The hit problem for $W(4)$ over F_2 by the differential operator algebra

Hemin Yang

A dissertation submitted to the Johns Hopkins University in
conformity with the requirements for the degree of Doctor of
Philosophy

Baltimore, Maryland
Sep. 2001

ABSTRACT

In this paper, we not only determine a basis of the quotient of $W(4)$, the polynomial algebra over F_2 generated by 4 variables, by the action of the divided differential operator algebra $\mathfrak{D}$, we are able to represent every element in the quotient as a linear combination of the basis elements. This leads to a description of the action of the symmetric group S_4 too.

Acknowledgement

First I would like to express my deep gratitude to my advisors, Professor Boardman and Professor Wilson. To Professor Boardman, for his very careful reading of my thesis, improving the presentation of section 4, providing a geometric proof to Proposition 7.1, simplifing many proofs and pointing out some gaps. To Professor Wilson, for his constant encouragement and support as well as tremendously useful discussions during my studies at Johns Hopkins University. I also have to thank Prof. Wilson for his program in Maple, which is very instructive for extracting the main results of this thesis.

Secondly, thanks are due to Dr. Wood for raising the problem, giving me a copy of Suo Xiao's thesis and his other help. I have also to thank Prof. Franklin Peterson for his encouragement. Thanks also go to all support staff of the Department of Mathematics, for their kindness and assistance.

Finally, I would like to thank my wife, Qu Xiong, for all her love and support. It is her to whom this work is humbly dedicated.

Contents

Introduction

For a long time people have been interested in the hit problem of polynomial algebras by the action of the Steenrod algebra. The task is to find a minimal basis for the quotient of the polynomial algebra with the relation that $\mathrm{Sq}^i w = 0$ for any $i > 0$ and any polynomial w. Franklin Peterson has a very interesting conjecture, Reg Wood proved his conjecture in [4], later William Singer generalized the conjecture in [5].

All the above results can determine that certain elements in the polynomial algebra are 0 in the quotient, but it is unfeasible to determine a minimal basis of the quotient in this way. Kameko [2] fulfilled such a task for $W(3)$.

In [6] Reg Wood raised a problem of determining a minimal basis of the quotient of a given polynomial algebra by the action of the divided differential operator algebra.

In this paper we completely solve this problem for a polynomial algebra generated by 4 variables. And actually we get far more than the minimal basis; since we are also able to represent every element as a sum of basis elements, we are able to understand the action of the group S_4.

1 Main Results

Before we state our results, let's recall some facts about the divided differential operator algebra and some already known results. Notations $W(n)$ and $\bar{W}(n)$ will be used, and here are the definitions.

Definition 1.1. *$W(n)$ is the polynomial algebra generated by n variables $x_1, x_2, \dots, x_n$ over F_2, with x_i in degree 1 for i from 1 to n. We will use $W^+(n)$ to denote the ideal generated by $x_1 x_2 \dots x_n$.*

Definition 1.2. *$\bar{W}(n)$ is the quotient of $W(n)$ by the action of the divided differential operator algebra (see below). If a and b are elements of $W(n)$, $a \equiv b$ means that they have the same image in $\bar{W}(n)$.*

Recall [6] that the divided differential operator algebra over the integer ring Z on the polynomial ring $Z[x_1, x_2, \dots, x_n]$ is generated by the $D_k^{\vee r}/r!$ (this will be denoted by $D(k^r)$)

under wedge product. Here

$$D_k = \sum_{i=1}^{n} x_i^{k+1} \frac{\partial}{\partial x_i}.$$

and the wedge product is defined as

$$D_{k_1} \vee D_{k_2} \vee \ldots \vee D_{k_r} = \sum_{(i_1,\ldots,i_r)} x_{i_1}^{k_1+1} \ldots x_{i_r}^{k_r+1} \frac{\partial^r}{\partial x_{i_1} \ldots \partial x_{i_r}}.$$

The summation in the above is taken over all r-vectors.

Actually it is shown that the space generated by the $D_k^{\vee r}/r!$ under wedge product is the same as the space generated by the $D_k^{\vee r}/r!$ under composition.

