New York Journal of Mathematics

New York J. Math. **4** (1998) 127–136.

Lifting Witt Subgroups to Characteristic Zero

Alan Koch

Abstract. Let k be a perfect field of characteristic $p > 0$. Using Dieudonné modules, we describe the exact conditions under which a Witt subgroup, i.e., a finite subgroup scheme of W_n, lifts to the ring of Witt Vectors $W(k)$.

Contents

Let k be a perfect field, char $k = p > 0$. Let R be a complete discrete valuation ring of characteristic 0 with residue field k. Suppose G is a finite affine commutative k-group scheme of p-power rank. Under what conditions does G "lift" to R? In other words, when does there exist an R-group scheme $\tilde{G}$ which is a free commutative group scheme of p-power rank over R (hereafter referred to as a *finite p-group* as in [F2]) so that $\tilde{G} \times_{\mathrm{Spec}\ (R)} \mathrm{Spec}\ (k) \cong G$? There are instances where the answer to this lifting question is clear. If G is étale, for example, then $G \times \mathrm{Spec}\ (\bar{k})$ is isomorphic to a direct sum of μ_{p^n}'s for various n, where μ_{p^n} is the group scheme that gives the p^{nth} roots of unity for a given $\bar{k}$-algebra. μ_{p^n} clearly lifts to R for all R: it lifts to the p^{nth} roots of unity functor over R. Since the question of lifting is preserved under base change [OM, 2.2] we have that G lifts. As another example, if G is of multiplicative type, G will always lift to R, since then G^* is étale (where $G^* = \mathrm{Hom}_{k-gr}(G, \mathbf{G}_m)$ is the linear dual of G) and lifting is preserved by duality.

Any finite affine commutative k-group scheme decomposes into a direct sum of an étale scheme and a connected scheme. The connected group scheme decomposes further into a group scheme of multiplicative type and a group scheme that is unipotent [W]. Thus the question of lifting is only of interest when G is both connected and unipotent. In the language of Hopf algebras, this simply means that H and its dual Hopf algebra H^* are local k-algebras, where $G = \mathrm{Spec}\ (H)$.

Received January 19, 1998.
Mathematics Subject Classification. 14L.
Key words and phrases. Group Schemes, Dieudonné Modules, Witt Vectors.

ISSN 1076-9803/98

In 1968, Oort and Mumford [OM] were the first to show that, for all such group schemes G, there is a complete discrete valuation ring R so that G lifts to R. In other words, they showed that all finite affine commutative group schemes lift to characteristic zero. However, it is known that not every group scheme lifts to every such R: the best known example being α_p, the unique connected unipotent group scheme of rank p over k. $\boldsymbol{\alpha}_p$ will lift only to rings which admit a factorization of p into elements in the maximal ideal [TO]. Thus this group scheme can not lift to $\mathbf{Z}_p$, the ring of p-adic integers, or for that matter any unramified extension of $\mathbf{Z}_p$. More generally, it was shown in 1992 by Roubaud [R, p. 72] that, for $p \geq 5$, any G will lift to any R with ramification index $1 < e \leq p-1$.

We shall focus our attention on the case $e = 1$. k-group schemes that can lift when $e = 1$ lift in the strongest possible sense, i.e., such group schemes will lift to any discrete valuation ring R with residue field $\ell \supseteq k$. These discrete valuation rings arise as the ring of Witt Vectors over some k, which shall be denoted $W(k)$. The issue we address is the following: for G a connected subgroup scheme of W_n (the group scheme of Witt Vectors of finite length n), when does G lift to $W(k)$? The collection of subgroups that do lift to $W(k)$ is surprisingly easy to describe when the question is described in terms of the Dieudonné module associated to the group scheme; and we shall see that the question of G lifting is equivalent to being able to identify the structure of much smaller group schemes.

