} = t_1^{p^{n-i}} - t_2$. We also have:

$$\begin{aligned} Vy' &= V\left(F^{n-i}x - y\right) = F^{n-i}Vx = F^{n-i+j}y \\ V^2 y' &= F^{n-i+j}Vy = 0, \end{aligned}$$

and hence,

$$\begin{aligned} H &\cong k[t_1, t_2] \Big/ \left(t_1^{n+n'-i}, t_2^i\right) \\ \Delta(t_1) &= S_1\left((T_{Vx} \otimes 1, T_x \otimes 1); (1 \otimes T_{Vx}, 1 \otimes T_x)\right) \end{aligned}$$

$$
\begin{aligned}
&= S_1\left(\left(T_{F^j y}\otimes 1, T_x\otimes 1\right); \left(1\otimes T_{F^j y}, 1\otimes T_x\right)\right)\\
&= S_1\left(\left(\left(t_1^{p^{n-i}}-t_2\right)^{p^j}\otimes 1, t_1\otimes 1\right); 1\otimes\left(\left(t_1^{p^{n-i}}-t_2\right)^{p^j}, 1\otimes t_1\right)\right)\\
&= t_1\otimes 1 + 1\otimes t_1\\
&\quad + \sum_{\ell=1}^{p-1}\binom{p}{\ell}\left(t_1^{p^{n-i}}-t_2\right)^{p^{j+\ell}}\otimes\left(t_1^{p^{n-1}}-t_2\right)^{p^{j+(p-\ell)}}\\
\Delta(t_2) &= S_1\left(\left(T_{Vy'}\otimes 1, T_{y'}\otimes 1\right); \left(1\otimes T_{Vy'}, 1\otimes T_{y'}\right)\right)\\
&= S_1\left(\left(T_{F^{n-i+j}y}\otimes 1, T_{y'}\otimes 1\right); \left(1\otimes T_{F^{n-i+j}y}, 1\otimes T_{y'}\right)\right)\\
&= S_1\left(\left(\left(t_1^{p^{n-i}}-t_2\right)^{p^{n+i-j}}\otimes 1, t_2\otimes 1\right);\right.\\
&\qquad\qquad\left.\left(1\otimes t_2, 1\otimes\left(t_1^{p^{n-i}}-t_2\right)^{p^{n+i-j}}\right)\right)\\
&= t_2\otimes 1 + 1\otimes t_2\\
&\quad + \sum_{\ell=1}^{p-1}\binom{p}{\ell}\left(t_1^{p^{n-i}}-t_2\right)^{p^{n+i-j+\ell}}\otimes\left(t_1^{p^{n-1}}-t_2\right)^{p^{n+i-j+(p-\ell)}}.
\end{aligned}
$$

REFERENCES

1. C. Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. Math. **152** (2000), 489–549.

2. Brian Conrad, *Finite group schemes over bases with low ramification*, Comp. Math. **119** (1999), 239–320.

3. M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, editeur, Paris, 1970.

4. Jean-Marc Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C.R. Acad. Sci. Paris **280** (1975), 1423–1425.

5. ———, *Groupes p-divisibles sur les vecteurs de Witt*, C.R. Acad. Sci. Paris **280** (1975), 1353–1356.

6. ———, *Sur la construction du module de Dieudonné d'un groupe formel*, C.R. Acad. Sci. Paris **280** (1975), 1273–1276.

7. A. Grothendieck, *Groupes de Barsotti-Tate et cristaux de Dieudonné*, The Presses at the University of Montréal, Montreal, Quebec, 1974.

8. A. Koch, *Monogenic Hopf algebras representing commutative p-group schemes*, preprint.

9. ———, *Monogenic bialgebras over finite fields and rings of Witt vectors*, J. Pure Appl. Algebra **163** (2001), 193–207.

10. A. Koch, *Witt subgroups and cyclic Dieudonné modules killed by p*, Rocky Mountain J. Math. **31** (2001), 1023–1038.

11. ———, *Monogenic Hopf algebras and local Galois module theory*, J. Algebra **264** (2003), 408–419.

12. ———, *Height one Hopf algebras in low ramification*, New York J. Math. **10** (2004), 295–306 (electronic).

13. W. Waterhouse, *Introduction to affine group schemes*, Grad. Texts Math. **66**, Springer-Verlag, New York, 1979.

Department of Mathematics, Agnes Scott College, 141 E. College Ave., Decatur, GA 30030
Email address: akoch@agnesscott.edu