CONSTRUCTING SEQUENCES OF DIVIDED POWERS

KENNETH NEWMAN

ABSTRACT. In my Sequences of divided powers in irreducible, cocommutative Hopf algebras, I demonstrated the existence of extensions of sequences of divided powers over arbitrary fields, if certain coheight conditions are met. Here, I show that if the characteristic of the field does not divide $n$, every sequence of divided powers of length $n - 1$, in a cocommutative Hopf algebra, has an extension that can be written as a polynomial in the previous terms. (An algorithm for finding these polynomials is given, together with a list of some of them.) Furthermore, I show that if one uses this method successively for constructing a sequence of divided powers over a primitive, the only obstructions will occur at powers of the characteristic of the field.

Some of the basic definitions of this paper are the following:

1. If $H$ is a Hopf algebra and $0 \neq g \in H$, then $g$ is a grouplike if $\Delta g = g \otimes g$.
2. If $h \in H$, then $h$ is a primitive if $\Delta h = h \otimes 1 + 1 \otimes h$.
3. A Hopf algebra will be called irreducible if every nontrivial subcoalgebra contains a fixed, nontrivial subcoalgebra, i.e., if $H$ is irreducible, the identity is the unique grouplike.
4. An irreducible Hopf algebra will be called graded, if there exists a set of subspaces $\{H_i\}_{i=0}^{\infty}$ such that
   a) $H = \bigoplus_{i=0}^{\infty} H_i$;
   b) $H_0 = 1 \cdot k$;
   c) $\Delta H_i \subset \bigoplus_{j=0}^{i} H_j \otimes H_{i-j}$;
   d) $H_i \cdot H_j \subset H_{i+j}$.
5. A sequence of divided powers $0x = 1, 1x, 2x, \ldots, nx$ is a set of elements in a cocommutative, irreducible Hopf algebra such that $\Delta^t x = \sum_{t=0}^{\infty} t^t x \otimes t^{-t} x$, for all $0 \leq t \leq n$. 
(6) \( n+1 \) will be called an extension of the sequences of divided powers 
\( 0x = 1, 1x, 2x, \ldots, nx, if \ 0x = 1, 1x, 2x, \ldots, nx, n+1x \) is also a sequence of divided powers.

**FACT.** An irreducible cocommutative bialgebra is a Hopf algebra.

**Proof.** Proposition 9.2.5, p. 196 of [3].

**NOTATION.** Throughout the remainder of this paper, \( H \) will be an irreducible, cocommutative, commutative Hopf algebra over a field \( k \). \( H \) will have argumentation \( \epsilon \), diagonalization \( \Delta \), and identity \( 1 \). All tensor products will be over \( k \).

Let \( J_n \equiv k[X_1, X_2, \ldots, X_n] \) and make it into a graded Hopf algebra via \( \Delta X_i = \sum_{j=0}^i X_j \otimes X_{i-j} \) (where \( X_0 \equiv 1 \)), and \( \epsilon(X_j) = 0 \) for \( 1 \leq i \leq n \), and \( \deg X_i = i \) for \( 0 \leq i \leq n \).

Note that \( J_n \) is an irreducible, cocommutative, commutative Hopf algebra with \( 1, X_1, X_2, \ldots, X_n \) forming a sequence of divided powers.

**Definition.** Let \( M = \prod X_i^{t_i} \) be a monomial in \( J_n \). The largest \( i \) such that \( X_i \neq 0 \) will be called the index of \( M \).

**Lemma 1.** In \( J_n \), the only monomial with index \( \leq r \) that contains \( T = (\prod_{i=1}^{r-1} X_i^{t_i}) \otimes X_r^{t_r}, t_r > 0 \), in its diagonalization with a nonzero coefficient is \( M = \prod X_i^{t_i} \).

**Proof.** It is clear that no monomial with index less than \( r \) can contain \( T \) in its diagonalization. Assume \( N = \prod_{i=1}^{r-1} X_i^{t_i} \) contains \( T \) in its diagonalization. Now \( \Delta N = \prod_{i=1}^{r-1} (\sum_{j=0}^i X_j \otimes X_{i-j})^{u_i} \) (where \( X_0 \equiv 1 \)) and, therefore, the only term in the expansion of \( \Delta N \) with only \( X_i \)'s on the right-hand side and no \( X_i \)'s on the left-hand side is \( (\prod_{i=1}^{r-1} X_i^{t_i}) \otimes X_r^{t_r} \). Therefore \( u_i = t_i, i = 1, 2, \ldots, r \), and \( N = M \).