The connected subgroups of W_n (called the *Witt subgroups*) correspond to the subclass of Dieudonné modules that are *cyclic*; that is, modules that are of the form E/I for some ideal $I \subset E$, where E is the non-commutative ring $W(k)[F, V]$ modulo some relations. We start by recalling a classification of cyclic Dieudonné modules, paying special attention to the modules that are killed by p. The process we shall use to lift these Witt subgroups was developed by Fontaine in [F2] using what are called "Finite Honda Systems." Then, we determine exactly which of the modules killed by p correspond to group schemes that lift. Finally, we answer the lifting question for all Witt subgroups.

Throughout this paper, let p be a fixed odd prime. Unless otherwise specified, all group schemes over k will be finite, affine, commutative, connected, and unipotent. The author would like to thank the referee for many helpful suggestions.

1. Cyclic Dieudonné Modules

Let G be a k-group scheme. Let E be the Dieudonné ring associated to k, that is E is the non-commutative ring $W(k)[F, V]$ with the relations $FV = VF = p$, $Fw = w^\sigma F$, and $wV = Vw^\sigma$; with $w \in W(k)$ and w^σ defined by raising each component of w to the p^{th} power. To G we can associate an E-module $D^*(G)$ via $D^*(G) = \mathrm{Hom}_{k-gr}(G, C)$ where C is the E-module functor of Witt Covectors as described in [F1, p. 1273]. D^* induces an anti-equivalence between connected unipotent group schemes and E-modules killed by a power of F and V. These modules will be called *Dieudonné modules.* If we do not insist on G being finite or connected (but still affine, commutative, and unipotent), we still have a correspondence, now between group schemes and E-modules killed by a power of V. Details on this correspondence can be found in [DG, V §1 4.3]. Since D^* is an exact functor and $D^*(W_n) = E/E(V^n)$ [DG, V §1 4.2], it is easy to see that Witt subgroups correspond precisely to cyclic Dieudonné modules. Note that W_n is viewed as a unipotent group scheme via

$$W_n(A) = \{(a_0, a_1, \dots, a_{n-1}) \;\mid\; a_i \in A\}$$

for any k-algebra A, with group operation induced from the law of addition of Witt vectors.

We begin with a survey of the results in [K]. The general structure of a cyclic Dieudonné module begins with the classification of cyclic Dieudonné modules killed by p. Each of these modules fits one of the following two forms:

$$E/E(F^n - \eta V^m, p) \tag{1}$$

$$E/E(F^n, p, V^m) \tag{2}$$

where $\eta \in k^\times$. (Moreover, $E/E(F^n - \eta_1 V^m, p) \cong E/E(F^n - \eta_2 V^m, p)$ if and only if there is an $a \in k^\times$ such that $\eta_1 = a^{p^{n+m}-1}\eta_2$, but this will not be needed for the results that follow.)

We will call these two forms type 1 and type 2 respectively. One major difference between the two types is the following:

Lemma 1.1. *A cyclic Dieudonné module killed by p is of type 1 if and only if* $\ker V = \mathrm{im}\ F$.

Proof. Let M be a cyclic Dieudonné module killed by p and $x = 1_M$, so M is generated as an E-module by x. It is clear that $\mathrm{im}\ F \subseteq \ker V$ as $VFx = px = 0$. Suppose M is of type 1. Then $M = E/E(F^n - \eta V^m, p)$ for some $m, n > 0$, $\eta \in k^\times$. M has a k-basis $\{x, Fx, F^2x, \dots F^n x, Vx, V^2x, \dots, V^{m-1}x\}$. Let $y \in \ker V$. We can write

$$y = \sum_{i=0}^{n} a_i F^i x + \sum_{j=1}^{m-1} b_j V^j x$$

with all of the a_i's and b_j's in k. Applying V gives

$$\begin{aligned} Vy &= a_0^{p^{-1}} Vx + \sum_{j=1}^{m-1} b_j^{p^{-1}} V^{j+1} x \\ &= a_0^{p^{-1}} Vx + \sum_{j=2}^{m} b_{j-1}^{p^{-1}} V^j x \\ &= a_0^{p^{-1}} Vx + \sum_{j=2}^{m-1} b_{j-1}^{p^{-1}} V^j x + b_{m-1}^{p^{-1}} \eta^{-1} F^n x = 0 \end{aligned}$$