By [6] Theorem 2.6, or originally from [3], the elements $D(1^{p^n})$ and $D(2^{p^n})$ generate the whole divided differential operator algebra $\mathfrak{D}$, here p ranges over all prime numbers.

When working mod 2, by lemma 2.2 of [6], we have

$$\mathrm{Sq}^r = D(1^r).$$

Since it is very easy to show $D(2^r)$ also satisfies the same Cartan formula as the Steenrod operation Sq^r, I will denote it by Sq_2^r.

Explicitly, we have

Proposition 1.1. *1.* $\mathrm{Sq}^r(x_i^m) = \binom{m}{r} x_i^{m+r}$.

2. $\mathrm{Sq}_2^r(x_i^m) = \binom{m}{r} x_i^{m+2r}$.

3. $\mathrm{Sq}^r(xy) = \sum_{a+b=r} \mathrm{Sq}^a(x)\mathrm{Sq}^b(y)$.

4. $\mathrm{Sq}_2^r(xy) = \sum_{a+b=r} \mathrm{Sq}_2^a(x)\mathrm{Sq}_2^b(y)$.

In the above, formula 3 and formula 4 are the Cartan formulae; all computations are over F_2.

Since the mod 2 divided differential operator algebra is generated by Sq^r and Sq_2^r with r nonnegative integers and the divided differential operators are additive, the above proposition determines the action of the mod 2 divided differential operator algebra on $W(n)$. For the same reason, it is very easy to notice the following proposition.

Proposition 1.2. *An element is hit by the mod 2 divided differential operator algebra if and only if it lies in the sum of the images of* Sq^{2^r} *for all* r ≥ 0 *and* Sq_2^r *for all* $r > 0$.

It is Suo Xiao [9] who first determined a basis for the quotient of $W(3)$, the polynomial algebra generated by 3 variables, acted on by the mod 2 divided differential operator algebra, though we have independently such a result. The result in our language is

Theorem 1.1. *The quotient of $W(3)$, the polynomial algebra over F_2 with 3 variables, by the action of the mod 2 divided differential operator algebra has*

- $(0,0,0)$ *in dimension* 0*;*
- $(0,0,1)$, $(0,1,0)$, $(1,0,0)$ *in dimension* 1*;*
- $(0,1,2)$, $(1,0,2)$, $(1,1,1)$, $(1,2,0)$ *in dimension* 3*;*
- $(1,2,3)$ *in dimension* 6*;*
- $(1,2^p-1,0)$, $(1,0,2^p-1)$, $(0,1,2^p-1)$, *in dimension* 2^p *for* $p \geq 1$*, also* $(1,1,2^p-2)$, $(1,2,2^p-3)$ *for* $p \geq 2$*;*
- $(1,2^p-1,1)$, $(1,1,2^p-1)$ *in dimension* 2^p+1 *for* $p \geq 2$*, also* $(1,3,2^p-3)$ *for* $p \geq 3$*;*

as an additive basis. Here (m,n,t) means the monomial $x_1^m x_2^n x_3^t$.

Xiao has also many results about the quotient of $W(4)$ by the mod 2 divided differential operator algebra. We may work in the ideal $W^+(4)$ since Theorem 1.1 takes care of other monomials. The following are Xiao's results:

Proposition 1.3. *A monomial (a,b,c,d) with a,b,c,d all positive and at least two of them even is hit except when* $a+b+c+d=2^k$ *for some k, or if the dimension is 6 or 10.*

Remark: It should be noticed that in Xiao's thesis, he did not exclude the dimensions 6 and 10, which is a mistake. We give a proof in section 2.

He stated the following conjecture 6.22 [9]:

Conjecture 1.1. *A monomial of the form* $(a,2^k-1,2^k+1,1)$ *is hit if it is not in dimension* 2^m+2^n *for some m, and for some n among the set* $\{0,1,k,k+1,-\infty\}$.

This would imply his conjecture 6.23:

Conjecture 1.2. *The non-hit elements in dimension* ≥ 8 *of* $W^+(4)$ *lie in odd dimensions* $2^m+1, 2^m+3$ *and in even dimensions* $2^m, 2^m+2^k$ *where* $m > k \geq 1$.

Remark: Actually, the condition dimension greater than or equal to 8 can be removed.

