

Generalized Dickson Invariants

by

Dan Arnon

B.Sc. in Mathematics, Hebrew University in Jerusalem (1985)

M.Sc. in Mathematics, Hebrew University in Jerusalem (1988)

Submitted to the
Department of Mathematics
in partial fulfillment of the requirements
for the degree of

Doctor of Philosophy

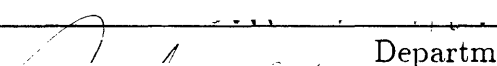
at the

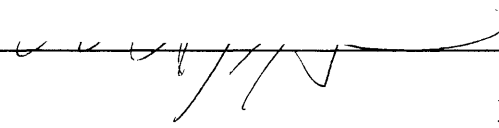
Massachusetts Institute of Technology

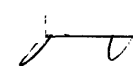
May 1994

© 1994 Dan Arnon. All rights reserved.

The author hereby grants to MIT permission to reproduce
and to distribute publicly paper and electronic copies
of this thesis document in whole or in part.

Signature of Author  Department of Mathematics
March 1, 1994

Certified by  Michael J. Hopkins
Professor of Mathematics
Thesis Supervisor

Accepted by  David A. Vogan, Chairman
Departmental Graduate Committee
Department of Mathematics

Science
MASSACHUSETTS INSTITUTE
OF TECHNOLOGY

AUG 11 1994

LIBRARIES

Generalized Dickson Invariants

by

Dan Arnon

Abstract

The action of the $GL(n, 2)$ on an n -dimensional vector space induces an action on the symmetric algebra over this vector space. The invariants of this action were computed by L.E. Dickson (see [Dk]). The Steenrod Algebra acts on the Dickson Invariants. This thesis is an attempt to shed light on this action by embedding the Dickson Algebra in a larger algebra, namely the invariants of a *root algebra* which is an extension of the polynomial algebra where the Frobenius homomorphism $x \rightarrow x^2$ is invertible. The generalized Dickson Algebras have a left action of a generalized Steenrod Algebra. Working in this expanded context not only simplifies the analysis of the action of the Steenrod Algebra but also sheds light on the structure of the Dickson Algebras themselves. In particular one can form an inverse limit of these algebras which is itself an algebra of invariants. Most of this thesis is dedicated to the study of this limit algebra. Being an inverse limit this algebra is complete with respect to a metric. It turns out that its dual algebra can be identified, through a certain pairing, with a subalgebra carrying a finer topology than the one induced by the metric. The finer structure comes from a norm with values in the positive integers. This norm induces a filtration on the dual algebra which is dual to the filtration of the primal algebra induced by the inverse limit. In particular there is a direct correlation, through the pairing, between the Dickson Algebra on k variables and the subalgebra of elements of norm k in the dual algebra. The pairing induces a Hopf Algebra structure on both the primal and the dual algebra and a right action of the generalized Steenrod algebra on both. Those new structures are studied in detail.

The basic ingredient needed for the investigation of the structure of the infinite Dickson Algebra and its dual is a sequence of polynomials recently defined by Frank Peterson. These polynomials turn out to form a cyclic module over the Steenrod Algebra and are the basic building blocks for all the constructions in this work.

Thesis Supervisor: Michael J. Hopkins

Title: Professor of Mathematics

Acknowledgements

I wish to thank my advisor Professor Mike Hopkins for his guidance and support and for giving me a glimpse into the far recesses of Mathematics.

I would like to express my appreciation for Professor Haynes Miller for the many hours of conversation, helpful ideas and keen interest in my work. It is also a pleasure to express my gratitude to Professor Frank Peterson whose ideas gave rise to this thesis. He has been a constant source of encouragement for me throughout my stay at MIT.

Special thanks go to Professor Dan Kan, who is both a teacher and a friend. Our early morning conversations during my first term at MIT helped me get through that difficult time.

Of the many people who enriched my stay at MIT I would like to mention two who were especially close both as friends and colleagues. Brooke Shipley for many enjoyable hours of mathematical discussion and for her friendship. Phil Hirschhorn for helping me through the rocky terrain of simplicial topology and especially the Yellow Monster which he managed to tame somehow.

To Phyllis Ruby thanks for her seemingly boundless resourcefulness. Without her this thesis and probably the rest of the math department would not be here today.

Thanks to the Alfred P. Sloan Foundation for their financial support during my last year at MIT.

Last, but not least, many thanks to my longtime companion, Tao Kai, for his love and support.

In memory of my dear grandfather
Dr. Noach Benninga

1. THE COMPLETE STEENROD ALGEBRA

Definition 1.1. A $\mathbb{Z}[\frac{1}{2}]$ -graded algebra A (resp. ring, module etc.) is an algebra of the form $A = \bigoplus_{n \in \mathbb{Z}[\frac{1}{2}]} A_n$ where multiplication is defined by maps $A_m \otimes A_n \rightarrow A_{m+n}$. The *doubling* of a $\mathbb{Z}[\frac{1}{2}]$ -graded object M , denoted $2M$, is a $\mathbb{Z}[\frac{1}{2}]$ -graded object with $(2M)_k = M_{\frac{1}{2}k}$. More generally one can define an object $2^k M$ for all $k \in \mathbb{Z}$.

Definition 1.2. The *halving homomorphism* on the Steenrod Algebra is the surjective map $D : \mathcal{A}_2 \rightarrow \mathcal{A}_2$ induced by

$$\begin{aligned} D(\text{Sq}^{2^n}) &= \text{Sq}^n \\ D(\text{Sq}^{2^{n+1}}) &= 0 \end{aligned}$$

The halving homomorphism is an algebra homomorphism, but it is not degree preserving. However, viewing \mathcal{A}_2 as a $\mathbb{Z}[\frac{1}{2}]$ -graded algebra which is zero in fractional degrees, one gets a degree preserving homomorphism $D : \frac{1}{2}\mathcal{A}_2 \rightarrow \mathcal{A}_2$. The *complete Steenrod Algebra* is the inverse limit of $\mathbb{Z}[\frac{1}{2}]$ -graded algebras

$$\hat{\mathcal{A}}_2 = \varprojlim \{ \cdots \xrightarrow{D} \frac{1}{2^{k+1}}\mathcal{A}_2 \xrightarrow{D} \frac{1}{2^k}\mathcal{A}_2 \xrightarrow{D} \frac{1}{2^{k-1}}\mathcal{A}_2 \xrightarrow{D} \cdots \}$$

Remark. It might seem arbitrary to complete the Steenrod Algebra using the particular epimorphism $\frac{1}{2}\mathcal{A}_2 \xrightarrow{D} \mathcal{A}_2$. However, it can be shown that it is the unique epimorphism respecting the algebra structure. It also preserves the coalgebra structure, and so the completed Steenrod Algebra is a completed Hopf algebra.

We filter $\hat{\mathcal{A}}_2$ by an increasing sequence of ideals

$$\cdots \subset I_{-1} \subset I_0 \subset I_1 \subset \cdots \subset \hat{\mathcal{A}}_2$$

where

$$I_n = \ker(\hat{\mathcal{A}}_2 \rightarrow 2^n \mathcal{A}_2)$$

Notice that one can define an isomorphism $D : \frac{1}{2}\hat{\mathcal{A}}_2 \rightarrow \hat{\mathcal{A}}_2$ induced from the halving homomorphism, and that $D(I_n) = I_{n-1}$.

Definition 1.3. A *root algebra* A is a $\mathbb{Z}[\frac{1}{2}]$ -graded commutative algebra over $\mathbb{Z}/2$ where the degree preserving homomorphism $D : 2A \rightarrow A$ defined by $D(x) = x^2$ is an isomorphism. In other words, one can take square roots in A .

Denote by $R[x_1, \dots, x_k]$ the free root algebra over $\mathbb{Z}/2$ generated by symbols x_1, \dots, x_k with some prescribed degrees. Notice that

$$R[x_1, \dots, x_k] = \varprojlim_D \frac{1}{2^i} P[x_1, \dots, x_k]$$

where $P[x_1, \dots, x_k]$ is the usual polynomial algebra over $\mathbb{Z}/2$ and D is the algebra homomorphism $D(x_i) = x_i^2$.

Define $R[x_1, x_2, \dots]$ to be the inverse limit

$$R[x_1, x_2, \dots] = \varprojlim_k R[x_1, \dots, x_k]$$

where the map $R[x_1, \dots, x_{k+1}] \rightarrow R[x_1, \dots, x_k]$ is the evaluation at $x_{k+1} = 0$. Let $R(n), n \leq \infty$ denote $R[x_1, \dots, x_n]$ or $R[x_1, x_2, \dots]$ where $|x_i| = 1$ for all i .

