ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

UNIVERSITY OF IOANNINA
DEPARTMENT OF MATHEMATICS

SUMMER SCHOOL IN IOANNINA

"Interactions between Algebraic Topology and Invariant Theory"

A SATELLITE CONFERENCE
OF THE THIRD EUROPEAN CONGRESS OF MATHEMATICS

26 - 30 JUNE 2000 IOANNINA, GREECE

PROCEEDINGS

Nondas E. Kechagias Editor

H. E. A. Campbell, *Modular Invariant Theory*

F. R. Cohen, *Algebraic Topology*

L. Smith, *Invariant Theory*

R. M. W. Wood, *Hit problems and the Steenrod algebra*

Number 3, Special Volume, December 2000

FOREWORD

An international Summer School was held at the University of Ioannina, from June 26 to June 30 2000, as a satellite conference of the European Congress of Mathematics during summer 2000.

The theme of the School was "*Interactions between Algebraic topology and Invariant Theory*" and the aim to enrich and strength research relations among young researchers working on algebraic topology, invariant theory, and related areas. The program employed to accomplish our objectives was by short courses given by leading experts in these fields and problem sessions where common problems and research methods were recognized and demonstrated on particular research projects.

Four mini courses were delivered by:
H. E. A. Campbell, *Modular Invariant Theory*;
F. R. Cohen, *Algebraic Topology*;
L. Smith, *Invariant Theory*;
R. M. W. Wood, *Hit problems and the Steenrod algebra.*

We thank all the participants who undoubtedly contributed to the success of the event and the speakers for their effort in the preparation of their lectures and these notes. We also thank Fred Cohen and Larry Smith who worked very hard for organizing such an excellent scientific program. Special thanks to Fred Cohen for his encouragement and smooth handle of various aspects during the preparation of the school and Reg Wood for replacing Said Zarati at the last moment.

We want to express our gratitude to the University of Ioannina and in particular all members of the Section of Algebra and Geometry in the Department of Mathematics for their continuing encouragement and support. We will not mention internal or external bureaus or committees, which did not respond, but we will mention the great support we received from the Greek General Secretariat for Research and Technology, Ministry of Education and Religious Affairs (EPEAEK), and Prefecture of Ioannina. Without them, that event would not have taken place.

Nondas Kechagias
December, 2000
Ioannina.

LIST OF PARTICIPANTS

1) Gemma Bastardas
Universitat Aut•noma de Barcelona
gemmab@mat.uab.es

2) Terrence P. Bisson
Canisius College
bisson@canisius.edu

3) Maxmilian Boratynski
University degli Studi di Bari
boratyn@pascal.dm.uniba.it

4) Maurizio Brunetti
University of Naples
brunetti@matna2.dma.unina.it

5) H.E.A. Campbell
Queen's University
eddy@mast.queensu.ca

6) Jianjun Chuai
Queen's University

7) Adriana Ciampella
University of Naples
ciampell@matna2.dma.unina.it

8) F. Cohen
University of Rochester
cohf@math.rochester.edu

9) Fotini Dempegioti
University of Athens
fdebeg@math.uoa.gr

10) Ramon Jesis Flores Dvaz
Universitad Aut•noma de Barcelona
ramonj@mat.uab.es

11) David Giordano
Queen's University

12) Javier Gutierrez
Universitad Aut•noma de Barcelona
jgutierr@mat.uab.es

13) Andreas Hallilaj
University of Ioannina

14) Julia Hartmann
Universitat Heidelberg
Julia.Hartmann@IWR.Uni-Heidelberg.De

15) Roozbeh Hazrat
University of Bielefeld
rhazrat@mathematik.uni-bielefeld.de

16) Konstantinos Karalis
University of Athens
kkaralis@yahoo.com

17) Nondas Kechagias
University of Ioannina
nkechag@cc.uoi.gr

18) Alexander Kuehn
Frankfurt Johann Wolfgang GoetheUniversity
kuehn@samson.math.uni-frankfurt.de

19) Sofia Lambropoulou
National Technical University of Athens
sofia@math.ntua.gr

20) Leonidas Linardakis
University of Ioannina

21) Dagmar Meyer
Universite Paris 13
dagmar@zeus.math.univ-paris13.fr

22) N. Marmaridis
University of Ioannina
nmarmar@cc.uoi.gr

23) Frank Neumann
Universitat Goettingen
neumann@cfgauss.uni-math.gwdg.de

24) Mara Neusel
Yale University
neusel@math.yale.edu

25) Joel Segal
Universitat Goettingen
joel@uni-math.gwdg.de

26) L. Smith
Universitat Goettingen
larry@sunrise.uni-math.gwdg.de

27) Dimosthenis Stalidis
University of Ioannina

27) Nicolas M. Thiery
Colorado School of Mines
nthiery@icare.Mines.EDU

29) Andrzej Tyc
N. Copernicus University
atyc@mat.uni.torun.pl

30) David Wehlau
Queen's University
wehlau@mast.queensu.ca

31) R. Wood
University of Manchester
reg@maths.man.ac.uk

32) Jie Wu
National University of Singapore
matwuj@nus.edu.sg

33) Miguel A. Xicotencatl
Max-Plank Institute
xico@mpim-bonn.mpg.de

34) Jennifer Joy Ziebarth
University of Wisconsin
ziebarth@math.wisc.edu

Contents

H. E. A. Campbell
Modular Invariant Theory 1

F. R. Cohen
Algebraic Topology 27

L. Smith
An Algebraic Introduction to the Steenrod Algebra.................................49

R. M. W. Wood
Hit problems and the Steenrod algebra..65

MODULAR INVARIANT THEORY
SUMMER SCHOOL ON ALGEBRAIC TOPOLOGY AND INVARIANT THEORY, IOANNINA, GREECE

H E A CAMPBELL

ABSTRACT. This modest work provides some insight into the subject of modular invariant theory.

CONTENTS

1. Introduction. 2
Acknowledgements. 3
2. Lecture On Elements of Invariant Theory 3
Homogeneous Systems of Parameters. 3
The Poincaré series 4
Structures. 5
Resolutions by means of syzygies. 5
Molien's Theorem. 6
Construction of invariants. 6
3. Examples. 7
Hand Calculations. 7
Example: Calculations in Magma. 8
Symmetric Functions. 9
The Alternating groups. 10
Invariants of Permutation Groups. 10
The Dickson Invariants. 12
Upper Triangular Invariants. 12
A 2-dimensional representation of C_3, $p = 2$, [**B**, pg 103.] 13
4. Lecture on Structures and Fundamental Questions. 13
Bounds for Generating Sets 14
Fleischmann on non-modular groups. 15
Vector Invariants 15
On the Structure of $\mathbb{F}[V]^G$: classical results. 16

Date: June 30, 2000.
1991 *Mathematics Subject Classification.* 13A20.
Key words and phrases. finite groups, positive characteristic, invariant theory.

Structure of $\mathbb{F}[V]^G$: modular case 16
A cautionary tale concerning p-groups. 17
Stong's example. 18
5. Lecture on the cyclic group of order p over $\mathbb{F}_p$ 19
Conjectures about Modular Groups 19
Generators for p-Groups? 20
6. Two Problems from Invariant Theory. 21
The Dixmier-Erdös-Nicholas Problem. 21
Steenrod module structures on the syzygies. 22
7. References 24
A word about the two lists that follow. 24
Queen's Papers 25

1. Introduction.

I have gathered here some of the results and problems of invariant theory that I find found particularly interesting and exciting together with some of the necessary background material. Of course, the summer school is intended for graduate students, so these lectures are aimed at them. These are the lectures that I would use to introduce a new student to the subject. My goal has been to illustrate that there are many interesting and fascinating problems that can be tackled with only a modest knowledge of the techniques of modern algebra. The books of Benson [**B**] and Smith [**Sm(a)**] are appropriate references.

In addition to my own interests, I have tried to track to some degree the lectures of the other speakers, and this led to several revisions of the original material while at the school.

The second and third sections of this note are intended to give students an idea of the elements of invariant theory: homogeneous systems of parameters, resolutions by syzygies, Poincaré series, and several examples: the symmetric and alternating groups in their usual representation, permutation groups, the general linear and upper triangular groups, as well as a few selected examples. An example of the MAGMA code needed to do a specific calculation is given here. The first lecture covered much of the second and third sections of this note.

The fourth section concentrates on the two fundamental questions, namely, given a group or a class of groups, what can be said about the structure of its ring of invariants: when is the invariant ring polynomial, a hypersurface, a complete intersection algebra, Gorenstein, or Cohen-Macaulay? Alternately, we'd like to be able to describe generators for such rings of invariants, and the relations among those generators.

Section five is a discussion of the case of the cyclic group of order p and its representations in characteristic p.

Section six consists of two distinct open problems in invariant theory. I included the second of these because it involves the Steenrod algebra and so related well to Smith's lectures.

I include here two lists of references, one from the literature at large, and a list of invariant theory papers I've been involved in over the past few years.

Acknowledgements. I would like to extend my warmest thanks to the participants in the summer school on connections between algebraic topology and invariant theory. Their enthusiasm and energy for the school made the week a fantastic and wonderful experience. I'd also like to congratulate Dr Epiminondas Kechagias, the University of Ioannina, and the City of Ioannina, whose hospitality and warmth made the conference a joy to attend, and a joy at which to speak. Thank you, Nondas.

2. Lecture On Elements of Invariant Theory

Suppose R is any non-negatively graded, finitely generated, connected commutative algebra over a field $\mathbb{F}$, so that $R = \oplus_{d \geq 0} R_d$. Here, of course, R_d denotes the elements of R of degree d, and we are assuming that $R_0 = \mathbb{F}$. Please refer to [**B**] and [**Sm(a)**] as needed.

The Krull dimension is the maximal number of algebraically independent elements in R, denoted here by n.

In our situation, we start with a (fixed representation of a) finite group $G \subset Gl(V)$ for V a vector space of dimension n over a field $\mathbb{F}$ of characteristic $p \geq 0$. We let $\mathbb{F}[V]^G = \{f \in \mathbb{F}[V] \mid \sigma(f) = f, \forall \sigma \in G\}$, denote the ring of invariants, $R = \mathbb{F}[V]^G \subset \mathbb{F}[V]$. We denote the order of G by $|G|$: in this note, we only consider finite groups. The Krull dimension of $\mathbb{F}[V]$ is n.

We denote a monomial $x_1^{i_1} \cdots x_n^{i_n}$ by x^I for the sequence $I = (i_1, \ldots, i_n)$ and we denote its degree by $|I| = i_1 + \cdots + i_n$. We note that the action of G on $\mathbb{F}[V]$ preserves degree, and therefore, in this series of lectures we always consider homogeneous polynomials, that is, $f = \sum_{|I|=d} a_I x^I$, where $a_I \in \mathbb{F}$.

Homogeneous Systems of Parameters. A homogeneous system of parameters for R is a set $\{f_1, \ldots, f_n\}$ with the property that R is finitely generated as an module over $H = \mathbb{F}[f_1, \ldots, f_n]$. Equivalently, $R/(H_+)$ is a (graded) finite dimensional algebra. Here, of course, (H_+) denotes the ideal of R generated by the positive degree elements of H.

The Noether normalization lemma (see [**S(a)**, pg 112]) guarantees that such a homogeneous system of parameters always exists.

If $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$, then $\{f_1, \dots, f_n\}$ is a homogeneous system of parameters if and only if the only common zero of this set over $\bar{\mathbb{F}}$ is $\{0\}$, see [**S(a)**, pg 114]. This is not, in general, all that easy to check. There are, however, some handy homogeneous systems of parameters available. If $\mathbb{F}$ is finite then we may always use the Dickson invariants as a homogeneous system of parameters, see section three. If our group is a permutation group, then the elementary symmetric functions form a homogeneous system of parameters, see section three. If our group is p-group represented over a finite field, then Múi has constructed a homogeneous system of parameters, see section three.

If our group is non-modular, that is, if $|G|^{-1} \in \mathbb{F}$, then there are regular sequences of maximal length n, and any such will form a homogeneous system of parameters. Recall that a sequence $\{f_1, \dots, f_n\}$ is regular if f_i is not a zero divisor in the quotient $R/(f_1, \dots, f_{i-1})$, for each i, $1 \leq i \leq n$. This may be difficult to check.

I note as well that we may form the Jacobian

$$\mathcal{J} = \mathcal{J}(f_1, \dots, f_n) = \det([\frac{\partial f_i}{\partial x_j}]).$$

If $\mathcal{J} \neq 0$ then $\{f_1, \dots, f_n\}$ is algebraically independent. However, this is a weaker condition: if $\mathbb{F}(V)$ denotes the field of fractions of the domain $\mathbb{F}[V]$, and $\mathcal{J}(f_1, \dots, f_n) \neq 0$, then $\mathbb{F}(V)$ is finitely generated over $\mathbb{F}(f_1, \dots, f_n)$ but $\mathbb{F}[V]$ need not be finitely generated over $\mathbb{F}[f_1, \dots, f_n]$. For example, the set $\{x, xy\}$ in $R = \mathbb{F}[x, y]$ has non-zero Jacobian, but R is not finite as a module over $\mathbb{F}[x, xy]$. However, it is easy to check whether or not the Jacobian is non-zero, and so its computation may be used to rule out certain sequences. See Benson, [**B**, pg 64] for more details.

Finally, we note that there is a construction due to Dade which provides a homogeneous system of parameters all of degrees less than $|G|$ provided the field is infinite. If the field is finite, we may extend the coefficients to $\bar{\mathbb{F}}$, use Dade's argument and then restrict to a finite extension of the original field. The construction can be found in Stanley's paper [**S**].

The Poincaré series. We define the Poincaré series of R as

$$P(R, t) = \sum_{i \geq 0} \dim_{\mathbb{F}}(R_i) t^i.$$

This series is sometimes called the Hilbert series of R as well.

Suppose $R = \mathbb{F}[h_1, \ldots, h_n]$ is a polynomial algebra on generators of degrees d_i. Then

$$P(R, t) = \prod_{i=1}^{n} \frac{1}{(1 - t^{d_i})}.$$

This is apparent when we consider that

$$\frac{1}{1 - t^d} = 1 + t^d + t^{2d} + \cdots + t^{md} + \cdots .$$

Suppose R is a free module over $H = \mathbb{F}[h_1, \ldots, h_n]$ on generators f_i, of degrees m_i, $i = 1, \ldots, r$. Then

$$P(R, t) = \frac{t^{m_1} + \cdots + t^{m_r}}{\prod_{i=1}^{n}(1 - t^{d_i})}.$$

Structures. If R is free over one homogeneous system of parameters, then it is free over all such, and we say that R is *Cohen-Macaulay.*

Because we can average polynomials over the group, it can be shown that all non-modular groups have Cohen-Macaulay rings of invariants. In more detail, we can form the *trace* or *transfer* map

$$\mathrm{Tr} : \mathbb{F}[V] \to \mathbb{F}[V]^G$$

by the rule $\mathrm{Tr}(f) = \sum_{\sigma \in G} \sigma(f)$. The transfer is a map of $\mathbb{F}[V]^G$-modules, and if G is a non-modular group, then the transfer is onto. This is false for modular groups, but there is still a lot of information imbedded in the image of the transfer, and the map is the subject of a fair amount of current research.

It seems to be rare that modular groups have Cohen-Macaulay rings of invariants, you'll read more about this later on.

You know what is meant if R is a polynomial algebra. If R is generated by $n+1$ elements then we say R is a *hypersurface.* If R/H_+ is a Poincaré duality algebra, then R is said to be *Gorenstein.* If R is a quotient of a polynomial algebra by the ideal generated by a regular sequence, then we say R is a *complete intersection algebra.*

All of these definitions deserve much fuller exploration, but we won't have space for much.

Resolutions by means of syzygies. We let $Q(R)$ denote the vector space of indecomposables R/R_+^2. Any lift of any basis for R determines a minimal generating set for R as an algebra.

Let $\{f_1, \ldots, f_s\}$ denote a minimal algebra generating set for R. Let $A = \mathbb{F}[z_1, \ldots, z_s]$ denote the polynomial algebra on generators z_i of degree $|f_i|$ and ρ the obvious map from A to R. The map ρ provides R with the structure of an A-module. A resolution of R as an A-module is called a resolution of R by means of syzygies. The resolution has length at most s. If R is Cohen-Macaulay then the resolution has length exactly $s - n$.

$$0 \to M_s \to \cdots \to M_1 \to A \to R \to 0.$$

We note that

$$P(R,t) = \sum_{i=0}^{s-n} (-1)^i P(M_i, t).$$

Since A is a polynomial algebra, we have that $P(A) = \prod_{i=1}^{s} \frac{1}{(1-t^{|f_i|})}$. And, as a free A-module, $M_i = \oplus_{j=1}^{k} A\phi_j$ for some $\{\phi_j \in M_i\}$ of degrees m_j. Therefore, $P(M_i,t) = t^{m_1} + \cdots + t^{m_r} / \prod_{i=1}^{s}(1 - t^{|f_i|})$.

Molien's Theorem. Suppose $|G|^{-1} \in \mathbb{F}$, that is, G is a non-modular group. Elements of representation theory give us a complex representation of G which shares the same Poincaré series as $\mathbb{F}[V]^G$, see [**Si**, pg 504]. Over the complex numbers, the elements of character theory give us the following.

Theorem. (Molien)

$$P(\mathbb{F}[V]^G, t) = \frac{1}{|G|}(\sum_{g \in G} \frac{1}{\det(1 - tg)})$$

As an example, we note that any permutation g of n variables is a product of cycles $g_{i_1} \cdots g_{i_k}$. Here I mean that g_{i_j} is a cycle of length i_j. It can be shown that $\det(1 - tg) = \prod_{j=1}^{k}(1 - t^{i_j})$.

As a further example, if g has eigenvalues $\lambda_1, \ldots, \lambda_n$ then

$$det(1 - tg) = \prod_{i=1}^{n}(1 - \lambda_i t).$$

Construction of invariants. Given $G \subset Gl(V)$ and an element $f \in \mathbb{F}[V]$ we define the *G-orbit* of f, to be $\{g(f) \mid g \in G\}$ denoted $\mathcal{O}_G(f)$. A slightly different way to define the orbit of f is to define $Stab_G(f) = \{g \in G \mid g(f) = f\}$. Then $\mathcal{O}_G(f) = \{g(f) \mid g \in G/Stab_G(f)\}$. Here $G/Stab_G(f)$ denotes a set of coset representatives.

Suppose, then, that $|\mathcal{O}_G(f)| = m$. From here, we can form the polynomial

$$\mathcal{P}_f(t) = \prod_{h \in \mathcal{O}_G(f)} (t - h) = \sum_{i=0}^{m} (-1)^i s_i t^{m-i},$$

where $s_i \in \mathbb{F}[V]^G$. The coefficients are elementary symmetric functions in the elements of $\mathcal{O}_G(f)$. That is, if we write $\mathcal{O}_G(F) = \{f_1, \ldots, f_m\}$, then

$$\begin{aligned} s_1 &= f_1 + \cdots f_m,\ s_2 = f_1 f_2 + \cdots f_{m-1} f_m, \ldots, \\ s_m &= f_1 \cdots f_m. \end{aligned}$$

Smith [**S(a)**] refers to the invariants so constructed as orbit Chern classes.

3. Examples.

Suppose $G = C_2$ acts on $V^* = \langle x, y \rangle$ by

$$\{I_2 = [\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}],\ g = [\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}]\}.$$

We observe that we have $g(x^i y^j) = x^j y^i$. In particular, $(xy)^i$ is invariant. If $i \neq j$ then $x^i y^j + x^j y^i$ is invariant. This suggests that if $i = j + k$ then we write

$$\begin{aligned} x^i y^j + x^j y^i &= (xy)^j (x^k + y^k) \\ &= (xy)^j (x+y)^k + \text{ other terms.} \end{aligned}$$

It isn't difficult to show from here that

$$\mathbb{F}[V]^G = \mathbb{F}[x+y, xy].$$

This is the best possible situation in invariant theory, in which the ring of invariant polynomials is again polynomial algebra. We see from this calculation, or from Molien's theorem, that

$$P(\mathbb{F}[V]^G, t) = \frac{1}{(1-t)(1-t^2)}.$$

Hand Calculations. Suppose G acts on $V^* = \langle x, y \rangle$ by the matrices $\{[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}],\ g = [\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}]\}$. We note that $g(x^i) = (-1)^i x^i$ so that x^i is invariant if and only if $i = 2j$. Similarly, y^i is invariant if and only if $i = 2j$. We have $x^{2j} = (x^2)^j$. Moreover, we observe that $g(x^i y^i) = x^i y^i$ is invariant.

It isn't hard to prove from here that $\mathbb{F}[V]^G = \mathbb{F}[x^2, y^2, xy]$. There are a variety of ways we can parse this, One view is that

$$\mathbb{F}[V]^G \cong \mathbb{F}[a, b, c]/(c^2 - ab)$$

where $|a| = |b| = |c| = 2$. In another, we observe that $\{x^2, y^2\}$ forms homogeneous system of parameters for $\mathbb{F}[V]^G$, and that $\mathbb{F}[V]^G$ is a free module over $H = \mathbb{F}[x^2, y^2]$ on the basis $\{1, xy\}$.

Q What is the Poincaré series of this ring of invariants?

Example: Calculations in Magma. Magma is a computer program that is, at the moment, the language of choice of the Invariant Theory Group at Queen's. It incorporates algorithms due to Gregor Kemper and others. Here is an excerpt from a Magma session that computes the example of Bertin. The example itself is important in the history of commutative algebra as the first example of a unique factorization domain which was not Cohen-Macaulay, answering a question of Kaplansky.

In what you read below, you will find the user input next to the

```
>
```

prompt, and the replies from Magma without such a prompt. Most of the Magma commands are self-explanatory. However, the reader should know that the command *PrimaryInvariants* computes a homogeneous system of parameters, while *SecondaryInvariants* computes a set of module generators for the ring of invariants over the polynomial algebra generated by the homogeneous system. The command *TotalDegree* reports on the degrees of the polynomials in the set given as its argument, while *FundamentalInvariants* computes a minimal generating set for the ring of invariants as an algebra.

```
[eddy@noether]$magmaV2.5

Magma V2.5-1       Mon Nov  1 1999 08:09:07

[Seed = 1416756397] Type ? for help.
Type <Ctrl>-D to quit.
> G := MatrixGroup<4,GF(2) |
[0,1,0,0, 0,0,1,0, 0,0,0,1, 1,0,0,0] >;
> #G;
4
> R := InvariantRing(G);
> time prim := PrimaryInvariants(R);
Time: 0.019
> [TotalDegree(f): f in prim];
[ 1, 2, 2, 4 ]
> S<x,y,z,w> := PolynomialRing(R);
> prim;
[
    x + y + z + w,
    x*y + x*w + y*z + z*w,
    x*z + y*w,
    x*y*z*w
]
> time sec := SecondaryInvariants(R);
Time: 0.029
> [TotalDegree(f): f in sec];
[ 0, 3, 3, 4, 5 ]
> IsCohenMacaulay(R);
false
> time fun := FundamentalInvariants(R);
Time: 0.000
> [TotalDegree(f): f in fun];

[ 1, 2, 2, 3, 3, 4, 4, 5 ]
```

Symmetric Functions. Consider $G = \Sigma_n \subset Gl(V)$ acting as all permutations of a basis $\{x_1, \dots, x_n\}$ for V^*. We note that $\mathcal{O}_G(x_1) = \{x_1, \dots, x_n\}$ and that $\mathcal{P}_{x_1}(t) = \prod_{i=1}^n (t - x_i) = \sum_{j=0}^n (-1)^j s_j t^{n-j}$. Here, the s_j is the j-th elementary symmetric function

$$s_j = x_1 x_2 \cdots x_j + \cdots + x_{n-j+1} x_{n-j+2} \cdots x_n.$$

Of course, the elementary symmetric functions enjoy many beautiful properties, and symmetric functions occur in many different situations in mathematics.

Exercise Prove that $\{s_1, \dots s_n\}$ are algebraically independent, and hence that $\mathbb{F}(s_1, \dots, s_n)$ has transcendence degree n.

Now we note that $\mathbb{F}(V)^G \subset \mathbb{F}(V)$ is a Galois extension, with Galois group G, hence of transcendence degree $|G| = n!$. Further,

$$\mathbb{F}(s_1, \dots, s_n) \subset \mathbb{F}(V)$$

has transcendence degree $\prod_{i=1}^n |s_i|$. Therefore, $\mathbb{F}(s_1, \dots, s_n) = \mathbb{F}(V)^G$. However, a polynomial algebra is integrally closed and hence

$$\mathbb{F}[s_1, \dots, s_n] = \mathbb{F}[V]^G.$$

The paragraph just above provides a general template for proving that rings of invariant are polynomial algebras, if, in fact, they are.

Of course, this is far from the end of the story. For example, given a symmetric function, how can it be written in terms of the elementary symmetric functions? As well, there are other generating sets for the symmetric functions, for example, the power sums

$$h_i = x_1^i + \dots x_n^i,$$

for $1 \leq i \leq n$. The sum of all monomials of a given degree d is called the complete symmetric function of degree d. There is great fun to be had in trying to understand how to rewrite symmetric functions expressed in one way or another in a different way.

The Alternating groups. We study A_n the sub-group of Σ_n consisting of all even permutations. We know that an alternating function is the sum of a symmetric function together with a symmetric function times the discriminant. Here the discriminant may be described as

$$\Delta_n = \prod_{1 \leq i < j \leq n} (x_j - x_i),$$

if $p = 0$ or if $p > 2$. Otherwise take the orbit sum of $x_1^{n-1}x_2^{n-2} \cdots x_{n-1}$.

In modern language, we have

$$\mathbb{F}[V]^{A_n} = \mathbb{F}[V]^{\Sigma_n} \oplus \mathbb{F}[V]^{\Sigma_n}\Delta.$$

Hence, $\mathbb{F}[V]^{A_n}$ is generated by $n+1$ elements as an algebra, and so $\mathbb{F}[V]^{A_n}$ is a hypersurface. It is easy to see that Δ^2 is invariant under Σ_n when $p = 0$ or $p > 2$.

All of this is nicely described in [**S(a)**, pg 10].

For now we note that we have two Galois extensions

$$\mathbb{F}(v)^{\Sigma_n} \subset \mathbb{F}(V)^{A_n} \subset \mathbb{F}(V).$$

The one on the right has Galois group A_n, hence has transcendence degree $|A_n|$. The Galois group from one end to the other is $|\Sigma_n| = n!$. Further, the index $[\Sigma_n : A_n] = 2$, and we have $\mathbb{F}(V)^{\Sigma_n}[\Delta^{\pm 1}]$ has degree two as an extension of the field of fractions of the ring $\mathbb{F}[V]^{\Sigma_n}$. Therefore $\mathbb{F}(V)^{\Sigma_n}[\Delta^{\pm 1}] = \mathbb{F}(V)^{A_n}$.

Exercise. Prove $\mathbb{F}(V)^{\Sigma_n}[\Delta^{\pm 1}] = \mathbb{F}(V)^{A_n}$ implies $\mathbb{F}[V]^{A_n} = \mathbb{F}[V]^{\Sigma_n} \oplus \mathbb{F}[V]^{\Sigma_n}\Delta$.

This kind of argument will work more generally for Cohen-Macaulay rings.

Invariants of Permutation Groups. Suppose $G \subset \Sigma_n \subset Gl(V)$. That is, G is a permutation group. A key observation is that every element of G takes monomials to monomials. Therefore, given a monomial x^I, we form the orbit sum $s(I) = \sum_{g \in G/Stab_G(x^I)} g(x^I)$.

Lemma. *The orbit sums $s(I)$ of degree d form a basis for $\mathbb{F}[V]^G_d$.*

Proof. Any $f \in \mathbb{F}[V]$ may be written as sum of monomials $f = \sum_{|I|=d} a_i x^I$. But for any $g \in G$ we have $g(f) = \sum a_I g(x^J)$. It follows that, if f is G-invariant and $x^J \in \mathcal{O}_G(x^I)$, then $a_J = a_I$. The result is immediate. ♠

Corollary. *The Poincaré series of $\mathbb{F}[V]^G$ depends only on $G \subset \Sigma_n$ and not on the field $\mathbb{F}$.*

Theorem. *(Göbel) If G is a permutation group then $\mathbb{F}[V]^G$ is generated in degrees less than or equal to* $\binom{n}{2}$.

Key idea. We say that a sequence I has no 2-gaps if the entries of I, *viewed as a set*, are consecutive, and include 0. We can show that any invariant of the form $s(I)$ where the entries of I are not consecutive, or are all positive, can be decomposed — shown to be a sum of product of elements of smaller degree — by subtracting 1's from every entry above the largest gap. Here are some of the details.

Proof. We are going to induct on the following order. Given an exponent sequence, I, of degree d, we think of I as a partition of d and write $\lambda(I) = (\lambda_0(I), \lambda_1(I), \ldots, \lambda_d(I))$ where λ_i is the number of entries of I equal to i. We compare exponent sequences I and J of the same degree by the lexicographic order on $\lambda(I)$ and $\lambda(J)$ from right to left, that is, by comparing the number of largest entries, and if they are equal, the number of next largest entries, and so on. Note that any two sequences of the same size in this order are permutations of each other.

In this notation, a sequence I has no 2-gaps if $\lambda_0(I) \neq 0$ and if $\lambda_{\ell+1}(I) \neq 0$ implies $\lambda_\ell(I) \neq 0$.

A stronger version of the theorem is that the sequences $s(I)$ with no 2-gaps, together with $s(1,\ldots,1)$, generates $\mathbb{F}[V]^G$. The version given here follows when we note that a sequence of largest degree with no 2-gaps is

$$(n-1, n-2, \ldots, 2, 1, 0).$$

Let $A \subset \mathbb{F}[V]^G$ denote the subalgebra generated by all elements $s(I)$ with no 2-gaps, together with $s(1,\ldots,1)$. We wish to show that, if I is a sequence with a 2-gap, then $s(I) \in A$. The argument given below can be used to start the induction, but the details are omitted.

Let r denote the largest 2-gap in I, that is, there is no entry of I equal to r, but there is at least one entry of I equal to $r+1$, and r is the largest integer with this property. That is, we assume that r is the largest integer with $\lambda_r(I) = 0$ and $\lambda_{r+1} \neq 0$.

Let K denote the sequence which has a 1 wherever I has an entry bigger than r and 0's elsewhere. Let $J = I - K$. We observe that $Stab_G(J) \subset Stab_G(K)$, although, to my amazement, we don't need this observation.

Consider the product $s(J)s(K)$. We observe that the exponent sequences which arise in this product are of the form $\sigma(J) + \tau(K)$. We show that $s(I)$ occurs with coefficient 1 in the product and, simultaneously, that $\sigma(J) + \tau(K)$ is smaller than I in our order, provided

$\sigma(J)+\tau(K) \notin \mathcal{O}_G(I)$. Suppose then, that $I = \sigma(J)+\tau(K)$, for some σ, and $\tau \in G \subset \Sigma_n$.

Now I has largest entries k in certain places, and therefore $\sigma(J)$ must have entries $k-1$ in those same places, and $\tau(K)$ must have 1's in those same places, or $\sigma(J)+\tau(K)$ will be smaller than I in our order. The same argument also applies in turn to those places where I has entries $k-1,\ldots,r+1$. But our argument shows that $\sigma(J)=J$ and $\tau(K)=K$, but this cannot happen for non-trivial σ and τ. ♠

The Dickson Invariants. Suppose $\mathbb{F}$ is a finite field of order $q=p^s$. Then consider $G=\mathrm{Gl}(V)$. Then any vector $v \in V^* \setminus \{0\}$ has $\mathcal{O}_G(v) = V^* \setminus \{0\}$. Now we obtain

$$\mathcal{P}_v(t) = \prod_{w \in \mathcal{O}_G(v)} (t-w) = \sum_{i=0}^{n} (-1)^{n-i} d_{i,n} t^{q^{n-i}}.$$

The $d_{i,n}$ are known as the Dickson invariants, and they enjoy many beautiful properties.

For example, when $p=2$ and $n=2$ we have

$$\mathcal{P}_v(t) = t(t+x)(t+y)(t+x+y)$$

so that $d_{1,2} = x^2+xy+y^2$ and $d_{2,2} = xy(x+y) = x^2y+xy^2$.

Exercise Develop recursive formulae for the Dickson invariants. That is write $d_{i,n}$ in terms of $d_{i,n-1}$ and x_n.

For now we note that $|d_{i,n}| = q^n - q^{n-i}$. Therefore, we have $\prod_{i=1}^{n} |d_{i,n}| = |\,\mathrm{Gl}(V)|$.

This latter calculation is very pretty. There are q^n vectors in V, and any one of them may be identified with the first row of a matrix in $\mathrm{Gl}(V)$ excepting the zero vector. Hence there are q^n-1 choices for the first row. Similarly, the second row corresponds to vectors in V that are linearly independent of the first, and there are q^n-q choices for these. And so on.

Exercise Prove that $\{d_{1,n},\ldots,d_{n,n}\}$ are algebraically independent. Carry on with an argument similar to the one given for the symmetric groups to show that $\mathbb{F}[d_{1,n},\ldots,d_{n,n}] = \mathbb{F}[V]^G$.

Upper Triangular Invariants. Suppose $\mathbb{F}_q$ is a finite field of order $q=p^s$. Consider $G=U_n(\mathbb{F}_q)$, the group of upper triangular matrices with 1's along the diagonal acting on V^* with respect to the basis $\{x_1,\ldots,x_n\}$. Note that $\mathcal{O}_G(x_i) = x_i + V_{i-1}$ where V_{i-1} denotes the subspace of V^* with basis $\{x_1,\ldots,x_{i-1}\}$. Therefore, we define

$$h_i = \prod_{v \in V_{i-1}} (x_i+v).$$

Note that the degree of h_i is q^{i-1}. Therefore, $\prod_{i=1}^{n} |h_i| = |U_n(\mathbb{F})|$.

When $p = 2$, we get $h_1 = x$, $h_2 = y(y+x) = y^2 + xy$. For arbitrary p, we have $h_2 = \prod_{\alpha \in \mathbb{F}_p} (y + \alpha x) = y^p - x^{p-1}y$.

Exercise Carry on with an argument similar to the one just given to show that $\mathbb{F}_q[h_1, \dots, h_n] = \mathbb{F}_q[V]^G$.

Exercise Prove that $U_n(\mathbb{F}_q)$ is a q-Sylow subgroup of $\mathrm{Gl}_n(\mathbb{F}_q)$.

A 2-dimensional representation of C_3, $p = 2$, [B, pg 103.] Suppose G acts on $V^* = \langle x, y \rangle$ by

$$\{I_2,\ g = [\begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}]\},$$

over the field $\mathbb{F}_2$. Note that $|G| = 3$, and, in our conventions, σ acting on $\mathbb{F}_2[V] = \mathbb{F}_2[x, y]$ sends x to y and sends y to $x + y$.

It is straightforward to calculate the ring of invariants for G. First we observe that the Dickson invariants $r = x^2 + xy + y^2, s = x^2y + xy^2$ form, as always, a homogeneous system for $\mathbb{F}_2[V]^G$. Second we observe that G has index 2 in $\mathrm{Gl}_2(\mathbb{F}_2)$, and that $t = x^3 + x^2y + y^3$ is invariant. It isn't hard to see using Galois theory that

$$\mathbb{F}_2[x, y]^G = \mathbb{F}_2[x^2 + xy + y^2, x^2y + xy^2, x^3 + x^2y + y^3],$$

and, therefore, this ring is a hypersurface. As part of this calculation, we note $t^2 = r^3 + s^2 + rs$.

Therefore, we obtain a resolution over the ring $A = \mathbb{F}_2[a, b, c]$ with $|a| = 2$, $|b| = |c| = 3$, and $\rho(a) = x^2 + xy + y^2$, $\rho(b) = x^2y + xy^2$, $\rho(c) = x^3 + x^2y + y^3$. We obtain

$$0 \to A(c^2 + a^3 + b^2 + bc) \to A \to \mathbb{F}_2[x, y]^G \to 0.$$

It follows that

$$\mathcal{P}(\mathbb{F}_2[V]^G, t) = \frac{1 + t^2 + t^4}{(1 - t^3)^2}.$$

4. Lecture on Structures and Fundamental Questions.

There are two sorts of problems to be considered

(1) Find generators for $\mathbb{F}[V]^G$. Failing that, find a bound for the degrees of a generating set.