By k-linear independence, this means $a_0 = b_1 = b_2 = b_3 = \cdots = b_{m-1} = 0$. Thus we must have

$$y = \sum_{i=1}^{n} a_i F^i x.$$

hence $y \in \mathrm{im}\ F$.

Conversely, if $M = E/E(F^n, p, V^m)$, i.e M is of type 2, it is clear that $\ker V \neq \mathrm{im}\ F$ as $V^{m-1}x \in \ker V$ but $V^{m-1}x \notin \mathrm{im}\ F$. $\square$

More generally, let M be a cyclic Dieudonné module of p-rank h. The term p-rank will be used to signify the smallest positive integer h such that $p^h M = 0$. M can be decomposed into a short exact sequence

$$0 \longrightarrow M' \xrightarrow{\ i\ } M \xrightarrow{\ \pi\ } M'' \longrightarrow 0$$

where $M' = p^{h-1}M$, $M'' = M/p^{h-1}M$, and π is the natural projection. Note that M' and M'' are cyclic of p-ranks 1 and $h-1$ respectively. From this we can see that the construction of cyclic modules of p-rank h can be obtained by finding cyclic Dieudonné modules M' and M'' of p-ranks 1 and $h-1$ so that there is a sequence

$$0 \longrightarrow M' \xrightarrow{\ f\ } M \xrightarrow{\ g\ } M'' \longrightarrow 0$$

so that $f(z) = p^{h-1}x$ and $g(x) = y$, where $x,\ \ y$, and z generate $M,\ \ M''$ and M' respectively as E-modules.

Given cyclic modules M' and M'' of p-ranks 1 and $h-1$ respectively, it is not always true that we can construct an M to fit into the short exact sequence above. The following gives a necessary (but not sufficient) condition on M' and M'':

Lemma 1.2. *Let M' and M'' be cyclic Dieudonné modules of p-ranks 1 and $h-1$ respectively, $h \geq 2$. Suppose there is a short exact sequence*

$$0 \longrightarrow M' \xrightarrow{\ f\ } M \xrightarrow{\ g\ } M'' \longrightarrow 0$$

so that M has p-rank h, $f(z) = p^{h-1}x$, and $g(x) = y$, where $x,\ \ y$, and z generate $M,\ \ M''$ and M' respectively. If $F^\ell y = \eta V^r y$, then $F^\ell z = \eta V^r z$.

Proof. If $F^\ell y = \eta V^r y$, then $(F^\ell - \eta V^r)x \in \ker g = \operatorname{im} f$. Thus there is an $e \in E$ such that $F^\ell x - \eta V^r x = ep^{h-1}x$. Thus

$$f(F^\ell z - \eta V^m z) = p^{h-1}(F^\ell x - \eta V^m x) = ep^{2h-2}x = 0$$

since $2h-2 \geq h$ for $h \geq 2$. Thus $F^\ell z = \eta V^m z$. □

We can categorize cyclic Dieudonné modules by picking modules killed by p that satisfy the above short exact sequence. If we pick an M' and an M'' killed by p we get a module M killed by p^2. If we then pick a different M' and set $M'' = M$, we get a new module M killed by p^3, and so on. By the repeated selection of cyclic modules killed by p in this manner we can obtain a complete classification of cyclic Dieudonné modules. (Note that, for a given M' and M'', the M constructed is usually not unique.) Thus we can associate to each cyclic Dieudonné module of p-rank h a sequence $M_0, M_1, \ldots M_{h-1}$ of cyclic Dieudonné modules killed by p. Each of these M_i's can be recovered from M: $M_i \cong p^i M / p^{i+1} M$. A consequence of the above lemma is that if $M_i = E/E(F^n - \eta V^r, p)$ and $M_j = E/E(F^{n'} - \eta' V^{r'}, p)$ with $i < j$, then $n \geq n'$ and $r \geq r'$. This observation will be important in Section 4.