**Theorem 2.** In \( J_{n-1} \) over \( Q \) (the rationals), the sequence of divided powers \( 1, X_1, X_2, \ldots, X_{n-1} \) can be extended uniquely by a homogeneous polynomial, \( P_n(X) \), of degree \( n \). The coefficients of this polynomial will be in \( Z[1/n] \). In fact, if \( M \) is a monomial in \( P_n(X) \) with index \( r \), its coefficient will be in \( Z[1/p_1 p_2 \ldots p_s] \) where the \( p_i \) are the prime factors of \( n \) such that \( n/r \geq p_i \). In particular, if \( r \) is larger than the largest nontrivial divisor of \( n \), its coefficient will be in \( Z \).

**Proof.** By Corollary 13.0.3, p. 278 of [3], any irreducible, cocommutative Hopf algebra \( H \) over a field of characteristic 0 is generated as an algebra by its primitives. Assume \( H \) is graded. Then each homogeneous component of each primitive is a primitive and we can say that \( H \) is generated by homogeneous primitives. Now consider \( J_n \). It is generated by homogeneous primitives and, therefore, there must exist a homogeneous primitive containing \( X_n \) as one of its terms. This primitive must, perforce, be of the form: \( X_n = P_n(X_1, X_2, \ldots, X_{n-1}) \). Since \( X_n \) is an extension of
1, X₁, X₂, · · · , Xₙ₋₁, and Xₙ - Pₙ(X₁, X₂, · · · , Xₙ₋₁) is a primitive if it follows that Pₙ(X₁, X₂, · · · , Xₙ₋₁) will be the desired extension in Jₙ₋₁.

We now investigate the coefficients of Pₙ(X). First, we show that the coefficient of Xⁱⁿⁱ in Pₙ(X) (for i | n) will be (-1)^n/i(i/n).

Since Pₙ(X) is an nth divided power of 1, X₁, X₂, · · · , Xₙ₋₁, ΔPₙ(X) contains the term Xᵢ ⊗ Xₙ₋ᵢ. A little thought will make it evident that the factors of a monomial containing Xᵢ ⊗ Xₙ₋ᵢ in its diagonalization must be Xᵢ and Xₙ₋ᵢ, i.e., the unique monomial containing Xᵢ ⊗ Xₙ₋ᵢ in its diagonalization is XᵢXₙ₋ᵢ. Therefore, the coefficient of XᵢXₙ₋ᵢ is 1.

Now, the diagonalization of XᵢXₙ₋ᵢ contains the term Xᵢ² ⊗ Xₙ₋₂ᵢ. Since this term does not appear in ΔPₙ(X), it must be cancelled by terms in the diagonalization of other monomials in Pₙ(X). Again, a little thought will show that for a monomial to contain Xᵢ² ⊗ Xₙ₋₂ᵢ in its diagonalization, it must contain as factors, combinations of Xᵢ, Xₙ₋₂ᵢ and Xₙ₋ᵢ. By checking all the possibilities, one can see that the only monomial other than XᵢXₙ₋ᵢ that contains Xᵢ² ⊗ Xₙ₋₂ᵢ in its diagonalization is XᵢXₙ₋₂ᵢ. Therefore, the coefficient of Xᵢ²Xₙ₋₂ᵢ is -1. Now, Δ(-Xᵢ²Xₙ₋₂ᵢ) contains the term -Xᵢ³ ⊗ Xₙ₋₃ᵢ and in a similar way to the above, we can show that the coefficient of XᵢXₙ₋₃ᵢ is +1.

Continuing in this manner, we find that the coefficient of Xⁿ/i₋₂X₂ᵢ is (-1)^(n/i-1). Since its diagonalization contains the term Xᵢⁿ/i₋₁ ⊗ Xᵢ, the coefficient of Xᵢⁿ/i (which contains the term (n/i)Xᵢⁿ/i₋₁ ⊗ Xᵢ in its diagonalization) must be (-1)^n/i(i/n).