$R(n)$ and $R(\infty)$ have a continuous action of $\hat{\mathcal{A}}_2$ defined on generators by

$$\text{Sq}(x_i) = x_i + x_i^2$$

which commutes with the squaring isomorphism D . Sq is the *total Square* defined as

$$\text{Sq} = \sum_{i \in \mathbb{Z}} \text{Sq}^{2^i}$$

$R(n)$ and $R(\infty)$ also have an action of $\text{GL}(n, 2)$ (resp. $\text{GL}(\infty, 2)$).

Notice that for $k < \infty$ there is a natural filtration on $R(k)$ by $\frac{1}{2^i} P[x_1, \dots, x_k]$ which is invariant under the action of $\hat{\mathcal{A}}_2$. The filtration stage $\frac{1}{2^i} P[x_1, \dots, x_k]$ is annihilated by the ideal $I_{-i} \subset \hat{\mathcal{A}}_2$. In particular, $P[x_1, \dots, x_k]$ has an action of $\hat{\mathcal{A}}_2$ which is annihilated by I_0 . But $\hat{\mathcal{A}}_2/I_0 = \mathcal{A}_2$ and the action is the usual action of the Steenrod Algebra. Therefore all the subsequent results that we will get on the action of $\hat{\mathcal{A}}_2$ on elements in $R(k)$ will remain valid when restricted to the action of \mathcal{A}_2 on the polynomial algebra.

2. THE GENERALIZED DICKSON ALGEBRA

Definition 2.1. For $k \leq \infty$ define the *generalized Dickson Algebra* D_k to be the invariance $R(k)^{\text{GL}(k, 2)}$.

Notice that the actions of $\hat{\mathcal{A}}_2$ and $\text{GL}(k, 2)$ commute, and so D_k is a $\hat{\mathcal{A}}_2$ -module. Also notice that D_∞ has a natural topology induced from the one on $R(\infty)$. We will refer to this topology as the *filtration topology* in the sequel. The structure of D_k is very similar to that of the usual Dickson Algebra. Before we make that statement precise, we need to define some elements in D_k which are going to play a central role. These elements were first defined by Franklin P. Peterson for the integral Dickson Algebras. This is their first appearance in the literature.

Definition 2.2 (Peterson). Fix $k \leq \infty$. For each $n \in \mathbb{N}[\frac{1}{2}]$ define

$${}_k \omega_n = \sum_{\substack{s_1 + \dots + s_k = n \\ s_i = 0 \text{ or } 2^{r_i}, r_i \in \mathbb{Z}}} x_1^{s_1} x_2^{s_2} \cdots x_k^{s_k}$$

This sum seems to be potentially infinite even if k is finite, but this is not so. In fact, one can give a precise lower bound on r_i which depends on k and n .

Definition 2.3. For a nonzero $n \in \mathbb{N}[\frac{1}{2}]$ define the *weight* $\alpha(n)$ to be the numbers of 1's in the dyadic expansion of n . Define $\nu(n)$ to be the highest power of 2 dividing n (this can be negative, of course). Define $\sigma(n) = \alpha(n) + \nu(n)$.

Proposition 2.4.

- (a) Fix $k < \infty$. If $n = \sum_{i=1}^k 2^{r_i}$, where $r_i \in \mathbb{Z}$, then $r_i \geq \sigma(n) - k$. In particular, ${}_k\omega_n$ is a finite polynomial when $k < \infty$, while ${}_\infty\omega_n$ contains a finite number of monomials of any fixed length. Therefore, ${}_k\omega_n \in R(k)$.
- (b) ${}_k\omega_n$ is $\text{GL}(k, 2)$ -invariant.

Proof.

- (a) If $\alpha(n) > k$ then n cannot be expressed as the sum of k powers of 2, and so $\alpha(n) \leq k$. We may assume that r_k is the minimal r . Notice that $r_k \leq \nu(n)$. In this case, $\alpha(n - 2^{r_k}) = \alpha(n) + \nu(n) - 1 - r_k$. Since $n - 2^{r_k} = \sum_{i=1}^{k-1} 2^{r_i}$ we know that $\alpha(n - 2^{r_k}) \leq k - 1$. comparison now gives the result.
- (b) ${}_k\omega_n$ is obviously symmetric, so it is enough to show that it is invariant under the linear transformation T that sends x_1 to $x_1 + x_2$ and x_i to itself for $i > 1$. Being lax on notation to avoid cumbersome formulas, rewrite ${}_k\omega_n$ as

$${}_k\omega_n = \sum_{0 < s_1 < s_2} (x_1^{s_1} x_2^{s_2} + x_1^{s_2} x_2^{s_1}) x_3^{s_3} \cdots x_k^{s_k} + \sum_{0 < s} (x_1^{2s} + x_2^{2s} + x_1^s x_2^s) x_3^{s_3} \cdots x_k^{s_k}$$

Since all the powers of x_1 in sight are of the form 2^r we have $T(x_1^s) = x_1^s + x_2^s$. Applying T to the above identity now easily gives the result.

□

The following corollary will become handy in Section 4.

Corollary 2.5. Let $n \in \mathbb{N}[\frac{1}{2}]$ and suppose $n = \sum_{i=1}^k r_i$ where $r_i \in \mathbb{N}[\frac{1}{2}]$ and $\alpha(r_i) \leq s$. Then $\nu(r_i) \geq \sigma(n) - ks$. In particular, there is only a finite number of ways to write n as such a sum when k and s are fixed.

Proof. Break each r_i into at most s powers of 2, then use part (a) of the proposition. □

Proposition 2.6.

(a)

$$D_k = \varinjlim_D \frac{1}{2^n} \tilde{D}_k \quad \text{For } k < \infty$$

$$D_\infty = \varprojlim_k D_k$$

Where \tilde{D}_k is the usual Dickson Algebra viewed as a $\mathbb{Z}[\frac{1}{2}]$ -graded algebra, and D is the squaring homomorphism induced from the polynomial algebra. In particular, \tilde{D}_k embeds in D_k .

- (b) Let $k \in \mathbb{N}$, $n \in \mathbb{N}[\frac{1}{2}]$, with $\alpha(n) \leq k$. Then ${}_k\omega_n$ will have no fractional exponents if and only if $k \leq \sigma(n)$, and will therefore reside in \tilde{D}_k in that case. If $\alpha(n) > k$, ${}_k\omega_n = 0$.
- (c) By [Dk], \tilde{D}_k is the free symmetric algebra on generators $\{Q_i\}_{i=0}^{k-1}$, where Q_i has degree $2^k - 2^i$. The embedding in (a) sends Q_i to ${}_k\omega_{2^k-2^i}$.
- (d) D_k is the free root algebra generated by $\{{}_k\omega_{2^i-1}\}_{i=1}^k$. D_∞ includes the free root algebra generated by $\{{}_\infty\omega_{2^i-1}\}_{i=1}^\infty$ as a dense subset.
- (e) ${}_k\omega_n^2 = {}_k\omega_{2n}$, and therefore $\{{}_k\omega_{2^{j+1}-2^i}\}_{0 \leq j-i < k}$ is a simple basis for D_k , i.e., every element can be written uniquely as a square-free polynomial in terms of these.

Proof.

- (a) Given any polynomial in D_k when $k < \infty$, one can apply D^{-1} to it a number of times to make all the powers integral. The second part follows since the action of $GL(\infty, 2)$ is compatible with the actions of $GL(k, 2)$ under the projections.
- (b) If $k \leq \sigma(n)$, the integrality follows directly from Proposition 2.4. The other direction follows from the observation that the bound in the proposition is tight. Specifically, for n with $\alpha(n) \leq k$ one has $\alpha(n - 2^{\sigma(n)-k}) = k - 1$ and therefore n can always be written as a sum of k powers of 2 the smallest of which is $2^{\sigma(n)-k}$. Therefore ${}_k\omega_n$ will not be integral unless $k \leq \sigma(n)$. If $\alpha(n) > k$, it is obvious that n cannot be written as a sum of k powers of 2, and so ${}_k\omega_n = 0$.
- (c) $\sigma(2^k - 2^i) = k$ and so by (b) ${}_k\omega_{2^k-2^i} \in \tilde{D}_k$. But the only nonzero element in \tilde{D}_k in that degree is Q_i and the claim follows.
- (d) For $k < \infty$, this follows from (a) and (c) and from the observation that ${}_k\omega_n^2 = {}_k\omega_{2n}$. For D_∞ this follows from noting that the projections $D_\infty \rightarrow D_k$ send ${}_\infty\omega_n$ to ${}_k\omega_n$.
- (e) Follows directly from Definition 2.2 and the linearity of the squaring operator.