2. Finite Honda Systems

Having described the construction of a cyclic Dieudonné module, we now focus on the tool used for finding lifts of group schemes to $W(k)$, namely the finite Honda systems. Finite Honda systems were first developed by Fontaine in [F2] in a manner analogous to (and relying heavily on) Honda's method to lift p-divisible groups.

Definition 2.1. A finite Honda system over $W(k)$ consists of a pair (M, L), where M is a Dieudonné module and L is a $W(k)$-submodule of M so that

i) $\ker V \cap L = 0$
ii) The canonical map $\overline{L} \to \overline{M} \to \operatorname{coker} F$ is an isomorphism, where $\overline{L}$ and $\overline{M}$ denote reduction mod p.

By a slight abuse of notation, we shall often identify $\overline{L}$ with its image in coker F and write condition (ii) as $L/pL = M/FM$. A *morphism* $(M_1, L_1) \to (M_2, L_2)$ consists of an E-module map $\varphi : M_1 \to M_2$ such that $\varphi(L_1) \subseteq L_2$. Thus the collection of finite Honda systems over k forms a category, which we shall denote $FH(W(k), k)$.

The lifting theory works as follows. Suppose $\tilde{G}$ is a $W(k)$-group scheme lifting the k-group scheme $G = \operatorname{Spec}(H)$. Let $M = D^*(G) = \operatorname{Hom}_{k-gr}(G, C)$. Then elements of M are in one-to-one correspondence with $\operatorname{Hom}_{Hopf-alg}(D, H)$, the Hopf algebra homomorphisms $D \to H$, where $C = \operatorname{Spec}(D)$. The set of all such maps is a subgroup of $\operatorname{Hom}_{k-alg}(D, H) \cong C(H)$, so we can embed $M \hookrightarrow C(H)$. Now for K the fraction field of $W(k)$ we have a map $w_H : C(H) \to (H \bigotimes_{W(k)} K)/H$ defined by

$$w_H(\ldots, h_{-2}, h_{-1}, h_0) = \sum_{i=0}^{\infty} \frac{\tilde{h}_{-i}^{p^i}}{p^{i+1}}$$

where $\tilde{h}_{-i}$ is a lift of h_{-i} to $W(k)$. (It is easy to see that the map does not depend on the choice of lift.) Let $L = \ker w_H|_M$. Then (M, L) is a finite Honda system.

Conversely, given a finite Honda system (M, L) the finite p-group $\tilde{G}$ over $W(k)$ it determines is given by, for any finite $W(k)$-algebra A,

$$\tilde{G}(A) = \{\phi \in G(A/pA) \,|\, C(\phi)(L) \subset \ker w_A\}$$

where $M = D^*(G)$.

It can be shown that morphisms between finite Honda systems induce morphisms on the $W(k)$-group schemes associated to them, and hence the correspondence outlined above determines a categorical anti-equivalence between $FH(W(k), k)$ and the category of finite p-groups over $W(k)$. As $(FH(W(k), k)$ is an abelian category [F2, Cor. 1], so is this category of $W(k)$-group schemes. Thus the kernel and cokernel of any morphism of two finite p-groups over $W(k)$ must also be a finite p-group.

Note that these systems are a special case of a more general system $FH(R, k)$ over any discrete valuation ring R of characteristic zero with residue field k. The objects in $FH(R, k)$ consist of quintuples (M, M', f, v, L) with $f : M \to M'$, $v : M' \to M$, so that $fv = p \cdot 1_{M'}$ and $vf = p \cdot 1_M$ and $L \subset M'$. The system described above correponds to the case $M = M' = D^*(G)$, $f = F$, $v = V$. See [R] for a complete description of these modules.