(2) Determine the structure of $\mathbb{F}[V]^G$. For example, determine for which groups G is $\mathbb{F}[V]^G$ a polynomial algebra, a hypersurface, Gorenstein or Cohen-Macaulay?

Both questions are interesting for either specific groups, or for classes of groups. In general, much more is known when $p = 0$ and in the non-modular case than in the modular case. These differences are the focus of this lecture.

Bounds for Generating Sets. Noether showed that generators of degree at most $|G|$ are required when $p = 0$. For non-modular groups with $p > |G|$, this theorem is still true. Richman, Smith and others have shown Noether's original bound, $|G|$, applies if G is solvable. Smith [**S(a)**, pg 175], Fleischmann [**Fl**], and others have shown that for non-modular groups $\mathbb{F}[V]^G$ is generated in degrees at most $\dim_{\mathbb{F}}(V)(|G|-1)$, see also [**FL**]. Here I need $\dim_{\mathbb{F}}(V) > 1$ and $|G| > 1$.

Up until last fall, it was a conjecture that non-modular groups have rings of invariants that are generated in degrees less than or equal $|G|$. The difference between the known bound and this conjectural bound was known as the problem of Noether's Gap: is there a non-modular group in the gap or not? In the fall of 1999, Peter Fleischmann gave a beautiful and clever variation of Noether's original argument that showed the conjecture was true (see below). Independently, Fogarty proved the same result.

It is proved in [**2**] that if $\mathbb{F}_p[V]^G$ is a hypersurface, then this ring is generated in degrees less than $|G|$ while if $\mathbb{F}_p[V]^G$ is Gorenstein, then the bound $\dim_{\mathbb{F}_p}(V)(|G| - 1)$ applies. More generally, Broer [**Br**] has shown that this latter bound applies if $\mathbb{F}_p[V]^G$ is Cohen-Macaulay.

Kemper conjectures that Noether's bound, $|G|$, applies whenever $\mathbb{F}[V]^G$ is Cohen-Macaulay.

Dade has shown that there exists a homogeneous system of parameters all of whose generators may be taken to be either from V^G or of degree $|G|$. This may involve a finite extension of the original field. Then $\dim_{\mathbb{F}}(V/V^G)(|G| - 1)$ is the degree of a top *module* generator of $\mathbb{F}[V]^G$ over this homogeneous system of parameters. In general, one would expect to find algebra generators in degrees somewhat less than this. However, there are examples where the bound $\dim_{\mathbb{F}}(V/V^G)(|G| - 1)$ is sharp (see below).

There is no explicit bound for modular groups known. It is easy to see that there is a bound that depends on $\dim_{\mathbb{F}}(V)$ and q, for $\mathrm{Gl}_n(\mathbb{F}_q)$ is a finite group, hence has finitely many subgroups, hence there are finitely many rings of invariants to be calculated, for any given n and q.

Fleischmann on non-modular groups. Suppose $G = \{g_1, \ldots, g_k\}$ is a non-modular group. Consider the vector space Z with basis

$$\{z_{ij} \mid 1 \leq i \leq n,\ 1 \leq j \leq k\},$$

together with the map $\rho : Z \to V$ defined by $\rho(z_{ij}) = g_j x_i$. We extend to a map

$$\mathbb{F}[Z] \to \mathbb{F}[V].$$

Note that G acts on Z by permuting the columns of the matrix z_{ij} in the obvious way, via the regular representation of G. This is the original construction of Emmy Noether.

We obtain $\rho : \mathbb{F}[Z]^{\Sigma_k} \to \mathbb{F}[V]^G$. For $f \in \mathbb{F}[V]$ we may define $a_j(z_{1j}, \ldots, z_{nj}) = f(z_{1j}, \ldots, z_{nj})$, with $\rho(a_j) = g_j f(x_1, \ldots, x_n)$. Therefore, if $f \in \mathbb{F}[V]^G$ we have $\frac{1}{k}\rho(\sum a_j) = f$. Further, $\sum a_j$ is the orbit sum of a_j over Σ_k.

Fleischmann's proof works as follows.

First, note that a_j is concentrated in a single "row" of the matrix z_{ij}.

He shows that the orbit sums of such row polynomials may be written as sums of products of the form ab where a is in $\mathbb{F}[Z]^{\Sigma_k}$, has positive degree, and is a product of invariants of degree less than or equal to k, and b is in $\mathbb{F}[Z]$.

Therefore, $f \in \mathbb{F}[V]^G$ may be written as a sum of terms of the form ab where $a \in \mathbb{F}[V]^G$ has positive degree, is a product of invariants of degree less than or equal to k, and $b \in \mathbb{F}[V]$.

But $\frac{1}{k}\operatorname{Tr}_G(f) = \frac{1}{k}\sum_{i=0}^{k} g_i(f) = f$, for $f \in \mathbb{F}[V]^G$. Applying the trace to each of the terms ab gives the result.

Vector Invariants. Consider the coordinate ring of $mV = V^{\oplus m}$ with the diagonal action of G. The ring $\mathbb{F}[mV]^G$ is called the ring of vector invariants of G, a terminology used by Weyl. Rings of vector invariants provide an important class of examples and counterexamples.

Hughes and I in [**6**] give generators, as conjectured by Richman [**R**], for $\mathbb{F}_p[mV]^{C_p}$ where C_p denotes the cyclic group of order p, and V denotes its 2-dimensional indecomposable representation. An easy corollary is the fact, first observed by Richman, that this invariant ring requires a generator of degree $m(p-1)$. Therefore, Noether's bound does not hold for p-groups, and the bound $\dim_{\mathbb{F}_p}(V/V^G)(|G|-1)$ is sharp in this example.

If G is a p-group and $m \geq 3$ then $\mathbb{F}_p[mV]^G$ cannot be Cohen-Macaulay, see [**2**]. Kemper has proved that, if G is any modular group, then $\mathbb{F}_p[mV]^G$ is not Cohen-Macaulay for all sufficiently large m. We know of no examples where "sufficiently large" is bigger than 3.

As an example of the kind of argument used here, consider $\mathbb{F}_p[3V_2] = \mathbb{F}_p[x_1, y_1, x_2, y_2, x_3, y_3]$ with an action of $\sigma(x_i) = x_i$ and $(y_i) = y_i + x_i$. We note that $u_{ij} = \left|\begin{smallmatrix} x_i & x_j \\ y_i & y_j \end{smallmatrix}\right| = x_i y_j - x_j y_i$ is invariant. Further, we have that the matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix}$$

has zero determinant, since two rows are equal, and, on the other hand, is equal to $x_1 u_{23} - x_2 u_{13} + x_3 u_{12}$. At Queen's, we call this the equation of the three amigos, and with a little work, it can be used to show that the ring in question is not Cohen-Macaulay. Generalizations of it are used in the papers listed above.

If we consider now $\mathbb{F}_p[mV_2] = \mathbb{F}_p[x_i, y_i \mid 1 \leq i \leq m]$ with the action of C_p described above, then we find, after a great deal of hard work (see **[6]**), that $\mathbb{F}_p[mV_2] = \mathbb{F}_p[x_i, N(y_i), u_{ij}, \mathrm{Tr}(m) \mid m|(y_1 \cdots y_m)^{p-1}]$. Of course, this ring is far from Cohen-Macaulay, but at least this collection of invariants appears to be understandable.

Kemper has also proved that, if G is a p-group and $\mathbb{F}_p[V]^G$ is Cohen-Macaulay, then G is generated by elements that fix a subspace of codimension at most 2 (such elements are known as *bi-reflections*). This theorem shows us how rarely we may expect to encounter Cohen-Macaulay rings as the invariants of p-groups.

On the Structure of $\mathbb{F}[V]^G$: classical results. The invariant theory of finite groups is much better understood in the non-modular case.

For example, in this situation, it is a famous and beautiful theorem that $\mathbb{F}[V]^G$ is a polynomial algebra if and only if G is generated by pseudo-reflections (Shephard-Todd, Chevalley, Serre, Clark-Ewing, Steinberg, Kane).

There are other beautiful and wonderful theorems concerning characterizations of hyper-surfaces (Nakajima), Gorenstein (Watanabe), or Cohen-Macaulay (Hochster and Eagon) in the non-modular case.

Structure of $\mathbb{F}[V]^G$: modular case. It is known (Serre) that groups with polynomial rings of invariants must be pseudo-reflection groups, and many groups are known to have polynomial rings of invariants — the symmetric groups, and the parabolic groups.

Nakajima has characterized those p-groups with polynomial rings of invariants when $\mathbb{F} = \mathbb{F}_p$. Roughly speaking, he shows that such groups resemble the ring of invariants of the Upper Triangular group, the last example of section 3. He gave examples of elementary Abelian reflection p-groups with non-Cohen-Macaulay invariant rings, a somewhat simpler example is given below. Nakajima's characterization fails over larger fields, as shown by an example due to Stong, see below.

Roughly speaking, Nakajima's characterization is as follows. Let G be a p-group represented over the finite field $\mathbb{F}_p$ on a vector space, V, of dimension n. Since $U_n(\mathbb{F}_p)$ is a p-Sylow subgroup of $\mathrm{Gl}_n(\mathbb{F}_p)$, we may find a basis for V with respect to which G is a subgroup of $U_n(\mathbb{F}_p)$. The theorem asserts that $\mathbb{F}_p[V]^G$ is a polynomial algebra if and only if there is a (upper triangular) basis $\{x_1, \ldots, x_n\}$ of V with respect to which G "stands up straight", that is, for each generating pseudo-reflection of G, there is a basis element of V, say x_i, such that σ fixes the hyperplane spanned by $x_1, \ldots, \hat{x}_i, \ldots, x_n$, where $\hat{x}_i$ indicates x_i has been deleted. Then we have that $\sigma(x_i) = x_i + v$ where v is a vector in the span of $x_1, \ldots, x_{i-1}$. The implication $\Leftarrow$ is easy, but the other direction is much harder.

Kemper and Malle have examined the class of irreducible representations of modular pseudo-reflection groups and determined which have polynomial rings of invariant. Unfortunately, irreducible representations are few and far between.

Much work remains to be done on characterizing groups with polynomial rings of invariants.

A cautionary tale concerning p-groups. Consider the group

$$G = \{ \begin{pmatrix} 1 & 0 & \alpha+\gamma & \gamma \\ 0 & 1 & \gamma & \beta+\gamma \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid \alpha,\ \beta,\ \gamma \in \mathbb{F}_p\}.$$

Our convention is that G acts on V^* with basis $\{x_1, x_2, y_1, y_2\}$ with x_1 and x_2 as fixed points. Then G has order p^3. Let H be the subgroup of G of order p^2 determined by the elements with $\gamma = 0$. Both G and H, of course, are elementary Abelian groups generated by pseudo-reflections (elements that fix a hyperplane). However, only H is a Nakajima group.

Let $N_i(y_i) = y_i - x_i^{p-1} y_i$ for $1 \leq i \leq 2$. It isn't hard to see that

$$\mathbb{F}_p[V]^H = \mathbb{F}_p[x_1, x_2, N(y_1), N(y_2)].$$

Further, since H is normal in G, we have an action of $G/H = C_p$ on $\mathbb{F}_p[V]^H$.

We let

$$\sigma = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and we calculate $\sigma(N_1(y_1)) = N_1(y_1) - N_1(x_2)$, and $\sigma(N_2(y_2) = N_2(y_2) - N_2(x_1)$. From here we can construct three new invariants:

$$\begin{aligned} &N_1(y_1)^p - N_1(x_2)^{p-1}N_1(y_1), \\ &N_2(y_2)^p - N_2(x_1)^{p-1}N_2(y_2) \\ &\text{and} \\ &N_1(x_2)N_2(y_2) - N_2(x_1)N_1(y_1). \end{aligned}$$

It can be shown without a great deal of difficulty that $\mathbb{F}_p[V]^G$ is the hypersurface generated by these three invariants together with x_1 and x_2.

Stong's example. We work over the field $\mathbb{F}_q$ with $q = p^3$. We may suppose the field has basis over $\mathbb{F}_p$ consisting of $\{1, \omega, \mu\}$. Let H be the group generated by the matrices

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and let G be the group generated by H and the matrix

$$\sigma = \begin{pmatrix} 1 & \omega & \mu \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

with respect to the basis $\{x, y, z\}$ of V^*. We note that both groups are generated by psuedo-reflections, but that G is not a "Nakajima" group, since we cannot choose a basis with respect to which each generating pseudo-reflection is concentrated in a single column.

It is not hard to see that $\mathbb{F}_q[V]^H = \mathbb{F}_q[x, N(y), N(z)]$, where $N(t) = t^p - x^{p-1}t$. We calculate $\sigma(N(y)) = N(y) - (\omega^p - \omega)x^p$, and $\sigma(N(z)) = N(z) - (\mu^p - \mu)p$. From here we can construct two G invariants $f_1 = (\mu^p - \mu)N(y) - (\omega^p - \omega)N(z)$ and $f_2 = N(y)^p - (\omega^p - \omega)^{(p-1)}n(y)x^{p(p-1)}$. It isn't hard to see that these form a homogeneous system of parameters, and that $\mathbb{F}_q[V] = \mathbb{F}_q[x, f_1, f_2]$.

5. Lecture on the cyclic group of order p over $\mathbb{F}_p$

There are p indecomposable representations of C_p over $\mathbb{F}_p$, one of dimension n for each n less than or equal p. We have a tower $V_1 \subset V_2 \subset \cdots \subset V_p$, and the matrix of the generator for V_n^* may be taken to be the $n \times n$ matrix

$$\sigma = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

It isn't hard to compute the rings of invariants associated to the three lowest dimensional representations. The first two are polynomial on "top" Chern classes of the basis elements (use the basis assumed above) and the third is a hypersurface. Shank [**Sh**] has given algebra generators for the rings of invariants associated to the four and five dimensional representations. Also, using techniques and results of Almqvist and Fossum, it can be shown that *any* representation V of C_p has its invariant ring generated in degrees less than or equal $\dim_{\mathbb{F}_p}(V)(p-1)$. Kemper and Hughes have a very nice paper about this.

We conjecture that the rings of invariants of all representations of C_p are generated by elements we call norms, traces and rational invariants. This latter class of invariants is obtained from certain classical invariants of binary forms studied by Hilbert and others working in the last century. We must show that the invariants of degree less than p are either traces or rational invariants. While this result seems to be in reach, we haven't yet proved it.

Conjectures about Modular Groups. Do norms, traces and rational invariants form a generating set for the invariant rings of all p-groups? Well, there are cohomology classes as well. I hope to say something about this at the end of the lecture.

I (and many others!) conjecture that modular groups are generated in degrees less than or equal to

$$\dim_{\mathbb{F}_p}(V/V^G)(|G|-1).$$

Of course, this bound is known to hold in all known examples, provided, of course, that $\dim_{\mathbb{F}_p}(V) > 1$ and $|G| > 1$.

Generators for p-Groups? Take N to be a normal subgroup of a p-group G with quotient group $G/N \simeq C_p$. Then $\mathbb{F}_p[V]^G = (\mathbb{F}_p[V]^N)^{C_p}$.

Suppose that we know $\mathbb{F}_p[V]^N = \mathbb{F}_p[f_1, \dots, f_r]$, perhaps by induction. Let $A = \mathbb{F}_p[z_1, \dots, z_r]$ mapping onto $\mathbb{F}_p[V]^N$ by the rule $z_i \longrightarrow f_i$, with kernel the ideal I. Suppose that C_p acts on A. This need not happen, and there may be a paper subsequent to this one in which this issue is explored.

Write $\Delta = 1 - \sigma$ and $\mathrm{Tr} = \sum_{i=0}^{p-1} \sigma^i$ where σ a generator of C_p. Because $\mathrm{Tr} = \Delta^{p-1}$, we obtain a resolution of $\mathbb{F}_p$ as the trivial module over the group ring $\mathbb{F}_pC_p$ as follows:

$$\dots \to \mathbb{F}_pC_p \xrightarrow{\Delta} \mathbb{F}_pC_p \xrightarrow{\mathrm{Tr}} \mathbb{F}_pC_p \to \cdots \to \mathbb{F}_pC_p \xrightarrow{\Delta} \mathbb{F}_pC_p \xrightarrow{\epsilon} \mathbb{F}_p,$$

where $\epsilon : \mathbb{F}_pC_p \to \mathbb{F}_p$ is defined by $\epsilon(\sum_{i=0}^{p-1} \alpha_i \sigma^i) = \sum_{i=0}^{p-1} \alpha_i$.

Then we have exact sequences of C_p-modules

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] & A \arrow[r] & \mathbb{F}_p[V]^N \arrow[r] & 0 & & \\
0 \arrow[r] & I^{C_p} \arrow[r] \arrow[u, phantom, "\cup"] & A^{C_p} \arrow[r] \arrow[u, phantom, "\cup"] & \mathbb{F}_p[V]^G \arrow[r] \arrow[u, phantom, "\cup"] & H^1(C_p, I) \arrow[r] & H^1(C_p, A) \arrow[r] & \dots
\end{tikzcd}$$

Hence the problem of determining elements of $\mathbb{F}_p[V]^G$ not determined by A^{C_p} amounts to understanding the right-hand side of the long exact sequence above. Of course, because of the periodic nature of the resolution of $\mathbb{F}_p$, we have

$$H^0(C_p, M) = \mathrm{Kernel}(M \xrightarrow{\Delta} M) = M^{C_p}$$

$$H^1(C_p, M) = \frac{\mathrm{Kernel}(M \xrightarrow{Tr} M)}{\mathrm{Im}(M \xrightarrow{\Delta} M)} = H^{\mathrm{odd}}(C_p, M)$$

$$H^2(C_p, M) = \frac{\mathrm{Kernel}(M \xrightarrow{\Delta} M)}{\mathrm{Im}(M \xrightarrow{Tr} M)} = H^{\mathrm{even}}(C_p, M)$$

Now the cohomology of C_p-modules is well understood. In particular, let's try and understand $H^*(C_p, V_n)$ for V_n an indecomposable representation of C_p. Let us denote a basis for V_n^* by $\{x_1, \dots, x_n\}$ and note that $\Delta(x_i) = x_{i-1}$ for $1 < i \leq n$, $\Delta(x_1) = 0$, and, therefore, that $\mathrm{Tr}(x_i) = 0$ for $1 \leq i < p$, and $\mathrm{Tr}(x_p) = x_1$.

We have that $x_i \in \mathrm{Im}(\Delta)$ for $1 \leq i < n$. Further, we have $\mathrm{Im}(\mathrm{Tr}) = 0$ for $n < p$ and $\mathrm{Im}(\mathrm{Tr}) =< x_1 >$, for $n = p$. Finally, $H^0(C_p, V_i) = V_i^{C_p} =$

$\mathbb{F}_p$ on the cohomology class associated to x_1. Putting all of this together we obtain

$$\begin{aligned}
&H^0(C_p, V_n) = \mathbb{F}_p, \text{ on the class associated to } x_1\\
&H^1(C_p, V_p) = 0 = H^2(C_p, V_p)\\
&H^1(C_p, V_n) = \mathbb{F}_p, \; n < p, \text{ on the class associated to } x_n\\
&H^2(C_p, V_n) = \mathbb{F}_p, \; n < p, \text{ on the class associated to } x_1
\end{aligned}$$

In our situation we must first understand the decomposition of (each graded piece of) I and A into C_p-modules, study the effect of mapping from one to other, and find the kernel of the induced mapping.

Shank and Wehlau have a recent preprint [**SW(b)**] in which they make use of this technology to prove the following. Suppose U is a sub-module of the C_p-module V. Suppose $\mathbb{F}_p[V]$ is generated in degrees less than or equal η. Then $\mathbb{F}_p[U]$ is generated in degrees less than or equal η. They further obtain a lower bound for η.

6. Two Problems from Invariant Theory.

The Dixmier-Erdös-Nicholas Problem. Let C_n be the cyclic group of order n over a field with a primitive n-th root of unity ω. The generator σ of the group with respect to the natural basis given by x_i corresponding to σ^i has the form

$$\sigma = \begin{pmatrix} 0\,0\,0 \dots 0\,1 \\ 1\,0\,0 \dots 0\,0 \\ 0\,1\,0 \dots 0\,0 \\ \vdots\;\vdots\;\vdots\;\ddots\;\vdots\;\vdots \\ 0\,0\,0 \dots 1\,0 \end{pmatrix}$$

Of course, C_n can be diagonalized, that is, there is a basis

$$\{y_0, y_1, \dots, y_{n-1}\}$$

with respect to which σ is diagonal of the form

$$\sigma = \operatorname{diag}(1, \omega, \omega^2, \dots, \omega^{n-1}).$$

We note immediately that y_0^i will be an invariant polynomial for all $i \geq 0$ and so we will work with the reduced regular representation, that is, we will take the vector space V with basis $\{y_1, \dots, y_{n-1}\}$.

The computation of $\mathbb{F}[V]^{C_n}$ is connected with problems in the representation theory of Lie groups of type A_n, and with problems in graph theory. We proceed as follows.

We note that $\sigma(y^I) = \omega^{i_1+2i_2+\cdots+(n-1)i_{n-1}} y^I$, so that the group maps monomials to monomials. It follows that invariant polynomials consist of sums of invariant monomials. Writing $\theta = (1, 2, \ldots, n-1)$ we see that y^I is invariant if and only if

$$\theta \cdot I = i_1 + 2i_2 + \cdots + (n-1)i_{n-1} = m(I)n,$$

for some $m(I) \in \mathbb{N}$. We refer to $m(I)$ as the *multiplicity* of I. We let $\mathcal{M}$ denote the collection of generating monomials, or rather, by abuse of notation, their exponent sequences. We denote by Δ_i the exponent sequence which consists of 0's everywhere except for a 1 in the i-th position. It is easy to see that the sequences $n\Delta_i$ are generators, and, in fact, the associated monomials form a homogeneous system for the ring of invariants. It follows that, if $I \in \mathcal{M}$, and I is not one of the $n\Delta_i$, then each entry in I is less than n.

We are interested in the problem of characterizing elements of $\mathcal{M}$, or in counting their number, denoted here $f(n)$. We've labeled the problem in the way we do because of a theorem due to Dixmier -Erdös-Nicholas, which says,

Theorem.

$$\liminf_{n\to\infty} \frac{f(n)}{\sqrt{n}p(n)} \log n \log\log(n) > 0.$$

Here $p(n)$ denotes the number of partitions of n. This theorem points to a phenomenonal growth in the number of generators for these rings of invariants as n grows.

One view is that the equation above takes place in $\mathbb{N}^{n-1} \subset \mathbb{Z}^{n-1} \subset \mathbb{R}^{n-1}$. If you prefer, we are studying an action of C_n on these three sets. Of course, we can interpret the action on $\mathbb{Z}^{n-1}$ as associated to the ring of Laurent polynomials. To continue, in Euclidean space, the equation defines the hyperplane of multiplicity m. We can find a integral basis for the multiplicity 0 hyperplane, the hyperplane through the origin. And then any of the multiplicity planes can be obtained by identifying just one integer vector in them, and using the basis above. We haven't been able to characterize the generators of our ring in this manner, though.

Special cases related to these sorts of invariants can be found in [**3**, **4**, **11**].

Steenrod module structures on the syzygies. First, we'll restrict our attention to the case $p = 2$. I'll try to illustrate with examples an interesting situation. Let V be a vector space of dimension 2 over the field $\mathbb{F}_2$. Let $G = C_3$ be the subgroup of $\mathrm{Gl}_2(\mathbb{F}_2)$ generated by the matrix $\sigma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. The group G has order 3, and we described the ring of invariants at the end of the section on examples.

We recall

$$\mathbb{F}_2[x, y]^G = \mathbb{F}_2[a, b, c]$$

where

$$\begin{aligned} a &= x^2 + xy + y^2, \\ b &= x^3 + x^2y + y^3, \text{ and} \\ c &= x^3 + xy^2 + y^3, \text{ with relation} \\ a^3 &= b^2 + bc + c^2, \end{aligned}$$

together with its resolution by syzygies over the ring $A = \mathbb{F}_2[a, b, c]$. Here $|a| = 2$, $|b| = |c| = 3$, and $\rho(a) = x^2 + xy + y^2$, $\rho(b) = x^2y + xy^2$, $\rho(c) = x^3 + x^2y + y^3$. We also had

$$0 \longrightarrow A(c^2 + a^3 + b^2 + bc) \longrightarrow A \longrightarrow \mathbb{F}_2[x, y]^G \longrightarrow 0.$$

We will refer to the relation by the name d.

Here is a table of Steenrod operations on A which we write down after considering the corresponding operations on $\mathbb{F}_2[V]^G$.

	Sq^1	Sq^2	Sq^3
a	b	a^2	0
b	0	ab	b^2
c	a^2	$ab + ac$	$\mathbf{c^2 + d}$

We won't go into the details here, but there is a proposition which states that if the Adem relations are satisfied on the generators of an algebra, and the action of the operations on products are given by the Cartan formula, then we obtain an action of the Steenrod algebra on the algebra. There are more sophisticated versions, but, for now, let's just point out that it is enough to determine $Sq^i(f)$ for $0 \leq i \leq |f|$ for each generator f of the algebra in question, and then verify $2^{|f|}$ Adem relations on f, beginning with $Sq^{2|f|-1}Sq^{|f|}(f) = 0$ and working our way down to $Sq^1Sq^1(f) = 0$.

In our example, because of the Adem relation $Sq^1Sq^2 = Sq^3$, we can calculate $Sq^3(c)$. However, we note that $Sq^3(c) \neq c^2$, so that A is not a $\mathcal{A}$-algebra, but rather a $\mathcal{A}$-module. We need to check that $Sq^3Sq^2 = 0$, $Sq^2Sq^2 = Sq^3Sq^1$. It is straightforward to observe that the $\mathcal{A}$-action preserves the ideal generated by d.

Here is another example. Let $A = \mathbb{F}_2[x, y]/(xy^2 + x^3)$ with $\mathcal{A}$ action given by $Sq^1(x) = xy$, and $Sq^1(y) = y^2$. It is trivial that $Sq^1Sq^1(y) = 0$, and we obtain $Sq^1Sq^1(x) = Sq^1(xy) = xy^2 + x^3 = 0$. These are the only Adem relations we need check, and therefore A carries the structure of a $\mathcal{A}$-module. However, it is fairly easy to see that the "natural" (from a certain point of view) algebra $B = \mathbb{F}_2[x, y]$ doesn't admit a compatible action of $\mathcal{A}$. In particular, there is no possible modification of our definition $Sq^1(x) = xy$. Therefore we obtain $Sq^1Sq^1(x) = xy^2 + x^3$ which is **not** 0 in B. Therefore, of course, B is not an $\mathcal{A}$-module, and can't be made to carry such a structure, given that the ideal (through which our choices might be modified) doesn't begin until degree 3. Of course, we might seek to modify B, but this is a story for another day.

There is much more to be said about even these two examples, and in the verification of the underlying theorems producing $\mathcal{A}$ actions, but these need await another time. We've computed a number of different examples, which we hope to analyze in more detail.

7. References

A word about the two lists that follow. In the beginning there was Stanley's paper [**S**]. Then came the books of Smith [**S(a)**] and Benson [**B**]. Smith's book, in particular, has an extensive bibliography. I urge the interested reader to consult it. I've included one limited list of references, and a list of the papers on invariant theory with which I have been involved. They were all lots of fun.

Stanley's paper appeared in the Bulletin of the AMS in the May 1979 volume. In many ways, our work since 1986 has been our attempt to understand how the theorems and techniques of this paper could be understood in positive characteristic.

Also recommended is the paper of Larry Smith, *A note on the realization of complete intersection algebras as cohomology algebras of a space*, Quart. J. Math. Ox. (2), **33** (1982), 379–384.

[**B**] D J Benson, *Polynomial invariants of finite groups*, LMS **190** Cambridge University Press (1993).

[**BZ**] D Bourguiba and S Zarati, *Depth and the Steenrod algebra*, Inventiones Math, **128** (1997) 589-602.

[**Br**] A Broer, *Remarks on invariant theory of finite groups*, preprint (1997).

[**DW**] W M Dwyer and C Wilkerson, *Kahler differentials, the T functor, and a theorem of Steinberg*, Trans AMS, **350** No 12 (1998) 4919–4930.

[**Fl**] P Fleischmann, *A new degree bound for vector invariants of symmetric groups* Trans AMS, **350** No 4 (1998) 1703–1712.

[**FL**] P Fleischmann and W Lempken, *On generators of modular invariant rings of finite groups* Bull AMS, **29** No 5 (1997) 585–591.

[K] R M Kane, *Poincaré duality and the ring of coinvariants*, Can Math Bull, **37** (1994) 82–88.

[N] H Nakajima, *Regular rings of invariants of unipotent groups*, Journal of Algebra, **85** (1983) 253–286.

[R] D R Richman,*On vector invariants over finite fields*, Advances in Math., **81** (1990) 30–65.

[Sh] R J Shank, *SAGBI bases for ring of formal modular semi-invariants*, Comment Math Helv, **73** No 4 (1998) 548-565.

[Si] W M Singer, *The transfer in homological algebra*, Math Z, **202** (1989) 493–523.

[SW(a)] R J Shank and D L Wehlau, *The transfer in modular invariant theory*, Journal of Pure and Applied Algebra, **141** No 3 (1999) 299-313.

[SW(b)] R J Shank and D L Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, preprint, August 2000.

[S(a)] L Smith, *Polynomial invariants of finite groups*, A. K. Peters, Wellesley MA USA (1995).

[S(b)] L Smith, *Polynomial invariants of finite groups. A survey of recent developments.* Bull AMS, **34** No 3 (1997) 211–250.

[S] R P Stanley,*Invariants of finite groups and their applications to combinatorics.*, Bull AMS , **1**, No 3 (1979) 475–511.

[W] C Wilkerson, *A primer on the Dickson invariants*, Proceedings of the Northwestern Homotopy Theory Conference, AMS, Cont Math, **19** (1983) 421–434.

Queen's Papers.

(1) H E A Campbell, I P Hughes, G Kemper, R J Shank, and D L Wehlau, *Depth of modular invariant rings*, Transformation Groups **5** No 1 (2000) 21–34.

(2) H E A Campbell, A V Geramita, I P Hughes, R J Shank, and D L Wehlau, *Non-Cohen-Macaulay vector invariants and a Noether bound for a Gorenstein ring of invariants*, Can Math Bull, **42 (2)**, (1999), 155–161.

(3) H E A Campbell, J Harris and D Wehlau, *On rings of invariants of non-modular Abelian groups*, Bulletin of the Australian Mathematics Society, **60** No 3 (1999) 509–520.

(4) H E A Campbell, J Harris and D Wehlau, *Internal duality for resolutions of rings*, Journal of Algebra, **215** (1999) 1–33.

(5) H E A Campbell and I P Hughes, *Rings of invariants of certain p-groups over the field* $\mathbf{F}_p$, Journal of Algebra, **211** (1999) 549–561.

(6) H E A Campbell and I P Hughes, *On the vector invariants of $U_2(\mathbf{F}_p)$: a proof of a conjecture of David Richman*, Advances in Math, **126** No 1 (1997) 1–20.

(7) H E A Campbell, I P Hughes, R J Shank, and D L Wehlau, *Bases for rings of covariants*, Transformation Groups, **1** No 4 (1996) 307–336.

(8) H E A Campbell and I P Hughes, *The ring of upper triangular invariants as a module over the Dickson invariants*, Mathematische Annalen, **306** (1996) 429–443.

(9) H E A Campbell and I P Hughes, *2-dimensional vector invariants of parabolic subgroups of $GL_2(\mathbf{F}_p)$*, Journal of Pure and Applied Algebra, **112** (1996) 1–12.

(10) R B Bell, H E A Campbell, and I P Hughes, *Properties of functions associated to invariant theory*, Comm in Alg **22** (1994), 381–396.

(11) H E A Campbell, I P Hughes, F Pappalardi, and P S Selick, *On the ring of invariants of $\mathbf{F}^*_{2^s}$*, Comment Math Helv **66** (1991) 322–331.

(12) H E A Campbell, I P Hughes, and R D Pollack, *Rings of invariants and p-Sylow subgroups*, Can Math Bull **34** No 1 (1991) 42–47.

(13) H E A Campbell, I P Hughes, and R D Pollack, *Vector invariants of symmetric groups*, Can Math Bull **33** No 4 (1990) 391–397.

Mathematics and Statistics Department, Queen's University, Kingston, Ontario, Canada, K7L 3N 6

E-mail address: eddy@mast.queensu.ca

LECTURES IN IOANINNA

FREDERICK R. COHEN[♮]

Abstract. One of the main themes of this conference addresses invariants, as well as their connection to endomorphisms of functors. These endomorphisms yield useful techniques for the analysis of certain natural problems in the subject.

At this point there is a dichotomy: Smith's lectures focus on functors which reflect "abelian properties" of an object in Algebraic Topology while Cohen's lectures focus on functors which reflect "non-abelian properties" in Algebraic Topology. Part of the role, and applications of these structures for classical homotopy groups will be addressed in these lectures. The four topics considered are as follows:

1. Splittings of spaces,
2. Endomorphisms of tensor algebras, and self-maps of loop spaces,
3. Braid groups, and homotopy groups of the 2-sphere, and
4. Cohomology of symmetric groups, and other groups.

I would like to thank Nondas Kechagias as well as the University of Ioannina for providing an extremely pleasant, and enjoyable atmosphere for this interesting, and fertile conference. I would also like to thank Larry Smith for his useful suggestions.

1. Splittings of spaces

The basic objects of study here are loop spaces, and suspension spaces. One goal is to obtain information about the homotopy groups, and homology groups of these spaces. These constructions also provide a natural continuation of the themes in Professor Smith's lectures in which he discusses classifying spaces.

For example, Milnor [20] showed that the loop space of a path-connected simplicial complex X has the homotopy type of a topological group G, and where BG has the homotopy type of X. This construction will be used below.

Principle: Many useful spaces are homotopy equivalent to a classifying space. This feature has informative consequences as illustrated below.

Theorem 1.1. *Let X be a topological space which is a connected CW-complex. Then there exists a topological group G such that X is homotopy equivalent to BG.*

Next consider the path loop fibration

$$\Omega X \to PX \to X$$

where PX denotes the path-space, the space of continuous functions $\{f : [0,1] \to X | f(0) = *\}$, and ΩX is the subspace of PX given by

$$\{f : [0,1] \to X | f(0) = * = f(1)\}.$$

[♮] Partially supported by the National Science Foundation.

Classically, there are isomorphisms

$$\pi_i(X) \rightarrow \pi_{i-1}(\Omega X).$$

Thus the study of the homotopy groups of a simply-connected space reduces to those for its' loop space. The point of view of these lectures is to regard X as a classifying space, and to learn properties about X from the loop space of X. Many of these properties are described in [30].

There are sometimes useful, and informative features of ΩX which then inform on X. It will be seen below that certain choices of invariant elements under the action of a symmetric group yield additional information about ΩX. Thus to continue a second theme in Professor Smith's lectures of invariant elements arising from natural actions of groups, the symmetric groups are used to give decompositions of certain loop spaces which arise from such invariants.

The first example in this context arises from the classical Hopf fibrations: There are homotopy equivalences

1. $\Omega S^2 \rightarrow S^1 \times \Omega S^3$,
2. $\Omega S^4 \rightarrow S^3 \times \Omega S^7$, *and*
3. $\Omega S^8 \rightarrow S^7 \times \Omega S^{15}$.

These decompositions represent reformulations of the classical Hopf invariant one problem, and are the the only cases for which such product decompositions for loop spaces of spheres exist. That these are the only spheres S^{n+1} such that ΩS^{n+1} is homotopy equivalent to $S^n \times \Omega S^{2n+1}$ is equivalent to the classical result on the non-existence of elements of Hopf invariant one.

However, after localization away from 2, there are homotopy equivalences

$$\Omega S^{2n} \rightarrow S^{2n-1} \times \Omega S^{4n-1}$$

given by classical results due to Serre. These decompositions will be reformulated below in terms of invariants of actions for certain symmetric groups. A general context together with applications to other natural spaces are given as well.

One method of proof here is as follows. Start with a principle G-bundle with a cross-section. It is a classical fact that such bundles are trivial. This method provides a process for showing that a loop space of X is sometimes homotopy equivalent to a product.