□

We now compute the action of $\hat{\mathcal{A}}_2$ on D_k . By the remark at the end of Section 1, this computation will be valid in \dot{D}_k as well. We first need a definition and a lemma.

Definition 2.7. Given $k, n \in \mathbb{N}[\frac{1}{2}]$, define the binomial coefficient $\binom{n}{k}$ to be the residue mod 2 of $\binom{2^N n}{2^N k}$ where N is big enough to make both terms integral. This definition makes sense since for nonnegative integers n, k one has $\binom{n}{k} \equiv \binom{2n}{2k} \pmod{2}$.

A convenient way to interpret this function is the following. $\binom{n}{k} = 1$ exactly when the positions of the 1's in the dyadic expansion of k are a subset of the positions of the 1's in the dyadic expansion of n

Lemma 2.8. Let $R = (r_1, \dots, r_k)$ be a vector of integers, and define $|R| = \sum_{i=1}^k 2^{r_i}$. For $k \in \mathbb{Z}[\frac{1}{2}]$ let $G_R(k)$ be the number of ways to express k as a partial sum of the terms 2^{r_i} . In other words, $G_R(k)$ is the number of solutions to the equation $k = \sum_{i=1}^k X_i 2^{r_i}$ where $X_i \in \{0, 1\}$. Then

$$G_R(k) \equiv \binom{|R|}{k} \pmod{2}$$

Proof. It is enough to prove the lemma for nonnegative vectors. Define

$$f_R(x) = \sum_{k \in \mathbb{N}[\frac{1}{2}]} G_R(k) x^k$$

Notice that this sum is finite. It is not difficult to show that given two vectors R, S one has $f_{RS} = f_R f_S$ where RS is the concatenation. It is also clear that

$$f_{(r)}(x) = 1 + x^{2^r}$$

Therefore

$$f_R(x) = \prod_{i=1}^k (1 + x^{2^{r_i}}) \stackrel{\text{mod } 2}{\equiv} \prod_{i=1}^k (1 + x)^{2^{r_i}} = (1 + x)^{\sum 2^{r_i}} = (1 + x)^{|R|}$$

And the claim follows from binomial expansion. \square

Theorem 2.9. given $t, n \in \mathbb{N}[\frac{1}{2}]$, the following holds

$$\text{Sq}^t {}_k\omega_n = \binom{n+t}{2t} {}_k\omega_{n+t}$$

Proof. All the monomials in ${}_k\omega_n$ have powers of 2 as exponents. Our first step will be to prove that when a Square acts on such a monomial, the result is a combination of such monomials, and so the monomials in $\text{Sq}^t {}_k\omega_n$ all come from ${}_k\omega_{n+t}$. The second step would be to compute how many times each monomial is to be taken.

For the first step, recall that $\hat{\mathcal{A}}_2$ acts on products through its diagonal map. Therefore we have

$$\text{Sq}^t(x_1^{s_1} x_2^{s_2} \cdots x_k^{s_k}) = \sum_{t_1+t_2+\cdots+t_k=t} \text{Sq}^{t_1}(x_1^{s_1}) \text{Sq}^{t_2}(x_2^{s_2}) \cdots \text{Sq}^{t_k}(x_k^{s_k})$$

In the monomials we are considering, s_i is a power of 2 and therefore

$$\text{Sq}^{t_i}(x_i^{s_i}) = \begin{cases} x_i^{s_i} & t_i = 0 \\ x_i^{2s_i} & t_i = s_i \\ 0 & \text{otherwise} \end{cases}$$

which proves the first part. For the second part, consider a monomial $x_{i_1}^{2^{r_1}} x_{i_2}^{2^{r_2}} \cdots x_{i_j}^{2^{r_j}}$ of ${}_k\omega_{n+t}$. By the first part, this monomial can be obtained from a monomial of ${}_k\omega_n$ by choosing a subset of the variables with exponents adding up to t and doubling them. To retrace the possible origins of this monomial, then, we have to find all subsets of its variables with exponents adding up to $2t$, and then half them. According to Lemma 2.8 the number of ways to do that is congruent modulo 2 to $\binom{n+t}{2t}$. \square

Corollary 2.10. *Let $Q_i^j \in \hat{\mathcal{A}}_2$ be the element defined by induction as $Q_i^i = \text{Sq}^{2^i}$ and $Q_i^{j+1} = [Q_i^j, \text{Sq}^{2^{j+1}}]$ (note that Q_i^j is not primitive in $\hat{\mathcal{A}}_2$). Then*

$$Q_i^j {}_k\omega_n = \binom{n + 2^{j+1} - 2^i}{2^{j+1}} {}_k\omega_{n+2^{j+1}-2^i}$$

Proof. We only have to consider the case $i = 0$ since all the other cases follow by applying the doubling isomorphism or its inverse an appropriate number of times. We use induction on j . The case $j = 0$ follows directly from Theorem 2.9. For the inductive step write

$$\begin{aligned} A &= \binom{n + 2^{j+2} - 1}{2^{j+1}} & C &= \binom{n + 2^{j+2} - 1}{2^{j+2}} \\ B &= \binom{n + 2^{j+1}}{2^{j+2}} & D &= \binom{n + 2^{j+1} - 1}{2^{j+1}} \end{aligned}$$

Then we have

$$\begin{aligned} Q_0^{j+1} {}_k\omega_n &= [Q_0^j, \text{Sq}^{2^{j+1}}] {}_k\omega_n = Q_0^j \text{Sq}^{2^{j+1}} {}_k\omega_n + \text{Sq}^{2^{j+1}} Q_0^j {}_k\omega_n \\ &= (AB + CD) {}_k\omega_{n+2^{j+2}-1} \end{aligned}$$

We have to show that $AB + CD \equiv C \pmod{2}$. We do that by considering the possible values of the residue of n modulo 2^{j+2} . Denote the residue by N . Notice that A and D depend only on N . If $0 < N \leq 2^{j+1}$ one readily sees that $A \equiv 0$ and $D \equiv 1$, and the result follows for this case. If $N > 2^{j+1}$ or $N = 0$ then $A \equiv 1$ and $D \equiv 0$. So in this case we have to show $B \equiv C$. Suppose $B \not\equiv C$. That means that

the $j+2$ bit of the number $n+2^{j+2}-1$ is different than that of $n+2^{j+1}$. This happens exactly when $0 < N < 2^{j+1}$, which is not the case here, and the result follows. \square

We now turn to the question of expressing a general ${}_k\omega_n$ in terms of the generators. This question is important since the ${}_k\omega_n$ play a central role in investigating the structure of D_k , as we will see in Sections 3 and 4.

From now on we will shorten ${}_\infty\omega_n$ to ω_n , and write $\omega_{\vec{m}}$ for $\omega_{m_1}\omega_{m_2}\dots\omega_{m_k}$ where $\vec{m} = (m_1, m_2, \dots, m_k)$.

Theorem 2.11. *Let $n \in \mathbb{Z}[\frac{1}{2}]$ and write $n = 2^N - \sum_{i=1}^{\ell} 2^{r_i}$, where $r_1 < \dots < r_\ell < N$. Then*

$$\begin{aligned}\omega_n &= \sum_{\substack{2^{s_1} + \dots + 2^{s_\ell} = 2^N \\ s_i - r_i \geq 0 \text{ for all } i}} \omega_{2^s - 2^r} \\ {}_k\omega_n &= \sum_{\substack{2^{s_1} + \dots + 2^{s_\ell} = 2^N \\ k \geq s_i - r_i \geq 0 \text{ for all } i}} {}_k\omega_{2^s - 2^r}\end{aligned}$$

where ω_0 , when it occurs, is just the unit. Notice that the right hand expression is finite and contains generators only.