3. The *p*-rank 1 Case

We start the application of Fontaine's theory to cyclic Dieudonné modules by dealing with the simplest type of cyclic modules, namely the p-rank 1 case. Here we can quickly determine which of the modules lift to $W(k)$.

Lemma 3.1. *Let M be a cyclic Dieudonné module killed by p. Then M lifts to $W(k)$ if and only if M is of type 1.*

Proof. We shall explicitly either construct the L necessary to have a finite Honda system, hence to have a lifting of G, or show that no such L can exist.

Type 1: Let $M = E/E(F^n - \eta V^m, p)$, and let $x = 1_M$, i.e., x is a generator of M. We can quickly find coker F: $M/FM{=}E/E(F,V^m)$. Let L be generated over $W(k)$ by $\{x, Vx, V^2x, ..., V^{m-1}x\}$. As $L \cap FM = 0$ and im $F = \ker V$, $L \cap \ker V = 0$, and it is clear by the definition of L that $L = L/pL = M/FM$. Thus (M, L) satisfies the properties of a finite Honda system, so G lifts to $W(k)$.

Type 2: Suppose we have an L so that (M, L) is a finite Honda system. Write $M = E/E(F^n, p, V^m)$. Then $M/FM = E/E(F, V^m)$ Clearly $\dim_k M = n + m - 1$ and $\dim_k M/FM = m$. Thus $\dim_k L/pL = \dim_k L = m$. But $\ker V$ has a k-basis $\{Fx, F^2x, \ldots, F^{n-1}x, V^{m-1}x\}$ and hence $\dim_k \ker V = n$. Thus,

$$\dim_k (L + \ker V) = n + m > \dim_k M$$

which is absurd. Thus no L can exist to make (M, L) a finite Honda system, hence the Witt subgroup corresponding to M does not lift. □

In the type 1 case, the $W(k)$-submodule is not unique – in fact there are many other possible choices for L.

Corollary 3.2. *Let $M = E/E(F^n - \eta V^m, p)$, $x = 1_M$. Let L' be the $W(k)$-submodule generated by*

$$\{(1 - Fe_0)x, (V - Fe_1)x, (V^2 - Fe_2)x, \ldots, (V^{m-1} - Fe_{m-1})x\}, \quad e_i \in E$$

Then (M, L') is a finite Honda system.

Proof. If we take L to be the $W(k)$-submodule generated by $\{x, Vx, V^2x, \ldots, V^{m-1}x\}$, then by the lemma (M, L) is a finite Honda system. As $V^i x \equiv (V^i - Fe_i)x \pmod{FM}$, it is clear that $L' = M/FM$. Since $FVx = px = 0$ it follows that $VL' = VL$, so $\ker V \cap L'$ must be zero. □

We shall refer to this corollary in the proof of Theorem 4.1.

Example 3.3. It was stated in the introduction that the group scheme α_p does not lift to $W(k)$. α_p is a Witt subgroup as α_p embeds naturally in $\mathbf{G}_a \cong W_1$. Lemma 3.1 provides a quick proof that it does not lift. As α_p is the unique k-group scheme of rank p, $D^*(\alpha_p)$ must be the unique simple object in the category of E-modules, hence $D^*(\alpha_p) \cong E/E(F, V) \cong k$. Since $E/E(F, V)$ is of type 2, α_p does not lift to $W(k)$.