To complete the proof, we show that the coefficient in Pₙ(X) of M = ∏ᵢ₌₁⁻ʳ Xᵢᵗ (tᵢ ≠ 0 and some tᵢ ≠ 0, 1 ≤ i ≤ r), a monomial of degree n, is an integral combination of the coefficients in Pₙ(X) of larger monomials. (We say one monomial is “larger” than another if its index is larger.) We will do this by (1) finding a term in ΔM, other than M ⊗ 1 or 1 ⊗ M, with coefficient one that occurs elsewhere only in the diagonalization of larger monomials. (2) Since the coefficient of every term in ΔPₙ(X) - 1 ⊗ Pₙ(X) - Pₙ(X) ⊗ 1 is either zero or one, (3) descending induction (on the index of the monomial) will complete the proof.

(1) A term in ΔM is T = (∏ᵢ₌₁ʳ Xᵢᵗᵢ) ⊗ Xᵢᵣ and one can check that it has coefficient one. By Lemma 1, every monomial other than M, that contains T in its diagonalization, must be larger than M.

(2) So let {Mᵢ}ᵢ∈I be the set of monomials larger than M in Jₙ₋₁, let bᵢ be the coefficient of T in ΔMᵢ, and let cᵢ be the coefficient of Mᵢ in Pₙ(X). Then e = c + ∑ᵢ∈I cᵢbᵢ where e is the coefficient of T in ΔPₙ(X) (either zero or one) and c is the coefficient of M in Pₙ(X).

(3) Now all the cᵢ's are in Z[1/p₁p₂ · · · pᵣ] where the pᵢ's are the prime factors of n such that n/r ⩾ pᵢ. (If Mᵢ is of the form Xᵢⁿ/i we proved this statement above, and if Mᵢ is not of this form it is true by the induction
hypothesis. Note that we showed, en passant, that the coefficient of the largest monomial, $X_{n-1}X_1$, is one.) Therefore, since all the $b_i$'s are integers, it follows that $c$ is in $\mathbb{Z}[1/p_1p_2 \cdots p_s]$.

Uniqueness is clear, since we have found the unique possible coefficient of each monomial in $P_n(X)$. Q.E.D.

**Remark.** We give here an algorithm to find the $P_n$'s as defined in the previous theorem. The algorithm is derived from methods used in the proof of the theorem and is not specifically proved.

In $P_n$:
(a) the coefficient of $X^{n-i}_i$ is $(-1)^{n-i}(i/n)$ ($1 \leq i < n$ and $i | n$);
(b) the coefficient of $X_iX_{n-i}$ is 1 ($1 \leq i < n/2$);
(c) the coefficient of $M = \prod_{i=1}^r X_{n-i}^i$ ($t_r \neq 0$, $M$ not of the form (a) or (b)) will be minus the sum of the coefficients of monomials of the form: $\prod_{i=1}^r X_{n-i}^i$ with $u_r \neq 0$, $2r > s > r$, $u_i + u_{r+i} = t_i$ ($1 \leq i < r$), and $\sum_{i=1}^r u_i = t_r$.

In Table I, I have listed the first seven polynomials (of degree 2–8). It is interesting to empirically observe (though I cannot explain it), that the coefficient of a term is positive, if the sum of its exponents is even and vice versa. (I have found this to be true for all the $P_n$'s I have computed, up to $n = 20$.)