Proof. Let V_a^b denote the vector space over $\mathbb{Z}/2$ generated by the symbols $\{x_i\}_{i=a+1}^b$, and write $V_k = V_0^k$. In [Dk] Dickson proves that

$$f_k(X) = \prod_{v \in V_k} (X + v) = \sum_{i=0}^k {}_k\omega_{2^k - 2^i} X^{2^i}$$

Notice that only X^{2^i} has non zero coefficients. Therefore f_k defines a linear operator, i.e. $f_k(X + Y) = f_k(X) + f_k(Y)$, and we get

$$\begin{aligned}(2.1) \quad f_{k+\ell}(X) &= \prod_{v \in V_{k+\ell}} (X + v) = \prod_{w \in V_k^\ell} \prod_{u \in V_k} (X + w + u) = \\ &= \prod_{w \in V_k^\ell} f_k(X + w) = \prod_{w \in V_k^\ell} (f_k(X) + f_k(w)) = \\ &= \sum_{i=0}^{\ell} {}_\ell\omega_{2^\ell - 2^i} (f_k(x_{k+1}), \dots, f_k(x_{k+\ell})) f_k(X)^{2^i}\end{aligned}$$

For the last identity we used the linearity of f_k to express $f_k(w)$ as a combination of $f_k(x_{k+i})$.

Given $n \in \mathbb{N}[\frac{1}{2}]$ with $\alpha(n) \leq k$ we now use the above formula to compute ${}_k\omega_n$ in terms of generators. Write $n = 2^N - \sum_{i=1}^{\ell} 2^{r_i}$ where $r_1 < \dots < r_\ell < N$. Recall that by Proposition 2.6, ${}_k\omega_n \in \check{D}_k$ if and only if $k \leq \sigma(n)$. In our case $\sigma(n) = \sigma(2^N - \sum_{i=1}^{\ell} 2^{r_i}) = N + 1 - \ell$ and so we need $N \geq k + \ell - 1$. If that condition is

not met we may enlarge N by considering ${}_k\omega_{2^e n}$ for a suitable power e . Once we compute the expansion for this case, we would be able to retrieve the expansion for the original term by taking square roots e times. Notice that we can do the same even when $N > k + \ell - 1$, using e negative, to force $N = k + \ell - 1$. This is not necessary, of course, but will simplify the formulas below.

All said, we may now write $n = 2^{k+\ell-1} - \sum_{i=1}^{\ell} 2^{r_i}$ where $r_1 < r_2 < \dots < r_{\ell} < k + \ell - 1$. Notice that we're now working inside D_k , so everything in sight is integral. Looking at equation 2.1, and comparing the coefficients of $X^{2^{k+\ell-1}}$ we get

$${}_{k+\ell}\omega_{2^{k+\ell-1}} = \ell\omega_{2^{\ell-1}}(f_k(x_{k+1}), \dots, f_k(x_{k+\ell})) + {}_k\omega_{2^{2^{\ell-1}}}$$

Now compare the coefficients of $x_{k+1}^{2^{r_1}} \dots x_{k+\ell}^{2^{r_{\ell}}}$ on both sides of the above formula. From Definition 2.2 it is easy to see that the comparison gives

$$(2.2) \quad \begin{aligned} {}_k\omega_n &= \sum_{\substack{2^{s_1} + \dots + 2^{s_{\ell}} = 2^{\ell-1} \\ k \geq r_i - s_i \geq 0 \text{ for all } i}} \prod_{i=1}^{\ell} {}_k\omega_{2^{s_i} - 2^{r_i - s_i}} = \\ &= \sum_{\substack{2^{s_1} + \dots + 2^{s_{\ell}} = 2^{\ell-1} \\ k \geq r_i - s_i \geq 0 \text{ for all } i}} \prod_{i=1}^{\ell} {}_k\omega_{2^{k+s_i} - 2^{r_i}} = \\ &= \sum_{\substack{2^{s_1} + \dots + 2^{s_{\ell}} = 2^{k+\ell-1} \\ k \geq s_i - r_i \geq 0 \text{ for all } i}} \prod_{i=1}^{\ell} {}_k\omega_{2^{s_i} - 2^{r_i}} \end{aligned}$$

This identity only holds in the case $N = k + \ell - 1$. However, if we rewrite

$$(2.3) \quad {}_k\omega_n = \sum_{\substack{2^{s_1} + \dots + 2^{s_{\ell}} = 2^N \\ k \geq s_i - r_i \geq 0 \text{ for all } i}} \prod_{i=1}^{\ell} {}_k\omega_{2^{s_i} - 2^{r_i}}$$

then the identity will hold for all n , where $n = 2^N - \sum_{i=1}^{\ell} 2^{r_i}$ with $r_1 < \dots < r_{\ell} < N$, which follows by taking the appropriate positive or negative power of 2 of equation 2.2.

Now observe that the identity for D_{∞} claimed at the statement of the theorem projects to equation 2.3 in D_k , since the elements $\omega_{2^s - 2^r}$ where $s - r > k$ project to 0 by Proposition 2.6, so the theorem follows by passing to limits. \square

Corollary 2.12. *The dense subalgebra of D_{∞} generated by $\{\omega_{2^k - 1}\}_{k=1}^{\infty}$ includes all the elements $\{\omega_n\}_{n \in \mathbb{N}[\frac{1}{2}]}$, and therefore all finite ω -polynomials (finite sums and products of ω_n 's).*

Definition 2.13. The algebra of finite ω -polynomials will be denoted $\text{Fin}(D_{\infty})$.

3. THE SCALAR PRODUCT

In this section we define a norm in D_∞ and a scalar product $B(D_\infty) \otimes D_\infty \rightarrow \mathbb{Z}/2$ where $B(D_\infty)$ is the subspace of bounded polynomials. Giving $B(D_\infty)$ a suitable topology makes the scalar product continuous in the product topology. We show that the product is nondegenerate, and symmetric when restricted to $\text{Fin}(D_\infty)$.

Definition 3.1. The *norm* of a monomial $M = x_1^{r_1} \dots x_k^{r_k}$ is defined to be

$$|M| = \max_{i=1}^k \alpha(r_i)$$

The norm of a polynomial is defined to be the supremum of the norms of its monomials. A polynomial P is said to be *bounded* if $|P| < \infty$.

Remark. We shall use the term “polynomial” as in the above definition to mean any element in $R(\infty)$.

Definition 3.2. For $P \in R(\infty)$ denote by $\mu(P)$ its filtration stage, i.e. the lowest k such that P project to a nonzero element in $R(k)$. The *norm topology* on $R(\infty)$ is given by the following basis for open sets at zero. For each nondecreasing, unbounded function $f : \mathbb{N} \rightarrow \mathbb{N}$ there is an open set $\{P \in R(\infty) \mid |P| < f(\mu(P))\}$. Define $B(R(\infty))$ to be the subspace of bounded polynomials, with the induced topology. Define a *Cauchy sequence* in $B(R(\infty))$ to be a Cauchy sequence with respect to the metric $1/\mu$ which has a global bound on the norm of its terms. Define

$$B(D_\infty) = B(R(\infty)) \cap D_\infty$$

Notice that by Definition 2.2 $|\omega_n| = 1$ and so $\omega_n \in B(D_\infty)$.

The converging sequences in $B(R(\infty))$ in this topology are exactly the Cauchy sequences, and in so in some sense this space is complete. $B(D_\infty)$ is a closed subspace, and therefore is likewise complete.

Proposition 3.3.

(a) $\text{GL}(\infty, 2)$ acts on $B(R(\infty))$, and therefore

$$B(D_\infty) = B(R(\infty))^{\text{GL}(\infty, 2)}$$

(b) For $P, Q \in B(R(\infty))$, $|PQ| \leq |P| + |Q|$, and so $B(R(\infty))$ and $B(D_\infty)$ are algebras. $\text{Fin}(D_\infty) \subset B(D_\infty)$.

Proof. (a) $\text{GL}(\infty, 2)$ is generated by the infinite symmetric group and the transvection T defined by

$$\begin{aligned} T(x_1) &= x_1 + x_2 \\ T(x_i) &= x_i \quad \text{for } i > 1 \end{aligned}$$

It is obvious that for any permutation σ and any $P \in B(R(\infty))$, we have $|P| = |\sigma(P)|$, so the symmetric group acts on $B(R(\infty))$. As for T , given any monomial $x_1^{s_1} \dots x_k^{s_k}$ of P , the action of T is

$$T(x_1^{s_1} \dots x_k^{s_k}) = \sum_{j \in [0, s_1]} \binom{s_1}{j} x_1^{s_1-j} x_2^{s_2+j} x_3^{s_3} \dots x_k^{s_k}$$

Where the sum is taken over an interval in $\mathbb{N}[\frac{1}{2}]$. The only nonzero terms in the sum are those where the 1's in the expansion of j are a subset of the 1's in the expansion of s_1 . In this case, $\alpha(s_1 - j) \leq \alpha(s_1) \leq |P|$ and $\alpha(s_2 + j) \leq \alpha(s_2) + \alpha(j) \leq \alpha(s_2) + \alpha(s_1) \leq 2|P|$, so $|T(P)| \leq 2|P|$, and T acts on $B(R(\infty))$ as well.