Example 3.4. On the other hand, the simplest Witt subgroup G that *does* lift is the one so that $D^*(G) \cong E/E(F - V, p)$. This group scheme is characterized as follows: for any k-algebra A we have

$$G(A) = \{a \mid a \in A,\ a^{p^2} = 0\}$$

with

$$a +_G b = a + b - \frac{(a^p + b^p)^p}{p}$$

with the addition on the right-hand side determined by the addition in A. The group scheme it lifts to is given by, for any finite $W(k)$-algebra R,

$$\tilde{G}(R) = \{r \mid r \in R/pR, \quad \tilde{r}^{p^2} + p\tilde{r} \in p^2 R \text{ for } \tilde{r} \text{ a lift of } r\}$$

with addition defined in the exact same way.

4. Lifts of Witt Subgroups

Finally, we are in a position to completely answer the question of lifting Witt subgroups to $W(k)$. We shall show that the question of lifting M is answered by examining the structure of the M_i's.

The following theorem shows not only which Witt subgroups lift, it also provides a finite Honda system.

Theorem 4.1. *Let G be a Witt subgroup, $M = D^*(G)$. Let h denote the p-rank of M, and set $M_i = p^i M/p^{i+1}M$, $i = 0, 1, 2, \ldots, h-1$. Then G lifts to $W(k)$ if and only if M_i lifts for all $0 \leq i \leq h-1$.*

This, when proved, will immediately give

Corollary 4.2. *G lifts if and only if all of the M_i's are of type 1.* □

Proof of 4.1. We can separate all cyclic Dieudonné modules into two distinct cases:

Case 1: *M is constructed by a series of cyclic modules killed by p, at least one of which is type 2.* Pick i so that M_i is a type 2 module.

We shall show that if M lifts, then so must $p^i M/p^{i+1}M$. If M lifts, then there is an L so that (M, L) is a finite Honda system. We shall denote the corresponding $W(k)$-group scheme by $\tilde{G}$. Define the morphism $[p^i]$ of p-groups over $W(k)$ by $[p^i]_A(g) = g + g + \cdots + g$ (p^i times) for A a $W(k)$-algebra and $g \in G(A)$. Since the category of finite p-groups is abelian, $[p^i]$ induces the following short exact sequence of finite p-groups over $W(k)$

$$0 \longrightarrow [p^i]\tilde{G} \longrightarrow \tilde{G} \longrightarrow \tilde{G}/[p^i]\tilde{G} \longrightarrow 0.$$

This corresponds to a short exact sequence of finite Honda systems

$$0 \longrightarrow (p^i M, L') \longrightarrow (M, L) \longrightarrow (M/p^i M, L'') \longrightarrow 0$$

for some choice of $W(k)$-modules L', L''. Applying a base change to group schemes from $W(k)$ to k commutes with $[p^i]$, and under this base change (M, L) (resp. $(p^i M, L')$, $(M/p^i M, L'')$) corresponds to M (resp. $p^i M$, $M/p^i M$). Thus we have finite Honda systems for $p^i M$ and $M/p^i M$, hence they correspond to liftable k-group schemes.

If we replace M with $p^i M$ and let $i = 1$, we get that $p^i M/p^{i+1}M$ corresponds to a liftable group scheme. As M_i is of type 2, it does not lift, hence neither does M.

Case 2: *M is constructed by a series of type 1 modules killed by p.* We will construct a specific finite Honda system for M after first setting down some notation.

Let $x = 1_M$. Since M is constructed of type 1's, we have

$$M_i = E/E(F^{n_i} - \eta_i V^{m_i}, p),$$

$\eta_i \in k^\times$, $0 \le i \le h-1$ with $m_{h-1} \le m_{h-2} \le m_{h-3} \le \cdots \le m_0 = m$. For notational convenience, we shall also define $m_h = 0$. Let $\Delta m_i = m_i - m_{i+1}$. Now, for all i, $(p^i \eta_i V^{m_i} - p^i F^{n_i})x \equiv 0 \pmod{p^{i+1}}$, hence $p^i(\eta_i V^{m_i} - F^{n_i} - p\alpha_i)x = 0$ for some $\alpha_i \in E$. Define $f_i = V^{m_i} - \eta_i^{-1}(F^{n_i} + p\alpha_i)$, $0 \le i \le h-1$, and $f_h = 1$. Thus $p^i f_i = 0$ but $p^{i-1} f_i \ne 0$, and the elements $p^{i-1}V^j f_i$ for $0 \le j \le m_i - 1$ form a k-basis for M_{i-1}/FM_{i-1}.