Proposition 1.2. *Let $E \rightarrow B$ be a fibration with homotopy theoretic fibre F. Assume that the natural map $i : F \rightarrow$ E admits a cross-section up to homotopy (thus there is a map $\sigma : E \rightarrow F$ such that $i \circ \sigma$ is homotopic to the identity). Then there is a homotopy equivalence*

$$F \rightarrow E \times \Omega B.$$

As an example, consider the natural homomorphisms $S^1 \rightarrow S^3$ to obtain a fibration $BS^1 \rightarrow BS^3$ with fibre S^2. "Backing up" this fibration, there is an induced fibration $\Omega S^2 \rightarrow S^1$ with homotopy theoretic fibre ΩS^3. Since there is a section for this last fibration, the product decomposition $\Omega S^2 \to S^1 \times \Omega S^3$ follows at once. This gives the product decomposition for ΩS^2 listed above. The other cases are similar.

Other important constructions which fit in this framework are the Whitehead product, and the Samelson product. Here consider a topological group G. The commutator map

$$[-,-] : G \times G \to G$$

is gotten by sending the ordered pair (a, b) to the commutator $[a, b]= a^{-1}b^{-1}ab$. Notice that if either a or b is equal to 1, then the commutator $[a, b]$ is equal to 1. There is an induced map

$$S : G \wedge G \to G$$

where $G \wedge H$ denotes the quotient $G \times H/(G \times \{1\} \cup \{1\} \times H)$.

Notice that $S^k \wedge S^n = S^{n+k}$. There is an induced bilinear map for all $i, j \geq 1$ on the level of homotopy groups

$$S_* : \pi_i G \otimes \pi_j G \to \pi_{j+k} G.$$

Regarding ΩX as a topological group G, there are analogous pairings induced on the level of homotopy groups for any simply-connected CW complex X. These pairings satisfy the (graded) antisymmetry law for a Lie bracket if the prime 2 is a unit, as well as the (graded) Jacobi identity if 3 is a unit. In the case of graded Lie algebras over $\mathbb{F}_2$, the element $[x, x]$ is required to be zero, and over $\mathbb{F}_3$, the element $[[x, x], x]$ is required to be zero. These last two properties fail in general for the Samelson product S_* without additional assumptions. In case x is of even degree, it is the case that $[x, x]$ is sometimes non-zero, and is of order 2. In case x is of odd degree, it is the case that $[[x, x], x]$ is sometimes non-zero, and is of order 3.

This pairing S_* is known as the Samelson product [26]. This pairing is related to the classical Whitehead product W by adjointness up to a sign, and gives the following commutative diagram where $\alpha : \pi_{q+1} X \to \pi_p \Omega X$ is the adjoint yielding a natural isomorphism, and the pairing $[x, y]$ in the homology of ΩX is given by $x \otimes y - (-1)^{degree(x)degree(y)} y \otimes x$ [6], page 215:

$$\begin{tikzcd}
\pi_{p+1}X \otimes \pi_{q+1}X \arrow[r, "W"] \arrow[d, "\alpha\otimes\alpha"'] & \pi_{p+q+1}X \arrow[d, "\alpha"'] \\
\pi_p\Omega X \otimes \pi_q\Omega X \arrow[r, "S_*"] \arrow[d] & \pi_{p+q}\Omega X \arrow[d] \\
H_p\Omega X \otimes H_q\Omega X \arrow[r, "{[-,-]}"] & H_{p+q}\Omega X
\end{tikzcd}$$

These constructions give rise to product decompositions of loop spaces in much the same way that elements of Hopf invariant one give rise to product decompositions above. This feature will be seen after the next example for which a product decomposition of a loop space arises from work of T. Ganea, and P. Hilton, and others.

Here consider the inclusion of the wedge $X \vee Y$ in the product $X \times Y$ with homotopy theoretic fibre F. Let $X^{(k)}$ denote the k-fold smash product where $X \wedge Y$ denotes $X \times Y/X \vee Y$. The following is a theorem of T. Ganea [14].

Theorem 1.3. *Let X, and Y be connected CW complexes, with the homotopy theoretic fibre of the natural inclusion $X \vee Y$ in $X \times Y$ denoted by F. Then*

1. *F is homotopy equivalent to the $\Sigma(\Omega X \wedge \Omega Y)$.*
2. *There is a homotopy equivalence*
$$\Omega(X) \times \Omega(Y) \times \Omega\Sigma(\Omega X \wedge \Omega Y) \rightarrow \Omega(X \vee Y).$$
3. *Furthermore, the choice of map $\Omega\Sigma(\Omega X \wedge \Omega Y) \rightarrow \Omega(X \vee Y)$ is the canonical multiplicative extension of the composition of the map*
$$\Omega(i) \wedge \Omega(j) : \Omega(X) \wedge \Omega(Y) \rightarrow \Omega(X \vee Y) \wedge \Omega(X \vee Y),$$
with the commutator map
$$S : \Omega(X \vee Y) \wedge \Omega(X \vee Y) \rightarrow \Omega(X \vee Y)$$
where $i : X \rightarrow X \vee Y$, and $j : Y \rightarrow X \vee Y$ are given by the natural inclusions.

Thus for example, if X and Y are $\mathbb{CP}^\infty$, then X, and Y have precisely one non-vanishing homotopy group. Since $\Omega\mathbb{C}P^\infty$ is homotopy equivalent to S^1, the theorem implies a homotopy equivalence
$$\Omega(\mathbb{CP}^\infty \vee \mathbb{C}P^\infty) \rightarrow S^1 \times S^1 \times \Omega S^3.$$
Thus the homotopy groups of $\mathbb{CP}^\infty \vee \mathbb{CP}^\infty$ are those of the 3-sphere plus 2 other copies of the integers (in degree 2). However, the spaces $\mathbb{CP}^\infty \vee \mathbb{CP}^\infty$, and $S^3 \times \mathbb{CP}^\infty \times \mathbb{CP}^\infty$ are not homotopy equivalent.

The next theorem is the classical Hilton-Milnor theorem in which the notation $X^{(k)}$ is used for the k-fold smash product as above.

Theorem 1.4. *Let X, and Y be connected CW complexes. Then there is a homotopy equivalence*
$$\Omega\Sigma(X \vee \Sigma Y) \rightarrow \Omega\Sigma(X) \times \Omega\Sigma(Y) \times \Omega\Sigma(\vee_{i,j \geq 1} X^{(i)} \wedge Y^{(j)}).$$

How do these "fit" with invariants ? How do they arise in some further way ? What are these good for ? Some of these questions will be addressed next. Two examples for which product decompositions have proven to be useful are listed next.

1. Product decompositions for the loop space of a $mod-p^r$ Moore space for p prime have useful applications. These decompositions impinge on the structure of the homotopy groups of spheres as well as other finite complexes.
2. More general splittings will be illustrated where spaces are localized at a fixed prime. For example, consider spaces X which are (1) double suspensions, and (2) their homology groups are non-trivial, and entirely torsion. Then the loop space of X admits a product decomposition with infinitely many non-trivial factors. These decompositions then directly give non-trivial elements in homotopy groups.

In what follows below, it will be assumed that the reduced homology of the spaces below are entirely torsion.

There are natural self-maps of $X^{(k)}$ given by elements in the symmetric group on k letters Σ_k. Thus, there is an "action" of the integral group ring $\mathbb{Z}[\Sigma_k]$on $\Sigma X^{(k)}$ given by adding via the suspension coordinate. These self-maps have been used widely to give decompositions of $\Sigma X^{(k)}$. Some examples are listed below.

Example 1.5. Example: Let k = 2, and let β_2 denote the element in the group ring given by $1 - (1,2)$ where $(1,2)$ is the transposition which interchanges 1, and 2. Then a direct computation gives $(\beta_2)^2 = 2\beta_2$.

Furthermore, if 2 is a unit in the reduced homology of X, then the elements β_2, and $2 - \beta_2$ give an orthogonal decomposition of the homology of $\Sigma X^{(2)}$. In addition, if 2 is unit in the reduced integer homology of $\Sigma X^{(2)}$, then there is a homotopy equivalence

$$\Sigma X^{(2)} \to L_2 \vee M_2$$

where L_2 denotes the homotopy direct limit of β_2, and M_2 denotes the homotopy direct limit of $2 - \beta_2$. This example is expanded below.

The Dynkin-Specht-Wever elements β_n are elements in the integral group ring of the symmetric group $\mathbb{Z}[\Sigma_n]$, which can be defined as follows: Regard the n-fold tensor product $V^{\otimes n}$ as a module over $\mathbb{Z}[\Sigma_n]$. Then β_n in $\mathbb{Z}[\Sigma_n]$ is obtained by the linear transformation which sends $v_1 \otimes v_2 \otimes \cdot \cdot \otimes v_n$ to the element $[[\cdot[v_1, v_2]v_3] \cdot \cdot\cdot]v_n]$ where the bracket $[x, y]$ means $x \otimes y - (-1)^{deg(x)deg(y)} y \otimes x$.

For simplicity, assume that a space Y is a suspension ΣX. There are induced self-maps $\beta_n, n - \beta_n : (\Sigma X)^{(n)} \to (\Sigma X)^{(n)}$. Let $L_n(\Sigma X)$ denote the homotopy direct limit of β_n and $M_n(\Sigma X)$ the homotopy direct limit of $n - \beta_n$.

Proposition 1.6.
1. *The formula $\beta_n \circ \beta_n = n\beta_n$ holds in homology for the self-maps $\beta_n : (\Sigma X)^{(n)} \to (\Sigma X)^{(n)}$.*
2. *If n is a unit in the reduced homology of X, then there is map which induces a homology isomorphism $(\Sigma X)^{(n)} \to L_n(\Sigma X) \vee M_n(\Sigma X)$.*

The proof is that singular homology commutes with the direct limit construction here, and that the maps are isomorphisms in homology with any field coefficients. The proof is a special case of what follows below. These constructions were given in work of the author, and J. Wu, and have been developed further in recent work of P. Selick, and J. Wu.

Namely, let $g : V \to V$ be an idempotent self-map of a vector space V. Thus $g^2 = g$, and so g, and $1-g$ give an orthogonal idempotents of V, and there is an isomorphism of vector spaces $V \to gV \oplus (1-g)V$. Notice that there is an isomorphism $gV \to \operatorname{inj}\lim_g V$. This proof has a topological analogue.

Proposition 1.7. *Let $f : \Sigma X \to \Sigma X$ be any map which is idempotent on the level of reduced homology groups. Then there is a map*

$$\Sigma X \to A \vee B$$

which induces an isomorphism on homology where

1. *$A = \operatorname{inj}\lim_f \Sigma X$, and*
2. *$B = \operatorname{inj}\lim_{1-f} \Sigma X$*

Thus if X has the homotopy type of a CW-complex, the map Θ is a homotopy equivalence.

This basic idea has been exploited in many beautiful ways by G. Cooke, N. Kuhn, S. Mitchell, G. Nishida, N. Ray, J. Smith, L. Smith, and R. Wood as well as many others.

The main point here is that invariants in linear algebra give topological information by exhibiting coalgebra decompositions of tensor algebras which can then be realized by topological spaces. Using this principle, the following theorem was proven in [8].

Theorem 1.8. *Fix a prime p, and assume that n is unit in the reduced mod-p homology of a CW-complex X. Then there is a homotopy equivalence*

$$\Omega\Sigma^2 X \rightarrow \Omega\Sigma^2 L_n(X) \times B(X)$$

for some choice of space $B(X)$. In addition, the mod-p homology of $L_n(X)$ is isomorphic to the module of Lie elements of tensor weight n in the tensor algebra $T[V]$ where V is the reduced mod-p homology of ΣX. Thus if the reduced mod-p of X has at least two linearly independent elements, then $L_n(X)$ has non-trivial homology for every n prime to p.

A specific example of the above theorem where X is a 2-cell complex given by a mod-2 Moore space is described below. A sketch of the proof of this theorem is given before this example as follows:

1. The Samelson product yields a map $Y^{(n)} \rightarrow \Omega\Sigma Y$.
2. Specialize to $Y = \Sigma X$ and appeal to Proposition 1.6 to obtain a map $L_n(\Sigma X) \rightarrow \Omega\Sigma Y$ with canonical multiplicative extension
$$\Omega\Sigma L_n(\Sigma X) \rightarrow \Omega\Sigma Y.$$
3. The Hopf invariant construction discussed in the next section is a map
$$\Omega\Sigma Y \rightarrow \Omega\Sigma Y^{(n)}.$$
Again, let $Y = \Sigma X$, and use Proposition 1.6 to project $\Omega\Sigma Y^{(n)} \rightarrow \Omega\Sigma L_n(\Sigma X)$.
4. The composite
$$\Omega\Sigma L_n(\Sigma X) \rightarrow \Omega\Sigma^2 X \rightarrow \Omega\Sigma L_n(\Sigma X)$$
induces a homology isomorphism by a direct (messy) computation. Alternatively, the composite can be shown to be homotopic to a loop map, and the computation is then direct.

Let $P^{n+1}(2)$ denote $\Sigma^{n-1}\mathbb{RP}^2$ where $\mathbb{RP}^2$ is the real projective plane. The next theorem follows by substituting $n = 3$ or 5 in the previous theorem where $P^n(2)$ denotes the (n-1)-sphere with an n cell attached by a degree 2 map. Thus there is a homotopy equivalence $\Sigma^{n-2}\mathbb{RP}^2 \rightarrow P^n(2)$.

Theorem 1.9. *Assume that $n > 2$. Then there are homotopy equivalences as follows:*

$$\Omega P^{n+1}(2) \simeq \begin{cases} \Omega P^{4\mu(5m-2,k)+2}(2) \times X(n+1) & \text{if } n+1 = 4m, \\ \Omega P^{4\mu(15m-2,k)+2}(2) \times Y(n+1) & \text{if } n+1 = 4m+1, \\ \Omega P^{4\mu(m,k)+2}(2) \times Z(n+1) & \text{if } n+1 = 4m+2, \\ \Omega P^{4\mu(3m+1,k)+2}(2) \times W(n+1) & \text{if } n+1 = 4m+3 \end{cases}$$

for all $k \geq 1$, where μ is defined by

$$\mu(n,k) = 9^{k-1}n + \sum_{j=0}^{k-2} 9^j.$$

It was proven by J. Mukai [23] or in [8] that if $n \geq 4$, and n is odd, then $\pi_{4n-2}P^n(2)$ contains $\mathbb{Z}/8\mathbb{Z}$.

Proposition 1.10. *If $n > 3$, then there are infinitely many elements of order 8 in the homotopy groups of $P^n(2)$.*

There are two outstanding conjectures in this subject:

1. Barratt's finite exponent conjecture: Assume that the suspension order of the identity for $\Sigma^2 X$ is p^r. Then p^{r+1} annihilates the homotopy groups of $\Sigma^2 X$.
2. Moore's conjecture: Assume that X is a simply-connected finite complex which has finitely many non-zero rational homotopy groups $\pi_i X \otimes \mathbb{Q}$. Then for any fixed prime p, the p-torsion in the homotopy groups of X have a bounded exponent for all i (depending on p).

The work above was directed toward considering these questions for mod-2 Moore spaces, and was inspired by the following two theorems which were proven much earlier using splitting techniques.

Theorem 1.11. [7] *If p is an odd prime, then p^n annihilates the p-torsion in the homotopy groups of S^{2n+1}.*

Theorem 1.12. [25] *If p is an odd prime, then p^{r+1} annihilates the homotopy groups of a simply-connected mod $- p^r$ Moore space $P^{n+1}(p^r)$.*

2. Endomorphisms of tensor algebras, and self-maps of loop spaces

In the previous lecture, certain product decompositions for loop spaces arose from natural coalgebra decompositions of the tensor algebra. This theme will be pursued here where the collection of all natural transformations with respect to certain analogous structures will be discussed.

Consider a graded free module V over the integers $\mathbb{Z}$ or a field $\mathbb{F}$. The modules V considered here will usually arise as the reduced homology groups of a path-connected space X. Thus it will be assumed that V is concentrated in degrees strictly greater than 0. Let $T[V]$ denote the tensor algebra generated by V.

Then $T[V] = \bigoplus_{n\geq 0} V^{\otimes n}$. In addition, $T[V]$ inherits the natural structure of a Hopf algebra by requiring the elements in V to be primitive, and thus $\Delta(v) = v \otimes 1 + 1 \otimes v$ for v in V where Δ denotes the coproduct. Hence, there is a natural diagonal map which is a morphism of Hopf algebras:

$$\Delta : T[V] \to T[V] \otimes T[V].$$

Notice that $T[V]$ is a functor from graded modules to graded Hopf algebras. One might ask for the natural transformations from this functor to itself which preserves the underlying structure of a coalgebra.

Part of the motivation here is that the tensor algebra $T[V]$ gives the homology of certain families of topological spaces by the following:

Theorem 2.1. *(Bott-Samelson) Let X be a topological space which is a connected CW-complex. Assume either that the integer homology is either (1) torsion free, or (2) the homology groups are taken with field coefficients $\mathbb{F}$. Let V denote the reduced homology of X. Then there is an isomorphism of algebras*

$$\Theta : T[V] \to H_*(\Omega\Sigma X).$$

If in addition, X is a suspension, then Θ is an isomorphism of Hopf algebras.

One could ask about self-maps of $\Omega\Sigma X$. The action of such a map in homology then gives a morphism of coalgebras of $T[V]$. One could ask further about the "generic self-maps", those maps which are natural for all spaces X, or all modules V.

First notice that the set of coalgebra self-maps of $T[V]$,

$$Hom^{coalg}(T[V], T[V])$$

forms a group where the product of two elements is defined as follows:

$$\begin{tikzcd}
T[V] \arrow[r, "\Delta"] \arrow[d, "\mathrm{id}"] & T[V] \otimes T[V] \arrow[d, "f\otimes g"'] \\
T[V] \arrow[r] \arrow[d, "\mathrm{id}"] & T[V] \otimes T[V] \arrow[d, "multiply"'] \\
T[V] \arrow[r, "f\cdot g"] & T[V]
\end{tikzcd}$$

The basic point here is that $T[V]$ admits natural self-maps which in fact correspond to self-maps of spaces. The structure of these then inform on spaces. In addition, Artin's braid group arises, and plays a significant role within classical homotopy theory.

Next consider self-maps of $T[V]$ as follows:

Definition 2.2. Let q be an integer.

1. The map $\phi_q : T[V] \to T[V]$ is given by the multiplicative map which sends each element v to qv.
2. The map $\psi_q : T[V] \to T[V]$ is given by the $q-th$ power map
3. The map $\lambda_q : T[V] \to T[V]$ is given by that map induced in homology by the composite
$$\Omega\Sigma^2 X \to \Omega\Sigma(\Sigma X)^{(n)} \to \Omega\Sigma^2 X$$
of
   (a) the q-th Hopf invariant $h_q : \Omega\Sigma^2 X \to \Omega\Sigma(\Sigma X)^{(q)}$ with
   (b) $\Omega\Sigma(\Sigma X)^{(n)} \to \Omega\Sigma^2 X$, the looping of the q-fold Whitehead product.

These maps all give natural transformations of $T[V]$. The maps $\lambda_q : T[V] \to T[V]$ are non-trivial, and intricate. Let H_∞ denote the group generated by these elements.

Theorem 2.3. *The group H_∞ is the inverse limit of a system*

$$\cdots \to H_n \to H_{n-1} \to \cdots \to H_2 \to H_1.$$

The maps $H_n \to H_{n-1}$ are non-split epimorphisms of groups with kernel given by the center Lie(n) of H_n. Furthermore, Lie(n) is a free abelian group of rank $(n-1)!$.

The algebraic maps above are all realized by self-maps of $\Omega\Sigma^2 X$. Thus there is a group homomorphism from the free group F generated by the elements in Definition 2.2 to the group of homotopy classes of self-maps $[\Omega\Sigma^2 X, \Omega\Sigma^2 X]$, say

$$\phi(X) : F \rightarrow \ [\Omega\Sigma^2 X, \Omega\Sigma^2 X]$$

together with an induced homomorphism

$$\Phi : F/ \cap ker\phi(X) \rightarrow \ [\Omega\Sigma^2 X, \Omega\Sigma^2 X]$$

where the intersection is over every space X.

Theorem 2.4. *The group H_∞ is isomorphic to $F/ \cap ker\phi(X)$. Furthermore H_∞ is isomorphic to the group of natural transformations of the functor $T[V]$ regarded as a coalgebra.*

The self-maps given by H_∞ are those used for the splittings in section 1. This group was introduced and analyzed by the author. Subsequently, Dwyer, and Rezk showed that H_∞ exhausts all of the natural transformations of $T[V]$ which preserve the underlying coalgebra structure. The groups Lie(n) are given by the homology of certain braid groups. Namely, the braid groups arise in the next section concerning the homotopy groups of the 2-sphere in which P_n denotes the n-th pure braid group. Then $Lie(n)$ is isomrphic as a module over the symmetric group to $H_{n-1}(P_n; \mathbb{Z})$ tensored with the sign representation [6]. The groups H_n are also closely connected to low dimensional topology, and the theory of "Brunnian" links. These connections will be addressed elsewhere.

3. Braid groups, and homotopy groups of the 2-sphere

The purpose of this lecture is to outline a specific description of a group of invariant elements by describing some work of Jie Wu concerning the homotopy groups of the 2-sphere. Namely, let G be a group acting on a set S, and let S^G denote the set of fixed points under the action of G. The basic example here arises from a classical representation constructed by E. Artin in 1924 [2, 3, 5] together with recent work of Wu [31] relating this representation to the homotopy groups of the 2-sphere S^2.

Artin's representation is a homomorphism from the n-stranded braid group to the automorphism group of a free group with n generators in which the following notation is used:

1. The group B_n denotes Artin's n-stranded braid group.
2. The group P_n denotes the pure n-stranded braid group, the subgroup of B_n which leaves the endpoints of a braid unpermuted.
3. The group F_n denotes the free group on n-letters with basis $\{x_1, x_2, \cdots, x_n\}$.
4. The groups $B_n(M)$, respectively $P_n(M)$ denote the n-stranded braid group, respectively the pure the n-stranded braid group for a surface M. The n-stranded pure braid group of a surface M, $P_n(M)$, is defined as the fundamental group of the configuration space $F(M, n)$, the subspace of M^n given by $\{(m_1, m_2, \cdots, m_n) | m_i \neq m_j, i \neq j\}$. The n-stranded braid group of a surface M, written $B_n(M)$ is the fundamental group of the quotient of $F(M, n)$ by the natural action of the n-th symmetric group $F(M, n)/\Sigma_n$.

Artin's representation is given by

$$\Phi : B_n \rightarrow \ Aut(F_n)$$

where

1. Artin's map Φ is faithful, and
2. the automorphisms f in the image of Φ are characterized by the following 2 properties which also characterize the braid group B_n:
   (a) $f(x_1 \cdot x_2 \cdots x_n) = x_1 \cdot x_2 \cdots x_n$, and
   (b) $f(x_i) = w_i \cdot x_{\sigma(i)} \cdot w_i^{-1}$ for all i, and where σ denotes an element in the symmetric group on n-letters.

Next, consider words given by commutators in the free group F_n of the form

$$[..[y_1, y_2], y_3], \cdots], y_t]$$

where the commutator $[a, b]$ is given by $a^{-1}b^{-1}ab$, and the y_j satisfy the following two conditions:

1. All of the y_j lie in the set
$$\{x_0, x_1, x_2, \cdots, x_n\}$$
where x_0 is the product $x_1 \cdot x_2 \cdots x_n$ arising in Artin's representation, and
2. there is an equality of sets:
$$\{y_1, y_2, y_3, \cdots y_t\} = \{x_0, x_1, x_2, \cdots, x_n\}.$$

Define the group W_n to be the quotient of F_n modulo the smallest normal subgroup containing all of the words $[...[y_1, y_2], y_3], \cdots]y_t]$ as given above. Observe that by the Hall-Witt identities, the smallest normal subgroup generated by all of the words $[...[y_1, y_2], y_3] \cdots]y_t]$ is invariant under the action of B_n acting through Artin's representation. Thus there is a representation

$$\Theta : B_n \to Aut(W_n)$$

which descends from Artin's representation.

Theorem 3.1. *(J. Wu)*

1. *The group of invariant elements $W_n^{P_n}$ is the center of W_n.*
2. *The group of invariant elements $W_n^{B_n}$ is the subgroup of the center of W_n generated by all elements of order 2.*
3. *For all $n > 2$, the center of W_n is isomorphic to $\pi_{n+1}S^2$ ($= \pi_{n+1}S^3$).*

Thus Artin's representation together with classical invariants contain the seeds of the homotopy groups of the 2-sphere. The audience should be cautioned that this theorem is not useful for direct computations as is traditional in homotopy theory. The methods of proof involve simplicial groups together with the property that Artin's representation descends to an action on certain simplicial groups.

The determination of the fixed set of the action of the braid group on W_n by (combinatorial) group theoretic techniques is almost certainly beyond the reach of current methods. On the other hand, braid groups have appeared in several areas of mathematics such as group theory, homotopy theory, low dimensional topology, Galois theory, complexity of algorithms, and mathematical physics. The point is that group theoretic methods will not inform on computations, but they may admit further applications. It is the purpose of this lecture to indicate where certain structures "fit" with Wu's theorem.

Since the methods of proof are via simplicial sets, a digression concerning basic properties of simplicial sets is given now [17, 9]. First of all, a simplicial set S_* is a collection of sets S_n indexed by the non-negative integers n = 0,1,2, ... with face operations $d_i : S_n \to S_{n-1}$ with $0 \leq i \leq n$, and degeneracy operations $s_j : S_n \to S_{n+1}$ with $0 \leq j \leq n$. The face, and degeneracy operations are required to satisfy certain compatibility conditions sometimes called simplicial identities and which are described next [9, 17].

1. $d_i d_j = d_{j-1} d_i$ for $i < j$,
2. $s_i s_j = s_j s_{i-1}$ for $i > j$,
3.

$$d_i s_j = \begin{cases} s_{j-1} d_i & \text{if } i < j, \\ identity & \text{if i=j or i = j+1, and} \\ s_j d_{i-1} & \text{if } i > j+1, \end{cases}$$

An example of a simplicial set is the singular simplices of a topological space which arises in the definition of singular homology for a topological space. A second example is listed next. The simplicial circle S^1 has n-simplices S^1_n given by the set of all ordered $(n+1)$-tuples $< 0, 0, ..., 0, 1, 1, 1.., 1 >=< 0^{n-i+1}, 1^i >= x_i$ for $0 \leq i \leq n+1$.

1. The face operations

$$d_0, \cdots, d_n : S^1_n \to S^1_{n-1}$$

are specified by the following formulas.

$$d_j(x_i) = \begin{cases} x_i & \text{if } j \leq n-i, \\ x_{i-1} & \text{if } j > n-i. \end{cases}$$

2. The degeneracy operations

$$s_0, \cdots, s_n : S^1_n \to S^1_{n-1}$$

are specified by the following formulas.

$$s_j(x_i) = \begin{cases} x_i & \text{if } j \leq n-i, \\ x_{i+1} & \text{if } j > n-i. \end{cases}$$

A simplicial group G_* is a simplicial set such that

1. the simplices in degree n for every n given by G_n is a group, and
2. the face and degeneracy operations are group homomorphisms.

The homotopy groups of a simplicial group were defined by J. C. Moore [22] in a purely group theoretic way as follows:

1. Let G_* be a simplicial group.
2. Define N_q, the chains in degree q, as the intersection of the kernels of

$$d_i : G_q \to G_{q-1}$$

for $1 \leq i \leq q$,

$$N_q = \cap_{1 \leq i \leq q} ker(d_i : G_q \to G_{q-1}).$$

3. Define the group of cycles in degree q by

$$Z_q = \cap_{0 \leq i \leq q} ker(d_i : G_q \to G_{q-1}).$$

4. Define the boundaries in degree q by

$$B_q = d_0(N_{q+1}).$$

5. Then the group B_q can be shown to be a normal subgroup of Z_q, and the q-th homotopy group of G_* is defined by
$$\pi_q(G_*) = Z_q/B_q.$$

Any functor F from the category of pointed sets to the category of groups "prolongs" to a functor from the category of simplicial sets to the category of simplicial groups. Two examples of such functors are given next.

(1) the functor A which sends a pointed set X with "base-point" p to the free abelian group generated by X with the single relation that the "base-point" p is the identity element is denoted $A[X]$.

(2) the functor F which sends a pointed set X with "base-point" p to the free group generated by X with the single relation that the "base-point" p is the identity element is denoted $F[X]$.

An example is as follows. Consider the simplicial set S^1 given above. Then consider $A[S^1]$, and $F[S^1]$, the simplicial groups obtained from the functors A, and F .

It is easy to compute the homotopy groups of $A[S^1]$. They are given by $\{0\}$ in all degrees not equal to 1, and by $\mathbb{Z}$ in degree 1. (This exercise is fun, and you might try it.) The case of $F[S^1]$ turns out to contain more information.

This free group construction was developed by Milnor [21], and is discussed next where one technical condition as well as the definition of "geometric realization" is required to state the result: a simplicial set S_* is said to be "reduced" provided the set of simplices in degree 0, S_0, is a single point. In addition, there is a functor from the category of simplicial sets to the category of topological spaces given by "geometric realization" where $|S|$ denotes the geometric realization of a simplicial set S. The realization is defined by
$$|S| = \cup_{q\geq 0}\Delta[q] \times S_q/R$$
where $\Delta[q]$ denotes the q-simplex, and "R" is the equivalence relation generated by

1. $(v, d_i x)$ is equivalent to $(\epsilon_i(v), x)$ for v in $\Delta[q-1]$, x in S_q, and with $\epsilon_i : \Delta[q-1] \to \Delta[q]$ given by the inclusion of the i-th face, and
2. $(v, s_i x)$ is equivalent to $(\eta_i(v), x)$ for v in $\Delta[q+1]$, x in S_q, and with $\eta_i : \Delta[q+1] \to \Delta[q]$ given by the projection to the i-th face.

Theorem 3.2. *(Milnor) Let K be a reduced simplicial set. Then the geometric realization of $F[K]$ is homotopy equivalent to $\Omega\Sigma|K|$.*

One corollary is the starting point of Wu's investigation.

Corollary 3.3. *There is an isomorphism of groups*
$$\pi_q F[K] \to \pi_q \Omega\Sigma|K|.$$
Thus $\pi_q F[S^1]$ is isomorphic to $\pi_q \Omega S^2 \cong \pi_{q+1} S^2$

The point of this corollary is that one can view the homotopy groups of the 2-sphere as a combinatorially defined object which can be studied through combinatorial methods. These methods are frequently quite interesting, although they rarely have immediate computational value. Part of the features of the structure here is the next theorem which indicates part of the role of the center in simplicial groups.

Theorem 3.4. *If G is a reduced simplicial group, then $\pi_n G$ is contained in the center of the quotient group G_n modulo B_n.*

Wu then defines an "r-centerless" simplicial group G_* which is a simplicial group for which the center of G_n is trivial for $n \geq r$. An example of such a G arises in case G_n is a free group on at least 2 generators for $n \geq r$. A specific example is given by $F[S^1]$ which is "2-centerless". In degree 1, the simplicial group $F[S^1]$ is isomorphic to the integers, and is thus not "1-centerless".

Theorem 3.5. *If G is a reduced "r-centerless" simplicial group, then $\pi_n G$ for $n \geq r+1$ is equal to the center of G_n/B_n.*

Wu then applies this to $F[S^1]$ in order to prove his theorem on fixed points, and the homotopy groups of the 2-sphere. There are further connections between this problem, and other features of braid groups.

There is another simplicial group AP_* which in degree n is Artin's pure braid group on $n+1$ strands, and which gives some further information concerning Wu's theorem. Thus this simplicial group is isomorphic to the integers in degree 1. In joint work of Wu, and the author, the unique homomorphism of simplicial groups

$$\Theta : F[S^1] \to AP_*$$

which sends a generator in degree one to a generator is studied. Some properties are listed next:

1. $\Theta : F[S^1] \to AP_*$ is a monomorphism in each degree,
2. thus the q-th homotopy group of $F[S^1]$ is a subquotient of P_{q+1},
3. the quotient simplicial set $AP_*/F[S^1]$ has geometric realization which is homotopy equivalent to the 2-sphere, and
4. the (simplicial) loop space of AP_* is isomorphic to Milnor's free group construction $F[\Delta[1]]$ where $\Delta[1]$ is the simplicial one simplex.

The morphism of simplicial groups $\Theta : F[S^1] \to AP_*$ is related to the set of isotopy classes of n-component links, $\mathcal{L}_n$, as follows. There is a morphism of sets from the n-th pure braid group to the set of isotopy classes of n-component links as given in classical work of Alexander, and Markov [5]:

$$AP_n \to \mathcal{L}_n,$$

and

$$AP_* \to \cup_{n \geq 0} \mathcal{L}_n.$$

One question which arises in this context is as follows. Describe the image of $F[S^1]$, as well as the subgroups given by chains, cycles, and boundaries in the set of isotopy classes of links. Two examples are given next.

1. A cycle which represents the Hopf map $\eta : S^3 \to S^2$ is given by $[x_1, x_2]$ in the set of 2-simplices for $F[S^1]$. The image of this cycle in the set of isotopy classes of 3 component links is the Borromean rings.
2. The cycle $[x_1, x_2]^2$ represents the Whitehead product $[\iota_2, \iota_2]$. The image of this cycle is a 3-component link where two circles are "twisted around each other twice" while the third circle links the other 2 as if they were the Borromean rings. (Try it. It is interesting.)

Two important questions which arise in Wu's work are given next. Consider the n natural homomorphisms

$$d_i : P_n \to P_{n-1}$$

obtained by deleting the $i-th$ strand for $1 \leq i \leq n$. Thus there is an induced homomorphism

$$d : P_n \to \prod_{1 \leq i \leq n} P_{n-1}.$$

The kernel of this map is a free group. What is a basis for the kernel of this map ?

A second homomorphism is given by

$$\gamma : P_n \to P_n(S^2),$$

the natural quotient of the pure braid group for the plane to the pure braid group for the 2-sphere S^2. This homomorphism is obtained by applying the fundamental group to the natural inclusion of the configuration spaces $F(\mathbb{R}^2, n) \to F(S^2, n)$.

What is the kernel of the natural homomorphism

$$\gamma \times d : P_n \to P_n(S^2) \times \prod_{1 \leq i \leq n} P_{n-1}?$$

4. Cohomology of symmetric groups, and other groups

This section addresses classical work on the cohomology of the symmetric groups, certain subgroups of symmetric groups, and related groups. A smattering of information about problems, and applications is included. First recall the ingredients required for the definition of the homology, and the cohomology of a discrete group π.

1. An abelian group A is said to be a trivial $\mathbb{Z}[\pi]$-module, or a trivial π-module, provided A is a module over the integral group ring of π, $\mathbb{Z}[\pi]$, such $\sigma(a) = a$ for every element a in A, and every element σ in π.
2. Let $\mathbb{Z}$ be a trivial $\mathbb{Z}[\pi]$-module, let M be a left $\mathbb{Z}[\pi]$-module, and let N be a right $\mathbb{Z}[\pi]$-module.
3. Let
$$\cdots \to R_3 \to R_2 \to R_1 \to R_0 \to \mathbb{Z} \to \{0\}$$
be a free resolution of $\mathbb{Z}$ by free left $\mathbb{Z}[\pi]$-modules R_i.

The definitions of group homology, and cohomology are as follows.

1. The homology of π with N coefficients is
$$H_*(\pi; N) = Tor_*^{\mathbb{Z}[\pi]}(\mathbb{Z}, N),$$

and is the homology of the chain complex

$$\cdots \to N \otimes_{\mathbb{Z}[\pi]} R_3 \to N \otimes_{\mathbb{Z}[\pi]} R_2 \to N \otimes_{\mathbb{Z}[\pi]} R_1 \to N \otimes_{\mathbb{Z}[\pi]} R_0.$$

2. The cohomology of π with M coefficients is

$$H^*(\pi; M) = Ext^*_{\mathbb{Z}[\pi]}(\mathbb{Z}, M),$$

and is the cohomology of the cochain complex

$$M^0 \to M^1 \to \cdots \to M^i \to M^{i+1} \to M^{i+2} \to \cdots$$

where $M^i = Hom_{\mathbb{Z}[\pi]}(R_i, M)$.

These functors are frequently informative, and frequently computable. They provide useful ways of measuring interesting behavior. The first few classical results are as follows.