- (b) The claim that $|PQ| \leq |P| + |Q|$ follows directly from the subadditivity of α . Since $|\omega_n| = 1$ it follows that $|\omega_{n_1} \dots \omega_{n_k}| \leq k$ and therefore any finite ω -polynomial has a bounded norm. Hence $\text{Fin}(D_\infty) \subset B(D_\infty)$.

□

Definition 3.4. Given two homogeneous elements $P \in B(D_\infty)$ and $Q \in D_\infty$, write

$$P = \sum C_{(r_1, \dots, r_k)} x_1^{r_1} \dots x_k^{r_k}$$

There is a unique expansion of Q in the simple basis $\{\omega_{2^r - 2^s}\}_{r > s}$,

$$Q = \sum_{\vec{r} > \vec{s}} D_{\vec{r}, \vec{s}} \omega_{2^{\vec{r}} - 2^{\vec{s}}}$$

Define the scalar product of P and Q to be

$$\langle P, Q \rangle = \sum_{\vec{r} > \vec{s}} D_{\vec{r}, \vec{s}} C_{2^{\vec{r}} - 2^{\vec{s}}}$$

Proposition 3.5.

- (a) *The scalar product is well defined for any pair $P \in B(D_\infty)$ and $Q \in D_\infty$.*
- (b) *The scalar product is continuous.*
- (c) *The scalar product is continuous in the left variable in the filtration topology when the right hand side is in $\text{Fin}(D_\infty)$.*

Proof. (a) Let $p_k : D_\infty \rightarrow D_k$ be the projection and let $i_k : D_k \rightarrow D_\infty$ be the map defined on generators by $i_k(\omega_n) = \omega_n$. Let $r_k = i_k \circ p_k$. Let $Q_k = p_k(Q)$. Q_k has the expansion

$$Q_k = \sum_{\substack{\vec{r} > \vec{s} \\ \|\vec{r} - \vec{s}\|_\infty \leq k}} D_{\vec{r}, \vec{s}} \omega_{2^{\vec{r}} - 2^{\vec{s}}}$$

Since $Q_k \in D_k$, only a finite number of the above coefficients can be nonzero. For all the other coefficients of Q , the vector $2^{\vec{r}} - 2^{\vec{s}}$ has at least one entry with

more than k 1's in its dyadic expansion. Therefore the proposition follows by taking $k \geq |P|$.

- (b) Let $P_i \rightsquigarrow P$ and $Q_i \rightsquigarrow Q$ be two converging sequences in the respective topologies. Let k be a global bound on the norms $|P_i|$. Let N be such that for $n > N$, $\mu(Q - Q_n) > k$. For such n , $\langle P_i, Q_n \rangle = \langle P_i, Q \rangle = \langle P_i, r_k(Q) \rangle$ for all i . $r_k(Q)$ has a finite ω -expansion, so let M be the length of the longest monomial. Let M' be such that for $m > M'$, $\mu(P - P_m) > M$. For such m , the shortest x -monomial in $P - P_m$ must have length bigger than M , the reason being that $P - P_m$ is a symmetric polynomial and so a shorter monomial would imply the existence of a monomial in the variables x_1, \dots, x_M and hence $\mu(P - P_m) \leq M$, a contradiction. By the definition of the scalar product, $\langle P - P_m, r_k(Q) \rangle = 0$ and so

$$\langle P_m, Q_n \rangle = \langle P_m, Q \rangle = \langle P_m, r_k(Q) \rangle = \langle P, r_k(Q) \rangle = \langle P, Q \rangle$$

- (c) The proof proceeds along the same lines as the second part of part (b). Q has a finite ω -expansion. Let M be the length of the longest monomial in Q . Let $P_i \rightsquigarrow P$ be a sequence converging in the filtration topology. There exists some M' such that for $m > M'$ one has $\mu(P_m - P) > M$. For such m , the shortest x -monomial in $P - P_m$ has length bigger than M , and hence, as above, $\langle P_m, Q \rangle = \langle P, Q \rangle$, so the scalar product is continuous in the left hand variable.

□

So far the scalar product looks mostly pointless. The following proposition shows that it has very interesting properties inside $\text{Fin}(D_\infty)$. In particular, we show that it's symmetric. We will later show that $\text{Fin}(D_\infty)$ is dense in $B(D_\infty)$ in the norm topology, so those properties will hold throughout $B(D_\infty)$ by continuity.

Proposition 3.6. *For any two monomials $\omega_{\vec{n}}$ and $\omega_{\vec{m}}$ $\langle \omega_{\vec{n}}, \omega_{\vec{m}} \rangle$ is the coefficient of the monomial $x_1^{n_1} x_2^{n_2} \dots x_\ell^{n_\ell}$ in $\omega_{\vec{m}}$ where $n = (n_1, n_2, \dots, n_\ell)$. The form \langle, \rangle is symmetric and nondegenerate in $\text{Fin}(D_\infty)$.*

Proof. Use the above identity as a definition of a new scalar product, defined over $\text{Fin}(D_\infty)$, then show that the two forms coincide. A priori this form does not look well defined. It is clear, at least, that the value of the form does not depend on the representative on the left hand side, since the form was defined in terms of the underlying polynomial in $R(\infty)$. Therefore, to show that it is well defined it is enough to show that it is symmetric.

In order to compute the coefficient of $x_1^{n_1} x_2^{n_2} \dots x_\ell^{n_\ell}$ in $\omega_{m_1} \omega_{m_2} \dots \omega_{m_k}$ we have to find how many ways are there to construct this monomial by multiplying monomials of the individual ω_{m_i} 's. Any such construction can be represented in a unique way

by a $k \times \ell$ matrix whose entries are either zero or powers of 2 (positive or negative), such that the columns add up to the vector \vec{m} and the rows add up to the vector \vec{n} . Transposing those matrices now shows the claimed symmetry.

The nondegeneracy is obvious since any nonzero element of $\text{Fin}(D_\infty)$ has at least one monomial with a nonzero coefficient.

We have to show that this new scalar product is really the old one. From Definition 3.4 it is clear that the two definitions coincide when the right hand side is a monomial in the simple basis and the left hand side is in $\text{Fin}(D_\infty)$. But these monomials span $\text{Fin}(D_\infty)$, and so the two definitions coincide throughout $\text{Fin}(D_\infty)$. \square

Corollary 3.7. *Let $P \in \text{Fin}(D_\infty)$. Then $x_1^{2^w} x_3^{r_3} \dots x_k^{r_k}$ is a monomial of P if and only if $x_1^w x_2^w x_3^{r_3} \dots x_k^{r_k}$ is. In other words, any two variables in a monomial of P that have the same exponent can be “squeezed” to one variable and any variable can be split into two.*

Proof. The first coefficient is computed by $\langle P, \omega_{2^w} \omega_{r_3} \dots \omega_{r_k} \rangle$. The second by $\langle P, \omega_w^2 \omega_{r_3} \dots \omega_{r_k} \rangle$. The claim follows since $\omega_w^2 = \omega_{2^w}$. \square

Corollary 3.8. *For any $P \in D_\infty$ (resp. $P \in B(D_\infty)$) and any monomial $M = \omega_{m_1} \dots \omega_{m_k}$, the scalar product $\langle M, P \rangle$ (resp. $\langle P, M \rangle$) is the coefficient of $x_1^{m_1} \dots x_k^{m_k}$ in P .*

Proof. We will prove the second claim. The first one is proved the same way since norms are not used in the proof. P can be approached from $\text{Fin}(D_\infty)$ in the filtration topology. If $P' \in \text{Fin}(D_\infty)$ is such that $\mu(P - P') > k$, then P and P' have the same monomials in x_1, \dots, x_k . Since $M \in \text{Fin}(D_\infty)$ Proposition 3.5 implies that there is an ℓ such that if $\mu(P - Q) > \ell$ then $\langle P - Q, M \rangle = 0$. Choosing P' such that $\mu(P - P') > \max(k, \ell)$ we have $\langle P, M \rangle = \langle P', M \rangle$. By Proposition 3.6 the right hand side is the coefficient of $x_1^{m_1} \dots x_k^{m_k}$ in P' which is the same as the coefficient in P . \square

4. THE DUALITY RELATION AND ITS CONSEQUENCES

In this section we investigate the topological structure of D_∞ and $B(D_\infty)$. We show that the scalar product turns D_∞ and $B(D_\infty)$ into dual topological Hopf Algebras carrying both a left and a right action of $\hat{\mathcal{A}}_2$. We compute the right action and the coproduct explicitly. The main technical difficulty is showing that $\text{Fin}(D_\infty)$ is dense in $B(D_\infty)$ in the norm topology. The proof of this fact constitutes the bulk of this section.