Let L be the $W(k)$-submodule consisting of all elements of the form

$$\sum_{i=0}^{h-1} \sum_{j=1}^{\Delta m_{h-i-1}} a_{ij} V^{j-1} f_{h-i} x, \qquad a_{ij} \in W(k),\ p^{h-i+1} \text{ not dividing } a_{ij} \text{ for all } j.$$

We shall show that (M, L) is a finite Honda system. We shall use the term V*-degree* on a monomial to give its power of V modulo p. It is easy to check that the V-degree of the term $a_{ij}V^{j-1}f_{h-i}x$ is $j-1+m_{h-i}$. We claim that each term in this double sum has one power of V less than the next term (when we order in the obvious way): clearly this is true for the terms with $j < \Delta m_{h-i-1}$. If $j = \Delta m_{h-i-1}$, then this term has V-degree

$$\Delta m_{h-i-1} - 1 + m_{h-i} = m_{h-i-1} - m_{h-i} - 1 + m_{h-i} = m_{h-i-1} - 1.$$

Let s be the smallest positive integer such that $\Delta m_{h-s} > 0$. Then the following term is $a_{i+s,0}V^0 f_{h-i-s}$, which has V-degree $m_{h-i-s} = m_{h-i-1}$, and the claim is proved.

The smallest V-degree is 0 and the largest is $m_0 - 1 = m-1$. Thus L is generated as a $W(k)$-module by

$$\{(1 - Fe_0)x, (V - Fe_1)x, (V^2 - Fe_2)x, \ldots, (V^{m-1} - Fe_{m-1})x\}$$

for the appropriate choice of e_i. Since $M/FM = \overline{M}/F\overline{M}$, where $\overline{M} = M/pM$, it follows from Corollary 3.2 that $M/FM = L/pL$.

To show $\ker V \cap L = 0$, suppose there exists a nonzero $\lambda \in L$ with $V\lambda = 0$. Write

$$\lambda = \sum_{i=0}^{h-1} \sum_{j=1}^{\Delta m_{h-i-1}} a_{ij} V^{j-1} f_{h-i} x.$$

Then

$$V\lambda = \sum_{i=0}^{h-1} \sum_{j=1}^{\Delta m_{h-i-1}} b_{ij} V^{j} f_{h-i} x = 0,$$

where $b_{ij} = a_{ij}^{\sigma^{-1}}$. Since the b_{ij} are not all zero, we can find a nonnegative integer ℓ so that $p^\ell | b_{ij}$ for all i, j and is the largest ℓ with this property. Of course, $\ell \le h-1$, by the definition of the a_{ij}'s. Writing $b_{ij} = p^\ell c_{ij}$ gives us

$$V\lambda = \sum_{i=0}^{h-1} \sum_{j=1}^{\Delta m_{h-i-1}} c_{ij} V^{j} p^\ell f_{h-i} x = 0.$$

If $i \ge h - \ell$ we have seen that $V^{j-1}p^\ell f_{h-i}x = 0$, so we may write this sum as

$$V\lambda = \sum_{i=0}^{h-\ell-1} \sum_{j=1}^{\Delta m_{h-i-1}} c_{ij} V^{j} p^\ell f_{h-i} x = 0.$$