Theorem 4.1. *Let π be a finite group of order n.*

1. *Then $n \cdot H^j(\pi; M) = 0$, and $n \cdot H_j(\pi; N) = 0$ for all $j > 0$. Thus if $j > 0$, $H^j(\pi; M)$ respectively $H_j(\pi; N)$ is the direct sum of its p-primary components ${}_pH^j(\pi; M)$ respectively ${}_pH_j(\pi; N)$ for all primes p which divide n.*
2. *Let π_p denote the p-Sylow subgroup π. Then the restriction map*

$$_pH^*(\pi; M) \to H^*(\pi_p; M)$$

is a split monomorphism.

3. *If π is a finite group with abelian p-Sylow subgroup π_p, then the mod-p cohomology of π is given by $H^*(\pi_p, \mathbb{Z})^{N(\pi_p)}$ the invariant elements under the action of the normalizer $N(\pi_p)$ of π_p in π.*

Again, the elementary abelian groups are basic examples, as we have seen in several of the lectures. Their cohomology is classical, basic, and important.

Theorem 4.2. 1. *The cohomology ring $H^*((\mathbb{Z}/2\mathbb{Z})^n; \mathbb{F}_2)$ is a polynomial ring with generators $x_1, ..., x_n$ of degree 1.*

2. *If $r \geq 2$ or p is an odd prime, then the cohomology ring $H^*((\mathbb{Z}/p^r\mathbb{Z})^n; \mathbb{F}_p)$ is the tensor product of an exterior algebra with generators $x_1, ..., x_n$ of degree 1 tensored with a polynomial ring with generators $y_1, ..., y_n$ of degree 2. Furthermore, the $r - th$ Bockstein β_r of x_i is defined and satisfies the formula $\beta_r(x_i) = y_i$.*

A second important example is the symmetric group on n letters Σ_n. The homology, and cohomology of symmetric groups is addressed next. Let Σ_∞ denote the colimit of the Σ_n under the natural inclusion. There are analogues for Artin's braid groups $Br_n \to Br_{n+1}$ with colimit denoted Br_∞. The homology of these groups is related to the homology of certain useful topological spaces.

One connnection between the cohomology of the symmetric groups, and that of elementary abelian p-groups is as follows: The regular representation of $(\mathbb{Z}/2\mathbb{Z})^n$, a homomorphism $(\mathbb{Z}/2\mathbb{Z})^n \to \Sigma_{2^n}$, induces a map $H^*(\Sigma_{2^n}; \mathbb{F}_2) \to H^*((\mathbb{Z}/2\mathbb{Z}))^n; \mathbb{F}_2)$ which has image given by the Dickson algebra on n generators, the invariant subalgebra under the natural $Gl(n, \mathbb{F}_2)$-action. There is a further connection to spaces of continuous functions as described next.

Consider the natural suspension map $X \to \Omega\Sigma X$ which is the adjoint of the identity $\Sigma X \to \Sigma X$. Iterating, there is a map $\Omega^n\Sigma^n X \to \Omega^{n+1}\Sigma^{n+1}X$ with $QX = \varinjlim \Omega^n\Sigma^n X$. Write $\Omega_0^n\Sigma^n X$, and Q_0X for the respective path component of the identity. One feature of the spaces QX is that if X is a CW-complex, then the i-th homotopy group of QX is isomorphic to the i-th stable homotopy group of X. Thus properties of QX impact the stable homotopy groups of X.

The following theorem concerning the symmetric groups has input from many people including Araki, Kudo, Nakaoka, Dyer, Lashof, Barratt, Priddy, and Quillen [4, 1, 24, 10, 15]. The second part was proven in work of May, Segal, and the author [29, 6, 18].

Theorem 4.3. *Assume that homology is taken with any trivial coefficients. (Namely, the fundamental group of each space acts on the coefficients by the identity map.)*

1. *There is a map $B\Sigma_\infty \to Q_0S^0$ which induces a homology isomorphism.*
2. *There is a map $BBr_\infty \to \Omega_0^2S^2$ which induces a homology isomorphism.*

A more general version is the Kan-Thurston theorem: If X is a path-connected CW-complex, then there exists a $K(\pi,1)$ together with a map $K(\pi,1) \to X$ which induces a homology isomorphism with any trivial coefficients. Thus, on the level of homology, many reasonable spaces behave as if they are $K(\pi,1)'s$.

Some preparation for applications of the homological properties above are given next. There are maps $\mathbb{RP}^\infty \to \Omega_0^\infty S^\infty$ which induce an isomorphism on the level of fundamental groups given by $\mathbb{Z}/2\mathbb{Z}$. One such map is induced by reflection through the hyperplane orthogonal to a given line through the origin. This gives a map to the -1-component of $O(n)$, $\mathbb{RP}^{n-1} \to O(n)$. Translating to the $+1$-component of $O(n)$, and letting n go to infinity gives $P^\infty \to SO \to \Omega_0^\infty S^\infty$. Let $\Theta : Q\mathbb{RP}^\infty \to \Omega_0^\infty S^\infty$ denote any extension which is a loop map. The following is the 2-primary Kahn-Priddy theorem. There is an odd primary version.

Theorem 4.4. *The map Θ has a 2-local section. Thus after localization at $p = 2$, the following is satisfied:*

1. *There is a 2-local homotopy equivalence*
$$Q\mathbb{RP}^\infty \to \Omega_0^\infty S^\infty \times X$$
for some space X.
2. *The map $\Theta : Q\mathbb{RP}^\infty \to \Omega_0^\infty S^\infty$ gives a split epimorphism on the 2-primary components of homotopy groups.*

A non-stable analogue of this theorem is gotten as follows. Consider the cofibration $S^2 \to S^2 \to P^3(2)$ where the map $S^2 \to S^2$ is degree 2. Applying the pointed mapping functor to this cofibration gives a fibration $q : \Omega^2S^n \to \Omega^2S^n$ given by the H-space squaring map with homotopy theoretic fibre denoted $map_*(P^3(2), S^n)$, where $map_*(A, B)$ denotes the space of pointed maps from A to B. Notice that $P^3(2)$ is homotopy equivalent to the suspension of the projective plane $\Sigma\mathbb{RP}^2$. Let W_n denote the homotopy theoretic fibre of the double suspension $E^2 : S^{2n-1} \to \Omega^2S^{2n+1}$.

Theorem 4.5. 1. *If p is an odd prime, then there is p-local equivalence*
$$map_*(P^3(p), S^{2p+1}) \to \Omega^2S^3 < 3 > \times W_p.$$

Thus $map_*(P^3(p), S^{2p+1}) \to \Omega^2 S^3 < 3 >$ induces a split epimorphism on the p-primary component of homotopy groups, and p annihilates the p-primary component of $\pi_i S^3$ for any $i > 3$.

2. *There is a 2-local equivalence*

$$map_*(\Sigma\mathbb{RP}^2, S^5) \to \Omega^2 S^3 < 3 > \times W_2.$$

Thus $map_*(\Sigma\mathbb{RP}^2, S^5) \to \Omega^2 S^3 < 3 >$ induces a split epimorphism on the 2-primary component of homotopy groups, and 4 annihilates the 2-primary component of $\pi_i S^3$ for any $i > 3$.

The method of proofs of these theorems is given by constructing maps, and then appealing to the cohomological results in Theorem 4.2 above to prove that a map is an equivalence. The Kahn-Priddy theorem is, of course, due to D. S. Kahn, and S. Priddy. The odd primary result in Thorem 4.5 above is due to P. Selick while the 2-primary theorem is due to the author.

Next consider further extensions given by the wreath product $\Sigma_n \wr G$ which is the group extension

$$1 \to G^n \to \Sigma_n \wr G \to \Sigma_n \to 1$$

which is specified as follows:

1. As a set $\Sigma_n \wr G$ is isomorphic to $\Sigma_n \times G^n$ with elements written as $(\sigma; g_1, ..., g_n)$.
2. The multiplication is specified by
$$(\sigma; g_1, ..., g_n)(\tau; h_1, ..., h_n) = (\sigma\tau; g_{\tau^{-1}(1)}h_1, ..., g_{\tau^{-1}(n)}h_n).$$
3. The fundamental group of $E\Sigma_n \times_{\Sigma_n} X^n$ is isomorphic to $\Sigma_n \wr G$ for path-connected spaces X with $\pi_1(X) = G$.

There is a slightly more general, and useful definition of the wreath product which fits in other contexts. Namely, given any homomorphism $f : \Pi \to \Sigma_n$, define the wreath product $\Pi \wr G$ (where the notation does not display the dependence of the extension on the homomorphism f) as a pull-back:

$$\begin{tikzcd}
\Pi \wr G \arrow[r] \arrow[d] & \Pi \arrow[d] \\
\Sigma_n \wr G \arrow[r] & \Sigma_n
\end{tikzcd}$$

Thus there is a morphism of group extensions:

$$\begin{tikzcd}
1 \arrow[r] \arrow[d, "1"'] & G^n \arrow[r] \arrow[d, "1"'] & \Pi \wr G \arrow[r] \arrow[d] & \Pi \arrow[r] \arrow[d, "f"'] & 1 \arrow[d, "1"'] \\
1 \arrow[r] & G^n \arrow[r] & \Sigma_n \wr G \arrow[r] & \Sigma_n \arrow[r] & 1
\end{tikzcd}$$

Consider the Lyndon-Hochschild-Serre spectral sequence for this extension with coefficients in a field $\mathbb{F}$ in homology. Then,

$$E^2_{s,t} = H_s(\Pi; H_t(G^n, \mathbb{F})).$$

A modification and interpretation of some earlier results of Steenrod are given in [6], Lemmas 4.1-4.3, and these imply that $E^2 = E^\infty$. A similar assertion applies in cohomology if $H^*(G;\mathbb{F})$ is of finite type.

Next, notice that $H_*(G^n;\mathbb{F})$ is isomorphic to $V^{\otimes n}$ for $V = H_*(G;\mathbb{F})$. As a module over Σ_n, and hence as a module over G, $V^{\otimes n}$ is a direct sum of cyclic Σ_n-modules which depend on choices of partitions of $\{1, 2, ..., n\}$, say M_Λ. For example, if G is the trivial group, then $V = \mathbb{F}$ concentrated in degree 0, and the modules M_Λ are always trivial.

As a second example, assume that the b_α run over a totally ordered basis for $H_*(G;\mathbb{F})$. Consider the cyclic Σ_n-module generated by the element

$$\lambda = b_{\alpha_1}^{\otimes n_1} \otimes b_{\alpha_2}^{\otimes n_2} \cdots \otimes b_{\alpha_q}^{\otimes n_q}$$

where

1. P is an ordered partition of n such that $P = (n_1, n_2, \cdots, n_q)$ for $n_i > 0$ with $n_1 + n_2 + \cdots + n_q = n$,
2. B is a sequence of strictly increasing basis elements with $B = (b_{\alpha_1}, b_{\alpha_2}, \cdots, b_{\alpha_q})$ for $b_{\alpha_1} < b_{\alpha_2} < \cdots < b_{\alpha_q}$, and
3. the pairs labelled by $\Lambda = (P, B)$ run over all distinct such pairs (P, B).

Then a direct sum decomposition for the Π-module $V^{\otimes n}$ is given by

$$\oplus_{\Lambda=(P,B)} M_\Lambda.$$

Consequently, there is a homology isomorphism

$$H_*(\Pi \wr G;\mathbb{F}) \to \oplus_\Lambda H_*(\Pi; M_\Lambda).$$

Furthermore, if $\Pi = \Sigma_n$, and $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, then $H_*(\Sigma_n; M_\Lambda)$ is isomorphic, apart from a degree shift given by the degree of $b_{\alpha_1}^{\otimes n_1} \otimes b_{\alpha_2}^{\otimes n_2} \cdots \otimes b_{\alpha_q}^{\otimes n_q}$, to

$$H_*(\Sigma_{n_1} \times \Sigma_{n_2} \times \cdots \Sigma_{n_q}; \mathbb{Z}/2\mathbb{Z})$$

where $\Sigma_{n_1} \times \Sigma_{n_2} \times \cdots \Sigma_{n_q}$ is the subgroup of Σ_n that fixes $b_{\alpha_1}^{\otimes n_1} \otimes b_{\alpha_2}^{\otimes n_2} \cdots \otimes b_{\alpha_q}^{\otimes n_q}$. Thus the mod-2 homology of the wreath product $\Sigma_n \wr G$ is given in terms of the mod-2 homology of subgroups of Σ_n with trivial coefficients in $\mathbb{F}_2$.

There is an analogous description over a field of odd characteristic for which modifications using trivial coefficients or coefficients in the sign representation are used. This case will not be addressed in these abbreviated notes.

Next notice that the Lyndon-Hochschild-Serre spectral sequence in cohomology with trivial coefficients in $\mathbb{F}$ collapses for the extension

$$1 \to G^n \to \Pi \wr G \to \Pi \to 1$$

by a cochain level argument provided the cohomology of G with $\mathbb{F}$ coefficients is of finite type. The resulting E_2-term is dually given in terms of (1) the cohomology of G, and (2) ordered partitions of n. This remark is stated as the following theorem.

Theorem 4.6. *The homology of $\Pi \wr G$ with field coefficients $\mathbb{F}$ is given by*

$$H_*(\Pi; H_*(G^n;\mathbb{F})) = \oplus_\Lambda H_*(\Pi; M_\Lambda).$$

Furthermore, the homology is naturally bigraded by

$$H_s(\Pi; H_t(G^n; \mathbb{F}))$$

in bidgree (s,t). The homology in total degree q is given by

$$H_q(\Pi \wr G; \mathbb{F}) = \oplus_{s+t=q} H_s(\Pi; H_t(G^n; \mathbb{F})).$$

In case $G = \Sigma_n$, these homology groups are given in terms of

1. *the additive structure of $H_*(G; \mathbb{F})$, and*
2. *ordered partitions of n as described above.*

A second interpretation of E_2 fits with the subjects in this conference. This interpretation will be illustrated in several cases below.

1. Assume that $G = \mathbb{Z}/2\mathbb{Z}$, and that the coefficient field is $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Then $H^*(BG^n; \mathbb{F}_2)$ is a polynomial ring in n indeterminates of degree 1 with the Σ_n-action specified by the polynomials in the fundamental representation of Σ_n, $\mathbb{F}_2[V_n]$. Thus the $E_2^{s,t}$-term of the Lyndon-Hochschild-Serre spectral sequence abutting to the mod-2 cohomology of $\Sigma_n \wr G$ is given by

   $$H^s(\Sigma_n; H^t((\mathbb{Z}/2\mathbb{Z})^n; \mathbb{F}_2).$$

   By the above remarks, this spectral sequence collapses, and so $E_2 = E_\infty$. Hence $H^*(\Sigma_n; \mathbb{F}_2[V_n])$ is given in terms of the cohomology of subgroups and partitions listed above.

   In addition, the cohomology of $\Sigma_n \wr G$ with field coefficients $\mathbb{F}$ is naturally bigraded, and is given by $H^s(\Sigma_n; H^t((G)^n; \mathbb{F})$ in bidegree (s,t). The invariant subalgebra $H^*(BG^n; \mathbb{F}_2)^{\Sigma_n}$ is given by $H^0(\Sigma_n; \mathbb{F}_2[V_n])$. The ring of invariants is precisely the mod-2 Dickson algebra, and has bidgree $(0,*)$ where $*$ denotes the standard grading for the Dickson algebra.

2. A similar assertion follows for $G = S^1$, and where the coefficient field is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The wreath product construction here is given by the normalizer of the maximal torus in the unitary group $U(n)$. Similarly, $H^*(BG^n; \mathbb{F}_p)$ is a polynomial ring in n indeterminates of degree 2 with the Σ_n-action specified by the fundamental representation of Σ_n, $\mathbb{F}_p[V_n])$. Again, $H^*(\Sigma_n; \mathbb{F}_p[V_n])$ is given in terms of the cohomology of subgroups of the symmetric group with the trivial representation, and partitions listed above. The resulting answer is (1) the cohomology of the wreath product, and (2) identifies the ring of invariants as the summand of cohomology group of the wreath product concentrated in bidegrees $(0,*)$.

3. Let $G = \mathbb{Z}/p^r\mathbb{Z}$, with the coefficient field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for an odd prime p. Then $H^*(BG^n; \mathbb{F}_p)$ is the tensor product of a polynomial ring in n indeterminates of degree 2 with an exterior algebra in n indeterminates of degree 1, $E[V_n]$. The Σ_n-action is specified by that on the fundamental representation which is extended multiplicatively to $\mathbb{F}_p[V_n] \otimes E[V_n]$. Again, $H^*(\Sigma_n; \mathbb{F}_p[V_n] \otimes E[V_n])$ is given in terms of the cohomology of subgroups of Σ_n with coefficients in either the trivial representation or the sign representation. The subgroups are of the form $\Sigma_{n_1} \times \Sigma_{n_2} \times \cdots \Sigma_{n_q}$ and fix $b_{\alpha_1}^{\otimes n_1} \otimes b_{\alpha_2}^{\otimes n_2} \cdots \otimes b_{\alpha_q}^{\otimes n_q}$ up to a sign.

4. These constructions are useful in characteristic zero where symmetric groups are replaced by other discrete groups such as $SL(2,\mathbb{Z})$, $Sp(2g,\mathbb{Z})$, mapping class

groups, or braid groups. In these cases, some answers are given in terms of constructions in analytic number theory. (Please see the problems below.)

5. Problems

(1): Let G be a discrete group together with a representation $\rho : G \to GL(n, R)$ for R either a finite field or the integers. Write V_n for the direct sum of n copies of R, the fundamental represention of $GL(n, R)$.

Functors given by $P[V_n]$, $E[V_n]$, and $T[V_n]$, the polynomial ring, exterior algebra, and tensor algebra respectively generated by V_n are naturally $GL(n, R)$-modules. What can be said about the cohomology groups of G with coefficients taken in $P[V_n]$, $E[V_n]$, and $T[V_n]$?

The motivation for this question is that there have been useful applications of known examples as suggested below.

1. When G is the symmetric group on n letters, Σ_n, with the natural n-dimensional representation, then the cohomology with coefficients in $P[V_n]$, $E[V_n]$, or their tensor product is known implicitly from work of Steenrod and others. For example, over the field of 2 elements, $H^*(\Sigma_n; \mathbb{F}_2[V_n])$ gives the $E_2 = E_\infty$ term of the Lyndon-Hochschild-Serre spectral sequence abutting to the mod-2 cohomology of the wreath product
$$\Sigma_n \wr \Sigma_2$$
(where $\Sigma_n \wr G$ is a group extension $1 \to G^n \to \Sigma_n \wr G \to \Sigma_n \to 1$).

   The additive structure of the E_2- term is given in terms of partitions, and the cohomology of certain choices of subgroups of the symmetric groups obtained from these partitions.

   Related remarks concerning representations, as well as subgroups of the symmetric groups are recalled in Cohen's lecture notes.

2. When $G = SL(2, \mathbb{Z})$, and $V_2 = \mathbb{Z} \oplus \mathbb{Z}$, the rational cohomology of G with coefficients in $P[V_2]$, $E[V_2]$, or their tensor product is known in terms of classical modular cusp forms based on the standard $SL(2, \mathbb{Z})$-action on the upper 1/2-plane. These calculations trace back to work of Eichler, and Shimura on automorphic forms [11, 29, 13].

3. When G is $GL(n, R)$, then S. Betley has proven a general vanishing theorem for these coefficients as n goes to infinity. According to Betley, the analogous question for the symplectic groups remain undecided.

4. When G is the mapping class group for a closed surface of genus g, Γ_g, there is an epimorphism
$$\Gamma_g \to Sp(2g, \mathbb{Z}).$$
The cohomology groups $H^*(\Gamma_g; \mathbb{Q}[V_{2g}])$ have been studied by E. Looijenga who has obtained a stability result. These groups as well as $H^*(\Gamma_g; \mathbb{Q}[V_{2g}] \otimes E[V_{2g}])$ inform on the cohomology of mapping class groups for punctured surfaces.

5. In the special case of $R = \mathbb{Z}/2\mathbb{Z}$, there is an isomorphism $\Sigma_6 \to Sp(4, R)$. What is $H^*(\Sigma_6; R[V_4] \otimes_{\mathbb{Z}/2\mathbb{Z}} E[V_4])$?

(2): Describe the Dyer-Lashof algebra as a collection of natural transformations as suggested by Bisson's lecture, and in the spirit of Smith's lectures. Selick, and Campbell have given a construction which pieces together the Steenrod algebra together with the Dyer-Lashof algebra into one giant natural algebraic construction. Is this object describing the natural transformations of certain natural choices of functors ?

(3): Two important questions which arise in Wu's work and which were stated above are as follows: Consider the n natural homomorphisms

$$d_i : P_n \to P_{n-1}$$

obtained by deleting the $i-th$ strand for $1 \leq i \leq n$. What is a free basis for the kernel of the induced homomorphism

$$d : P_n \to \prod_{1 \leq i \leq n} P_{n-1}?$$

What is the kernel of the natural homomorphism

$$\gamma \times d : P_n \to P_n(S^2) \times \prod_{1 \leq i \leq n} P_{n-1}?$$

(4): Characterize the image of $F[S^1]$, as well as the subgroups given by chains, cycles, and boundaries in the set of isotopy classes of links.

(5): Find useful group theoretic characterizations of the homotopy groups of spheres. Do these "fit" with the braid groups ? How does the structure of the isotopy classes of n-component links impact the homotopy groups of the 2-sphere ? Find interesting analogues of the Kahn-Priddy theorem which apply to the $(2n+1)$-sphere and which are natural extensions of the analogue for the 3-sphere.

References

[1] S. Araki, and T. Kudo, *Topology of H_n-spaces and H-squaring operations*, Mem. Fac. Sci. Kyūsyū Univ. Ser. A. 10 (1956), 85–120.

[2] E. Artin, *Theorie der Zöpfe* Hamburg Abhandlung, **4** (1925), 47-72.

[3] E. Artin, *Theory of braids*, Ann. of Math., **48** (1947), 101-126.

[4] M. G. Barratt and P. J. Eccles, *Γ^+-structures. I. A free group functor for stable homotopy theory*, Topology **13** (1974), 25–45, *Γ^+-structures. II. A recognition principle for infinite loop spaces*, Topology **13** (1974), 113–126, and *Γ^+-structures. III. The stable structure of $\Omega^\infty\Sigma^\infty A$*, Topology **13** (1974), 199–207.

[5] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies, **82** (1974), Princeton University Press.

[6] F. R. Cohen, *Homology of C_{n+1}-spaces* , Springer-Verlag, L. N. M. **533** (1976), 207–351.

[7] F. R. Cohen, J. C. Moore and J. A. Neisendorfer, *The double suspension and exponents of the homotopy groups of spheres*, Annals of Math., 110 (1979), 549–565.

[8] F. R. Cohen, and J. Wu, A remark on the homotopy groups of $\Sigma^n\mathbb{RP}^2$, Cont. Math. 181 (1995), 65–81.

[9] E. Curtis, *Simplicial Homotopy Theory*, Advances in Math., 6 (1968), 107–209.

[10] E. Dyer and R. Lashof, *Homology of iterated loop spaces*, Amer. J. Math., **84** (1962), 35–88.

[11] M. Eichler, *Eine Verallgemeinerung der Abelschen Integrale*, Math. Zeit., 67(1957), 267-298.

[12] E. Fadell and L. Neuwirth, *Configuration spaces*, Math. Scand. **10** (1963), 111–118.

[13] M. Furusawa, M. Tezuka, and N. Yagita, *On the cohomology of classifying spaces of torus bundles, and automorphic forms*, J. London Math. Soc., (2)37(1988), 528-543.

[14] T. Ganea, *A generalization of the homology and homotopy suspension*, Comment. Math., Helv. 39 1965 295–322.

[15] D. S. Kahn, S. B. Priddy, *The transfer and stable homotopy theory*, Math. Proc. Cambridge Philos. Soc. 83 (1978), no. 1, 103–111.

[16] W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory*, Dover Publications, Inc., 1966.

[17] J. P. May *Simplicial objects in Algebraic Topology*, van Nostrand Math Studies, 11,1967.

[18] J. P. May, *The Geometry of Iterated Loop Spaces*, Springer-Verlag, L. N. M., **271** (1972).

[19] R. J. Milgram, *Iterated loop spaces*, Ann. of Math., **84** (1966), 386–403.

[20] J. Milnor *Universal Bundles I and II* , Ann. of Math..

[21] J. Milnor *On the construction $F(K)$*, Algebraic Topology- A Student Guide, by J.F. Adams, 119-136,Cambridge Univ. Press.

[22] J. C. Moore, *Homotopie des complexes monöideaux* Seminaire Henri Cartan, (1954-55).

[23] J. Mukai, *On the attaching map in the Stiefel manifold of 2-frames*, Math. J. Okayama Univ. 33 (1991), 177–188.

[24] M. Nakaoka, *Homology of the infinite symmetric group*, Ann. of Math. (2) 73 1961

[25] J. A. Neisendorfer, *The exponent of a Moore space*, Annals of Math. Studies, 113 (1987), 35-58.

[26] H. J. Samelson, *A connection between the Whitehead and the Pontryagin product*, Amer. J. Math., 75, (1953). 744–752.

[27] G. Segal, *Configuration spaces and iterated loop spaces*, Invent. Math., **21** (1973), 213–221.

[28] P. Selick, *Odd primary torsion in $\pi_k(S^3)$*, Topology 17 (1978),4, 407–412.

[29] G. Shimura, *Introduction to the arithmetic theory of automorphic forms*, Publications of the Mathematical Society of Japan 11, Iwanami Shoten, Tokyo; University Press, Princeton, 1971.

[30] G. W.Whitehead, *Elements of Homotopy Theory*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, and New York, 1978.

[31] J. Wu, *Combinatorial descriptions of the homotopy groups of certain spaces*, Math. Proc. Camb. Philos. Soc. to appear.

Department of Mathematics, University of Rochester, Rochester, NY 14627
E-mail address: `cohf@math.rochester.edu`
URL: `http://www.math.rochester.edu/u/cohf`

An Algebraic Introduction to the Steenrod Algebra
Summer School
Interactions Between Invariant Theory and Algebraic Topology
Ioannina, Greece, June 26 – June 30, 2000

Larry Smith

AG-Invariantentheorie

PRELIMINARY

MATHEMATICS SUBJECT CLASSIFICATION : 13A50 Invariant Theory

Typeset by *LS*TEX

During the month of June 2000 Fred Cohen (University of Rochester, USA) and I, directed, and lectured to, a summer school at the University of Ioannina in Greece. The purpose of the summer school was to make some of the recent developments on the interface of invariant theory and algabraic topology accesible to students. This proved not to be an easy undertaking, and in the year before the summer school, Fred and I spent many hours discussing in person, and weeks exchanging `e-mail` mesages, the problems connected with organizing a coherent program, i.e., selecting from the material with which we were familiar to create a program that hung together well.

One topic that seemed central to our planning was the Steenrod algebra. Beginning with the paper of J. F. Adams and C. W. Wilkerson [1], it has had a significant influence on the development of invariant theory (see e.g. [21], [22], [18], and [17] and their reference lists). This presented us with the problem of explaining the Steenrod algebra to non algebraic topologists in a concise, motivated, and nontechnical[1] algebraic manner. A decade ago at Yale I was confronted with the same problem when teaching a course on invariant theory to an audience consisting primarily of algbraicists, group theorists, and number theorists. I explained how I did this to Fred: the basic idea was to regard the total Steenrod operation as a perturbation of the Frobenius map, and to define the Steenrod algebra as a subalgebra of the endomorphisms of a certain functor gotten from this perturbation.

This got Fred to thinking about some things he was familiar with, which had a similar nature. These he explained to me. In the course of doing so, we found that a common, but not well brought out theme, in many of the topics we felt to be relevent for the summer school, was the structure of a subgroup, or subalgebra, of automorphisms of a functor: generally a simple and easily understood functor, where the subgroup, or subalgebra, had a natural origin. We decided to organize the summer school around this theme.

The purpose of these notes is to provide an introduction to the Steenrod algebra in this manner, i.e., presented as a subalgebra of the algebra of endomorphisms of a functor. The functor assigns to a vector space over a Galois field the algebra of polynomial functions on that vector space, and the subalgebra is specified by means of the Frobenius map.

The material presented here is not new: in fact most of the ideas go back to the middle of the last century, and are to be found in papers of H. Cartan [6], [7], J.-P. Serre [19], R. Thom [28] and Wu-Wen Tsün [33], with one key ingrediant being supplied by S. Bullet and I. Macdonald [5] (see also T.P. Bisson [3]). My contribution, if there is one, is to reorganize the presentation of this material so that no algebraic topology is used, nor is it necessary to assume that the ground field is the prime field. This way of presenting things appeared in print spread through Chapters 10 and 11 of[2] [21]. (See also [20].) For the summer school I collected all this, stripped it of the applications to algebraic topology, and expanded it to include the Hopf algebra structure of the Steenrod algebra due to J.W. Milnor [13] for the prime field.

I have kept these notes to a minimum, and can only encourage the reader to consult the vast literature on the Steenrod algebra. For orientation in this morass the reader can do no better than to consult the excellent survey artical [31]. In addition to the references already mentioned, the course notes from the lectures of Prof. R. Wood at the Summer School [32] in Ioannina provide an excellent list of accesible papers and problems (sic!).

In what follows we adhere to the notations and terminology of [21] and [18]. In particular,

[1] No Eilenberg-MacLane spaces, no $\cup_1$ products, etc.

[2] The emphasis in Chapter 10 of [21] is on certain topological applications: in these notes, and at the summer school in Ioannina, I replaced this with some examples from invariant theory.

if $\mathbb{F}$ is a field and $V = \mathbb{F}^n$ is an n-dimenaional vector space over $\mathbb{F}$, then $\mathbb{F}[V]$ denotes the graded algebra of polynomial functions on V. This may be regarded as the symmetric algebra on the dual vector space V^* of V, where the elements of V^*, the linear forms, have degree 1. Note carefully we ignore the usual topological sign conventions, since graded commutation rules play no role here. (For a discussion of gradings see e.g., [18] Appendix A Section 1.) The correspondence $V \rightsquigarrow \mathbb{F}[V]$ defines a contravariant functor from vector spaces over $\mathbb{F}$ to graded connected algebras, which is at the center of what follows.

§1. The Steenrod Algebra

We fix once and for all a Galois field $\mathbb{F}_q$ of characteristic p containing $q = p^\nu$ elements. Denote by $\mathbb{F}_q[V][[\xi]]$ the power series ring over $\mathbb{F}_q[V]$ in an additional variable ξ, and set $\deg(\xi) = 1 - q$. Define an $\mathbb{F}_q$-algebra homomorphism of degree zero

$$P(\xi) : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V][[\xi]],$$

by requiring

$$P(\xi)(\ell) = \ell + \ell^q \xi \in \mathbb{F}_q[V][[\xi]], \quad \forall \text{ linear forms } \ell \in V^*.$$

For an arbitrary polynomial $f \in \mathbb{F}_q[V]$, we have after separating out homogeneous components, [3]

$$(\bigstar) \qquad P(\xi)(f) = \begin{cases} \sum\limits_{i=0}^{\infty} \mathcal{P}^i(f)\xi^i & \text{if } p \text{ is odd,} \\ \sum\limits_{i=0}^{\infty} \mathrm{Sq}^i(f)\xi^i & \text{if } p = 2. \end{cases}$$

This defines $\mathcal{P}^i$, resp. Sq^i, as $\mathbb{F}_q$-linear maps

$$\mathcal{P}^i, \mathrm{Sq}^i : \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V].$$

These maps are functorial in V. The operations $\mathcal{P}^i$, respectively Sq^i, are called **Steenrod reduced power operations**, respectively **Steenrod squaring operations**, or collectively, **Steenrod operations**. In order to avoid a separate notation for the case $p = 2$, with the indulgence of topologists, [4] we set $\mathrm{Sq}^i = \mathcal{P}^i$ for all $i \in \mathbb{N}_0$.

The sums appearing in ($\bigstar$) are actually finite. In fact $P(\xi)(f)$ is a *polynomial* in ξ of degree $\deg(f)$ with leading coefficient f^q. This means the Steenrod operations acting on $\mathbb{F}_q[V]$ satisfy the **unstability condition**

$$\mathcal{P}^i(f) = \begin{cases} f^q & \text{if } i = \deg(f), \\ 0 & \text{if } i > \deg(f), \end{cases} \quad \forall f \in \mathbb{F}_q[V].$$

Note that these conditions express both a triviality condition, viz., $\mathcal{P}^i(f) = 0$ for all $i > \deg(f)$, and, a nontriviality condition, viz., $\mathcal{P}^{\deg(f)}(f) = f^q$. It is the interplay of these two requirements that seems to endow the unstability condition with the power to yield unexpected consequences.

Next, observe that the multiplicativity of the operator $P(\xi)$ leads to the formulae:

$$\mathcal{P}^k(f'f'') = \sum_{i+j=k} \mathcal{P}^i(f')\mathcal{P}^j(f''), \quad \forall f', f'' \in \mathbb{F}_q[V].$$

These are called the **Cartan formulae** for the Steenrod operations. (N.b., in field theory, a family of operators satisfying these formulae is called a **higher order derivation**. See, e.g., [12] Chapter 4, Section 9.)

[3] Let me emphasize here, that we will have no reason to consider nonhomogeneous polynomials, and implicitly, we are always assuming, unless the contrary is stated, that all algebras are graded, and if nonnegatively graded, also connected. The algebra $\mathbb{F}[V][[\xi]]$ is graded, but no longer connected.

[4] This is **not** the usual topological convention, which would be to set $\mathcal{P}^i = \mathrm{Sq}^{2i}$. This is only relevant for this algebraic approach when it is necessary to bring in a Bockstein operation.

As a simple example of how one can compute with these operations consider the quadratic form

$$Q = x^2 + xy + y^2 \in \mathbb{F}_2[x, y].$$

Let us compute how the Steenrod operations Sq^i act on Q by using linearity, the Cartan formula, and unstability.

$$\begin{aligned}
\mathrm{Sq}^1(Q) &= \mathrm{Sq}^1(x^2) + \mathrm{Sq}^1(xy) + \mathrm{Sq}^1(y^2)\\
&= 2x\mathrm{Sq}^1(x) + \mathrm{Sq}^1(x)\cdot y + x\cdot \mathrm{Sq}^1(y) + 2y\mathrm{Sq}^1(y)\\
&= 0 + x^2y + xy^2 + 0 = x^2y + xy^2,\\
\mathrm{Sq}^2(Q) &= Q^2 = x^4 + x^2y^2 + y^4,\\
\mathrm{Sq}^i(Q) &= 0 \text{ for } i > 2.
\end{aligned}$$

Since the Steenrod operations are natural with respect to linear transformations between vector spaces they induce endomorphisms of the functor

$$\mathbb{F}_q[-] : \mathcal{V}ect_{\mathbb{F}_q} \longrightarrow \mathcal{A}lg_{\mathbb{F}_q}$$

from $\mathbb{F}_q$-vector spaces to commutative graded $\mathbb{F}_q$-algebras. They therefore commute with the action of $\mathrm{GL}(V)$ on $\mathbb{F}_q[V]$. If $G \hookrightarrow \mathrm{GL}(n, \mathbb{F}_q)$ is a faithful representation of a finite group G then the Steenrod operations restrict to the ring of invariants $\mathbb{F}_q[V]^G$, i.e., map invariant forms to invariant forms. Hence they can be used to produce new invariants from old ones. This is a new feature of invariant theory over finite fields as opposed to arbitrary fields (but do see in this connection [10]). Here is an example to illustrate this. It is based on a result, and the methods of [23].

EXAMPLE 1: Let $\mathbb{F}_q$ be the Galois field with q elements of odd characteristic p, and consider the action of the group $\mathrm{SL}(2, \mathbb{F}_q)$ on the space of binary quadratic forms over $\mathbb{F}_q$ by change of variables. A typical such form is $Q(x, y) = ax^2 + 2bxy + cy^2$.

$$\mathbf{T}_Q = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

The space of such forms can be identified with the vector space $\mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)$ of 2×2 symmetric matrices over $\mathbb{F}_q$. Under this identification the form Q corresponds to the matrix $\mathbf{T}_Q$ at the left, and the action of $\mathrm{SL}(2, \mathbb{F}_q)$ is given by $\mathbf{T}_Q \longmapsto \mathbf{S}\mathbf{T}_Q\mathbf{S}^{\mathrm{tr}}$, where $\mathbf{S} \in \mathrm{SL}(2, \mathbb{F}_q)$, with $\mathbf{S}^{\mathrm{tr}}$ the transpose of $\mathbf{S}$. The element $-\mathbf{I} \in \mathrm{SL}(2, \mathbb{F}_q)$ acts trivially. By dividing out the subgroup it generates, we receive a faithful representation of $\mathrm{PSL}(2, \mathbb{F}_q) = \mathrm{SL}(2, \mathbb{F}_q)/\{\pm\mathbf{I}\}$ on the space of binary quadratic forms. This group has order $q(q^2 - 1)/2$.