We start with a remark about bases. The root algebra basis and the simple basis defined in Proposition 2.6 give vector space bases for D_k and $\text{Fin}(D_\infty)$, the first by

taking monomials in the algebra basis and the second by taking square-free monomials in the simple basis. What Proposition 2.6 says is that those two monomial bases are identical, and we will think of them as one basis where each element has two different representations. To pass from one representation to another, take each term $\omega_{2^k-1}^r$, expand r dyadically $r = \sum 2^t$ and use the identity $\omega_{2^k-1}^r = \prod \omega_{2^{k+t}-2^t}$.

Definition 4.1. An *admissible monomial* is an ω -monomial $\omega_{r_k} \omega_{r_{k-1}} \dots \omega_{r_1}$ where $r_i \geq 2r_{i+1}$. A *basic ω -monomial* is a square-free monomial in the simple basis defined in Proposition 2.6. The *complexity vector* of a basic ω -monomial $M = \prod_{i=1}^{\ell} \omega_{2^{s_i}-2^{t_i}}$ is the vector $(r_k, r_{k-1}, \dots, r_1)$, where $k = \max(s_i - t_i)$ and

$$r_j = \sum_{s_i=t_i+j} 2^{t_i}$$

When M is written in the root algebra generators, it has the form $M = \prod_{i=1}^k \omega_{2^i-1}^{r_i}$. Notice that $\ell = \sum_{i=1}^k \alpha(r_i)$.

A *basic x -monomial* is a monomial $M = x_1^{2^{s_1}-2^{t_1}} \dots x_\ell^{2^{s_\ell}-2^{t_\ell}}$ for some integers $s_i \geq t_i$, such that $s_{i+1} - t_{i+1} \leq s_i - t_i$ and in case of equality, $s_{i+1} < s_i$. The *complexity vector* of a basic x -monomial M is the vector (r_k, \dots, r_1) where $k = s_1 - t_1$ and

$$r_j = \sum_{s_i=t_i+j} 2^{t_i}$$

Notice also that a basic x -monomial can be reconstructed from its complexity, so there is exactly one basic monomial for each complexity. The same is true for ω -monomials.

A vector (r_k, \dots, r_1) is *higher* than a vector (s_ℓ, \dots, s_1) if it is larger than the second vector in the left lexicographical ordering, where vectors of different length are compared by padding the shorter vector with zeros on the left.

Theorem 4.2.

- (a) Let $M = \omega_{r_k} \omega_{r_{k-1}} \dots \omega_{r_1}$ be an admissible monomial. The highest complexity of a basic x -monomial in M is $(r_k, r_{k-1} - 2r_k, \dots, r_1 - 2r_2)$.
- (b) For any k, t and d there is a finite set of complexity vectors of length t such that any homogeneous $P \in B(D_\infty)$ of degree d with $|P| \leq t$ which has no basic x -monomials of those complexities has filtration higher than k , that is $\mu(P) > k$.
- (c) $\text{Fin}(D_\infty)$ is dense in $B(D_\infty)$. Moreover, if $P \in B(D_\infty)$ has norm t , it can be approximated by a sum of admissible ω -monomials of length at most t , so in particular it can be approximated by elements of norm at most t .

Proof. (a) The monomial M has length k , and therefore $|M| \leq k$, so all the basic x -monomials in M have norm k or less and therefore complexity vectors

of length k or less. Given any basic x -monomial N with complexity vector (s_k, \dots, s_1) write

$$N = N_k^{2^k-1} N_{k-1}^{2^{k-1}-1} \dots N_1$$

where

$$N_i = \prod_{j=\alpha(s_k)+\dots+\alpha(s_{i+1})+1}^{\alpha(s_k)+\dots+\alpha(s_i)} x_j^{2^{t_{ij}}} \quad \sum_j 2^{t_{ij}} = s_i \quad t_{ij} > t_{i(j+1)}$$

N is an x -monomial in M and is therefore

$$N = L_k L_{k-1} \dots L_1$$

Where L_i is an x -monomial in ω_{r_i} . Since $|\omega_{r_i}| = 1$, each monomial contributes just one digit to the exponent of each variable. But the variables $x_1, \dots, x_{\alpha(s_k)}$ have k digits in their exponent, so each one comes from a different L_i and they all contribute. In particular L_k contributes a digit to each of these variables, and the amount it contributes to each x_j is at least $2^{t_{kj}}$. Therefore

$$r_k \geq \sum_{j=1}^{\alpha(s_k)} 2^{t_{kj}} = s_k$$

If $r_k > s_k$ we're done. Otherwise $r_k = s_k$, which can only happen in case L_k contributed all of its exponents to the first $\alpha(s_k)$ variables, and only if the digit contributed to x_i was $2^{t_{ki}}$. In that case $L_k = N_k$. Set $N' = N/N_k$. N' is an x -monomial in the product $\omega_{r_{k-1}} \dots \omega_{r_1}$, specifically $N' = L_{k-1} \dots L_1$. N' is not necessarily basic, since it might have repeated powers. However by Corollary 3.7 there is a basic x -monomial in $\omega_{r_{k-1}} \dots \omega_{r_1}$ having the same complexity. Since this is the only parameter of N' we are interested in, we can work with N' as if it were basic. Writing N' the same way N was written above, we get

$$N' = N'_{k-1}^{2^{k-1}-1} \dots N'_1$$

where $N'_i = N_i$ for $i < k-1$ and $N'_{k-1} = N_k^2 N_{k-1}$.

The complexity vector of N' is $(s_{k-1} + 2r_k, s_{k-2}, \dots, s_1)$. By induction we have $(s_{k-1} + 2r_k, s_{k-2}, \dots, s_1) \leq (r_{k-1}, r_{k-2} - 2r_{k-1}, \dots, r_1 - 2r_2)$ and so $(s_{k-1}, s_{k-2}, \dots, s_1) \leq (r_{k-1} - 2r_k, \dots, r_1 - 2r_2)$ and since $s_k = r_k$ we get $(s_k, \dots, s_1) \leq (r_k, r_{k-1} - 2r_k, \dots, r_1 - 2r_2)$. The proof also demonstrates how to pick L_i in order to achieve the maximum complexity. Namely

$$L_i = N_i N_{i+1}^2 \dots N_k^{2^{k-i}}$$

As it is clear from the proof that this is the unique way to produce the monomial of maximal complexity, it necessarily has coefficient 1, i.e. the maximal complexity is achieved in M .

(b) By Corollary 2.5 there is a finite number of ways to express d as a sum of k numbers in $\mathbb{N}[\frac{1}{2}]$ of weight t or less. Write any such sum as a k -vector, and let A be the set of all such vectors. By Theorem 2.11 for each $\vec{m} \in A$ the ω -monomial $\omega_{\vec{m}}$ has a finite expansion in basic ω -monomials. Let B be the set of all basic ω -monomials that appear in any of these expansions. Suppose $P \in B(D_\infty)$ has degree d and $|P| \leq t$. Let $M \in B$ and suppose P has no basic x -monomial with a complexity vector equal to the complexity vector of M . Then by Corollary 3.8 we have $\langle P, M \rangle = 0$. If P misses all the complexity vectors of monomials in B , then it is orthogonal to B and therefore orthogonal to all $\omega_{\vec{m}}$ for $\vec{m} \in A$. Suppose P has filtration k or less. Then P has a monomial $x_1^{m_1} \dots x_k^{m_k}$. Since $|P| \leq t$ we get that $\alpha(m_i) \leq t$, and of course $\sum_{i=1}^k m_i = d$. Therefore $(m_1, \dots, m_k) \in A$ and therefore $\langle P, \omega_{m_1} \dots \omega_{m_k} \rangle = 0$ contradicting Corollary 3.8.

Some of the complexity vectors that we got might be longer than t . However, since P cannot include monomials with complexity vectors longer than its norm, we can discard such vectors should they occur.