This is an element of $p^\ell M$, so we may project it onto M_ℓ and we obtain

$$\overline{\lambda} = \sum_{i=0}^{h-\ell-1} \sum_{j=1}^{\Delta m_{h-i-1}} \overline{c_{ij}} V^j f_{h-i} z = 0$$

where $z = 1_{M_\ell}$. The highest V-degree in $\overline{\lambda}$ is the V-degree of $\overline{c_{h-\ell-1,\Delta m_\ell}} V^{\Delta m_\ell} f_{\ell+1}$, which is m_ℓ. Since the collection of all $V^j f_{h-i} z$'s are k-linearly independent, $0 \leq i \leq h-\ell-1$, $1 \leq j \leq \Delta m_{h-i-1}$ (all of the terms have a different V-degree and $V^m M_\ell \neq 0$), and it is clear that $\overline{c_{ij}} = 0$ for all i and j, i.e., p divides c_{ij}, contradicting our choice of ℓ. Thus $\lambda \notin \ker V$, and the theorem is proved. $\square$

Remark 1. While the statement of the theorem is quite simple, the constructed L is rather complicated. One might hope that the $W(k)$-submodule L_0 generated by $\{x, Vx, V^2x, \ldots, V^{m-1}x\}$ might also lead to a finite Honda system. It can be shown that (M, L_0) is a finite Honda system when all of the M_i are isomorphic, however the following example shows that this result does not hold for more general M.

Example 4.3. Let $M = E/E(F^3 - V^3, pF - pV, p^2)$. Here L_0 is generated by $\{x, Vx, V^2x\}$. While it is clear that $M/FM = L_0/pL_0$, we have that $pVx \in L_0 \cap \ker V$.

However, since $M/pM = E/E(F^3 - V^3, p)$ is of type 1, we can construct a lift. By the construction given in the theorem, L is generated by $\{x, (V-F)x, (V^2-p)x\}$. Notice how the problem with L_0 is cleared up with L: instead of pVx, we now have $p(V-F)x$, which is already zero. In fact, L is constructed by starting with L_0 and adjusting terms in such a way so that anything that could be in the kernel of V is already zero. It is because of this that we believe that this L is the "simplest" general formula for constructing a lift.

References

[DG] M. Demazure and P. Gabriel, *Groupes Algebriques, Tome* I, North Holland, Amsterdam, 1970.

[F1] J. M. Fontaine, *Sur la construction du module de Dieudonné d'un groupe formel*, C. R. Acad. Sci. Paris **280**, 1975, 1273–1276.

[F2] J. M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C. R. Acad. Sci. Paris **280**, 1975, 1423–1425.

[K] A. Koch, *Witt subgroups and cyclic Dieudonné modules killed by p*, preprint.

[M] W. Messing, *The Crystals Associated to Barsotti-Tate Groups, With Applications to Abelian Schemes*, Lecture Notes in Mathematics, no. 264, Springer-Verlag, Berlin, 1972.

[O] F. Oort, *Embeddings of finite group schemes into abelian schemes*, Mimeographed notes, Bowdoin College, 1967.

[OM] F. Oort and D. Mumford, *Deformations and liftings of finite commutative group schemes*, Inv. Math. **5** 1968, 317–334

[R] J. Roubaud, *Schémas en Groupes Finis Sur un Anneau de Valuation Discrète et Systèmes de Honda Associés*, Publications Mathematiques d'Orsay, no. 91-01, Université de Paris-Sud, Department de Mathematique, Orsay, 1991, MR 92m:14059.

[TO] J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. Ecole Norm. Sup. **3** 1970, 1–21.

[W] W. Waterhouse, *Introduction to Affine Group Schemes*, Springer-Verlag, Berlin, 1979, MR 82e:14003.

Department of Mathematics, Hope College, P.O. Box 9000, Holland, MI 49424-9000

Current address: Department of Mathematics, St. Edward's University, 3001 S. Congress Ave., Austin, TX 78704-6489

alank@admin.stedwards.edu http://www.cs.stedwards.edu/~koch/

This paper is available via http://nyjm.albany.edu:8000/j/1998/4-9.html.