**Table 1**

The polynomial of degree $n$ ($n = 2, \cdots , 8$) which will extend the sequence of divided powers $1, X_1, X_2, \cdots , X_{n-1}$ in $J_{n-1}$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$P_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$\frac{1}{2} X_1^2$</td>
</tr>
<tr>
<td>3</td>
<td>$X_2X_1 - \frac{1}{2} X_1^3$</td>
</tr>
<tr>
<td>4</td>
<td>$X_3X_1 + \frac{1}{2} X_2^2 - X_2X_1^2 + \frac{1}{3} X_4^3$</td>
</tr>
<tr>
<td>5</td>
<td>$X_4X_1 + X_3X_2 - X_3X_1^2 - \frac{1}{3} X_2X_1 - \frac{1}{3} X_5^3$</td>
</tr>
</tbody>
</table>
| 6    | $X_5X_1 + X_4X_2 - X_4X_1^2 + + X_3X_1^3 + \frac{1}{2} X_2^2 - 2X_3X_2X_1 + X_3X_1^3$  
  |                                      | $- \frac{1}{3} X_2^3 + 1\frac{1}{2} X_2X_1^2 - X_2X_1^3 + \frac{1}{3} X_4^3$ |
| 7    | $X_6X_1 + X_5X_2 - X_5X_1^2 + X_4X_2 - 2X_4X_2X_1 + X_4X_1^3$          
  |                                      | $- X_3X_1^3 - X_3X_2^2 + 3X_3X_2X_1^2 - X_5X_1^4$  
  |                                      | $+ X_2^3X_1 - 2X_2X_1^3 + X_2X_1^5 + \frac{1}{3} X_7^3$ |
| 8    | $X_7X_1 + X_6X_2 - X_6X_1^2 + X_5X_3$                                  
  |                                      | $- 2X_5X_2X_1 + X_5X_1^3 + \frac{1}{3} X_8^3 - 2X_4X_3X_1$  
  |                                      | $- X_4X_2^3 + 3X_4X_2X_1^2 - X_4X_1^4 - X_5^3X_2$  
  |                                      | $+ 1\frac{1}{2} X_5^3X_1^2 + 3X_3X_2X_1 - 4X_3X_2X_3^3$  
  |                                      | $+ X_3X_1^5 + \frac{1}{3} X_8^2 - 2X_2^3X_1^2 + 2\frac{1}{2} X_2X_1^4$  
  |                                      | $- X_2X_1^6 + \frac{1}{3} X_8^3$. |
Corollary 3. Let char $k = a$ (a either 0 or positive). If $0^x = 1, 1^x, \cdots, n^{-1}x$ is a sequence of divided powers in $H$, then the sequence can be extended by a polynomial in $1^x, 2^x, \cdots, n^{-1}x$ if $a \nmid n$ or if $a = 0$.

Proof. Consider $J_{n-1}$ over $k$. Define a Hopf algebra map $\chi$ between $J_{n-1}$ and $H$ via $X_i \rightarrow i^x$. By the theorem the coefficients of $P_n(X)$ are in $\mathbb{Z}[1/n]$ and therefore $P_n(X)$ can be written in $J_{n-1}$. The image of $P_n(X)$ under $\chi$ will be the desired extension of $1, 1^x, \cdots, n^{-1}x$. Q.E.D.

Note that if $a > 0$, the coheight (in the sense of [1]) of the extension will be the same as the coheight of $n^x$.

Corollary 4. Assume char $k = p > 0$. If $0^x = 1, 1^x, \cdots, m^x$ and $0^y = 1, 1^y, \cdots, n^y$ are 2 sequences of divided powers such that $i^x = i^y$, $0 \leq i \leq t$, and if $0^x, 1^x, \cdots, m^x$ can be extended to $i^y$, then $0^y, 1^y, \cdots, n^y$ can be extended to $i^y$ by polynomials in $1^x, 2^x, \cdots, i^{yp}, 1^y, 2^y, \cdots, n^y$.