The action of $\mathrm{PSL}(2, \mathbb{F}_q)$ on $\mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)$ preserves the quadratic form $\det : \mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ and since there is only one, up to isomorphism, nonsingular quadratic form in 3 variables over $\mathbb{F}_q$ (cf., [9] §169–173), we receive an unambiguous faithful representation $\rho : \mathrm{PSL}(2, \mathbb{F}_q) \hookrightarrow \mathbb{O}(3, \mathbb{F}_q)$. Denote by

$$\begin{bmatrix} x & y \\ y & z \end{bmatrix} \in \mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)^*$$

a generic linear form on the dual space of the 2×2 symmetric matrices over $\mathbb{F}_q$. Per definition the quadratic form

$$\det = xz - y^2 \in \mathbb{F}_q[\mathrm{Mat}^{\mathrm{sym}}_{2,2}(\mathbb{F}_q)] = \mathbb{F}_q[x, y, z]$$

is $\mathbb{O}(3, \mathbb{F}_q)$-invariant. If we apply the first Steenrod operation to this form we receive the new invariant form of degree $q + 1$, viz.,

$$\mathcal{P}^1(\det) = x^q z + xz^q - 2y^{q+1} \in \mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)}.$$

The full ring of invariants of the orthogonal group $\mathbb{O}(3, \mathbb{F}_q)$ is known (see, e.g., [8] or [23]). To wit

$$\mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)} \cong \mathbb{F}_q[\det, \mathcal{P}^1(\det), \mathbf{E}_{\det}].$$

Here $\mathsf{E}_{\det}$ is the Euler class (see e.g. [26] or [18] Chapter 4) associated to the configuration of linear forms defining the set of external lines to the projective variety $\mathfrak{X}_{\det}$ in the projective plane $\mathbb{PF}_q(2)$ over $\mathbb{F}_q$ defined by the vanishing of the determinant [5] (see [11] Section 8.2 and [23]). The form $\mathsf{E}_{\det}$ has degree $q(q-1)$. The three forms $\det, \mathcal{P}^1(\det), \mathsf{E}_Q \in \mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)}$ are a system of parameters [23].. Since the product of their degrees is $|\mathbb{O}(3, \mathbb{F}_q)|$ it follows from [21] Proposition 5.5.5 that $\mathbb{F}_q[x, y, z]^{\mathbb{O}(3,\mathbb{F}_q)}$ must be a polynomial algebra as stated.

The pre-Euler class $\mathsf{e}_{\det}$ of the set of external projective lines to $\mathfrak{X}_{\det}$ is an $\mathbb{O}(3, \mathbb{F}_q)$ det-relative invariant, so is $\mathbb{SO}(3, \mathbb{F}_q)$-invariant. It has degree $\binom{q}{2}$, and together with the forms det and $\mathcal{P}^1(\det)$ it forms a system of parameters for $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3,\mathbb{F}_q)}$, so again we may apply Proposition 5.5.5 and conclude that $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3,\mathbb{F}_q)}$ is a polynomial algebra, viz., $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3,\mathbb{F}_q)} = \mathbb{F}_q[\det, \mathcal{P}^1(\det), \mathsf{e}_{\det}]$.

Finally, $\mathrm{PSL}(2, \mathbb{F}_q)$ is the commutator subgroup of $\mathbb{SO}(3, \mathbb{F}_q)$ and has index 2 in $\mathbb{SO}(3, \mathbb{F}_q)$, so by a Proposition in [25] the ring of invariants of $\mathrm{PSL}(2, \mathbb{F}_q)$ acting on the space of binary quadratic forms is a hypersurface. It has generators $\det, \mathcal{P}^1(\det), \mathsf{e}_{\det}$ and a certain form ω which satisfies a monic quadratic equation over the subalgebra generated by the first three. A choice for ω is the pre-Euler class of the configuration of interior projective lines to the variety $\mathfrak{X}_{\det} \subset \mathbb{PF}(3)$.

The Steenrod operations can be collected together to form an algebra, in fact a Hopf algebra (see Section 4), over the Galois field $\mathbb{F}_q$.

DEFINITION: The **Steenrod algebra** $\mathscr{P}^*(\mathbb{F}_q)$ is the $\mathbb{F}_q$-subalgebra of the endomorphism algebra of the functor $\mathbb{F}_q[-]$, generated by $\mathcal{P}^0 = 1, \mathcal{P}^1, \mathcal{P}^2, \ldots$

NOTATION: In most situations, such as here, the ground field $\mathbb{F}_q$ is fixed at the outset, and we therefore abreviate $\mathscr{P}^*(\mathbb{F}_q)$ to $\mathscr{P}^*$.

The next sections develop the basic algebraic structure of the Steenrod algebra

§2. The Adem-Wu Relations

The Steenrod algebra is by no means freely generated by the Steenrod reduced powers. For example, when $p=2$ it is easy to check that $\mathrm{Sq}^1\mathrm{Sq}^1 = 0$ by verifying this is the case for monomials $z^E = z_1^{e_1}, \ldots, z_n^{e_n}$: to do so one needs the formula, valid for any linear form, $\mathrm{Sq}^1(z^k) = kz^{k+1}$, which follows by induction immediately from the Cartan formula. [6]

Traditionally, relations between the Steenrod operations are expressed as commutation rules for $\mathcal{P}^i\mathcal{P}^j$, respectively $\mathrm{Sq}^i\mathrm{Sq}^j$. These commutation relations are called **Adem-Wu relations**. In the case of the prime field $\mathbb{F}_p$ they were originally conjectured by Wu Wen-Tsün based on his study of the mod p cohomology of Grassmann manifolds [33] and proved by J. Adem in [2], H. Cartan in [6], and for $p = 2$ by J.-P. Serre in [19]. These relations are usually written as follows:

$$\mathcal{P}^i\mathcal{P}^j = \sum_{k=0}^{[i/q]} (-1)^{i-qk} \binom{(q-1)(j-k)-1}{i-qk} \mathcal{P}^{i+j-k}\mathcal{P}^k \quad \forall\, i, j \geq 0,\, i < qj.$$

Note for any Galois field $\mathbb{F}_q$ the coefficients are still elements in the prime subfield $\mathbb{F}_p$ of $\mathbb{F}_q$.

The proof of these relations is greatly simplified by the **Bullett-Macdonald identity**, which provides us with a well-wrapped description of the relations among the Steenrod operations, [5]. To describe this identity, as in [5], extend $P(\xi)$ to a ring homomorphism $P(\xi)$:

[5] The projective plane of $\mathbb{F}_q$ is defined by $\mathbb{PF}_q(2) = (\mathbb{F}_q^3 \setminus \{0\})^{\mathbb{F}^\times}$ where $\mathbb{F}^\times$ acts via scalar multiplication on the vectors of $\mathbb{F}_q^3$ In this discussion we are identifying $\mathbb{F}_q^3$ with $\mathrm{Mat}_{2,2}^{\mathrm{sym}}(\mathbb{F}_q)$, so this is the same as the set of lines through the origin in $\mathrm{Mat}_{2,2}^{\mathrm{sym}}$. The pre-Euler class $\mathsf{e}_{\det}$ may be taken to be the product of a set of linear forms $\{\ell_{\mathsf{L}}\}$, indexed by the $\binom{q}{2}$ external lines $\{\mathsf{L}\}$ to $\mathfrak{X}_{\det}$, and satisfying $\ker(\ell_{\mathsf{L}}) = \mathsf{L}$. The Euler class $\mathsf{E}_{\det}$ is its square.

[6] In fact every element in the Steenrod algebra is nilpotent: but the index of nilpotence is known only in a few cases, see e.g. [15], [16], [29], [30] and [31] for a resumé of what is known.

$\mathbb{F}[V][\eta] \longrightarrow \mathbb{F}[V][\eta][\xi]$ by setting $P(\xi))(\eta) = \eta$. Next, set $u = (1-t)^{q-1} = 1 + t + \cdots + t^{q-1}$ and $s = tu$. Then the Bullet-Macdonald identity is

$$P(s) \circ P(1) = P(u) \circ P(t^q).$$

Since $P(\xi)$ is additive and multiplicative, it is enough to check this equation for the basis elements of V^*, which is indeed a short calculation. Rumor says, Macdonald, like most of us, could not remember the coefficients that appear in the Adem relations, so devised this identity so that he could derive them on the spot when J. F. Adams came to talk with him.

REMARK: For $p = 2$ T.P. Bisson has pointed out (see [4]) that the Bullet-Macdonald may be viewed as a commutation rule, viz., $P(\xi)P(\eta) = P(\eta)P(\xi)$. For a general Galois $\mathbb{F}_q$, one needs to demand $\mathrm{GL}(2, \mathbb{F}_q)$-invariance of $P(\zeta)$, where $\zeta \in \mathrm{Span}_{\mathbb{F}_q}\{\xi, \eta\}$.

To derive the Adem-Wu relations we provide details for the residue computation [7] sketched in [5]. First of all, direct calculation gives:

$$P(s)P(1) = \sum_{a,\, k} s^a \mathcal{P}^a \mathcal{P}^k$$

$$P(u)P(t^q) = \sum_{a,\, b,\, j} u^{a+b-j} t^{qj} \mathcal{P}^{a+b-j} \mathcal{P}^j$$

which the Bullett-Macdonald identity says are equal. Recall from complex analysis that

$$\frac{1}{2\pi i} \oint_\gamma z^m dz = \begin{cases} 1 & m = -1 \\ 0 & \text{otherwise} \end{cases}$$

where γ is a small circle around $0 \in \mathbb{C}$. Therefore we obtain

$$\begin{aligned} \sum_k \mathcal{P}^a \mathcal{P}^k &= \frac{1}{2\pi i} \oint_\gamma \frac{P(s)P(1)}{s^{a+1}} ds \\ &= \frac{1}{2\pi i} \oint_\gamma \frac{P(u)P(t^q)}{s^{a+1}} ds \\ &= \frac{1}{2\pi i} \sum_{a,\, b,\, j} \oint_\gamma \frac{u^{a+b-j} t^{qj}}{s^{a+1}} ds \mathcal{P}^{a+b-j} \mathcal{P}^j \end{aligned}$$

The formula $s = t(1-t)^{q-1}$ gives $ds = (1-t)^{q-2}(1-qt)dt$, so substituting gives

$$\begin{aligned} \frac{u^{a+b-j} t^{qj}}{s^{a+1}} ds &= \frac{(1-t)^{(q-1)(a+b-j)} t^{qj} (1-t)^{q-2}(1-qt)}{\left[t(1-t)^{q-1}\right]^{a+1}} dt \\ &= (1-t)^{(b-j-1)(q-1)+(q-2)} t^{qj-a-1}(1-qt)dt \\ &= (1-t)^{((b-j)(q-1)-1)} t^{qj-a-1}(1-qt)dt \\ &= \left[\sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} t^k\right] t^{qj-a-1}(1-qt)dt \\ &= \sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} \left[t^{k+qj-a-1} - q t^{k+qj-a}\right] d\,t. \end{aligned}$$

Therefore

$$\begin{aligned} \mathcal{P}^a \mathcal{P}^b &= \sum_j \left[\frac{1}{2\pi i} \oint_\gamma \frac{u^{a+b-j} t^{qj}}{s^{a+1}} ds\right] \mathcal{P}^{a+b-j} \mathcal{P}^j \\ &= \sum_j \frac{1}{2\pi i} \oint \sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} \left[t^{k+qj-a-1} - q t^{k+qj-a}\right] dt \mathcal{P}^{a+b-j} \mathcal{P}^j. \end{aligned}$$

[7] The following discussion is based on conversations with E.H. Brown Jr. I do hope I have come close to getting the indices correct for once.

Only the terms where

$$\begin{aligned} k + qj - a - 1 &= -1 \quad (k = a - qj) \\ k + qj - a &= -1 \quad (k = a - qj - 1) \end{aligned}$$

contribute anything to the sum, so

$$\mathcal{P}^a\mathcal{P}^b = \sum_j \left[(-1)^{a-qj)}\binom{(b-j)(q-1)-1}{a-qj} + (-1)^{a-qj-1}q\binom{(b-j)(q-1)-1}{a-qj-1}\right]\mathcal{P}^{a+b-j}\mathcal{P}^j$$

and since

$$\binom{(b-j)(q-1)-1}{a-qj} - q\binom{(b-j)(q-1)-1}{a-qj-1} \equiv \binom{(b-j)(q-1)-1}{a-qj} \bmod p$$

we conclude

$$\mathcal{P}^a\mathcal{P}^b = \sum_j (-1)^{a-qj}\binom{(b-j)(q-1)-1}{a-qj}\mathcal{P}^{a+b-j}\mathcal{P}^j.$$

Thus there is a surjective map from the free associative algebra with 1 generated by the Steenrod operations modulo the ideal generated by the Adem-Wu relations,

$$\mathcal{P}^a\mathcal{P}^b - \sum_j (-1)^{a-qj}\binom{(b-j)(q-1)-1}{a-qj}\mathcal{P}^{a+b-j}\mathcal{P}^j \quad a, b \in \mathbb{N} \text{ and } a < qb,$$

onto the Steenrod algebra. Denote this quotient algebra by $\mathcal{B}^*$. In fact, this map, $\mathcal{B}^* \longrightarrow \mathcal{P}^*$ is an isomorphism, so the Adem-Wu relations are a complete set of defining relations for the Steenrod algebra. The proof of this, and some of its consequences, is the subject of the next section.

§3. The Basis of Admissible Monomials

In this section we show that the relations between Steenrod operations that are universally valid all follow from the Adem-Wu relations. To do so we extend some theorems of of H. Cartan, [6], J.-P. Serre, [19], and Wu Wen Tsün, [33] from the case of the prime field to arbitrary Galois fields. We also rearrange their proofs so that they do not make any direct use of topology.

An **index sequence** is a sequence $I = (i_1, i_2, \ldots, i_k, \ldots)$ of nonnegative integers, almost all of which are zero. If I is an index sequence we denote by $\mathcal{P}^I \in \mathcal{P}^*$ the monomial $\mathcal{P}^{i_1} \cdot \mathcal{P}^{i_2} \ldots \mathcal{P}^{i_k} \ldots$ in the Steenrod operations $\mathcal{P}^i$, with the convention that trailing 1s are ignored. The degree of the element $\mathcal{P}^I$ is $(q-1)(j_1 + j_2 + \cdots + j_k + \cdots)$. These iterations of Steenrod operations are called **basic monomials**. An index sequence I is called **admissible** if $i_s \geq q i_{s+1}$ for $s = 1, \ldots$. We call k the **length** of I if $i_k \neq 0$ but $i_s = 0$ for $s > k$. Write $\ell(I)$ for the length of I. It is often convenient to treat an index sequence as a finite sequence of nonnegative integers by truncating it to $\ell(I)$ entries.

A basic monomial is defined to be **admissible** if the corresponding index sequence is admissible. The strategy of H. Cartan and J.-P. Serre to show that the Adem-Wu relations are a complete set of defining relations for the Steenrod algebra is to prove that the admissible monomials are an $\mathbb{F}_q$ basis for $\mathcal{P}^*$.

Recall that $\mathcal{B}^*$ denotes the free, graded, associative algebra generated by the symbols $\mathcal{P}^k$ modulo the ideal spanned by the Adem-Wu relations. We have a surjective map $\mathcal{B}^* \longrightarrow \mathcal{P}^*$, and so with his notation our goal is to prove:

THEOREM 3.1: *The admissible monomials span $\mathcal{B}^*$ as an $\mathbb{F}_p$-vector space. The images of the admissible monomials in the Steenrod algebra are linearly independent.*

PROOF: We begin by showing that the admissible monomials span $\mathscr{B}^*$. For a sequence $I = (i_1, i_2, \ldots, i_k)$, the **moment** of I, denoted by $m(I)$, is defined by $m(I) = \sum_{s=1}^{k} s \cdot i_s$. We first show that an inadmissible monomial is a sum of monomials of smaller moment. Granted this it follows by induction over the moment that the admissible monomials span $\mathscr{B}^*$.

Suppose that $\mathcal{P}^I$ is an inadmissible monomial. Then there is a smallest s such that $i_s < q i_{s+1}$, i.e.,

$$\mathcal{P}^I = \mathcal{Q}' \mathcal{P}^{i_s} \mathcal{P}^{i_{s+1}} \mathcal{Q}''$$

where $\mathcal{Q}'$, $\mathcal{Q}''$ are basic monomials, and $\mathcal{Q}'$ is admissible. It is therefore possible to apply an Adem-Wu relation to $\mathcal{P}^I$ to obtain

$$\mathcal{P}^I = \sum_j a_j \mathcal{Q}' \mathcal{P}^{i_s + i_{s+1} - j} \mathcal{P}^j \mathcal{Q}''$$

for certain coefficients $a_j \in \mathbb{F}_p$. The terms on the right hand side all have smaller moment than $\mathcal{P}^I$, and so, by induction on s we may express $\mathcal{P}^I$ as a sum of admissible monomials. (N.b. The admissible monomials are *reduced* in the sense that no Adem-Wu relation can be applied to them.)

We next show that the admissible monomials are linearly independent as elements of the Steenrod algebra $\mathscr{P}^*$. This we do by adapting an argument of J.-P. Serre [19] and H. Cartan [6] which makes use of a formula of Wu Wen-Tsün.

Let $e_n = x_1 x_2 \cdots x_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ be the n-th elementary symmetric function. Then,

$$\begin{aligned} P(\xi)(e_n) &= P(\xi)(\prod_{i=1}^{n} x_i) = \prod_{i=1}^{n} P(\xi)(x_i) \\ &= \prod_{i=1}^{n}(x_i + x_i^q \xi) = \prod_{i=1}^{n} x_i \cdot \prod_{i=1}^{n}(1 + x_i^{q-1}\xi) \\ &= e_n(x_1, \ldots, x_n) \cdot \left(\sum_{i=1}^{n} e_i(x_1^{p-1}, \ldots, x_n^{q-1}) \xi^i \right), \end{aligned}$$

where $e_i(x_1, \ldots, x_n)$ denotes the i-th elementary symmetric polynomial in $x_1, \ldots, x_n$. So we have obtained a formula of Wu Wen-Tsün:

$$\mathcal{P}^i(e_n) = e_n \cdot e_i(x_1^{p-1}, \ldots, x_n^{q-1}).$$

We claim that the monomials

$$\left\{ \mathcal{P}^I \mid \mathcal{P}^I \text{ admissible and } \deg(\mathcal{P}^I) \le 2n \right\}$$

are linearly independent in $\mathbb{F}_q[x_1, \ldots, x_n]$. To see this note that in case $\ell(I) \le n$, each entry in I is at most n (so the following formula makes sense), and

$$\mathcal{P}^I(e_n) = e_n \cdot \prod_{j=1}^{s} e_{i_j}(x_1^{q-1}, \ldots, x_n^{q-1}) + \ldots$$

where $I = (i_1, \ldots, i_s)$, $\mathcal{P}^I = \mathcal{P}^{i_1} \cdots \mathcal{P}^{i_s}$ and the remaining terms are lower in the lexicographic ordering on monomials. So $e_n \cdot \prod_{j=1}^{s} e_{i_j}(x_1^{q-1}, \ldots, x_n^{q-1})$ is the largest monomial in $\mathcal{P}^I(e_n)$ in the lexicographic order. Thus

$$\left\{ \mathcal{P}^I(e_n) \mid \mathcal{P}^I \text{ admissible and } \deg(\mathcal{P}^I) \le 2n \right\},$$

have distinct largest monomials, so are linearly independent.

By letting $n \longrightarrow \infty$ we obtain the assertion, completing the proof. □

Thus the Steenrod algebra may be regarded (this is one traditional definition) as the graded free associative algebra with 1 generated by the Sq^i respectively $\mathcal{P}^i$ modulo the ideal generated by the Adem-Wu relations. This means we have proven:

THEOREM 3.2: *The Steenrod algebra $\mathcal{P}^*$ is the free associative $\mathbb{F}_q$-algebra generated by the reduced power operations $\mathcal{P}^0, \mathcal{P}^1, \mathcal{P}^2, \ldots$ modulo the Adem-Wu relations.* □

COROLLARY 3.3: *The admissible monomials are an $\mathbb{F}_q$-basis for the Steenrod algebra $\mathcal{P}^*$.* □

Since the coefficients of the Adem-Wu relations lie in the prime field $\mathbb{F}_p$, the operations $\mathcal{P}^{p^i}$ for $i \geq 0$ are indecomposables in $\mathcal{P}^*$. In particular, over the Galois field $\mathbb{F}_q$, the Steenrod algebra $\mathcal{P}^*$ is **not** generated by the operations $\mathcal{P}^{q^i}$ for $i \geq 0$: one needs all $\mathcal{P}^{p^i}$ for $i \geq 0$. This will become even clearer after we have developed the Hopf algebra structure of $\mathcal{P}^*$ in the next section.

EXAMPLE 1: Consider the polynomial algebra $\mathbb{F}_2[Q, T]$ over the field with 2 elements, where the indeterminate Q has degree 2 and T has degree 3. If the Steenrod algebra were to act unstably on this algebra then the unstability condition would determine $\mathrm{Sq}^i(Q)$ and $\mathrm{Sq}^j(T)$ apart from $i = 1$ and $j = 1$ and 2. If we specify these as follows

$$\mathrm{Sq}^1(Q) = T, \quad \mathrm{Sq}^1(T) = 0, \quad \mathrm{Sq}^2(T) = QT,$$

and demand that the Cartan formula hold, then using these formulae we can compute Sq^k on any monomial, and hence by linearity, on any polynomial in Q and T. For example

$$\mathrm{Sq}^1(QT) = \mathrm{Sq}^1(Q) \cdot T + Q \cdot \mathrm{Sq}^1(T) = T^2 + 0 = T^2,$$

and so on. Note that since $\mathrm{Sq}^1 \cdot \mathrm{Sq}^1 = 0$ is an Adem-Wu relation, $\mathrm{Sq}^1(T) = 0$ is forced from $\mathrm{Sq}^1(Q) = T$. To verify the unstability conditions, suppose that

$$\mathrm{Sq}^a \mathrm{Sq}^b = \sum_{c=0}^{[\frac{a}{2}]} \binom{b-1-c}{a-2c} \mathrm{Sq}^{a+b-c}\mathrm{Sq}^c, \qquad 0 < a < 2b,$$

is an Adem-Wu relation. We need to show that

$$\left(\mathrm{Sq}^a \mathrm{Sq}^b - \sum_{c=0}^{[\frac{a}{2}]} \binom{b-1-c}{a-2c} \mathrm{Sq}^{a+b-c}\mathrm{Sq}^c \right) (Q^i T^j) = 0$$

for all $i, j \in \mathbb{N}_0$. By a simple argument using the Cartan formulae, see, e.g., [27] Lemma 4.1, it is enough to verify that these hold for the generators Q and T, and this is routine. It is a bit more elegant to identify Q with $x^2 + xy + y^2$ and T with $x^2y + xy^2 \in \mathbb{F}_2[x, y]$. The action of the Steenrod operations on Q and T then coincides with the restriction of the action from $\mathbb{F}_2[x, y]$. This way, it is then clear that $\mathbb{F}_2[Q, T]$ is an unstable algebra over the Steenrod algebra, because with some topological background we recognize this as just $H^*(B\mathbb{SO}(3); \mathbb{F}_2)$.

§4. The Hopf Algebra Structure of the Steenrod Algebra

Our goal in this section is to complete the traditional picture of the Steenrod algebra by proving that $\mathcal{P}^*(\mathbb{F}_q)$ is a Hopf algebra [8] and extending Milnor's Hopf algebra [13] structure theorems from the prime field $\mathbb{F}_p$ to an arbitrary Galois field. It should be emphasized that this requires no new ideas, only a careful redoing of Milnor's proofs avoiding reference to algebraic topology and cohomology operations, and carefully replacing p by q where appropriate.

[8] One quick way to do this is to write down as comultiplication map

$$\nabla(\mathcal{P}^k) = \sum_{i+j=k} \mathcal{P}^i \otimes \mathcal{P}^j, \quad k = 1, 2, \ldots,$$

and verify that it is compatible with the Bullett-Macdonald identity, and hence also with the Adem-Wu relations.

PROPOSITION 4.1: *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. Then the Steenrod algebra of $\mathbb{F}_q$ is a cocommutative Hopf algebra over $\mathbb{F}_q$ with respect to the coproduct*

$$\nabla : \mathscr{P}^* \longrightarrow \mathscr{P}^* \otimes \mathscr{P}^*$$

defined by the formulae

$$\nabla(\wp^k) = \sum_{i+j=k} \wp^i \otimes \wp^j, \quad k = 1, 2, \dots .$$

PROOF: Consider the functor $V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V]$ that assigns to a finite dimensional vector space V over $\mathbb{F}_q$ the commutative graded algebra $\mathbb{F}_q[V] \otimes \mathbb{F}_q[V]$ over $\mathbb{F}_q$. There is a natural map of algebras

$$\mathscr{P}^* \otimes \mathscr{P}^* \longrightarrow \mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])$$

given by the tensor product of endomorphisms. Since there is an isomorphism $\mathbb{F}_q[V] \otimes \mathbb{F}_q[V] \cong \mathbb{F}_q[V \oplus V]$, that is natural in V, the functor $\mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])$ is a subfunctor of the functor $\mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V])$ that assigns to a finite dimensional vector space V over $\mathbb{F}_q$ the polynomial algebra $\mathbb{F}_q[V]$. Hence restriction defines a map of algebras

$$\mathscr{P}^* \longrightarrow \mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])$$

and we obtain a diagram of algebra homomorphisms

$$\begin{tikzcd} & \mathscr{P}^* \otimes \mathscr{P}^* \arrow[d, "\tau"] \\ \mathscr{P}^* \arrow[ur, dotted] \arrow[r, "\rho"] & \mathrm{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V]) \end{tikzcd}$$

What we need to show is that $\mathrm{Im}(\rho) \subseteq \mathrm{Im}(\tau)$, for since τ is monic $\nabla = \tau^{-1}\rho$ would define the desired coproduct. Since $\wp^k$ for $k = 1, 2, \dots,$ generate $\mathscr{P}^*$ it is enough to check that $\rho(\wp^k) \in \mathrm{Im}(\tau)$ for $k = 1, 2, \dots, .$ But this is immediate from the Cartan formula. Since ∇ is a map of algebras the Hopf condition is satisfied, so $\mathscr{P}^*$ is a Hopf algebra. □

If J is an admissible index sequence then

$$e(J) = \sum_{s=1}^{\infty} (j_s - q j_{s+1})$$

is called the **excess** of J. For example, the sequences

$$M_k = (q^{k-1}, \dots, q, 1), \ k = 1, 2, \dots$$

are all the admissible sequences of excess zero. Note that

$$\deg(\wp^{M_k}) = \sum_{j=1}^{k} q^{k-j}(q-1) = q^k - 1, \ \text{for } k = 1, 2, \dots .$$

Recall by Corollary 3.3 that the admissible monomials are an $\mathbb{F}_q$-vector space basis for $\mathscr{P}^*$. Let $\mathscr{P}_*(\mathbb{F}_q)$ denote the Hopf algebra dual to the Steenrod algebra $\mathscr{P}^*(\mathbb{F}_q)$. We define $\xi_k \in \mathscr{P}_*(\mathbb{F}_q)$ to be dual to the monomial $\wp^{M_k} = \wp^{q^{k-1}} \cdots \wp^q \cdot \wp^1$ with respect to the basis of admissible monomials for $\mathscr{P}^*$. This means that we have:

$$<\wp^J \mid \xi_k> = \begin{cases} 1 & \text{if } J = M_k, \\ 0 & \text{otherwise,} \end{cases}$$

where we have written $<\wp \mid \xi>$ for the value of an element $\wp \in \mathscr{P}^*(\mathbb{F}_q)$ on an element $\xi \in \mathscr{P}_*(\mathbb{F}_q)$. Note that $\deg(\xi_k) = q^k - 1$ for $k = 1, \dots, .$

If $I = (i_1, i_2, \dots, i_k, \dots)$ is an index sequence we call ℓ the **length** of I, denoted by $\ell(I)$, if $i_k = 0$ for $k > \ell$, but $i_\ell \neq 0$. We associate to an index sequence $I = (i_1, i_2, \dots, i_k, \dots)$ the element $\xi^I = \xi_1^{i_1} \cdot \xi_2^{i_2} \cdots \xi_\ell^{i_\ell} \in \mathscr{P}_*(\mathbb{F}_q)$, where $\ell = \ell(I)$. Note that

$$\deg(\xi^I) = \sum_{s=1}^{\ell(I)} i_s(q^s - 1).$$

To an index sequence $I = (i_1, i_2, \dots, i_k, \dots)$ we also associate an admissible sequence $J(I) = (j_1, j_2, \dots, j_k, \dots)$ defined by

$$(ϭ) \qquad j_1 = \sum_{s=1}^{\infty} i_s q^{s-1}, \quad j_2 = \sum_{s=2}^{\infty} i_s q^{s-2}, \dots, \quad j_k = \sum_{s=k}^{\infty} i_s q^{s-k}, \dots.$$

It is easy to verify that as I runs over all index sequences that $J(I)$ runs over all admissible sequences. Finally, note that $\deg(\mathcal{P}^{J(I)}) = \deg(\xi^I)$ for any index sequence I.

The crucial observation used by Milnor to prove the structure theorem of $\mathscr{P}_*(\mathbb{F}_q)$ is that the pairing of the admissible monomial basis for $\mathscr{P}^*(\mathbb{F}_q)$ against the monomials in the ξ_k is upper triangular. To formulate this precisely we order the index sequences lexicographically from the right, so for example $(1, 2, 0, \dots) \prec (0, 0, 1, \dots)$.

LEMMA 4.2 (J. W. Milnor): *With the preceding notations we have that the inner product matrix* $<\mathcal{P}^{J(I)} \mid \xi^K>$ *is upper triangular with* 1 *s on the diagonal, i.e.,*

$$<\mathcal{P}^{J(I)} \mid \xi^K> = \begin{cases} 1 & \text{if } I = K, \\ 0 & \text{if } I < K. \end{cases}$$

PROOF: Let the length of K be ℓ and define $K' = (k_1, k_2, \dots, k_{\ell-1})$, so

$$\xi^K = \xi^{K'} \cdot \xi_\ell \in \mathscr{P}_*(\mathbb{F}_q).$$

If ∇ denotes the coproduct in $\mathscr{P}^*(\mathbb{F}_q)$, then we have the formula

$$(✣) \qquad <\mathcal{P}^{J(I)} \mid \xi^K> = <\mathcal{P}^{J(I)} \mid \xi^{K'} \cdot \xi_\ell> = <\nabla(\mathcal{P}^{J(I)}) \mid \xi^{K'} \otimes \xi_\ell>$$

If $J(I) = (j_1, j_2, \dots, j_k, \dots)$ then one easily checks that

$$\nabla(\mathcal{P}^{J(I)}) = \sum_{J' + J'' = J(I)} \mathcal{P}^{J'} \otimes \mathcal{P}^{J''}.$$

Substituting this into (✣) gives

$$(✠) \qquad <\mathcal{P}^{J(I)} \mid \xi^K> = \sum_{J' + J'' = J(I)} <\mathcal{P}^{J'} \mid \xi^{K'}> \cdot <\mathcal{P}^{J''} \mid \xi_\ell>.$$

By the definition of ξ_ℓ we have

$$<\mathcal{P}^{J''} \mid \xi_\ell> = \begin{cases} 1 & \text{if } J'' = M_\ell, \\ 0 & \text{otherwise.} \end{cases}$$

If $J'' = M_\ell$ then unravelling the definitions shows that $J' = J(I')$, for a suitable I', so if K and I have the same length ℓ, we have shown

$$<\mathcal{P}^{J(I)} \mid \xi^K> = <\mathcal{P}^{J(I')} \mid \xi^{K'}>,$$

and hence it follows from induction over the degree that

$$<\mathcal{P}^{J(I)} \mid \xi^K> = \begin{cases} 1 & \text{if } I = K, \\ 0 & \text{if } I < K. \end{cases}$$

If, on the other hand, $\ell(I) < \ell$ then all the terms

$$<\mathcal{P}^{J''} \mid \xi_\ell>$$

in the sum (✠) are zero and hence that $<\mathcal{P}^{J(I)} \mid \xi^K> = 0$ as required. □

THEOREM 4.3: *Let p be a prime integer, $q = p^{\nu}$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. Let $\mathscr{P}_*(\mathbb{F}_q)$ denote the dual Hopf algebra to the Steenrod algebra of the Galois field $\mathbb{F}_q$. Then, as an algebra*

$$\mathscr{P}_* \cong \mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots],$$

where $\deg(\xi_k) = q^k - 1$ *for* $k \in \mathbb{N}$. *The coproduct is given by the formula*

$$\nabla_*(\xi_k) = \sum_{i+j=k} \xi_i^{q^j} \otimes \xi_j, \quad k = 1, 2, \ldots.$$

PROOF: By Milnor's Lemma (Lemma 4.2) the monomials $\{\xi^I\}$ where I ranges over all index sequences are linearly independent in $\mathscr{P}_*(\mathbb{F}_q)$. Hence $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots] \subseteq \mathscr{P}_*(\mathbb{F}_q)$. But $\mathscr{P}_*(\mathbb{F}_q)$ and $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots]$ have the same Poincaré series, since $\deg(\wp^{J(I)}) = \deg(\xi^I)$ for all index sequences I, and the admissible moniomials $\wp^{J(I)}$ are an $\mathbb{F}_q$-vector space basis for $\mathscr{P}^*(\mathbb{F}_q)$. So $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots] = \mathscr{P}_*(\mathbb{F}_q)$, and it remains to verify the formula for the coproduct. To this end we use the test algebra $\mathbb{F}_q[u]$, the polynomial algebra on one generator, as in [13]. Note that for admissible sequences we have

$$(\star) \qquad \wp^J(u) = \begin{cases} u^{q^k} & \text{if } J = M_k, \\ 0 & \text{otherwise.} \end{cases}$$

Define the map

$$\lambda^* : \mathbb{F}_q[u] \longrightarrow \mathbb{F}_q[u] \otimes \mathscr{P}_*$$

by the formula

$$\lambda^*(u^i) = \sum \wp^{J(I)}(u^i) \otimes \xi^I$$

where the sum is over all index sequences I. Note that in any given degree the sum is finite and that λ^* is a map of algebras. Moreover

$$(\lambda^* \otimes 1)\lambda^*(u) = (1 \otimes \nabla_*)\lambda^*(u),$$

i.e., the following diagram

$$☯ \qquad \begin{tikzcd}
\mathbb{F}_q[u] \otimes \mathscr{P}_*(\mathbb{F}_q) \otimes \mathscr{P}_*(\mathbb{F}_q) & \mathbb{F}_q[u] \otimes \mathscr{P}_* \arrow[l, "1\otimes\nabla_*"'] \\
\mathbb{F}_q[u] \otimes \mathscr{P}_* \arrow[u, "\lambda^*\otimes 1"] & \mathbb{F}_q[u] \arrow[l, "\lambda^*"'] \arrow[u, "\lambda^*"']
\end{tikzcd}$$

is commutative.

From $(\star)$ it follows that

$$\lambda^*(u) = \sum u^{q^k} \otimes \xi_k$$

which when raised to the q^r-th power gives

$$\lambda^*(u^r) = \sum u^{q^{k+r}} \otimes \xi_k^{q^r},$$

and leads to the formula

$$(\lambda^* \otimes 1)(\lambda^*(u)) = (\lambda^* \otimes 1)\Big(\sum_k u^{q^k} \otimes \xi_k\Big) = \sum_r \sum_k u^{q^{k+r}} \otimes \xi_r^{q^k} \otimes \xi_k.$$

Whereas, the other way around the diagram ☯ leads to

$$(1 \otimes \nabla_*)(\lambda^*(u)) = \sum_j u^{q^j} \otimes \nabla_*(\xi_k),$$

and equating these two expressions leads to the asserted formula for the coproduct. □

As remarked at the end of the previous Section the operations $\mathscr{P}^{p^i}$ for $i > 0$ are indecomposables in $\mathscr{P}^*$, so $\mathscr{P}^*$ is not generated by the operations $\mathscr{P}^{q^i}$ for $i \geq 0$; we need all the $\mathscr{P}^{p^i}$ for $i > 0$. This can be readily seen on hand from the dual Hopf algebra, where, since $\mathbb{F}_q$ has characteristic p, the elements $\xi_1^{p^i}$ for $i \geq 0$ are all primitive, [14]. The following Corollary also indicates that passing from the prime field $\mathbb{F}_p$ to a general Galois field $\mathbb{F}_q$ is not just a simple substitution of q for p.