(c) Let $P \in B(D_\infty)$ be homogeneous of degree d and norm t . To approximate P in the norm topology is to approximate it in the filtration topology by a sequence of bounded norm. We show that this can actually be done at norm t . Fix k . By part (b) there is a finite set B_k of complexity vectors of length t or less such that $\mu(P) > k$ when B_k does not occur in P . The complexity vectors in B_k are ordered by height, and by part (a) for each $c \in B_k$ there is an admissible word K_c of length t (and hence of norm at most t) whose highest complexity is c . Let c_1 be the highest complexity in B_k which appears in P , and define by induction c_{i+1} to be the highest complexity in B_k appearing in $P + K_{c_1} + \dots + K_{c_i}$. Stop the process when no such complexity exists, and suppose c_n was the last to be defined. Then by part (b) the polynomial $\sum_{i=1}^n K_i$ is an approximation of P up to filtration k , and $|\sum_{i=1}^n K_i| \leq \max_{i=1}^n |K_i| \leq t$.

□

Corollary 4.3. *The scalar product is symmetric in $B(D_\infty)$, and continuous in the left variable with respect to the filtration topology.*

Theorem 4.4. *Let $B(D_\infty)^*$ be the graded vector space of norm-continuous $\mathbb{Z}/2$ -valued homogeneous functionals on $B(D_\infty)$. Let D_∞^* be the graded vector space of $\mathbb{Z}/2$ -valued homogeneous functionals on D_∞ continuous in the filtration topology. Then the maps $\varphi : B(D_\infty) \rightarrow D_\infty^*$ and $\varphi : D_\infty \rightarrow B(D_\infty)^*$ defined by $\varphi(P) = \langle P, - \rangle$ (resp. $\langle -, P \rangle$) are vector space isomorphisms.*

Proof. The maps are injective by the nondegeneracy of the scalar product. The main problem is to show surjectivity. Let $f \in B(D_\infty)^*$ be a continuous functional of degree

d. Define

$$P = \sum_{m_1 + \dots + m_k = d} f(\omega_{m_1} \dots \omega_{m_k}) x_1^{m_1} \dots x_k^{m_k}$$

We claim that $\varphi(P) = f$. This seems to follow directly from Corollary 3.8 by computing $\varphi(P)$ on ω -monomials. There is a problem, however, which is that it is not at all clear why $P \in D_\infty$ in the first place. To show that it is, observe that a polynomial $Q \in R(\infty)$ with expansion

$$Q = \sum C_{m_1, \dots, m_k} x_1^{m_1} \dots x_k^{m_k}$$

is invariant if and only if it is symmetric and for each sequence (n_1, \dots, n_ℓ) the following holds

$$\sum_{j \in (0, n_2]} \binom{n_1 + j}{n_1} C_{n_1 + j, n_2 - j, n_3, \dots, n_\ell} = 0$$

The above condition insures that Q is invariant under the transvection T . Notice that the above sum is always finite for $Q \in R(\infty)$. In the case of P , it is obviously symmetric and we have to show that

$$\sum_{j \in (0, n_2]} \binom{n_1 + j}{n_1} f(\omega_{n_1 + j} \omega_{n_2 - j} \omega_{n_3} \dots \omega_{n_\ell}) = 0$$

For each $n_1 + \dots + n_\ell = d$. The series

$$\sum_{j \in (0, n_2]} \binom{n_1 + j}{n_1} \omega_{n_1 + j} \omega_{n_2 - j} \omega_{n_3} \dots \omega_{n_\ell}$$

converges in the norm topology since it has a norm bounded by ℓ and for all but a finite values of j either $\omega_{n_1 + j}$ or $\omega_{n_2 - j}$ has a high filtration. We claim that the series converges to 0. To show that, take any ω -monomial Q . Write

$$Q = \sum C_{m_1, \dots, m_k} x_1^{m_1} \dots x_k^{m_k}$$

Then

$$\begin{aligned} & \langle Q, \sum_{j \in (0, n_2]} \binom{n_1 + j}{n_1} \omega_{n_1 + j} \omega_{n_2 - j} \omega_{n_3} \dots \omega_{n_\ell} \rangle \\ &= \sum_{j \in (0, n_2]} \binom{n_1 + j}{n_1} \langle Q, \omega_{n_1 + j} \omega_{n_2 - j} \omega_{n_3} \dots \omega_{n_\ell} \rangle \\ &= \sum_{j \in (0, n_2]} \binom{n_1 + j}{n_1} C_{n_1 + j, n_2 - j, n_3, \dots, n_\ell} = 0 \end{aligned}$$

Where the last equality follows since $Q \in B(D_\infty)$. From the continuity of f we get

$$\sum_{j \in (0, n_2]} \binom{n_1 + j}{n_1} f(\omega_{n_1+j} \omega_{n_2-j} \omega_{n_3} \dots \omega_{n_\ell}) = 0$$

and therefore $P \in D_\infty$.

Supposing now that $f \in D_\infty^*$, we can construct P the same way as before. Since f is continuous in the coarse filtration topology, its restriction to $B(D_\infty)$ is automatically continuous in the finer norm topology. Since P was constructed using only values of f evaluated in $B(D_\infty)$, we get for free that $P \in D_\infty$, using the previous case. We only have to show that P has a bounded norm. Since f is continuous in the filtration topology, there exists a t such that for $P \in D_\infty$ with $\mu(P) > t$ one has $f(P) = 0$. If $|x_1^{m_1} \dots x_k^{m_k}| > t$ then $\mu(\omega_{m_1} \dots \omega_{m_k}) > t$ and therefore the coefficient of this monomial in P is zero, and so $|P| \leq t$. \square

Corollary 4.5. $B(D_\infty)$ has a right action of \hat{A}_2 defined by

$$\langle P \text{Sq}^t, Q \rangle = \langle P, \text{Sq}^t Q \rangle$$

Corollary 4.6. $B(D_\infty)$ has a completed Hopf Algebra structure with diagonal ψ defined by

$$\langle \psi(P), Q \otimes R \rangle = \langle P, QR \rangle$$

Corollary 4.7. $B(D_\infty)$ has a basis dual to the basic ω -monomials. We shall denote elements of this basis by M^* where M is a basic ω -monomial.

Definition 4.8. For $n \in \mathbb{N}[\frac{1}{2}]$ and $t > 0$ an integer. Let $n = \sum_{i \in \mathbb{Z}} C_i 2^i$ be the dyadic expansion of n where $C_i \in \{0, 1\}$. Define the t -modular weight vector $\alpha_t(n)$ to be the vector $(\alpha_0, \dots, \alpha_{t-1})$ where

$$\alpha_r = \sum_{i \in \mathbb{Z}} C_{ti+r}$$

Define

$${}_k \omega_{n,t} = \sum_{\substack{s_1 + \dots + s_k = n \\ s_i = 0 \text{ or } \alpha_t(s_i) = (1, 1, \dots, 1)}} x_1^{s_1} \dots x_k^{s_k}$$

Notice that ${}_k \omega_n = {}_k \omega_{n,1}$.

Theorem 4.9.