Proof. Assume inductively that we have extended $0^y, 1^y, \cdots, n^{-1}y$ to $0^y, 1^y, \cdots, u^{-1}y$, $n < u \leq tp$, using polynomials in $1^x, 2^x, \cdots, i^{yp}, 1^y, 2^y, \cdots, n^y$. If $p \nmid u$, then we can extend again using Corollary 3. So assume $u = rp$, $r \leq t$. Let $J = k[X_1, X_2, \cdots, X_{rp}, Y_{t+1}, Y_{t+2}, \cdots, Y_{r-1}]$ where $\epsilon(X_i) = \epsilon(Y_i) = 0$ ($i \geq 1$), $\Delta X_i = \sum_{j=1}^i X_j \otimes X_{i-j}$, and $\Delta Y_i = \sum_{j=0}^i Y_j \otimes Y_{i-j}$ (letting $Y_0 = X_0 = 1$ and $Y_i = X_i$ if $i \leq t$). Consider $P_{rp}(Y) - P_{rp}(X) + X_{rp}$. Since $Y_i = X_i$ ($i \leq t$) all monomials have index greater than $t$ and $t \geq r$. According to the theorem, the coefficients of such monomials in $P_{rp}(X)$ are in $\mathbb{Z}[1/p_1p_2 \cdots p_r]$ where the $p_i$'s are the prime factors of $u$ less than $p$. Therefore, we can write $P_{rp}(Y) - P_{rp}(X) + X_{rp}$ in $J$. Since $X_{rp} - P_{rp}(X)$ is a primitive, $P_{rp}(Y) - P_{rp}(X) + X_{rp}$ will be an extension of $1, Y_1, Y_2, \cdots, Y_{r-1}$ in $J$. Now map $J \rightarrow H$ via $X_i \rightarrow i^x$ and $Y_i \rightarrow i^y$. The image of $P_{rp}(Y) - P_{rp}(X) + X_{rp}$ will be the desired extension. Q.E.D.

We have shown that if $H$ is an irreducible, cocommutative, commutative Hopf algebra over a field of characteristic $p > 0$, an extension to any sequence of divided powers of length $n - 1$ can be constructed if $p \nmid n$. If $p \mid n$, this is not, in general, true. However, if we start with a primitive, use the $P_n$'s of Theorem 2 to construct a $p - 1$ length sequence, and if, in some manner, we can find a $p^i$ divided power, we can then use the $P_n$'s to construct a $p^i - 1$ length sequence. Further, if we can now find a $p^2$ divided power, the $P_n$'s allow us to construct a $p^3 - 1$ sequence. This process may be continued indefinitely. In other words, obstructions can only arise at $p^n$th divided powers, not at every $np$ divided power. This is the import of Theorem 7 and Corollary 8, below. First, however, we need the following:
Lemma 5. Let $n$ be any positive integer greater than one, and $p$ any prime. Then there exists $a$, $1 \leq a < n$, such that $p^{a} \not| \binom{n}{a}$, if $n$ is not a power of $p$. If $n$ is a power of $p$, there exists $a$, $1 \leq a < n$, such that $p^{a} \not| \binom{n}{a}$.

The proof is trivial.

Definition 6. (a) Let $p$ be a prime. If $n$ is a power of $p$, $P_{n,p} = X_{n}$. If $n$ is not a power of $p$, define $P_{n,p}$ inductively by substituting $P_{s,p}$ for $X_{i}$, $i = 1, 2, \ldots, n-1$, in $P_{n,p}$.

(b) Make $k[X_{1}, X_{p}, \ldots, X_{pm}]$ into a graded Hopf algebra via $\Delta X_{pi} = \sum_{j=0}^{p} P_{j,p} \otimes P_{p-i,p}$ (with $P_{0,p} \equiv 1$), $\epsilon(X_{pi}) = 0$ and deg $X_{pi} = p^{i}$.

Note that $1; P_{1,p}; P_{2,p}; \ldots$ is a sequence of divided powers and that $P_{i,p}$ is homogeneous of degree $i$. The $k[X_{1}, X_{p}, \ldots, X_{pm}]$ are isomorphic to the familiar Witt Hopf algebras. See Theorem 2.23, p. 70 of [2].

Theorem 7. For any $n$ and any prime $p$, the coefficients of $P_{n,p}$ as a polynomial in $X_{1}, X_{p}, \ldots, X_{pm}$ ($p^{m} \leq n < p^{m+1}$) are in $\mathbb{Z} - \mathbb{Z}[1/2, 1/3, 1/5, \ldots, 1/p, \ldots]$.