COROLLARY 4.4: *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. The indecomposable module $Q(\mathscr{P}^*)$ of the Steenrod algebra of $\mathbb{F}_q$ has a basis consisting of the elements $\mathscr{P}^{p^i}$ for $i \in \mathbb{N}_0$, and the primitive elements $P(\mathscr{P}^*)$ has a basis consisting of the elements $\mathscr{P}^{\Delta_k}$ for $k \in \mathbb{N}$, where, for $k \in \mathbb{N}$, $\mathscr{P}^{\Delta_k}$ is dual to ξ_k with respect to the monomial basis for $\mathscr{P}_*$.* □

§5. The Milnor Basis and Embedding one Steenrod Algebra in Another

If $I = (i_1, i_2, \ldots, i_k, \ldots)$ is an index sequence we denote by $\mathscr{P}(I) \in \mathscr{P}^*(\mathbb{F}_q)$ the element in the Steenrod algebra that is dual to the corresponding monomial ξ^I in $\mathscr{P}_*(\mathbb{F}_q)$ with respect to the monomial basis for $\mathscr{P}_*(\mathbb{F}_q)$. This is not the same as the monomial $\mathscr{P}^I = \mathscr{P}^{i_1} \cdot \mathscr{P}^{i_2} \cdots \mathscr{P}^{i_k} \cdots$, these two elements do not even have the same degrees. As I ranges over all index sequences the collection $\mathscr{P}(I)$ ranges over an $\mathbb{F}_q$-basis for $\mathscr{P}^*(\mathbb{F}_q)$ called the **Milnor basis.**

To give some examples of elements written in the Milnor basis introduce the index sequence Δ_k which has a 1 in the k-th position and otherwise 0s. Then $\mathscr{P}^k$ is $\mathscr{P}(k\Delta_1)$, and, as noted at the end of Section 4, **the Milnor primitive elements** $\mathscr{P}^{\Delta_k} = \mathscr{P}(\Delta_k)$, for $k > 0$, form a basis for the subspace of all primitive elements. In terms of the reduced power operations these elements can also be defined by the inductive formulae

$$\mathscr{P}^{\Delta_k} = \begin{cases} \mathscr{P}^1 & \text{if } k = 1 \\ [\mathscr{P}^{q^{k-1}}, \mathscr{P}^{\Delta_k}] & \text{for } k > 0, \end{cases}$$

where $[\mathscr{P}', \mathscr{P}'']$ denotes the commutator $\mathscr{P}' \cdot \mathscr{P}'' - \mathscr{P}'' \cdot \mathscr{P}'$ of $\mathscr{P}'$ and $\mathscr{P}''$. In Milnor's paper one can also find a formula for the product $\mathscr{P}(I) \cdot \mathscr{P}(J)$ of two elements in the Milnor basis. The basis transformation matrix from the admissible to the Milnor basis and its inverse is quite complicated, so we will say nothing more about it.

To each index sequence I we can make correspond both an admissible sequence over $\mathbb{F}_p$ and one over $\mathbb{F}_q$ via the equations (e) from the previous Section. This correspondence gives us a map $\vartheta : \mathscr{P}^*(\mathbb{F}_q) \longrightarrow \mathscr{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$.

THEOREM 5.1: *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. The map*

$$\vartheta : \mathscr{P}^*(\mathbb{F}_q) \longrightarrow \mathscr{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$$

embeds the Steenrod algebra $\mathscr{P}^*(\mathbb{F}_q)$ of $\mathbb{F}_q$ as a Hopf subalgebra in the Steenrod algebra of $\mathbb{F}_p$ extended from $\mathbb{F}_p$ up to $\mathbb{F}_q$.

PROOF: It is much easier to verify that the dual map

$$\vartheta_* : \mathscr{P}_*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q \longrightarrow \mathscr{P}_*(\mathbb{F}_q),$$

which is defined by the requirement that it be a map of algebras, and take the values

$$\vartheta_*(\xi_k(p) \otimes 1) = \begin{cases} \xi_m(q) & \text{if } k = m\nu \text{ (so } p^k - 1 = q^m - 1) \\ 0 & \text{otherwise,} \end{cases}$$

on algbera generators, is in fact a map of Hopf algebras. This is a routine computation. □

The Steenrod algebra over the prime field $\mathbb{F}_p$ has a well known interpretation as the mod p cohomology of the Eilenberg - MacLane spectrum. By flat base change $\mathscr{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$ may be regarded as the $\mathbb{F}_q$-cohomology of the same. By including the Eilenberg - MacLane spectrum $\mathbf{K}(\mathbb{F}_p)$ for the prime field into the Eilenberg - MacLane spectrum $\mathbf{K}(\mathbb{F}_q)$ we may view the elements of $\mathscr{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$ as defining stable cohomology operations in $\mathbb{F}_q$-cohomology. By Theorem 5.1 this also allows us to interpret elements of $\mathscr{P}^*(\mathbb{F}_q)$ as stable cohomology operations acting on the $\mathbb{F}_q$-cohomology of a topological space. Which elements appear in this way is described in cohomological terms in [24].

§6. Closing Comments

Algebraic topologists will of course immediately say *"but that isn't the Steenrod algebra, it is only the algebra of reduced power operations; there is no Bockstein operator unless* $q = 2$*."* This is correct, the full Steenrod algebra, with the Bockstein, has not yet played a significant role in invariant theory, so I have not treated it here. But, if one wishes to have a definition for the full Steenrod algebra in the same style as the one presented here, all one needs to do for $q \neq 2$ is to replace the functor $V \rightsquigarrow \mathbb{F}[V]$ with the functor $V \rightsquigarrow H(V)$, where $H(V)$ is defined to be $H(V) = \mathbb{F}[V] \otimes E[V]$, with $E[V]$ the exterior algebra on the dual vector space V^* of V. Since V^* occurs *twice* as a subspace of $H(V)$, once as $V^* \otimes \mathbb{F} \subset \mathbb{F}[V] \otimes \mathbb{F}$ and once as $\mathbb{F} \otimes V^* \subset E[V]$, we need a way to distinguish these two copies. One way to do this is to write z for a linear form $z \in V^*$ when it is to be regarded as a polynomial function, and dz for the same linear form when it is to be regarded as an alternating linear form. This amounts to identifying $H(V)$ with the algebra of polynomial differential forms on V.

Next introduce the Bockstein operator $\beta : H(V) \longrightarrow H(V)$ by requiring it to be the derivation where, for an alternating linear form dz one has $\beta(dz) = z$, where z is the corresponding polynomial linear form, and for any polynomial linear form z one has $\beta(z) = 0$. The operators $\mathcal{P}^k$ for $k \in \mathbb{N}_0$ together with β generate a subalgebra of the algebra of endomorphisms of the functor $V \rightsquigarrow H(V)$, and this subalgebra is the full Steenrod algebra of the Galois field $\mathbb{F}_q$.

Finally, at the summer school T.P. Bisson spoke about his work with A. Joyal on a universal algebra approach to both the Dyer-Lashof algebra and the Steenrod algebra [4]. The interested reader should consult this paper which contains many informative facts.

References

[1] J. F. Adams and C.W. Wilkerson, *Finite H-spaces and Algebras over the Steenrod Algebra,* Annals of Math. 111 (1980), 95–143.

[2] J. Adem, *The Relations on Steenrod Powers of Cohomology Classes,* in: Algebraic Geometry and Toplogy, Edited by, R.H. Fox, D.C. Spencer and A.W. Tucker, Princeton Umiv. Press 1957.

[3] T. P. Bisson, *Divided Sequences and Bialgebras of Homology Operations,* PhD Thesis, Duke University, 1977.

[4] T. P. Bisson and A. Joyal, *Q-Rings and the Homology of the Symmetric Group,* Contemp. Math. 202 (1997), 235–286.

[5] S. R. Bullett and I. G. Macdonald, *On the Adem Relations,* Topology 21 (1982), 329–332.

[6] H. Cartan, *Sur l'Iteration des Opérations de Steenrod,* Comment. Math. Helv. 29 (1955), 40–58.

[7] H. Cartan, *Algèbres d'Eilenberg-Mac Lane et Homotopie,* Séminaire Henri Cartan, 1954/55, W. A. Benjamin, New York 1967.

[8] S. D. Cohen, *Rational Functions Invariant under an Orthogonal Group,* Bull. London Math. Soc. 22 (1990), 217 – 221.

[9] L. E. Dickson, *Linear Groups,* Dover Publications Inc., New York 1958.

[10] O. E. Glenn, *Modular Invariant Processes,* Bull. of the Amer. Math. Soc. 21 (1914-15), 167 – 173.

[11] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* Oxford Mathematical Monographs, Oxford Science Publications, Oxford 1998 second edition.

[12] N. Jacobson, *Lectures in Abstract Algebra* III *Theory of Fields and Galois Theory,* Springer-Verlag, Heidelberg, Berlin, New York, 1975.

[13] J. W. Milnor, *The Steenrod algebra and its Dual,* Annals of Math. (2) 67 (1958), 150–171.

[14] J. W. Milnor and J. C. Moore, *The Structure of Hopf Algebras,* Ann. of Math. 81 (1965), 211–265.

[15] K.G. Monks, *Nilpotence in the Steenrod Algebra,* Bol. Soc. Mat. Mexicana (2) (1992), 401–416.

[16] K.G. Monks, *The Nilpotence Height of P_t^s,* Proc. of the Amer. Math. Soc. 124 (1996), 1297–1303.

[17] M. D. Neusel, *Inverse Invariant Theory and Steenrod Operations,* Memoirs of the Amer. Math. Soc. No. 692 Vol.146, AMS, Providence RI 2000.

[18] M. D. Neusel and L. Smith, *Polynomial Invariants of Finite Groups,* Springer-Verlag, Heidelberg, Berlin, Encyclopedea of Mathematics (to appear).

[19] J.-P. Serre, *Cohomologie modulo 2 des complexes d'Eilenberg-Mac Lane,* Comment. Math. Helv. 27 (1953), 198–232.

[20] L. Smith, *$\mathscr{P}*$-Invariant Ideals in Rings of Invariants,* Forum Mathematicum 8 (1996), 319–342.

[21] L. Smith, *Polynomial Invariants of Finite Groups,* A.K. Peters, Ltd., Wellesley, MA, 1995, second printing 1997.

[22] L. Smith, *Polynomial Invariants of Finite Groups: A Survey of Recent Developments,* Bull. of the Amer. Math. Soc. 34 (1997), 211–250.

[23] L. Smith, *The Ring of Invariants of* $O(3, \mathbb{F}_q)$, Finite Fields and their Applications 5 (1999), 96–101.

[24] L. Smith, *Cohomology Automorphisms over Galois Fields and Group-Like Elements in the Steenrod Algebra,* Preprint, AG-Invariantentheorie, 2000.

[25] L. Smith, *Invariants of* 2×2 *Matrices over Finite Fields,* AG-Invariantentheorie, Preprint 2000.

[26] L. Smith and R. E. Stong, *On the Invariant Theory of Finite Groups: Orbit Polynomials, Chern Classes and Splitting Principles,* J. of Algebra 109 (1987), 134–157.

[27] N. E. Steenrod, *Polynomial Algebras over the Algebra of Cohomology Operations,* in: *H-Spaces, Actes de la reunion de Neuchâtel (Suisse), Auot 1970*, Lecture Notes in Math. 196, Springer-Verlag, Heidelberg, Berlin, New York 1971.

[28] R. Thom, *Quelques propriétés globales des variétés différentiables,* Comm. Math. Helv. 28 (1954), 17–86.

[29] G. Walker and R. Wood, *The Nilpotence Height of* Sq^{2^n}, Proc. of the Amer. Math. Soc. 124 (1996), 1291–1295.

[30] G. Walker and R. Wood, *The Nilpotence Height of* $\mathcal{P}^{p^n}$, Math. Proc. Camb. Phil. Soc. 123 (1998), 85–93.

[31] R. Wood, *Problems in the Steenrod Algebra,* Bull. London Math. Soc. 30 (1998), 449–517.

[32] R. Wood, *Hit Problems and the Steenrod Algebra,* Notes from a Lecture Course at the University of Ioannina, june 2000.

[33] Wu Wen-Tsün, *Sur les puissance de Steenrod,* Colloque de Topologie de Strasbourg, 1951.

Larry Smith
AG-Invariantentheorie
Mittelweg 3
D 37133 Friedland
Federal Republic of Germany
e-mail: LARRY@SUNRISE.UNI-MATH.GWDG.DE

INDEX

$\mathbb{F}_q[V][[\xi]]$ 2
$\mathbf{e}_{\det}$ 4
$\mathbf{E}_{\det}$ 4
$\mathcal{P}^i(-)$ 2
$\mathrm{CGA}_{\mathbb{F}_q}$ 3
$\mathrm{Sq}^i(-)$ 2
$\mathrm{Vect}_{\mathbb{F}_q}$ 3

Adem-Wu relations 4
admissible monomial 6
algebra of polynomial functions 2

basic monomials 6
Bullett-Macdonald identity 5

Cartan formulae 2

Euler class 4
Example $\mathbb{O}(3, \mathbb{F}_q)$ 3
Example, $H^*(B\mathbb{SO}(3); \mathbb{F}_2)$ 8
Example, $\mathbb{SO}(3, \mathbb{F}_q)$ 4
Example, $\mathrm{PSL}(2, \mathbb{F}_q)$ 3
Example, $\mathrm{SL}(2, \mathbb{F})$ 3
excess 9

higher order derivation 3
Hopf algebra 4

index sequence 6

length 6
linear forms 2

Milnor basis 12
Milnor primitive elements 12
moment 7

pre-Euler class 4

Steenrod algebra 2, 3, 4
Steenrod operations 2
Steenrod reduced power operations 2
Steenrod squaring operations 2

unstability condition 2

Hit problems and the Steenrod algebra
Lecture course
University of Ioannina
Greece
June 2000

R. M. W. Wood

revised July 2000

This course of lectures will make intelligible a number of problems, listed in the last section, concerning the action of the Steenrod algebra on polynomials. The subject matter is rather technical but we shall try to indicate how some of the problems fit into the wider context of algebraic topology and invariant theory.

Contents

1 The hit problem **3**
1.1 The action of the Steenrod algebra on polynomials 5
1.2 Binary blocks and order relations 9
1.3 Results for $\mathbf{P}(n)$ 11

2 The symmetric hit problem **13**
2.1 Symmetrisation 13
2.2 The symmetrised χ-trick 14
2.3 Results for $\mathbf{B}(n)$ 17
2.4 The submodules $\mathbf{M}(n)$ 19

3 Modular representations and hit problems **20**
3.1 Modular representations and topological splittings 24
3.2 Linking first occurences by Steenrod operations 26
3.3 The Steinberg piece 28
3.4 The trivial piece 28

[0] 1991 mathematics subject classification 55S10

4 **The hit problem for the differential operator algebra** 29
4.1 The hit problem for $\mathcal{D}$ modulo 2 31
4.2 The rational hit problem for $\mathcal{D}$ 31
4.3 Remark 32

5 **Problems** 33

The first section introduces the hit problem in a general algebraic setting for graded left modules over a graded ring with a right semigroup action. A couple of examples from topology and invariant theory illustrate the ideas. Then we restrict attention to the main example which is to do with the Steenrod algebra $\mathcal{A}$ at the prime 2 acting on the polynomial algebra $\mathbf{P}(n) = \mathbb{F}_2[x_1, \ldots, x_n]$ in n variables x_i over the field $\mathbb{F}_2$ of two elements, with the right action of the matrix semigroup $M(n, \mathbb{F}_2)$.

The next section describes recent joint work with Ali Janfada on hit problems for symmetric polynomials.

In the third section we explain some interconnections between modular representation theory of the semigroup algebra $\mathbb{F}_2[M(n, \mathbb{F}_2]$ and the splitting theory of the stable types of the classifying spaces of certain groups. We describe some recent work with Grant Walker on the Steinberg representation and more general questions about the linkage of first occurrences of irreducible representations via Steenrod operations in the polynomial algebra.

In the fourth section the scope of the investigation is extended to the differential operator algebra $\mathcal{D}$, as the ring of operators, which is the natural setting for studying hit problems over the integers and at odd primes. We refer to [49] for a fairly extensive bibliography concerning the action of the Steenrod algebra on polynomials.

1 The hit problem

For any graded left module $\mathbf{M}$ over a graded ring $\mathcal{R}$ with unit, we write $\mathbf{M}^d$ for the elements of grading d. An element $f \in \mathbf{M}^d$ is called *hit* if it can be written as a finite sum

$$f = \sum_i \Theta_i f_i,$$

where the elements Θ_i belong to $\mathcal{R}$ and the f_i are homogeneous elements in $\mathbf{M}$ of grading strictly less than d. We refer to this representation of f as a *hit equation.* The hit elements form a submodule $\mathbf{N}$ of $\mathbf{M}$. The quotient $\mathbf{Q} = \mathbf{Q}(\mathbf{M}) = \mathbf{M}/\mathbf{N}$ is essentially a graded abelian group because the ring acts trivially. A minimal generating set for $\mathbf{Q}$ lifts to a minimal generating set for $\mathbf{M}$ as a module over $\mathcal{R}$. For the sake of brevity we shall sometimes say that f is equivalent to g in $\mathbf{Q}$ and write $f \cong g$ when, strictly speaking, we mean $f - g$ is hit in $\mathbf{M}$ and the equivalence classes of f and g are equal in $\mathbf{Q}$.

In particular we can view $\mathbf{R} = \mathcal{R}$ as left module over itself. In this case a hit element is traditionally called *decomposable* and the hit problem is then concerned with writing an element of $\mathbf{R}$ as a sum of products of elements of lower grading.

For present purposes we concentrate on the restricted situation where our modules are vector spaces over a field $\mathbb{F}$, have no elements of negative grading and are of finite type, which means that $\dim(\mathbf{M}^d)$ is finite for each d. We also assume that $\mathcal{R}$ is a connected algebra over $\mathbb{F}$, which means that $\mathcal{R}_0 = \mathbb{F}$. Topological motivation for studying these objects is provided by the example of the cohomology $\mathbf{M} = \mathbf{H}^*(X; \mathbb{F}_2)$ of a complex X of finite type over $\mathbb{F}_2$ under the left action of the Steenrod algebra $\mathcal{A}$.

It is worth pointing out here how decomposability can sometimes be the last stage in an argument requiring several intermediate steps of a geometric or topological nature. A famous example is the solution by Frank Adams of the problem about non-singular multiplications on Euclidean space. Early pioneers in topology translated the problem through geometry and topology into a question about the cohomology ring of a certain topological space under the action of the Steenrod algebra. Without going into details at this stage, we note that $\mathcal{A}$ is generated by elements Sq^r called *Steenrod squares* in gradings $r \geq 0$ subject to certain relations. It turns out that all Steenrod squares in positive grading are decomposable in $\mathcal{A}$ except when $r = 2^k$ for some k. It was this fact which first led Adem to a proof that non-singular multiplications on Euclidean space $\mathbf{R}^n$ cannot exist for dimensions other than $n = 2^k$. By extending the notion of decomposability into the broader context of 'secondary' operations Adams succeded in decomposing Sq^{2^k} for $k > 3$, thereby proving the long oustanding conjecture that non-singular multiplications on Euclidean space can only exist for $n = 1, 2, 4, 8$, where they are realised by real, complex, quaternionic and Cayley multiplication.

We shall be concerned in this course with a number of related questions.

Problems 1.1 *1. Find a criterion for $f \in \mathbf{M}^d$ to be hit.*

2. Find a minimal generating set for $\mathbf{M}$ or, equivalently, a basis of $\mathbf{Q}$.

3. When is the dimension of $\mathbf{Q}^d$ equal to zero?

4. Is the dimension of $\mathbf{Q}^d$ bounded independently of d?

The hit problem can be enhanced by introducing a right action of a group or semigroup Γ on the module $\mathbf{M}$ compatible with the left action of $\mathcal{R}$. To be precise, we suppose that each $\mathbf{M}^d$ is a right representation of Γ and for each $\Theta \in \mathcal{R}^t$ the left linear map $\Theta\colon \mathbf{M}^d \to \mathbf{M}^{d+t}$ is a map of right Γ-modules. For $\Theta \in \mathcal{R}, x \in \mathbf{M}, \pi \in \Gamma$ we can write $\Theta x \pi$ unambiguously. Hit problems then receive an equivariant flavour. For example, the quotient $\mathbf{Q}$ becomes a graded representation of Γ. We can also study hit problems for the fixed point set $\mathbf{M}^\Gamma$ as an $\mathcal{R}$-submodule of $\mathbf{M}$. More generally, we can examine the decomposition of $\mathbf{M}$ into summands afforded by idempotents in the semigroup algebra of Γ. Each such summand is then an $\mathcal{R}$-submodule of $\mathbf{M}$ and the investigation of hit problems for these summands is intimately related to the modular representation theory of Γ over the ground field $\mathbb{F}$. In the case of the Steenrod algebra and the matrix semigroup, there are also topological implications to do with the stable splitting of classifying spaces.

So we study the case where $\Gamma = M(n, \mathbb{F}_2)$ is the semigroup of $n \times n$ matrices $A = (a_{ij})$ over $\mathbb{F}_2$ acting on the right of $\mathbf{P}(n)$ by linear substitution of variables,

$$x_i A = \sum_s a_{is} x_s.$$

In this case, Γ contains the subgroup of non-singular matrices $GL(n, \mathbb{F}_2)$, which in turn contains the symmetric group Σ_n consisting of matrices with a single non-zero entry in each row or column. The action extends to the 'rook' semigroup of all matrices over $\mathbb{F}_2$ with at most one non-zero entry in each row or column. Let $\mathbf{B}(n) = \mathbf{P}(n)^{\Sigma_n}$ be the ring of invariants, in other words the symmetric polynomials in $\mathbf{P}(n)$. It turns out that the Steenrod squares commute with the action of $M(n, \mathbb{F}_2)$, in particular with Σ_n and $GL(n, \mathbb{F}_2)$. This raises some interesting hit problems in $\mathbf{B}(n)$, and in the *Dickson algebra* $\mathbf{D}(n) = \mathbf{P}(n)^{GL(n,\mathbb{F}_2)}$.

Before embarking on the main topic, we consider a hit problem in which the ring of invariants plays a different role, this time as the ring of operators $\mathcal{R}$ rather than the module acted on. The example is taken from Larry Smith's book on invariant theory [37], recouched in the language of an equivariant hit problem.

Example 1.2 *Let $\mathbf{M} = \mathbb{Q}[x_1, \cdots, x_n]$ be the polynomial algebra over the rationals in n variables. Let Σ_n act on the right of $\mathbf{M}$ in the usual way. Take for $\mathcal{R}$ the ring of symmetric polynomials in $\mathbf{M}$ acting on the left of $\mathbf{M}$ by the usual multiplication of polynomials. Clearly the $\mathcal{R}$-action commutes with the Σ_n action.*

For this example we can answer some of the questions posed in Problems 1.1.

1. All homogeneous polynomials of degree greater than $n(n-1)/2$ are hit.
2. A basis for $\mathbf{Q}$ consists of the $n!$ monomials $x_1^{i_1}x_2^{i_2}\cdots x_{n-1}^{i_{n-1}}$, where $0 \leq i_r \leq r$.
3. In fact $\mathbf{Q}$ is a graded version of the regular representation of Σ_n.

For example, in the case $n = 3$, the monomials

$$1, x_1, x_2, x_1^2, x_2^2, x_1^2x_2$$

generate $\mathbf{Q}$. From elementary representation theory, it is known that the three irreducible representations of Σ_3 over the rationals must appear in $\mathbf{Q}$ with multiplicity equal to their dimension. Indeed, the trivial representation appears once, generated by 1 in grading 0. The sign representation appears once, generated by $x_1^2x_2$ in grading 3, and the irreducible 2-dimensional representation of Σ_3 appears twice, generated by x_1, x_2 in grading 1 and by x_1^2, x_2^2 in grading 2. Every homogeneous polynomial f of degree at least 4 is hit; in other words, it can be written in the form

$$f = \Theta_1 + \Theta_2 x_1 + \Theta_3 x_2 + \Theta_4 x_1^2 + \Theta_5 x_2^2 + \Theta_6 x_1^2 x_2,$$

where the Θ_i are symmetric polynomials of positive degree.

This example has some special features which will not apply in general. For example, the product of a hit element by a polynomial is also hit because the ring of operators commutes with multiplication of polynomials. Hence the hit elements form an ideal and $\mathbf{Q}$ is just the algebra of coinvariants [37] of the symmetric group. We shall refer back to this example in the last section.

The algebras $\mathbf{P}(n)$ and subalgebra $\mathbf{B}(n)$ of $\mathbf{P}(n)$ are of particular interest in topology because they realise respectively the cohomology of the product of n copies of infinite real projective space and the cohomology of the classifying space $BO(n)$ of the orthogonal group $O(n)$. This is the universal place for studying Stiefel-Whitney classes of manifolds. Symmetric polynomials, divisible by the product of the variables $x_1 \cdots x_n$ also has a topological interpretation as the cohomology $\mathbf{M}(n) = H^*(MO(n), \mathbb{F}_2)$ of the Thom space $MO(n)$ in positive dimensions. Thom spaces are important in studying the immersion and embedding theory of manifolds.

1.1 The action of the Steenrod algebra on polynomials

In this section we explain how Steenrod squares act on polynomials and state some facts about the hit problem for $\mathbf{P}(n)$.

N.B. Throughout these lectures we adopt the non-standard convention of writing numbers in *reversed* dyadic expansion. For example 0101 is the reversed dyadic expansion of the number 10. Dyadic positions are counted from 0 on the left. It is customary to denote by $\alpha(d)$ the number of digits 1 in the expansion of d. We call this the α-count of d. For future reference it should be noted that if d has a digit 1 in position k then $\alpha(d+2^k) \leq \alpha(d)$ and there is strict inequality if d also has a digit 1 in position $k+1$ because of the carry forward effect of binary addition.

Another numerical function that features frequently in this subject is $\mu(d)$, which is the least number k for which it is possible to write $d = \sum_{i=1}^{k}(2^{\epsilon_i} - 1)$.

The Steenrod algebra $\mathcal{A}$ is defined to be the graded algebra over the field $\mathbb{F}_2$, generated by symbols Sq^k, called Steenrod squares, in grading k, for $k \geq 0$, subject to the Adem relations [40] and $Sq^0 = 1$. For present purposes we need to know that the Steenrod algebra acts by composition of linear operators on $\mathbf{P}(n)$ and the action of the Steenrod squares $Sq^k\colon \mathbf{P}^d(n) \to \mathbf{P}^{d+k}(n)$ on monomials $f, g \in \mathbf{P}(n)$ is determined by the following rules [49].

Proposition 1.3 *1. $Sq^k f = f^2$ if $\deg(f) = k$ and $Sq^k f = 0$ if $\deg(f) < k$.*

2. The Cartan formula $Sq^k(fg) = \sum_{0 \leq r \leq k} Sq^r(f) Sq^{k-r}(g)$.

In principle these rules enable the evaluation of a Steenrod operation on any polynomial by induction on degree.

The next results are elementary consequences of the rules in Proposition 1.3.

Proposition 1.4 *Let $f = x_1^{d_1} \cdots x_n^{d_n}$ be a monomial in $\mathbf{P}(n)$ and x a typical variable.*

1. *$Sq^r(f) = \sum_{r_1+\cdots+r_n=r} Sq^{r_1}(x_1^{d_1}) \cdots Sq^{r_n}(x_n^{d_n})$.*

2. *$Sq^r(x^d) = 0$ unless, for each position j where there is a binary digit 1 of r, there is also a binary digit 1 of d in position j. In this case $Sq^r(x^d) = x^{r+d}$. In particular, $Sq^{2^k}(x^d) = x^{2^k+d}$ if and only if d has a digit 1 in position k.*

3. *The power x^r is in the image of a positive Steenrod square if and only if r is not of the form $2^\epsilon - 1$.*

4. *If r is odd then $Sq^r(f^2) = 0$, whereas $Sq^{2r}(f^2) = (Sq^r(f))^2$. Consequently the action of the Steenrod algebra on $\mathbf{P}(n)$ is 'fractal' in the sense that a copy of the algebra acts on squares of polynomials by duplication of the suffices of the operators.*

5. *Steenrod squares commute with the right action of the symmetric group Σ_n, which permutes the variables $x_1, \ldots, x_n$.*

6. *Steenrod squares commute with the right action of the full semigroup of $n \times n$ matrices acting by linear substitution in the variables [49].*

Item 5 explains algebraically why $\mathbf{B}(n)$ is a submodule of $\mathbf{P}(n)$. Item 6 is a stronger statement and explains why the Dickson algebra $\mathbf{D}(n)$ is a module over $\mathcal{A}$. There are topological reasons why $\mathbf{B}(n)$ and $\mathbf{M}(n)$ are modules over the Steenrod algebra because these are cohomology algebras of certain topological spaces. For $\mathbf{D}(n)$, however, this is not the case if $n > 5$ [38]. So invariance of $\mathbf{D}(n)$ under $\mathcal{A}$ is an algebraic bonus. We shall say more about this matter in section 3.

We recall [49] that a monomial $x_1^{d_1} \cdots x_n^{d_n}$ is called a *spike* if every exponent d_i is of the form $2^{\epsilon_i} - 1$. It follows from items 1, 3 of Proposition 1.4 that a spike can never appear as a term in a hit polynomial in $\mathbf{P}(n)$ when written irredundantly. Hence the spikes must always appear in any set of minimal generators of the module $\mathbf{P}(n)$.

There are a few deeper facts about the Steenrod algebra which are needed later to analyse the hit problem. A string of Steenrod squares

$$Sq^{k_1} Sq^{k_2} \cdots Sq^{k_t}$$

of length $t \geq 1$. is called *admissible* if $k_i \geq 2k_{i+1}$ for $1 \leq i < t$. This includes all Sq^i as admissible for $i \geq 0$.

Proposition 1.5 *As a vector space, $\mathcal{A}$ is generated by the admissible strings of Steenrod squares.*

Also important for hit problems is the following result already referred to earlier.

Proposition 1.6 *As an algebra, $\mathcal{A}$ is generated by the Steenrod squares Sq^{2^k} for $k \geq 0$.*

In the first place a hit equation for $f \in \mathbf{P}(n)$ has the general form $f = \sum_i \Theta_i f_i$, where the elements $\Theta_i \in \mathcal{A}$ have positive grading, but because the Sq^i generate $\mathcal{A}$ there must then be a hit equation of the form $f = \sum_{i>0} Sq^i g_i$ and, in the light of Proposition 1.6, f will also satisfy a hit equation of the form

$$f = \sum_{k \geq 0} Sq^{2^k} h_k,$$

where f_i, g_i, h_k are homogeneous elements of $\mathbf{P}(n)$.

The Steenrod algebra is a Hopf algebra with diagonal defined by

$$\psi(Sq^k) = \sum_{0 \leq i \leq k} Sq^i \otimes Sq^{k-i}.$$

It then admits a *conjugation* operator χ, which is an anti-automorphism of order 2. For an element $\Theta \in \mathcal{A}$ we use the notation $\chi(\Theta) = \widehat{\Theta}$. Conjugation satisfies the recursion formulae

$$\sum_{i=0}^{k} Sq^i \widehat{Sq^{k-i}} = 0,$$

for $k > 0$, from which it is possible, at least in principle, to work out $\widehat{Sq^k}$ in terms of Steenrod squares by induction on k.

The following formulae are useful for handling conjugate squaring operators.

Proposition 1.7 *There is a conjugate Cartan formula*

$$\widehat{Sq^k}(fg) = \sum_{0\leq r\leq k} \widehat{Sq^r}(f)\widehat{Sq^{k-r}}(g)$$

and evaluation of a conjugate square on powers of a single variable is given by

$$\widehat{Sq^r}(x^{2^k}) = \begin{cases} x^{2^m}, & \text{if } r = 2^m - 2^k,\ m \geq k, \\ 0, & \text{otherwise.} \end{cases}$$

As with Steenrod squares themselves, these formulae enable the evaulation of a conjugate operation on any polynomial by induction on degree.

The next result plays a major role in solving hit problems [12, 13, 49].

Proposition 1.8 *Let u, v denote homogeneous elements in $\mathbf{P}(n)$. Then*

$$uSq^k(v) - \widehat{Sq^k}(u)v = \sum_{i>0} Sq^i(u\widehat{Sq^{k-i}}(v)).$$

An immediate consequence, known as the χ-trick, is that $uSq^k(v)$ is hit in $\mathbf{P}(n)$ if and only if $\widehat{Sq^k}(u)v$ is hit in $\mathbf{P}(n)$. By iterating the formula of Proposition 1.8 on compositions of Steenrod squares and using linearity, we obtain a more general statement.

Proposition 1.9 *Let u, v denote homogeneous elements in $\mathbf{P}(n)$. Then, for any $\Theta \in \mathcal{A}$, there is a hit equation of the form*

$$u\Theta(v) - \widehat{\Theta}(u)v = \sum_{i>0} Sq^i(\sum_{l} \Theta_{il}(u)\Phi_{il}(v)),$$

for certain elements $\Theta_{il}, \Phi_{il} \in \mathcal{A}$. In particular we have the equivalence $u\Theta(v) \cong \widehat{\Theta}(u)v$ in $\mathbf{Q}(\mathbf{P}(n))$.

The *excess* of an element Θ in $\mathcal{A}$ is defined as the smallest positive integer s such that $\Theta(x_1x_2\cdots x_s) \neq 0$. The following result goes back to Milnor [30, 35, 49].

Proposition 1.10 *The excess of $\widehat{Sq^k}$ is $\mu(k)$.*

This result has been improved in [26, 35].

Theorem 1.11 *The excess of $\widehat{Sq^d}\widehat{Sq^{2d}}\cdots\widehat{Sq^{2^{k-2}d}}\widehat{Sq^{2^{k-1}d}}$ is $(2^k - 1)\mu(d)$.*

From 1.8 and 1.11 we obtain the following corollary [35, 49].

Theorem 1.12 *Let $f = uv^{2^k}$ be a monomial in $\mathbf{P}(n)$ and suppose* $\deg(u) < (2^k - 1)\mu(\deg(v))$. *Then f is hit.*

To prove this statement, we write

$$\Theta = Sq^{2^{k-1}d}Sq^{2^{k-2}d}\cdots Sq^{2d}Sq^{d}$$

and observe that $v^{2^k} = \Theta(v)$ where $d = \deg(v)$. The χ-trick of Proposition 1.9 and Theorem 1.11 then complete the argument.

1.2 Binary blocks and order relations

As an intuitive aid to understanding many of the processes involving the action of Steenrod operations in $\mathbf{P}(n)$ it is useful to exhibit a monomial f as a binary block of digits 0 or 1 [8]. This means the matrix whose rows are the reversed binary expansions of the exponents of the variables $x_1, \dots, x_n$ in f. We shall adopt the convention of denoting a monomial by a lower case letter and its binary block by the corresponding upper case letter. For example, the monomial $f = x_1^3x_2^2x_3^5$ is represented by the binary block

$$F = \begin{matrix} 1 & 1 & \\ 0 & 1 & \\ 1 & 0 & 1 \end{matrix}$$

Normal matrix notation will be used, except that the columns are counted from 0 to be consistent with 2-adic exponents. It should be noted in particular that the juxtaposition of two blocks UV corresponds to the monomial uv^{2^k}, where $k-1$ is the position of the last column of U. The double suffix notation $F_{(i,k)}$ refers to the entry of the binary block F in row i and column k. It is the digit in position k of the reversed binary expansion of d_i in the monomial $f = x_1^{d_1}\cdots x_n^{d_n}$. We shall occasionally use the notation $F_{(i)}$ to refer to row i of F.