$$\omega_{n,t} = (\omega_{2^t-1}^n)^*$$

In particular, $\omega_n = (\omega_1^n)^*$

Proof. The dual of $\omega_{2^t-1}^n$ represents the functional f which assigns one to this monomial and zero to all other basic monomials. To compute the dual, we have to compute this functional on all ω -monomials. Given a monomial $\omega_{n_1} \dots \omega_{n_\ell}$, we first have to expand each ω_{n_i} in terms of the basic monomials using Theorem 2.11. Since the set of basic monomials is closed under products, those expansions will multiply to give an expansion of the whole monomial. This expansion will contain a monomial of the form $\omega_{2^t-1}^m$ (where $m = \frac{1}{2^t-1} \sum n_i$) if and only if for each i the expansion of ω_{n_i} contains the monomial $\omega_{2^t-1}^{m_i}$ where $m_i = \frac{n_i}{2^t-1}$. So we have reduced the problem to determining for which values of n the expansion of ω_n contains a basic monomial of the form $\omega_{2^t-1}^m$. Write $n = 2^N - \sum_{i=1}^{\ell} 2^{r_i}$ where $r_1 < \dots < r_\ell < N$. Looking at Theorem 2.11 one can see that this situation occurs when we can arrange that for each i either $s_i = r_i$ or $s_i = r_i + t$. If there are three different indices i_1, i_2, i_3 for which $s_{i_1} = s_{i_2} = s_{i_3}$ then two of $r_{i_1}, r_{i_2}, r_{i_3}$ are equal, which is impossible since they were defined to be distinct. So the vector \vec{s} has at most double values, and since it adds up to 2^N one can show that the elements of \vec{s} are necessarily $N-1, N-2, \dots, N-\ell+1, N-\ell+1$, not necessarily in that order. For $N-\ell+1 < i < N-1$ denote by $r(i)$ the value of the entry in \vec{r} corresponding to the value i in \vec{s} . Then $r(i)$ is either i or $i-t$. In particular $r(i) \equiv i \pmod{t}$. Given a residue class $0 \leq j < t$ such that $j \not\equiv N-\ell+1 \pmod{t}$, the set $\{r(i) | i \equiv j\}$ covers all the residue class of j in the range $[N-\ell-t+1, N-1]$ except for one omitted value. That is because the variable i covers the residue class of j in the interval $[N-\ell+1, N-1]$ which is one element smaller than the same residue class in the larger interval, and because the $r(i)$'s are known to be distinct. As for the residue class of $N-\ell+1$, the value $N-\ell+1$ appears twice in \vec{s} and therefore necessarily corresponds to both values $N-\ell+1, N-\ell-t+1$ in the vector \vec{r} . Therefore \vec{r} contains the set $\{r(i) | i \equiv j \text{ and } i > N-\ell+1\} \cup \{N-\ell+1, N-\ell-t+1\}$ of representatives of the residue class j which is exactly the size of that residue class in $[N-\ell-t+1, N-1]$ and so no value in this class is omitted. Denote by $s(j)$ the omitted value in the residue class of j for $j \not\equiv N-\ell+1$. For $j \equiv N-\ell+1$ write $s(j) = N-\ell-t+1$. Then

$$n = 2^N - \sum_{i=1}^{\ell} 2^{r_i} = 2^N - \sum_{i=N-\ell-t+1}^{N-1} 2^i + \sum_{\substack{j=0,1,\dots,t-1 \\ j \not\equiv N-\ell+1}} 2^{s(j)} = \sum_{j=0}^{t-1} 2^{s(j)}$$

The numbers $s(0), \dots, s(t-1)$ are all distinct mod t and so $\alpha_t(n) = (1, 1, \dots, 1)$.

We have established that the monomials $\omega_{n_1} \dots \omega_{n_\ell}$ for which $f(\omega_{n_1} \dots \omega_{n_\ell}) = 1$ are exactly those in which $\alpha_t(n_i) = (1, 1, \dots, 1)$. Therefore the dual of $\omega_{2^t-1}^n$ is as stated. \square

Theorem 4.10.

$$\omega_n \text{Sq}^t = \binom{n-t}{t} \omega_{n-t}$$

The action on products is through the diagonal map of \hat{A}_2 .

Proof. Let \vec{m} and \vec{s} be vectors with $|\vec{s}| - |\vec{m}| = t > 0$. Let k be the length of \vec{s} and ℓ the length of \vec{m} . For any vector \vec{i} of length k and total degree t let $A_{\vec{i}}$ be the set of all $\ell \times k$ matrices with power 2 or zero entries whose column sum is \vec{m} and whose row sum is $\vec{s} - \vec{i}$. For any vector \vec{j} of length ℓ and total degree t let $B_{\vec{j}}$ be the set of all $\ell \times k$ matrices with power 2 or zero entries whose column sum is $\vec{m} + \vec{j}$ and whose row sum is \vec{s} .

Define a marked matrix to be a matrix in which a subset of the nonzero entries has been singled out or “marked”. For each $M \in A_{\vec{i}}$ let C_M be the set of all markings of M where the row sum of the marked entries is \vec{i} . For each $N \in B_{\vec{j}}$ let D_N be the set of all markings of N where the column sum of the marked entries is $2\vec{j}$.

One readily sees that there is a bijection, namely doubling of the marked entries

$$2 : \prod_{\vec{i}} \prod_{M \in A_{\vec{i}}} C_M \rightarrow \prod_{\vec{j}} \prod_{N \in B_{\vec{j}}} D_N$$

And therefore

$$\sum_{\vec{i}} \sum_{M \in A_{\vec{i}}} |C_M| = \sum_{\vec{j}} \sum_{N \in B_{\vec{j}}} |D_N|$$

By Lemma 2.8 we have

$$|C_M| \equiv \binom{\vec{s} - \vec{i}}{\vec{i}} \pmod{2} \quad \text{and} \quad |D_N| \equiv \binom{\vec{m} + \vec{j}}{2\vec{j}} \pmod{2}$$

where the binomial coefficient of two vectors is the product of the coordinatewise binomial coefficients. Therefore

$$\sum_{\vec{i}} \binom{\vec{s} - \vec{i}}{\vec{i}} |A_{\vec{i}}| \equiv \sum_{\vec{j}} \binom{\vec{m} + \vec{j}}{2\vec{j}} |B_{\vec{j}}| \pmod{2}$$

By the proof of Proposition 3.6 we have

$$|A_{\vec{i}}| \equiv \langle \omega_{\vec{s} - \vec{i}}, \omega_{\vec{m}} \rangle \pmod{2} \quad \text{and} \quad |B_{\vec{j}}| \equiv \langle \omega_{\vec{s}}, \omega_{\vec{m} + \vec{j}} \rangle \pmod{2}$$

so we have

$$\left\langle \sum_{\vec{i}} \binom{\vec{s} - \vec{i}}{\vec{i}} \omega_{\vec{s} - \vec{i}}, \omega_{\vec{m}} \right\rangle \equiv \left\langle \omega_{\vec{s}}, \sum_{\vec{j}} \binom{\vec{m} + \vec{j}}{2\vec{j}} \omega_{\vec{m} + \vec{j}} \right\rangle \pmod{2}$$

By the Cartan formula, the right hand side is $\langle \omega_{\vec{s}}, \text{Sq}^t \omega_{\vec{m}} \rangle$, and therefore

$$\omega_{\vec{s}} \text{Sq}^t = \sum_{\vec{i}} \binom{\vec{s} - \vec{i}}{\vec{i}} \omega_{\vec{s} - \vec{i}}$$

□

Theorem 4.11. *The coproduct is given by*

$$\psi(\omega_n) = \sum_{i+j=n} \omega_i \otimes \omega_j$$

In particular ψ is cocommutative.

Proof. Set

$$\psi(\omega_n) = \sum_{M \text{ a basic } \omega\text{-monomial}} P_M \otimes M^*$$

Recall that $\omega_n = (\omega_1^n)^*$. Let Q be any basic ω -monomial. Then

$$\langle P_M, Q \rangle = \langle P_M \otimes M^*, Q \otimes M \rangle = \langle \psi(\omega_n), Q \otimes M \rangle = \langle \omega_n, QM \rangle = \langle (\omega_1^n)^*, QM \rangle$$

So $P_M = 0$ unless $M = \omega_1^i$ for some i , and in that case P_M is orthogonal to all the basic monomials except $Q = \omega_1^{n-i}$. Therefore $P_M = (\omega_1^{n-i})^* = \omega_{n-i}$ and $M^* = (\omega_1^i)^* = \omega_i$ and the theorem follows. \square

REFERENCES

- [Dk] Dickson L.E.: *A Fundamental System of Invariants of the General Modular Linear Group with a Solution of the Form Problem.* Trans. Amer. Math. Soc. **12**, 75-98 (1911)
- [Ma] Madsen I.: *On the Action of the Dyer-Lashof Algebra in $H_*(G)$.* Pacific Jr. of Math. **60**, 235-275 (1975)
- [Mi] Miller H.R.: *The Sullivan Conjecture on Maps from Classifying Spaces.* Ann. of Math. **120**, 39-87 (1984)
- [Ng] Nguyễn Hữu Việt Hưng: *The Action of the Steenrod Algebra on the Modular Invariants of Linear Groups.* Proc. Amer. Math. Soc. **113**, 1097-1104 (1991)
- [NgPe] Nguyễn Hữu Việt Hưng, Peterson F.P.: *A-Generators for the Dickson Algebra.* To Appear.
- [Sr] Serre J.-P.: *Cohomologie Modulo 2 des Complexes d'Eilenberg-MacLane.* Comm. Math. Helv. **27**, 198-231 (1953)
- [SmSw] Smith L., Switzer R.: *Realizability and Non-realizability of Dickson Algebras as Cohomology Rings.* Proc. Amer. Math. Soc. **89**, 303-313 (1983)
- [Wi] Wilkerson C.: *A primer on the Dickson Invariants.* Contemporary Mathematics, Amer. Math. Soc. **19**, 421-434 (1983)