Proof. Assume inductively that the theorem is true for $P_{i,p}$, $i < n$, and that $n$ is not a power of $p$ (otherwise, the theorem is clear). Let $\chi$ be the natural map:

$Z_{p}[X_{1}, X_{p}, \ldots, X_{pm}] \rightarrow k[X_{1}, X_{p}, \ldots, X_{pm}]$

where $k$ is any field of characteristic $p$. Since we have assumed that the $P_{i,p}$'s ($i < n$) are in $Z_{p}[X]$, we can use them to define a sequence of divided powers, $1, \chi(P_{1,p}), \chi(P_{2,p}), \ldots, \chi(P_{n-1,p})$ in $k[X]$. By Theorem 2 and Sublemma 3 of [1], $1, \chi(P_{1,p}), \chi(P_{2,p}), \ldots, \chi(P_{n-1,p})$ has an extension in $k[X]$. Call the homogeneous component of degree $n$ of that extension (which is also an extension) $E$. We will show that $\chi(P_{n,p}) = E$ (and in the process show that $\chi$ is well defined on $P_{n,p}$, i.e., the coefficients of $P_{n,p}$ are in $Z_{p}$).

Let $M \equiv \prod_{i=1}^{r} X_{pi}$ be a monomial of degree $n$ and index $p^{r}$. Assume its coefficient is $c$ in $P_{n,p}$ and $c'$ in $E$. We want to show that $\chi(c) = c'$. Assume that this statement is true for all monomials larger than $M$. (This set may be vacuous.) If $M$ is of the form $X_{p}^{t}$, let $T = X_{p}^{t} \otimes X_{p}^{t}$, where $\alpha$ is the integer found in Lemma 5 for $n = t_{p}$. If $M$ is not of this form, let $T \equiv (\prod_{i=1}^{r} X_{pi}^{s}) \otimes X_{p}^{s}$. Among the monomials of degree $n$, $T$ will occur only in the diagonalization of $M$ or terms of larger degree. (If $T$ is of the first form, the statement is clear. Otherwise, use a slight modification of Lemma 1.) Remember $\Delta P_{n,p} = P_{n,p} \otimes 1 + 1 \otimes P_{n,p} + \sum_{i=1}^{n-1} P_{i,p} \otimes P_{n-i,p}$ and $\Delta E = E \otimes 1 + 1 \otimes E + \sum_{i=1}^{n-1} \chi(P_{i,p}) \otimes \chi(P_{n-i,p})$. Therefore, $e$, the coefficient of $T$ in $\Delta P_{n,p}$ is in $Z_{p}$, and $\chi(e)$ is the coefficient of $T$ in $\Delta E$.

Now let $\{M_{i}\}_{i \in I}$ be the set of monomials of degree $n$ larger than $M$. Let
the coefficient of $M_i$ in $P_n,\rho$ be $c_i$, and let the coefficient of $T$ in $\Delta M_i$ be $b_i$. Then, $e = cb + \sum_{i \in I} c_i b_i$, where we have let $b$ be the coefficient of $T$ in $\Delta M$. It is clear that each $b_i \in \mathbb{Z}$. Also by the second induction hypothesis, we know that each $c_i \in \mathbb{Z}_p$ and that if $c'_i$ is the coefficient of $M_i$ in $E$, $\chi(c_i) = c'_i$. Therefore $c b \in \mathbb{Z}_p$ and $\chi(c b) = c' b$. If $M = X^{t_r}_{p^r}$ and $t_r$ is not a power of $p$, then $b = \binom{t_r}{2}$ which we assumed not to be divisible by $p$. Therefore $b \in \mathbb{Z}_p$, $c b \in \mathbb{Z}_p \Rightarrow c \in \mathbb{Z}_p$ and $\chi(c) = c'$. If $M = X^{t_r}_{p^r}$, $t_r$ a power of $p$, then $c b \equiv 0 \pmod{p}$. But we assumed that $b = \binom{t_r}{2}$ was not divisible by $p^a$. Therefore, the denominator of $c$ is not a multiple of $p$, i.e., $c \in \mathbb{Z}_p$ and $\chi(c) = c'$. And lastly, if $M$ is not of the form $X^{t_r}_{p^r}$, $b = 1$ and we are done.

**Corollary 8.** If $x$ is a primitive in $H$, then a sequence of divided power can be constructed over $x$ using the polynomials defined in Definition 6(a). The obstructions can only occur at powers of $p$.

**Proof.** Similar to Corollary 3, using Theorem 7 instead of Theorem 2.

**Bibliography**


**McGill University, Montreal, Quebec, Canada**

Current address: University of Illinois at Chicago Circle, Chicago, Illinois 60680