There are several ways of ordering monomials of $\mathbf{P}(n)$ to be compatible with the action of the Steenrod algebra. The order relation used in [8, 49], called the ω-order, is defined as follows. Let $\omega_j(F) = \sum_i F_{(i,j)}$ denote the sum of the digits in column j of the binary block F. Now form the ω-vector $\omega(F) = (\omega_0(F), \omega_1(F), \dots, \omega_k(F), \dots)$ and order such vectors in left lexicographic order.

The transpose of the ω-order, which we shall call the α-order, is defined as follows. For a block F the α-counts of the rows of F are arranged as the components of a vector in non-decreasing order of magnitude from left to right. Such α-vectors are then compared lexicographically. This process defines the α-order relation on monomials and is again symmetric in the variables. For example, if the smallest α-count of the exponents in the monomial f is less than the smallest α-count of the exponents in the monomial g then $f <_\alpha g$. If these numbers are equal we look at the next smallest and so on.

The following statement explains the compatibility of the action of the Steenrod algebra with the order relations and is an easy consequence of items in Proposition 1.4.

Proposition 1.13 *Any monomial produced by the action of any positive element in the Steenrod algebra on a monomial f has strictly lower ω-order than that of f and no greater α-order.*

We shall say that a monomial f is ω-reducible if there is a hit equation of the form

$$f - g = \sum_i \Theta_i f_i,$$

for positively graded elements $\Theta_i \in \mathcal{A}$, where the ω-order of every monomial in g is lower than the ω-order of f. There is a similar definition for the α-order relation.

In the next couple of propositions the χ-trick is used to show how in certain situations the ω-order of a monomial can be reduced. Statements are sometimes more transparent when phrased in the language of binary blocks.

Proposition 1.14 *Let $F = UV$ be a binary block corresponding to a monomial $f = uv^{2^k}$ in $\mathbf{P}(n)$, where $k-1$ is the last column position of U. Suppose that v is hit. Then F is ω-reducible in $\mathbf{P}(n)$. In fact the ω-vector of the reduction can be assumed to be reduced in some position prior to k.*

To prove this result formally we first write

$$v = \sum_i \Theta_i(f_i)$$

for elements Θ_i of positive grading in the Steerod algebra and polynomials f_i in $\mathbf{P}(n)$. We then appeal to the fractal nature of the Steenrod algebra as explained in item 4 of Proposition 1.4 to write

$$v^{2^k} = \sum_i \Phi_i(f_i^{2^k}),$$

where the Φ_i are constructed from the Θ_i by iterated duplication of suffices in compositions of squaring operations. Then by the χ-trick of Proposition 1.9 we obtain the equivalence

$$uv^{2^k} = \sum_i u\Phi_i(f_i^{2^k}) \cong \sum_i (\widehat{\Phi}_i u) f_i^{2^k}.$$

Finally we apply Proposition 1.13 to see that the the ω-order of every monomial in $\widehat{\Phi}_i u$ is lower that the ω-order of u, indeed in a position prior to k. It follows that all monomials in $(\widehat{\Phi}_i u) f_i^{2^k}$ have ω-order lower than f as required.

We shall sometimes paraphrase proofs of this kind by saying simply that $F = UV$ is reducible because V is hit.

The following result is an immediate corollary.

Proposition 1.15 *Let F be a binary block with a zero column in position k, but with a non-zero column in some higher position. Then F is ω-reducible. Furthermore the reduction may be taken with no higher α-order than that of F.*

To demonstrate this result, suppose that the first zero column of F occurs at position k. Then split the block $F = UV$ vertically between positions $k-1$ and k, as in the previous proposition, where now the first column of V is zero. Then V is a perfect square and therefore hit. Proposition 1.14 completes the argument as far as reduction is concerned. The hit equation for V effectively moves all columns of V back one place, which does not change the α-count of the rows of V. An appeal to Proposition 1.13 finishes the proof.

1.3 Results for $\mathbf{P}(n)$

We shall now list a number of results about the hit problem for $\mathbf{P}(n)$ in answer to some of the questions posed in Problems 1.1. Most of these results are well known and can be found in various sources [1, 2, 8, 11, 22, 23, 31, 32, 34, 36, 44, 45, 46, 47, 49]. It should be mentioned a this point that we are taking the 'cohomology' approach to the hit problem. For the alternative 'homology' approach, we refer to [1, 11], where the problem is treated in terms of kernels of the adjoint action of Steenrod squares.

The solution of the Peterson conjecture [46, 47, 49] gives the following answer to question 3 of Problems 1.1.

Theorem 1.16 *The quotient space $\mathbf{Q}^d(\mathbf{P}(n))$ is zero if and only if $\mu(d) > n$.*

To prove this result we note first of all that in degree d, when $\mu(d) \leq n$, there is a spike which shows that the dimension of $\mathbf{Q}^d(\mathbf{P}(n))$ is non-zero. In the other direction, when $\mu(d) > n$, consider splitting a block $F = UV$ between column positions 0 and 1. Then $d = \deg U + 2\deg V$. It can be seen that $\mu(\deg(V)) > \deg(U)$, otherwise we would be able to write

$$\deg(V) = \sum_{i=1}^{\deg(U)} (2^{\epsilon_i} - 1),$$

in which case

$$\deg U + 2\deg V = \sum_{i=1}^{\deg(U)} (2^{\epsilon_i + 1} - 1),$$

contradicting $\mu(d) > n$, since $\deg U \leq n$. The result now follows from Theorem 1.12 in the case $k = 1$.

An answer to the second and fourth question in 1.1 can be found in in [22, 23, 8] for low values of n. The first three questions in 1.1 are answered in detail by classification results for hit monomials in $\mathbf{P}(2)$ and $\mathbf{P}(3)$, which can be found in Kameko's thesis [22] and more recently in Janfada's thesis [21].

Theorem 1.17 *The dimension of $\mathbf{Q}^d(\mathbf{P}(n))$ is bounded independently of d for all n. The best bounds for $n = 1, 2, 3$ are respectively $1, 3, 21$.*

Kameko conjectures that the best bound for the case of $\mathbf{P}(n)$ is $(1)(3) \cdots (2^n - 1)$.

The following table, taken form [22, 2], shows the dimensions of $\mathbf{Q}^d(\mathbf{P}(3))$ in terms of d.

Theorem 1.18 *The dimension of $\mathbf{Q}^d(\mathbf{P}(3))$ is zero unless $d = 2^{s+t+u} + 2^{t+u} + 2^u - 3$, where $s \geq 0, t \geq 0, u \geq 0$. In this case the dimension is independent of u when $u > 0$ and depends on s, t as follows.*

dim	$u = 0$	$u \geq 0$				
$\mathbf{Q}^d(\mathbf{P}(3))$	$s = 0$	$s = 1$	$s = 2$	$s = 3$	$s = 4$	$s > 4$
$t = 0$	1	3	7	10	13	14
$t = 1$	3	8	15	14	14	14
$t = 2$	6	14	21	21	21	21
$t > 2$	7	14	21	21	21	21

The following result [8] provides a set of generators for $\mathbf{P}(n)$ as an $\mathcal{A}$-module but is not minimal.

Theorem 1.19 *The $\mathcal{A}$ module $\mathbf{P}(n)$ is generated by monomials $x_1^{e_1} \cdots x_n^{e_n}$ where, up to permutation of the variables, $\alpha(e_i + 1) \leq i$.*

This result leads to a proof of Theorem 1.17 [8] . We quote one final result [36] in this section which narrows down the scope of a minimal generating set and refines Theorem 1.16.

Theorem 1.20 *If a monomial in $\mathbf{P}^d(n)$ has ω-order less than that of a minimal spike in degree d, then f is hit. A generating set for $\mathbf{P}(n)$ can be chosen from monomials whose ω-order is between that of a minimal and maximal spike in any degree.*

There are degrees for which there is only one spike up to permutation of the variables. In such degrees d it can be verified that the dimension of $\mathbf{Q}^d(\mathbf{P}(n))$ is bounded by the product $1(3) \cdots (2^n - 1)$ and a generating set can be written down. The difficulty in proving the Kameko conjecture in general seems to be in degrees where there are spikes of various ω-orders.

2 The symmetric hit problem

An element π in the symmetric group Σ_n acts on the right of a polynomial $f \in \mathbf{P}(n)$ by permuting the variables and the action is clearly multiplicative i.e. $(fg)\pi = (f\pi)(g\pi)$ for two polynomials $f, g \in \mathbf{P}(n)$. A hit equation in $\mathbf{B}(n)$ may always be taken, when convenient, in the form of a finite sum

$$a = \sum_{k \geq 0} Sq^{2^k} b_i,$$

where a and the b_i are symmetric polynomials.

As we shall explain in the next section, $\mathbf{B}(n)$ is generated additively by the symmetrised monomials. The ω-order and α-order are symmetric in the variables and apply therefore to monomial symmetric functions in $\mathbf{B}(n)$.

2.1 Symmetrisation

Given a monomial f in a subset of the variables $x_1, \ldots, x_n$, we can form the *symmetrisation* of f which means the smallest symmetric function $\sigma(f)$ in $\mathbf{B}(n)$ containing f as a term. To be more precise, let $\pi_1, \cdots, \pi_t$ be a set of left coset representatives for the stabiliser of the monomial f in Σ_n. Then $\sigma(f) = \sum_{i=1}^{t} f\pi_i$. For example, if the exponents of the variables $x_1, \ldots, x_n$ in f are all distinct then the stabiliser of f is trivial and $\sigma(f) = \sum_\pi f\pi$, where the summation is taken over the whole of Σ_n. This is the classical transfer of invariant theory. At the other extreme, if all exponents of f are the same then the stabiliser is the whole of Σ_n and $\sigma(f) = f$. If $\pi_1, \cdots, \pi_t$ are left coset representatives for a subroup of the stabiliser of f it is still true, of course, that $\sum_{j=1}^{t} f\pi_j$ is symmetric but the expression may be zero. It should be emphasised that the meaning of $\sigma(f)$ depends on the set of variables over which symmetrisation is taking place. For example $\sigma(x_1)$ means $x_1 + x_2$ in $\mathbf{P}(2)$ but $x_1 + x_2 + x_3$ in $\mathbf{P}(3)$. The symmetrised monomials form a vector space basis of $\mathbf{B}(n)$. In recent literature on invariant theory [37] the symmetrisation operator σ is referred to as the first Chern class.

What we would like to do is convert hit equations in $\mathbf{P}(n)$ into hit equations in $\mathbf{B}(n)$ by symmetrisation. The following example shows that a naive approach to this problem does not always work.

Example 2.1 *In $\mathbf{P}(2)$ we have the hit equation*

$$x_1^2 x_2^2 = Sq^1(x_1 x_2^2).$$

If we symmetrise this equation we obtain

$$0 = Sq^1(x_1 x_2^2 + x_1^2 x_2)$$

because we are working modulo 2. So we cannot prove this way that $x_1^2x_2^2$ is symmetrically hit. But, as it happens, there is a symmetric hit equation in $\mathbf{B}(2)$ *namely*

$$Sq^2(x_1x_2) = x_1^2x_2^2,$$

which shows that $x_1^2x_2^2$ is indeed symmetrically hit.

It is this phenomenon which prompts the questions raised in Problems 5.7 about whether the symmetrisation of a hit monomial in $\mathbf{P}(n)$ is symmetrically hit. There are examples of monomials which are not hit in $\mathbf{P}(n)$ but whose symmetrisations are hit in $\mathbf{B}(n)$. There are also examples of polynomials in $\mathbf{B}(n)$ which are hit in $\mathbf{P}(n)$ but not symmetrically hit in $\mathbf{B}(n)$.

However, there are circumstances in which we can symmetrise hit equations in $\mathbf{P}(n)$, based on the following observation.

Proposition 2.2 *Let f be a monomial and g a polynomial in $\mathbf{P}^d(n)$. Suppose there is a hit equation*

$$f - g = \sum_i \Theta_i f_i$$

in $\mathbf{P}^d(n)$, satisfying the condition that the stabiliser of f is a subgroup of the stabiliser of g and a subgroup of the stabiliser of each polynomial f_i. Let $\pi_1, \ldots, \pi_t$ be a collection of left coset representatives for the stabiliser of f in the symmetric group Σ_n. Then

$$\sigma(f) - \sum_{j=1}^{t} g\pi_j = \sum_i \Theta_i(\sum_{j=1}^{t} f_i\pi_j),$$

is a symmetric hit equation in $\mathbf{B}(n)$.

The reason is that $\sigma(f)$ is equal to $\sum_{j=1}^t f\pi_j$ by definition, and the expressions

$$\sum_{j=1}^{t} g\pi_j, \quad \sum_{j=1}^{t} f_i\pi_j$$

are symmetric by our earlier discussion about stabiliser subgroups. Under the given conditions we have the equivalence $\sigma(f) \cong \sum_{j=1}^t g\pi_j$ in $\mathbf{Q}(\mathbf{B}(n))$.

2.2 The symmetrised χ-trick

We now develop some useful symmetric hit equations by exploiting Proposition 2.2.

Proposition 2.3 *If the exponents of a hit monomial f in $\mathbf{P}(n)$ are all distinct. Then $\sigma(f)$ is symmetrically hit.*

In this case $\sigma(f)$ is the transfer of f and the stabiliser of f is the trivial group. The conditions of Proposition 2.2 are obviously satisfied with $g = 0$.

We can form a symmetrical version of Proposition 1.14

Proposition 2.4 *Let $f = uv^{2^k}$ be a monomial in $\mathbf{P}(n)$, with $\omega_j(u) = 0$ for $j \geq k$. Assume that u is symmetric and that $\sigma(v)$ is symmetrically hit. Then $\sigma(f)$ is symmetrically ω-reducible in $\mathbf{B}(n)$. In fact the ω-vector of the reduction can be assumed to be reduced in some position prior to k.*

To prove this result we note first of all that $\sigma(f) = u\sigma(v^{2^k})$ because u is symmetric. Since $\sigma(v)$ is symmetrically hit, the argument in the proof of Propostion 1.14 goes through when applied to $\sigma(v)$ in place of v, maintaining symmetry at each stage.

We continue with a symmetric analogue of Proposition 1.9.

Proposition 2.5 *Let $f = uv$ be a monomial in $\mathbf{P}(n)$ with the property that the stabiliser of f also stabilises u and v separately. Let $\pi_1, \ldots, \pi_t$ be a collection of left coset representatives for the stabiliser of f in the symmetric group Σ_n. Then for any element $\Theta \in \mathcal{A}$ there is a symmetric hit equation in $\mathbf{B}(n)$ of the form*

$$\sum_{j=1}^{t}(u\Theta(v))\pi_j - \sum_{j=1}^{t}(\widehat{\Theta}(u)v)\pi_j = \sum_{i>0} Sq^i \sum_{j=1}^{t}\sum_{l}(\Theta_{il}(u)\Phi_{il}(v))\pi_j,$$

for certain elements $\Theta_{il}, \Phi_{il} \in \mathcal{A}$. In particular we have the equivalence

$$\sum_{j=1}^{t}(u\Theta(v))\pi_j \cong \sum_{j=1}^{t}(\widehat{\Theta}(u)v)\pi_j$$

in $\mathbf{Q}(\mathbf{B}(n))$.

The proof follows immediateley from Propositions 1.9 and 2.2. We apply this result to obtain the symmetric analogue of Proposition 1.12.

Theorem 2.6 *Let $f = uv^{2^k} \in \mathbf{P}(n)$ be a monomial and suppose* $\deg(u) < (2^k - 1)\mu(\deg(v))$. *Then $\sigma(f)$ is symmetrically hit.*

To prove this statement, we first observe that the stabiliser of f also stabilises u and v. Hence Proposition 2.5 applies to the choice

$$\Theta = Sq^{2^{k-1}d}Sq^{2^{k-2}d}\cdots Sq^{2d}Sq^{d},$$

where d is the degree of v. The rest of the argument follows the same pattern as the proof of Theorem 1.12, noting that

$$\sigma(f) = \sum_{j=1}^{t}(u\Theta(v))\pi_j$$

for the particular choice of coset representatives π_j.

Before stating the next corollary, we need to make a few more remarks about symmetrisation. Consider a monomial f in $\mathbf{P}(n)$ expressed in the form $f = gh$ where g involves only the variables $x_1, \ldots, x_p$ and h involves only the remaining variables $x_{p+1}, \ldots, x_{p+q}$, where $p+q = n$. Let us suppose also that no exponent in the monomial g is equal to any exponent in the monomial h. Then the stabiliser of f is a subgroup of the cartesian product $\Sigma_p \times \Sigma_q$ which permutes the first p variables and last q variables separately. There is a set of left coset representatives for the stabiliser of f of the form $(\rho_i \times \tau_j)\zeta_k$, where the ρ_i run through a set of coset representatives for the stabiliser of g in Σ_p, the τ_j do the same for the stabiliser of h in Σ_q and the ζ_k are the shuffle permutations which preserve the orders of the two separate lists of variables $x_1, \ldots, x_p$ and $x_{p+1}, \ldots, x_{p+q}$. We then have the following lemma.

Lemma 2.7 *The symmetrisation of $f = gh$ in the n variables $x_1, \ldots, x_n$ is given by*

$$\sigma(f) = \sum_k (\sigma'(g)\sigma''(h))\zeta_k,$$

where σ', σ'' denote symmetrisation in the subsets $x_1, \ldots, x_p$ and $x_{p+1}, \ldots, x_{p+q}$ separately, and the ζ_k run through the shuffles of the first set in the second set.

The next corollary may be viewed in terms of a horizontal splitting of a block.

Proposition 2.8 *Let $f = gh$ in $\mathbf{P}(n)$ be a monomial factorised such that g involves only the variables $x_1, \ldots, x_p$ and h involves only the remaining variables $x_{p+1}, \ldots, x_{p+q}$, where $p+q = n$. Assume also that no exponent in the monomial g is equal to any exponent in the monomial h. Suppose there is a symmetric hit equation in $\mathbf{B}(q)$ of the form*

$$\sigma''(h) = \sum_r \Omega_r h_r,$$

for positively graded elements Ω_r in the Steenrod algebra. Then there is a symmetric equivalence in $\mathbf{B}(n)$ of the form

$$\sigma(f) \cong \sum_k \sum_r (\widehat{\Omega_r}(\sigma'(g))h_r)\zeta_k.$$

The proof of this result follows the line of argument in Proposition 2.5, once we observe that the stabiliser of f must stabilise g and h individually because these monomials have no exponents in common. We have

$$\sigma'(g)\sigma''(h) = \sum_r \sigma'(g)\Omega_r h_r = \sum_r (\widehat{\Omega_r}(\sigma'(g))h_r + \sum_r \sum_{i>0} Sq^i(\sum_k(\Theta_{ikr}(u)\Phi_{ikr}(v)),$$

for certain elements Θ_{ikr}, Φ_{ikr} in the Steenrod algebra. Now all terms in this equation are stabilised by the stabiliser of f. It follows that an application of the shuffle operators ζ_k to both sides of the equation, and adding over k, produces a symmetric hit equation. By Lemma 2.7 the left hand side becomes $\sigma(f)$ and the result is established.

2.3 Results for $\mathbf{B}(n)$

We now state answers to some of the basic Problems 1.1 about $\mathbf{B}(n)$ in parallel with the corresponding answers for $\mathbf{P}(n)$. First of all, the Peterson conjecture remains true for $\mathbf{B}(n)$, with the same condition as for $\mathbf{P}(n)$.

Theorem 2.9 *The quotient space* $\mathbf{Q}^d(\mathbf{B}(n))$ *is zero if and only if* $\mu(d) > n$.

The proof is an immediate consequence of Theorem 2.6 and the arguments used in the proof of Theorem 1.16.

It should be emphasised what this result actual says. It follows immediately from Theorem 1.16 that a homogeneous symmetric polynomial is hit in $\mathbf{P}(n)$ if its degree d satisfies $\mu(d) > n$. It is not so obvious, however, why this should imply that the polynomial is symmetrically hit in these degrees, in other words why it should be hit as an element of the module $\mathbf{B}(n)$. It was only by constructing the specially adapted hit equations that we were able to prove the symmetrised Peterson conjecture. This leads once again to the more general questions about symmetric hit elements posed in Problems 5.7.

For small values of n we have an analogue of Theorem 1.17.

Theorem 2.10 *For* $n = 1, 2, 3$, *the best upper bounds for the dimension of* $\mathbf{Q}^d(\mathbf{B}(n))$ *are respectively* $1, 1, 4$.

We ask in Problem 5.8 for a bound for the dimension of $\mathbf{Q}^d(\mathbf{B}(n))$ in general and some sensible upper estimate of it, analogous to the Kameko conjecture.

As far as minimal bases are concerned, the situation for $n = 1$ is straightforward since $\mathbf{B}(1) = \mathbf{P}(1)$ and $\mathbf{B}(1)$ is generated by the spikes $x_1^{2^\epsilon - 1}$.

In the 2-variable case, the answer is also quite simple.

Theorem 2.11 *The collection of symmetric functions*

$$x_1^{2^r-1}x_2^{2^r-1}, \quad x_1^{2^s-1}x_2^{2^t-1} + x_1^{2^t-1}x_2^{2^s-1},$$

for $r \geq 0$ *and* $s > t \geq 0$, *forms a minimal generating set for* $\mathbf{B}(2)$.

Theorem 2.11 indicates that the symmetrised spikes are enough to furnish a generating set of the module in the case of two variables. The situation for three variables is more complicated. We provide a table, by analogy with Theorem 1.18, showing the dimensions of $\mathbf{Q}^d(\mathbf{B}(3))$ in degrees d where the dimensions are non-zero.

Theorem 2.12 *The dimension of $\mathbf{Q}^d(\mathbf{B}(3))$ is zero unless $d = 2^{s+t+u} + 2^{t+u} + 2^u - 3$, where $s \geq 0, t \geq 0, u \geq 0$. In this case the dimension is independent of u when $s > 0$ and depends on s, t as follows.*

dim	$u = 0$	$u \geq 0$			
$\mathbf{Q}^d(\mathbf{B}(3))$	$s = 0$	$s = 1$	$s = 2$	$s = 3$	$s > 3$
$t = 0$	1	1	2	3	4
$t > 0$	1	1	2	2	2

The form of the degree d in the above theorem implies of course that $\mu(d) \leq 3$ in accordance with Theorem 2.9. The next statement exhibits a list of minimal generators for $\mathbf{B}(3)$.

Theorem 2.13 *A minimal generating set for $\mathbf{B}(3)$ as a module over the Steenrod algebra consists of the symmetrised spikes together with the symmetrisations of monomials $x_1^{\epsilon_1} x_2^{\epsilon_2} x_3^{\epsilon_3}$ of three types.*

$$\epsilon_1 = 2^{u+s-1} - 1, \quad \epsilon_2 = \epsilon_3 = 2^u + 2^{u+s-2} - 1, \qquad \textit{for } u \geq 0, s > 2$$

$$\epsilon_1 = 2^{u+2} - 1, \quad \epsilon_2 = \epsilon_3 = 2^{u+s-1} - 2^u - 1, \qquad \textit{for } u \geq 0, s > 3$$

$$\epsilon_1 = 2^u - 1 + 2^{u+t+s-1}, \quad \epsilon_2 = 2^{u+t} - 1, \quad \epsilon_3 = 2^{u+t+s-1} - 1 \qquad \textit{for } u \geq 0, t > 0, s > 1$$

The three types of monomials exhibited in Theorem 2.13 can be visualised in terms of their binary block diagrams as exhibited below.

$$A_1 = \begin{array}{ccccccc} 1 & - & 1 & 1 & - & 1 & 1 \\ 1 & - & 1 & 0 & - & 0 & 1 \\ 1 & - & 1 & 0 & - & 0 & 1 \end{array} \qquad A_2 = \begin{array}{cccccccc} 1 & - & 1 & 1 & 1 & & & \\ 1 & - & 1 & 0 & 1 & 1 & - & 1 \\ 1 & - & 1 & 0 & 1 & 1 & - & 1 \end{array}$$

$$A_3 = \begin{array}{cccccccccc} 1 & - & 1 & 0 & - & 0 & 0 & - & 0 & 1 \\ 1 & - & 1 & 1 & - & 1 & & & & \\ 1 & - & 1 & 1 & - & 1 & 1 & - & 1 & \end{array}$$

The first two monomials A_1, A_2 lie in degree $2^{u+s} + 2^{u+1} - 3$ for $u \geq 0, s > 2$, where there are also two symmetrised spikes. The third monomial A_3 lies in degree $2^{u+t+s} + 2^{u+t} + 2^u - 3$ for $u \geq 0, t > 0, s > 1$, where there is just one symmetrised spike. There are alternative sets of generators for $\mathbf{B}(3)$ which serve various purpose. For more details on the classification of symmetrised monomials into hits and non-hits, in answer to question 1 of Problems 1.1 we refer to Janfada's thesis [21].

2.4 The submodules $\mathbf{M}(n)$

We note that $\mathbf{B}(n)$ splits as a module over $\mathcal{A}$ into a direct sum of certain submodules $\mathbf{T}(r)$ for $r \leq n$. To be precise

$$\mathbf{B}(n) = \bigoplus_{r=1}^{n} \mathbf{T}(r),$$

where $\mathbf{T}(r)$ is generated by the symmetrisation of monomials involving precisely r of the n variables $x_1, \ldots x_n$. One sees therefore that $\mathbf{T}(r)$ is isomorphic to $\mathbf{M}(r)$ as a module over the Steenrod algebra and we deduce the following dimension formulae.

Proposition 2.14 $\dim \mathbf{Q}^d(\mathbf{M}(n)) = \dim \mathbf{Q}^d(\mathbf{B}(n)) - \dim \mathbf{Q}^d(\mathbf{B}(n-1))$

$$\dim \mathbf{Q}^d(\mathbf{B}(n)) = \textstyle\sum_{r=1}^{n} \dim \mathbf{Q}^d(\mathbf{M}(r)).$$

There are topological problems [39, 29] associated with these algebraic statements that we shall discuss later.

3 Modular representations and hit problems

As general references for this section we cite [3, 15, 16, 17, 27, 28, 44].

There are 2^n distinct irreducible modular representations of $M(n, \mathbb{F}_2)$ over the natural field $\mathbb{F}_2$, parametrised by sequences of non-negative integers

$$\lambda = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq 0,$$

subject to the constraints $\lambda_i - \lambda_{i+1} \leq 1$ for $1 \leq i < n$ and $\lambda_n \leq 1$, called 2-*column regularity*. The irreducible representations of $GL(n, \mathbb{F}_2)$ correspond to those λ with $\lambda_n = 0$.

In the literature on the representation theory of symmetric groups and general linear groups, the sequence λ is usually referred to as a partition of length n of the number $|\lambda| = \lambda_1 + \lambda_2 + \cdots + \lambda_n$ and depicted by a *Ferrers diagram*, which is a matrix with a mark at each position (i, j) for $1 \leq j \leq \lambda_i$, and other positions empty. The non-empty positions are called the 'nodes' of the diagram. The transpose of the Ferrers diagram of λ corresponds to the *conjugate* sequence λ', where λ'_i is the number of rows k such that $\lambda_k \geq i$. The sequence λ' is again a partition of $|\lambda| = |\lambda'|$ but does not necessarily correspond to an irreducible representation of $M(n, \mathbb{F}_2)$. If λ is 2-column regular, then λ' is strictly monotonic. Such sequences are also referred to in the literature as 2-regular. For example, the diagram of $\lambda = (3, 3, 2, 2, 1)$ and its transpose are shown below.

$$\lambda = \begin{array}{ccc} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & \\ 1 & 1 & \\ 1 & & \end{array} \qquad \lambda' = \begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & \\ 1 & 1 & & & \end{array}$$

The nodes of a Ferrers diagram are sometimes replaced by squares in which other information is inserted.

The empty diagram corresponds to the trivial representation of $M(n, \mathbb{F}_2)$, where every matrix acts as the identity. The Ferrers diagram with just one entry is the natural representation of $n \times n$ matrices on n-dimensional vectors. More generally, the diagram with just one column containing r entries is the r-th exterior power of the natural representation. In particular, when $r = n$, we obtain the determinant representation in which all non-singular matrices act as the identity but singular matrices act as 0. The Ferrers diagram with the maximal allowable number of entries, corresponding to the triangular partition $(n, n-1, \ldots, 1)$, is referred to as the Steinberg representation for the semigroup $M(n, \mathbb{F}_2)$. The partition $(n-1, \ldots, 1, 0)$ is the Steinberg representation for the group $GL(n, \mathbb{F}_2)$. If a Ferrers diagram with $\lambda_n = 0$ is interpreted as a representation of $GL(n, \mathbb{F}_2)$, then adding 1 to each λ_i produces a full Ferrers diagram (now $\lambda_n = 1$), which corresponds to tensoring with the determinant representation, where the singular matrices now act as 0. Conversely, a representation of $M(n, \mathbb{F}_2)$ corresponding to a full Ferrers diagram may be interpreted in this way, as arising from a representation of $GL(n, \mathbb{F}_2)$. Of course any Ferrers diagram with $\lambda_n = 0$ may also be interpreted as a representation of $M(n, \mathbb{F}_2)$ but it is not obvious how this is related to the group interpretation, except in cases like the natural represention. For more explanation on this point see Harris and Kuhn [17].

For further discussion of the representation theory of $M(n, \mathbb{F}_2)$ we need to work with the equivalent theory of the representations of the semigroup algebra

$$\mathbb{F}_2[M(n, \mathbb{F}_2)].$$

An element e in an algebra is called *idempotent* if $e^2 = e$. The elements $0, 1$ are the *trivial* idempotents. Two idempotents e, f are *orthogonal* if $ef = fe = 0$. An idempotent e is primitive if it cannot be written as a sum two non-trivial orthogonal idempotents. The idempotent is *central* if it commutes with all elements of the algebra. A central idempotent is *centrally primitive* if it is not the sum of non-trivial orthogonal central idempotents. In the finite dimensional algebras that concern us, there is a uniquely determined finite set of centrally primitive idempotents whose sum is the identity of the algebra.

Example 3.1 *There are three centrally primitive idempotents in the semigroup algebra* $\mathbb{F}_2[M(n, \mathbb{F}_2)]$.

$$z_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

$$\begin{aligned} z_1 = {} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ & + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \\ & + \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

$$\begin{aligned} z_2 = {} & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \\ & + \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \end{aligned}$$

Then we see that

$$1 = z_0 + z_1 + z_2$$

and it can be checked that these idempotents are orthogonal. The display is arranged to highlight the sums of the non-singular matrices in z_1 *and* z_2, *which provide the two centrally primitive idempotents in the group algebra* $\mathbb{F}_2[GL(2, \mathbb{F}_2)]$.

In the semigroup algebra $\mathbb{F}_2[M(n,\mathbb{F}_2)]$ each central idempotent decomposes into a sum of orthogonal primitive idempotents. This decomposition is not unique. It turns out that the conjugacy classes of the primitive idempotents are in bijective correspondence with the irreducible representations λ. Let $\delta(\lambda)$ denote the dimension of the representation associated with the partition λ. Then there is a decomposition of the identity of the algebra into a maximal set of orthogonal primitive idempotents

$$1 = \sum_{\lambda} \sum_{i=1}^{\delta(\lambda)} e_{\lambda,i},$$

where the $e_{\lambda,i}$, for $1 \leq i \leq \delta(\lambda)$, is a set of conjugate primitive orthogonal idempotents associated with the same irreducible representation λ. It is customary to write, somewhat inaccurately,

$$1 = \sum_{\lambda} \delta(\lambda) e_{\lambda},$$

where e_{λ} stands for a typical idempotent associated with λ. Although the decomposition of 1 into orthogonal primitive idempotents is not unique, any two such sets of idempotents are conjugate by an invertible element in the semigroup ring in a way that matches idempotents associated with the same irreducible representation. In particular, in any decomposition of 1 into orthogonal primitive idempotents, there will be some way of grouping the idempotents into subsets which add up to the central idempotents but exactly how this works is a complicated matter to do with block theory of modular representations. We content ourselves here with an illustration of how it works for one particular decomposition in the case of 2×2 matrices over $\mathbb{F}_2$.

Example 3.2 *There are six elements in any choice of a maximal set of primitive orthogonal idempotents decomposing* 1 *in* $\mathbb{F}_2[M(n,\mathbb{F}_2)]$. *Such a set can be chosen to refine the central idempotents in the following way.*

$$e_0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

$$e_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

$$e_1' = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

$$e_{11} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$$e'_{21} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then we have the following decompositions of the central idempotents

$$z_0 = e_0, \quad z_1 = e_1 + e'_1 + e_{11}, \quad z_2 = e_{21} + e'_{21}$$

and the maximal decomposition of the identity

$$1 = e_0 + e_1 + e'_1 + e_{11} + e_{21} + e'_{21}.$$

Note that the e_0, e_1, e'_1 are the singular parts of e_{11}, e_{21}, e'_{21}. On the other hand, the non-singular parts g_0, g_1, g'_1 of e_{11}, e_{21}, e'_{21} provide a maximal set of three orthogonal primitive idempotents for the group algebra $\mathbb{F}_2[GL(2, \mathbb{F}_2)]$.

The idempotent e_0 corresponds to the trivial representation of $\mathbb{F}_2[M(n, \mathbb{F}_2)]$ with empty Ferrers diagram. The conjugate idempotents e_1 and e'_1 are associated with the natural representation, e_{11} with the determinant representation and the conjugate idempotents e_{21}, e'_{21} with the Steinberg representation. For $GL(2, \mathbb{F}_2)$, the idempotent g_0 corresponds to the trivial representation and g_1, g'_1 are conjugate idempotents corresponding to the Steinberg representation, which happens to coincide with the natural representation in case $n = 2$.

The action of $M(n, \mathbb{F}_2)$ on $\mathbf{P}(n)$ extends naturally to an action of the semigroup ring $\mathbb{F}_2[M(n, \mathbb{F}_2)]$ and the idempotents induce a corresponding decomposition of the polynomial algebra

$$\mathbf{P}(n) = \oplus_\lambda \delta(\lambda) \mathbf{P}(n) e_\lambda,$$

compatible with the left action of the Steenrod algebra. Each 'piece' $\mathbf{P}(n)e_\lambda$ occurs $\delta(\lambda)$ times in the decomposition and is an indecomposable $\mathcal{A}$-submodule (but no longer a right $\mathbb{F}_2[M(n, \mathbb{F}_2)]$-module). The dimension

$$\nu_d(\lambda) = \dim(\mathbf{P}^d(n) e_\lambda)$$

is the number of occurrencies of λ as a composition factor in $\mathbf{P}^d(n)$. One can think of the action of e_λ on $\mathbf{P}^d(n)$ as picking off a 1-dimensional vector subspace of $\mathbf{P}^d(n)$ for each occurrence of λ as a composition factor.

One way of tackling the hit problem for $\mathbf{P}(n)$ over $\mathcal{A}$ is to solve the hit problem for each piece separately. If an element of $\mathbf{P}^d(n)e_\lambda$ is hit in $\mathbf{P}(n)$ then it is already hit in $\mathbf{P}^d(n)e_\lambda$, as can be seen by applying the idempotent to both sides of a hit equation in $\mathbf{P}(n)$. This approach to the hit problem demands good control over the idempotents, which is lacking in general, but there are some interesting particular cases where progress can be made. In particular, we see that the central idempotents preserve symmetric functions and induce a decomposition of $\mathbf{B}(n)$ into $\mathcal{A}$-module summands. By following through the action of the idempotent splitting in Example 3.2 on symmetric functions, we obtain a splitting of $\mathbf{B}(2)$ into four $\mathcal{A}$-submodules

$$\mathbf{B}(2) = \mathbf{B}(2)e_0 \oplus \mathbf{B}(2)e_1 \oplus \mathbf{B}(2)e_{11} \oplus \mathbf{B}(2)e_{21},$$

where $\mathbf{B}(2)e_1$ is isomorphic as an $\mathcal{A}$-module to $\mathbf{B}(1)$, generated by $x_1^a + x_2^a$ for $a > 0$: the module $\mathbf{B}(2)e_{11}$ is isomorphic to the Dickson algebra $\mathbf{D}(2)$, generated by

$$(x_1 + x_2)^a(x_1^b + x_2^b) + (x_1 + x_2)^b(x_1^a + x_2^a) + x_1^a x_2^b + x_1^b x_2^a,$$

for $a, b > 0$: the module $\mathbf{B}(2)e_{21}$ is generated by

$$(x_1 + x_2)^a(x_1^b + x_2^b) + (x_1 + x_2)^b(x_1^a + x_2^a),$$

for $a, b > 0$. We note that $\mathbf{B}(2)e_1', \mathbf{B}(2)e_{21}'$ are 0 and $\mathbf{B}(2)e_0$ is trivial, concentrated in dimension 0. By restricting to symmetric functions divisible by by x_1x_2 we obtain a splitting of the A-module $\mathbf{M}(2)$ into two pieces

$$\mathbf{M}(2) = \mathbf{M}(2)e_{11} \oplus \mathbf{M}(2)e_{21},$$

where $\mathbf{M}(2)e_{11}$ is the Dickson algebra $\mathbf{D}(2)$.

It is debatable whether the attempt to solve the hit problem for $\mathbf{B}(2)$ by decomposition methods is any better than the direct approach in arriving at Theorem 2.11 but it does raise a number of interesting Problems 5.9, 5.12 and 5.11 about the algebraic splittings of $\mathbf{P}(n), \mathbf{B}(n), \mathbf{M}(n)$ and hit problems for individual pieces.

We now turn to some topological aspects of the problem.

3.1 Modular representations and topological splittings

We use the notation $L(\lambda)$ for a $M(n, \mathbb{F}_2)$-module which affords the irreducible representation corresponding to λ. It is known that $L(\lambda)$ occurs as a composition factor in $\mathbf{P}^d(n)$ for some value of d. Indeed, it actually occurs as a submodule of $\mathbf{P}^d(n)$ for some (usually higher) value of d. The following statements indicate when these phenomena first happen [6].

Theorem 3.3 *The irreducible $M(n,\mathbb{F}_2)$-representation corresponding to the 2-column regular partition λ occurs for the first time as a composition factor in $\mathbf{P}^d(n)$ in degree*

$$\zeta(\lambda) = \sum_i 2^{\lambda_i} - 1$$

and for the first time as a submodule in $\mathbf{P}^d(n)$ in degree

$$\eta(\lambda) = \sum_i \lambda_i 2^{i-1}.$$

In the above formulae we note that the $\zeta(\lambda) < \eta(\lambda)$ except when λ is a triangular sequence $(m, m-1, \ldots, 2, 1)$. Note also that $\eta(\lambda) = \zeta(\lambda')$.

Since a singular matrix must annihilate some non-zero element in $\mathbf{P}^d(n)$ for $d > 0$, it follows that the trivial representation of $M(n,\mathbb{F}_2)$ can only occur once, namely in dimension 0. This is consistent with the fact that the trivial representation corresponds to the empty Ferrers diagram where all $\lambda_i = 0$, in which case $\zeta = \eta = 0$. On the other hand the determinant representation, where $\lambda_i = 1$ for $1 \leq i \leq n$, occurs for the first time in degree $\zeta = n$ as a composition factor headed by the product of the variables $x_1 \cdots x_n$. As a submodule it appears for the first time in degree $\eta = 2^n - 1$.

Little is known about the odd prime analogue of the first occurrence problem as a composition factor, although a few cases are resolved [4]. The first occurrence as a submodule is known for all primes [25]. Even where we have explicit models for the irreducible representations of $M(n,\mathbb{F}_2)$ as submodules of $\mathbf{P}(n)$, there seems to be no known closed formulae for their dimensions.

We now explain how the numbers $\delta(\lambda), \nu_d(\lambda), \zeta(\lambda), \eta(\lambda)$ can be interpreted topologically. For an early reference on the use of idempotents in splitting suspended spaces we cite [9].

Recall that $\mathbf{P}(n)$ is the cohomology of the product of n copies of infinite real projective space, otherwise known as the classifying space $B(\mathbf{Z}/2)^n$ of the group $(\mathbf{Z}/2)^n$. Let Y denote the suspension of $B(\mathbf{Z}/2)^n$. For each irreducible representation λ of $M(n,\mathbb{F}_2)$ there is an associated topological space Y_λ such that, up to homotopy type, Y decomposes into the one-point union

$$Y \simeq \vee_\lambda \delta(\lambda) Y_\lambda,$$

each Y_λ occurring $\delta(\lambda)$ times in the splitting. The cohomology $\mathbf{H}^*(Y_\lambda,\mathbb{F}_2)$ can be identified with $\mathbf{P}(n)e_\lambda$, with a shift in grading. In particular the dimension of $\mathbf{H}^d(Y_\lambda,\mathbb{F}_2)$ is $\nu_d(\lambda)$ and $\zeta(\lambda)$ corresponds to the connectivity of the piece Y_λ. None of the pieces Y_λ can be further split stably into a one-point union of non-trivial spaces. The piece associated with the idempotent corresponding to the trivial representation, given by the empty Ferrers diagram, is a single point. In practice, therefore, there are $2^n - 1$ interesting spaces in the splitting of Y.

We refer to [15, 27, 28, 33] for a detailed analysis of the topological pieces obtained for the case $n = 2$ in the stable splittings of $B(\mathbb{Z}/2)$ and $BO(2)$. In the terminology of Example 3.2 there is a stable homotopy equivalence

$$Y \simeq Y_0 \vee 2Y_1 \vee Y_{11} \vee 2Y_{21}.$$

We have topological Problems 5.15, 5.16, analogous to the algebraic Problems 5.9, 5.12.

We now look at a few particular problems related to the general discussion above.

3.2 Linking first occurences by Steenrod operations

In this section we shall describe an explicit Steenrod operation which links the first occurrence of the irreducible representation λ as composition factor with its first occurrence as submodule in $\mathbf{P}(n)$. We need some preliminary notation.

In the Ferrers diagram of λ, the kth *anti-diagonal* of λ consists of the nodes (i, j) such that $i + j = k + 1$. Suppose the nodes of the k-th anti-diagonal are $(k, 1), (k-1, 2), \ldots, (k-s+1, s)$. The associated van der Monde determinant is defined by

$$v_k(\lambda) = \begin{vmatrix} x_k & x_{k-1} & \cdots & x_{k-s+1} \\ x_k^2 & x_{k-1}^2 & \cdots & x_{k-s+1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_k^{2^{s-1}} & x_{k-1}^{2^{s-1}} & \cdots & x_{k-s+1}^{2^{s-1}} \end{vmatrix}.$$

The product of these expressions is denoted by

$$v(\lambda) = \prod_k v_k(\lambda).$$

For example, when $\lambda = (2, 1, 1)$,

$$v(\lambda) = x_1 \cdot [x_1, x_2^2] \cdot x_3 = x_1^3 x_2 x_3 + x_1^2 x_2^2 x_3.$$

In general, the 'leading' term of $v(\lambda)$, i.e. the monomial with highest exponents in the left lexicograhic order, is $\prod_k x_k^{2^{\lambda_k}-1}$, which is a spike. The polynomial $v(\lambda)$ is therefore not hit.

We shall also use following notation for the particular van der Monde determinant

$$w(n) = [x_1, x_2^2, \cdots, x_n^{2^{n-1}}] = \begin{vmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{2^{n-1}} & x_2^{2^{n-1}} & \cdots & x_n^{2^{n-1}} \end{vmatrix},$$

where the shorthand form in square brackets lists just the diagonal elements of the determinant. Then we associate with λ the polynomial

$$w(\lambda) = \prod_k w_k(\lambda_k).$$

For example, when $\lambda = (2, 1, 1)$,

$$w(\lambda) = [x_1, x_2^2]x_2x_3, \qquad w(\lambda') = [x_1, x_2^2, x_3^4]x_1.$$

Note that $\deg(v(\lambda)) = \eta(\lambda), \deg(w(\lambda)) = \zeta(\lambda)$. We now state the main results [41].

Theorem 3.4 *Let λ be a 2-column regular partition of length n. Then the corresponding irreducible $M(n, \mathbb{F}_2)$-module $L(\lambda)$ appears as a top composition factor of the module generated in $\mathbf{P}_{\zeta(\lambda)}(n)$ by $v(\lambda)$ and also as the submodule in $\mathbf{P}_{\eta(\lambda)}(n)$ generated by $w(\lambda')$.*

Theorem 3.5 *Let λ be a 2-column regular partition of length n. For $1 \leq k \leq \lambda_1$, let $r_k = (2^{\lambda'_k} - 1) - \sum_{i \leq \lambda'_k} 2^{\lambda_i - k}$. Then*

$$\chi(Sq^{r_1}Sq^{r_2}\dots Sq^{r_{\lambda_1}})v(\lambda) = w(\lambda').$$

The sequence of numbers $(r_1, r_2, \dots, r_{\lambda_1})$ can be conveniently calculated from the tableau obtained by inserting integers into the Ferrers diagram of λ as follows: if the (i, λ_i) is the highest node in its antidiagonal, insert $2^{i-1} - 1$ in that position and continue down the diagonal by doubling the number entered at each step. The sum of the numbers entered in column k is then r_k.

Example 3.6 For $\lambda = (3, 3, 2, 2, 1)$ we obtain $(r_1, r_2, r_3) = (18, 9, 1)$ using the tableau shown below.

0	0	0
0	0	1
0	2	
4	7	
14		

The statement of Theorem 3.5 in this case is

$$\chi(Sq^{18}Sq^9Sq^1)(x_1 \cdot [x_1, x_2^2] \cdot [x_1, x_2^2, x_3^4] \cdot [x_2, x_3^2, x_4^4] \cdot [x_4, x_5^2])$$
$$= [x_1, x_2^2, x_3^4, x_4^8, x_5^{16}] \cdot [x_1, x_2^2, x_3^4, x_4^8] \cdot [x_1, x_2^2].$$

3.3 The Steinberg piece

The Steinberg representation of $GL(n, \mathbb{F}_2)$, corresponding to the triangular sequence

$$St = (n-1, \ldots, 1, 0)$$

plays a special role in the representation theory of the general linear group. Every occurrence of St is a submodule. The following statement solves the hit problem for the Steinberg piece [41] arising from the general linear group.

Theorem 3.7 *There is a choice of indecomposable idempotent e_{St} in the group algebra $\mathbb{F}_2[GL(n, \mathbb{F}_2)]$ associated with the Steinberg representation St of $GL(n, \mathbb{F}_2)$ such that the piece $\mathbf{P}(n)e_{St}$ is generated minimally by the symmetrised spikes*

$$\sigma(x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}),$$

for distinct *exponents $d_1, d_2, \ldots, d_n$.*

The actual choice of idempotent e_{St} is constructed as follows. Let $\overline{U}_n$ denote the sum of the upper triangular matrices in $GL(n, \mathbb{F}_2)$ and $\overline{\Gamma}_n$ the sum of the elements in the symmetric group Σ_n. Then

$$e_{St} = \overline{U}_n \overline{\Sigma}_n.$$

By construction we see that the action of this particular choice of Steinberg idempotent on $\mathbf{P}(n)$ preserves symmetric functions and therefore splits $\mathbf{B}(n)$ into a Steinberg piece and another piece. We refer to [27, 28, 33] for the topological realisation of this splitting and to [39, 29] for the stable splitting of $BO(n)$ into pieces corresponding to the submodules $\mathbf{T}(r)$ mentioned in Proposition 2.4.

3.4 The trivial piece

Recently, Hung and Nam [19] have proved Hung's conjecture that all elements in the Dickson algebra $\mathbf{D}(n)$ are hit in $\mathbf{P}(n)$ for $n \geq 3$. Now the Dickson algebra is only a part of the piece $\mathbf{P}(n)g_0$, corresponding to the trivial representation of the group $GL(n, \mathbb{F}_2)$. The Dickson algebra affords the *submodule* occurrences of the trivial representation in $\mathbf{P}(n)$. The hit problem for the Dickson algebra itself is difficult and has only been solved for small values of n [20]. It would be interesting to give a a minimal generating set for $\mathbf{P}(n)g_0$ by analogy with the Steinberg case. The Hung-Nam result says that all submodule occurences are hit by earlier composition factors in the determinant piece at least for $n \geq 3$.

We saw earlier how, in the case $n = 2$, the idempotent e_{11} splits off the Dickson algebra $\mathbf{D}(2)$ from $\mathbf{M}(2)$. Now $\mathbf{D}(2)$ is topologically realisable by $H^*(BSO(3))$ over the field of two elements. This raises again the question concerning the topological splitting of Thom complexes $MO(n)$.

4 The hit problem for the differential operator algebra

The action of the Steenrod square Sq^k on $\mathbf{P}(n)$ can be lifted to the action of an operator SQ^k on the polynomial algebra

$$\mathbf{W}(n) = \mathbb{Z}[x_1, x_2, \dots, x_n]$$

over the integers. Integral squaring operators are members of a larger ring of operators $\mathcal{D}$, called the *differential operator algebra.* The formal definition of $\mathcal{D}$ and some of its properties can be found in [49, 48]. Topologists know $\mathcal{D}$ as the Landweber-Novikov algebra. For present purposes we recall from [49, 48] some of the main features concerning the action of $\mathcal{D}$ on $\mathbf{W}(n)$. An additive basis for $\mathcal{D}$ is formed from *wedge* products of the primitive partial differential operators

$$D_k = \sum_{i\geq 1} x_i^{k+1}\frac{\partial}{\partial x_i},$$

for $k \geq 1$, acting in the usual on $\mathbf{W}(n)$. Although D_k is formally an infinite sum, its action on a polynomial involves only a finite number of variables in any instance. The wedge product $\vee$ of two differential operators, with variable coefficients, is defined by allowing the derivatives of the first operator to pass the variable coefficients of the second operator without acting. The wedge product is commutative and gives the term of highest differential order in the composition of the operators. For example, the composite $D_1 \circ D_1$ is given by

$$(\sum_{i\geq 1} x_i^2\frac{\partial}{\partial x_i})(\sum_{i\geq 1} x_i^2\frac{\partial}{\partial x_i}) = 2(\sum_{i\geq 1} x_i^3\frac{\partial}{\partial x_i}) + \sum_{(i_1,i_2)} x_{i_1}^2x_{i_2}^2\frac{\partial^2}{\partial x_{i_1}\partial x_{i_2}},$$

where the last summation is taken over all 2-vectors of non-negative integers (i_1, i_2). Hence $D_1 \circ D_1 = 2D_2 + D_1 \vee D_1$. It should be noted that $D_1 \vee D_1$ is divisible by 2 as an integral operator. More generally, an iterated wedge product is given by the formula

$$D_{k_1} \vee D_{k_2} \vee \cdots \vee D_{k_r} = \sum_{(i_1,\dots,i_r)} x_{i_1}^{k_1+1}\cdots x_{i_r}^{k_r+1}\frac{\partial^r}{\partial x_{i_1}\cdots\partial x_{i_r}},$$

where the summation is taken over all r-vectors of non-negative integers. It can be seen from this that the iterated wedge product $D_k^{\vee r}$ is divisible by $r!$ as an integral operator. By definition, $\mathcal{D}$ is generated over the integers by the divided operators $D_k^{\vee r}/r!$ under wedge product. For convenience we use the multiset notation $K = k_1^{r_1}k_2^{r_2}\dots k_a^{r_a}$ to denote a set of positive distinct integers k_i repeated r_i times. Then

$$D(K) = \frac{D_{k_1}^{\vee r_1}}{r_1!} \vee \frac{D_{k_2}^{\vee r_2}}{r_2!} \vee \cdots \vee \frac{D_{k_a}^{\vee r_a}}{r_a!}$$

denotes the iterated wedge product of divided differential operators. For example,

$$D(k) = D_k, \quad D(k^r) = \frac{D_k^{\vee r}}{r!}.$$

The collection $D(K)$, as K ranges over multisets of distinct integers, forms an additive basis for $\mathcal{D}$. A significant fact is that $\mathcal{D}$ is closed under composition of operators. Furthermore, the natural coproduct $\psi(D_n) = 1 \otimes D_n + D_n \otimes 1$ makes $\mathcal{D}$ into a Hopf algebra with respect to both the composition and the wedge products.

We define the *integral Steenrod squares* by $SQ^r = D(1^r)$. It is shown in [49] that the modulo 2 reduction of SQ^k is Sq^k. For example

$$SQ^1 = D(1) = \sum_{i \geq 1} x_i^2 \frac{\partial}{\partial x_i}.$$

Additively, the Steenrod algebra is generated by the modulo 2 reductions of those $D(K)$ for which the elements K have the form $k_i = 2^{\lambda_i} - 1$. This is called the *Milnor basis* of the Steenrod algebra.

Since $\mathcal{D}$ is defined over the integers we have the possibility of reduction at any prime as well as rational reduction. For example, the collection of modulo p reductions of those $D(K)$ for which the elements of K have the form $k_i = p^{\lambda_i} - 1$ constitute the Milnor basis of the Steenrod algebra of p-th power operators at an odd prime p. The analogue of $SQ^r = D(1^r)$ in the odd prime case is $P^r = D((p-1)^r)$.

We can pose the hit Problem 5.19 for the action of the differential operator algebra $\mathcal{D}$ on $\mathbf{W}(n)$ over the integers, but this would seem to be a very difficult question to answer in more than a few variables. For $n = 1$ the answer is simple because $D_k(x) = x^{k+1}$. Hence $\mathbf{Q}(\mathbf{W}(1))$ has rank 1 generated by x_1. This result generalises in the following way. Note first of all that the action of $\mathcal{D}$ commutes with the right action of the symmetric group because the differential operators are themselves symmetric in the variables and partial derivatives. On the other hand it does not commute with the action of all matrices over the integers. We lose the analogue of the Dickson algebra but retain the representation theory of the symmetric group. In particular we can study the hit problem for symmetric polynomials over the integers, viewed as a $\mathcal{D}$-module.

Theorem 4.1 *Any symmetric polynomial in $\mathbf{W}(n)^{\Sigma_n}$ divisible by $x_1 \cdots x_n$ and of degree strictly greater than n is hit by a differential operator in $\mathcal{D}$.*

Problems 5.20 remain for representations of the symmetric group other than the trivial one. Since integral representation theory of Σ_n is difficult, we look instead at modular and rational reductions.

4.1 The hit problem for $\mathcal{D}$ modulo 2

Integral results about the action of $\mathcal{D}$ on $\mathbf{W}(n)$ can be passed down to modular reductions. For example the statement of Theorem 4.1 is true for the action of $\mathcal{D} \otimes \mathbb{F}_2$ on $\mathbf{P}(n)$. As observed earlier $\mathcal{D} \otimes \mathbb{F}_2$ contains $\mathcal{A}$ as a sub-algebra. To solve the hit problem for the action of $\mathcal{A}$ on $\mathbf{P}(n)$, we might ask a prior question about the hit problem for $\mathbf{P}(n)$ as a $\mathcal{D}\otimes\mathbb{F}_2$-module, where we would expect fewer elements in a minimal generating set than in the Steenrod algebra case.

For two variables, the answer has been worked out by Walker and Xiao and appears in the second author's doctoral thesis.

Theorem 4.2 *For the action of $\mathcal{D}\otimes\mathbb{F}_2$ on $\mathbf{P}(2)$ a basis for $\mathbf{Q}(\mathbf{P}(2))$ is given by the monomials $1, x_1, x_2, x_1^2x_2, x_1^{2^n-1}x_2$ for $n \geq 1$.*

For comparison we quote the corresponding result for the Steenrod algebra.

Theorem 4.3 *For the action of $\mathcal{A}$ on $\mathbf{P}(2)$, a basis for $\mathbf{Q}(\mathbf{P}(2))$ is given by the the monomials $x_1^{2^k-1}x_2^{2^r-1}$ for $k, r \geq 0$, and $x_1^{2^a-1}x_2^{2^{a-1}-1+2^a(2^b-1)}$ for $a, b \geq 1$.*

In the general n-variable problem spikes are never hit under the action of the Steenrod algebra but can be hit under the action of differential operator algebra. There is a question about the exact relationship between the the two hit Problems 5.18.

4.2 The rational hit problem for $\mathcal{D}$

In this section we shall write $\mathbf{Q}(n)$ as a temporary notation for $\mathbf{Q}(\mathbf{W}(n)\otimes\mathbb{Q})$. It can be shown that $\mathcal{D}\otimes\mathbb{Q}$ is generated under composition by the operators D_k. In fact D_1, D_2 form a minimal algebraic generating set. The hit problem in this case reduces to the question of finding criteria on a polynomial g such that the differential equation

$$D_1 f_1 + D_2 f_2 = g$$

can be solved for polynomials f_1, f_2. In the two-variable case, it can be shown that $1, x_1, x_2, x_1x_2, x_1^2x_2$ form a basis of $\mathbf{Q}(2)$. In particular, the quotient is finite dimensional, as in Example 1.2. Furthermore, the differential equation $D_1f_1 + D_2f_2 = g$ can be solved for any homogeneous polynomial g of degree at least 4. Another similarity with Example 1.2 is that the monomials $x_1x_2, x_1^2x_2$ generate the regular representation of Σ_2 in $\mathbf{Q}(2)$. The monomial x_1x_2 generates the trivial representation, and the equation $D_1(x_1x_2) = x_1^2x_2 + x_1x_2^2$ shows that $x_1^2x_2$ generates the sign representation of Σ_2 in $\mathbf{Q}(2)$.

In the case of three variables, $n = 3$, it is shown in [43] that the monomials

$$1, x_1, x_2, x_3, x_1x_2, x_1x_3, x_2x_3,$$

$$x_1^2x_2, x_1^2x_3, x_2^2x_3, x_1x_2x_3, x_1x_2^2x_3, x_1x_2x_3^2, x_1x_2^2x_3^2, x_1x_2x_3^3, x_1x_2^2x_3^3$$

generate $\mathbf{Q}(3)$. The regular representation is generated by those monomials in the list which are divisible by $x_1x_2x_3$. This time, the differential equation $D_1f_1 + D_2f_2 = g$ can be solved if the homogeneous polynomial g has degree at least 7. In the general case of n variables, it is known that $\mathbf{Q}(n)$ is finite dimensional. However, the following conjecture, suggested by the above particular cases, seems harder to prove.

Conjecture 4.4 *For the action of the differential operator algebra $\mathcal{D} \otimes \mathbb{Q}$ on the polynomial algebra $\mathbb{Q}[x_1, \cdots, x_n]$, $\mathbf{Q}(n)$ contains the regular representation of the symmetric group Σ_n generated by the monomials divisible by the product of the variables $x_1 \cdots x_n$. In particular, the highest grading of $\mathbf{Q}(n)$ is $d = n(n+1)/2$ and, in this grading, $\mathbf{Q}^d(n)$ is the 1-dimensional sign representation of Σ_n, generated by the $x_1x_2^2 \cdots x_n^n$. Furthermore, monomials of the form*

$$x_1^{i_1}x_2^{i_2} \cdots x_n^{i_n},$$

where $1 \leq i_r \leq r$, form a basis of the part of $\mathbf{Q}(n)$ divisible by $x_1 \cdots x_n$.

This conjecture implies, in particular, that every homogeneous polynomial f of degree greater than $n(n+1)/2$ is hit; in other words, the differential equation

$$D_1f_1 + D_2f_2 = g$$

can be solved for any g in these degrees. There is clearly a close connection between the representation theory of the symmetric group and the hit problem for the differential operator algebra. The decomposition of $\mathbf{W} \otimes \mathbb{Q}$ by a complete set of orthogonal idempotents associated with the irreducible representations of Σ_n is preserved by the action of $\mathcal{D} \otimes \mathbf{Q}$. The piece of $\mathbf{W} \otimes \mathbf{Q}$ corresponding to the trivial representation is the subspace of symmetric polynomials.

4.3 Remark

The algebra $\mathcal{D}$ preserves rings of invariants of permutation groups. More precisely, if $\Gamma \subset \Sigma_n$ is a subgroup the symmetric group, then $\mathbf{W}^\Gamma$ is a left module over $\mathcal{D}$. It would be interestind to investigate such modules both rationally and in the modular cases.

5 Problems

The following list of problems refers mainly to the prime 2 unless otherwise stated. There are of course analogous problems at any prime.

Problem 5.1 *Find a minimal generating set for* $\mathbf{P}(n)$ *as a module over* $\mathcal{A}$ *for* $n \geq 4$.

Problem 5.2 *Is the best bound for* $\dim \mathbf{Q}^d(\mathbf{P}(n))$ *the product* $(1)(3)\cdots(2^n-1)$*?*

Problem 5.3 *Is it true that the product of two non-hit polynomials in disjoint sets of variables is non-hit over* $\mathcal{A}$*?*

Problem 5.4 *Is it true that if a* monomial *in* $\mathbf{P}(n)$ *is non-hit over* $\mathcal{A}$*, then some matrix transformation of it contains a spike?*

Problem 5.5 *Find a formula for the excess of* $\widehat{\Theta}$*, where* Θ *is a composite of Steenrod squares, with a view to enhancing the use of the* χ*-trick.*

Problem 5.6 *Find a minimal generating set for* $\mathbf{B}(n)$ *as a module over* $\mathcal{A}$ *for* $n \geq 4$.

Problem 5.7 *If* f *is a hit monomial in* $\mathbf{P}(n)$ *over* $\mathcal{A}$*, is its symmetrisation* $\sigma(f)$ *hit symmetrically in* $\mathbf{B}(n)$*?*

Problem 5.8 *What is the best bound for the dimension of* $\mathbf{Q}^d(\mathbf{B}(n))$ *as a function of* n *independent of* d*?*

Problem 5.9 *Describe, for general* n*, the pieces of the maximal splitting of* $\mathbf{P}(n)$ *afforded by a complete set of orthogonal primitive idempotents in the semigroup ring* $\mathbb{F}_2[M(n,\mathbb{F}_2)]$*. How many distinct pieces are there? How many times does a piece occur. Find the Poincaré series of the pieces.*

Problem 5.10 *How do we write down the central idempotents in* $\mathbb{F}_2[M(n,\mathbb{F}_2)]$*? How do they decompose into primitives?*

Problem 5.11 *Describe the subalgebra of the semigroup algebra*

$$\mathbb{F}_2[M(n, \mathbb{F}_2]$$

whose action on $\mathbf{P}(n)$ *preserves symmetric functions. In particular find idempotents in this algebra.*

Problem 5.12 *Describe, for general* n*, the pieces of the maximal splitting of* $\mathbf{B}(n)$ *and* $\mathbf{M}(n)$ *afforded by a complete set of symmetry preserving orthogonal idempotents in the semigroup algebra* $\mathbb{F}_2[M(n, \mathbb{F}_2)]$. *How many pieces are there? How many times does a piece occur?*

Problem 5.13 *Solve the first occurrence problems for the irreducible modules of general linear groups as composition factors in the polynomial algebra at odd primes.*

Problem 5.14 *Solve the first occurrence problems for the irreducible modules of the symmetric groups in the polynomial algebra at odd primes.*

Problem 5.15 *Find the Poincaré series of the pieces* Y_λ *in the splitting of*

$$\Sigma(\mathbb{R}P^\infty \times \ldots \times \mathbb{R}P^\infty)$$

afforded by the irreducible representations λ *of the matrix semigroup* $M(n, \mathbb{F}_2)$.

Problem 5.16 *What is the maximal splitting of the stable homotopy type of* $BO(n)$*? How does it relate to the central idempotent splitting of* $\mathbf{B}(n)$*?.*

Problem 5.17 *Does the Thom complex* $MO(n)$ *split stably for* $n \geq 2$*?*

Problem 5.18 *What is the relation between the hit problems for* $\mathbf{P}(n)$ *as a module over* $\mathcal{A}$ *and as a module over* $\mathcal{D}$*?*

Problem 5.19 *Solve the hit problem for the action of* $\mathcal{D}$ *on* $\mathbf{W}(n)$ *for* $n \geq 2$ *over the rationals.*

Problem 5.20 *Investigate hit problems for the action of* $\mathcal{D}$ *on the pieces of* $\mathbf{W}(n)$ *split off by idempotents associated with irreducible representations of the symmetric group* Σ_n *in the modular case.*

Problem 5.21 *Is it true that the product of two non-hit polynomials in disjoint sets of variables is non-hit over $\mathcal{D}$?*

Problem 5.22 *What is the best bound for* $\dim(\mathbf{Q}^d(\mathbf{P}(n))$ *for* $\mathbf{P}(n)$ *as a module over $\mathcal{D}$?*

Problem 5.23 *Investigate rings of invariants of permutation groups as modules over $\mathcal{D}$.*

References

[1] M. A. Alghamdi, M. C. Crabb and J. R. Hubbuck, Representations of the homology of BV and the Steenrod algebra I, Adams Memorial Symposium on Algebraic topology vol 2, London Mathematical Society Lecture Notes Series 176, Cambridge University Press (1992), 217–234.

[2] J. M. Boardman, Modular representations on the homology of powers of real projective spaces, Algebraic Topology, Oaxtepec 1991, Contemp. Math. 146 (1993), 49–70.

[3] H. E. A. Campbell and P. S. Selick, Polynomial algebras over the Steenrod algebra, Comment. Math. Helv. 65 (1990), 171–180.

[4] D. P. Carlisle, The modular representations of $GL(n,p)$ and applications, Thesis, Manchester (1985).

[5] D. P. Carlisle, P. Eccles, S. Hilditch, N. Ray, L. Schwartz, G. Walker and R. Wood, Modular representations of $GL(n,p)$, splitting $\Sigma(CP^\infty \times \cdots \times CP^\infty)$ and the β-family as framed hypersurfaces, Math. Z. 189 (1985), 239–261.

[6] D. P. Carlisle and N. J. Kuhn, Subalgebras of the Steenrod algebra and the action of matrices on truncated polynomial algebras, J. of Algebra 121 (1989), 370–387.

[7] D. P. Carlisle and G. Walker, Poincaré series for the occurrence of certain modular representations of $GL(n,p)$ in the symmetric algebra, Proceedings of the Royal Society of Edinburgh 113A (1989), 27–41.

[8] D. P. Carlisle and R. M. W. Wood, The boundedness conjecture for the action of the Steenrod algebra on polynomials, Adams Memorial Symposium on Algebraic Topology vol. 2, London Mathematical Society Lecture Notes Series 176, Cambridge University Press (1992), 203–216.

[9] F. R. Cohen, Splitting certain suspensions with self maps, Ill. J. Math 20 (1976), 336–347.

[10] M. C. Crabb, M. D. Crossley and J. R. Hubbuck, K-theory and the anti-automorphism of the Steenrod algebra, Proc. Amer. Math. Soc. 124 (1996), 2275–2281.

[11] M. C. Crabb and J. R. Hubbuck, Representations of the Homology of BV and the Steenrod Algebra II, Algebraic topology: new trends in localization and periodicity (San Feliu de Guixols 1994), Prog. Math. 136, Birkhaüser (1996), 143–154.

[12] M. D. Crossley, H^*V is of bounded type over $\mathcal{A}_p$, Preprint, Barcelona (1996).

[13] M. D. Crossley, $\mathcal{A}(p)$-annihilated elements of $H_*(CP^\infty \times CP^\infty)$, Math. Proc. Camb. Phil. Soc. 120 (1996), 441–453.

[14] P. J. Eccles and W. P. R. Mitchell, Splitting $\Sigma(CP^\infty \times CP^\infty)$ localised at 2, Quart. J. Math. Oxford 39 (1988), 285–289.

[15] J. C. Harris, Thesis, Chigago,(1985).

[16] J. C. Harris, On certain stable wedge summands of $B(\mathbb{Z}/p)^n_+$, Preprint, Department of Mathematics, Toronto.

[17] J. C. Harris and N. J. Kuhn, Stable decompositions of classifying spaces of finite abelian groups, Math. Proc. Cam. Phil. Soc. 103 (1988), 427–449.

[18] N. H. V. Hung, Spherical classes and the algebraic transfer, to appear in Trans. Amer. Math. Soc.

[19] N. H. V. Hung and T. N. Nam, The hit problem for the Dickson algebra, Preprint (1999).

[20] N. H. V. Hung and F. P. Peterson, $\mathcal{A}$-generators for the Dickson algebra, Trans. Amer. Math. Soc. 347, (1995), 4687–4728.

[21] A. Janfada, Ph.D. thesis, Manchester 2000.

[22] M. Kameko, Products of projective spaces as Steenrod modules, Thesis, Johns Hopkins University (1990).

[23] M. Kameko, Generators of the cohomology of BV_3, J. Math. Kyoto Univ. 38 (1998).

[24] D .M . Meyer, Hit polynomials and excess in the mod p Steenrod algebra, preprint (1999).

[25] P .A . Minh and T .T . Tri , The first occurrence for the irreducible modules of general linear groups in the polynomial algebra, preprint.

[26] D .M . Meyer and J . H . Silverman, Corrigendum to "Hit polynomials and conjugation in the dual Steenrod algebra", preprint (1999).

[27] S. Mitchell and S. Priddy, Symmetric product spectra and splittings of classifying spaces , Amer. J. math. 106 (1984), 219–232.

[28] S. Mitchell and S. Priddy, Stable splittings derived from the Steinberg module, Topology 22 91983, 285–298.

[29] S. Mitchell and S. Priddy, A double coset formula for Levi subgroups and splitting $BGL(n)$, Algebraic topology (Arcata 1986), Lecture Notes in Math. 1370, Springer (1989), 325–334.

[30] J. Milnor, The Steenrod algebra and its dual, Annals of Math. 67 (1958), 150–171.

[31] F. P. Peterson, $\mathcal{A}$-generators for certain polynomial algebras, Math. Proc. Camb. Phil. Soc. 105 (1989), 311–312.

[32] F. P. Peterson, Generators of $\mathbf{H}^*(RP^\infty \wedge RP^\infty)$ as a module over the Steenrod algebra, Abstracts Amer. Math. Soc. (1987), 833-55-89.

[33] S. Priddy, Recent progress in stable splittings, London Mathematical Society Lecture Notes 117, Homotopy Theory, Cambridge University Press (1987), 149–174.

[34] J. Repka and P. Selick, On the subalgebra of $H_*(RP^\infty)^n; \mathbb{F}_2)$ annihilated by Steenrod operations, J. Pure Appl. Algebra 127 (1998), 273–288.

[35] J. Silverman, Conjugation and excess in the Steenrod algebra, Proc. Amer. Math. Soc. 119 (1993), 657–661 .

[36] W. Singer, On the action of Steenrod squares on polynomial algebras, Proc. Amer. Math. Soc. 111 (1991), 577–583.

[37] L. Smith, Polynomial invariants of finite groups, Research Notes in Mathematics, vol. 6, A. K. Peters Ltd, Wellesley MA (1995).

[38] L. Smith and R .Switzer, Realizability and non-realizability of Dickson algebras as cohomology rings, Proc. Amer. Math. Soc. 89 (1983), 303-313.

[39] V. Snaith, Lecture Notes in Mathematics 673, Springer, Berlin, (1978), 123–157.

[40] N. E. Steenrod and D. B. A. Epstein, Cohomology operations, Annals of Math. Studies 50, Princeton University Press (1962).

[41] G. Walker and R. M. W. Wood, The hit problem for the Steinberg module over the Steenrod algebra, Preprint, Manchester, (1999).

[42] G. Walker and R. M. W. Wood, The action of $\chi(Sq^r)$ on products of linear polynomials. Preprint, Manchester (1999).

[43] G. Walker and R. M. W. Wood, The rational hit problem for the differential operator algebra. Preprint, Manchester, (1999).

[44] R. M. W. Wood, Modular representations of $GL(n, \mathbb{F}_p)$ and homotopy theory, Algebraic topology Göttingen 1984, Lecture Notes in Mathematics 1172 Springer-Verlag (1985), 188–203.

[45] R. M. W. Wood, Splitting $\Sigma(CP^\infty \times \ldots \times CP^\infty)$ and the action of Steenrod squares on the polynomial ring $\mathbb{F}_2[x_1, \ldots, x_n]$, Algebraic Topology Barcelona 1986, Lecture Notes in Mathematics 1298, Springer-Verlag (1987), 237–255.

[46] R. M. W. Wood, Steenrod squares of polynomials and the Peterson conjecture, Math. Proc. Camb. Phil. Soc 105 (1989), 307–309.

[47] R. M. W. Wood, Steenrod squares of Polynomials, Advances in homotopy theory, London Mathematical Society Lecture Notes 139, Cambridge University Press (1989), 173–177.

[48] R. M. W. Wood, Differential operators and the Steenrod algebra, Proc. London Math. Soc. 75 (1997), 194–220.

[49] R. M. W. Wood, Problems in the Steenrod algebra, Bull. London Math. Soc. 30 (1998), 449-517.

Department of Mathematics
University of Manchester
Manchester M13 9PL