The first result of this paper is a proof of Xiao's conjecture, let's state it as:

Theorem 1.2. *All elements of* $W^+(4)$ *in dimensions other than* $2^m, 2^m+2^k (m > k \geq 0), 2^m+3$ *are hit.*

The second result is for dimension 2^n for $n \geq 4$.

Theorem 1.3. *In dimension* 2^n *with* $n \geq 4$,

- $(1,1,1,2^n-3)$,
- $(1,1,2,2^n-4)$,
- $(1,1,2^{n-1}-1,2^{n-1}-1)$,
- $(1,2,1,2^n-4)$,
- $(1,3,2^{n-1}-3,2^{n-1}-1)$,
- $(1,2^{n-1}-1,1,2^{n-1}-1)$

form a basis of the quotient of $W^+(4)$ *by the mod 2 divided differential operator algebra. Moreover, in terms of this basis,*

1. (a,b,c,d) *with* d *odd contains a term* $(1,1,1,2^n-3)$ *unless* a,b,c,d *are all odd and* $a+d=2^{n-1}$.
2. (a,b,c,d) *with* $a+c$ *odd contains a term* $(1,1,2,2^n-4)$.
3. (a,b,c,d) *with* a,b,c,d *all odd and* $a+c=2^{n-1}$ *contains a term* $(1,1,2^{n-1}-1,2^{n-1}-1)$.
4. (a,b,c,d) *with* $a+b$ *odd contains a term* $(1,2,1,2^n-4)$.
5. (a,b,c,d) *with* a,b,c,d *all odd and no two the same and the sum of two of them* 2^{n-1} *contains a term* $(1,3,2^{n-1}-3,2^{n-1}-1)$.
6. (a,b,c,d) *with* a,b,c,d *all odd and* $a+b=2^{n-1}$ *contains a term* $(1,2^{n-1}-1,1,2^{n-1}-1)$.

Monomials not listed here are 0.

For dimension 8, we have basis elements:$(1,1,1,5)$, $(1,1,2,4)$, $(1,1,3,3)$, $(1,2,1,4)$, $(1,2,3,2)$, $(1,3,1,3)$. *In terms of basis elements, we have*

1. (a,b,c,d) *with* d *odd contains a term* $(1,1,1,5)$ *unless* a,b,c,d *are all odd and* $a+d=4$.
2. (a,b,c,d) *with* $a+c$ *odd contains a term* $(1,1,2,4)$.
3. (a,b,c,d) *with* a,b,c,d *all odd and* $a+c=4$ *contains a term* $(1,1,3,3)$.
4. (a,b,c,d) *contains a term* $(1,2,1,4)$ *if* $c=1$ *and* (a,b,d) *is any permutation of* $(1,2,4)$, *or if* $c=2$ *and* (a,b,d) *is any permutation of* $(1,2,3)$.
5. (a,b,c,d) *contains a term* $(1,2,3,2)$ *if* $d=1$ *and* (a,b,c) *is any permutation of* $(1,2,4)$, *or if* $d=2$ *and* (a,b,c) *is any permutation of* $(1,2,3)$.
6. (a,b,c,d) *with* a,b,c,d *all odd and* $a+b=4$ *contains a term* $(1,3,1,3)$.

Monomials not listed here are 0.

Dimension 4 has only $(1,1,1,1)$ *trivially.*

The third result is about dimension 2^n+1.

Theorem 1.4. *In dimension* 2^n+1 *with* $n \geq 3$,

- $(1,1,1,2^n-2)$,
- $(1,1,2,2^n-3)$,
- $(1,1,3,2^n-4)$,
- $(1,1,2^n-2,1)$,
- $(1,2,1,2^n-3)$,
- $(1,2,3,2^n-5)$,
- $(1,2,2^n-3,1)$,
- $(1,3,1,2^n-4)$

form a basis of the quotient of $W^+(4)$ *by the divided differential operator algebra. Moreover, in terms of this basis,*

1. (a,b,c,d) *with* $b>1$ *odd and* $a>1$ *and* $c=1$*; or with* $b>1$ *odd and* $c>1$ *and* $a=1$*; or with* $a>1$ *odd and* $c>1$ *and* $b=1$*; or with* a *even and both* b *and* c *equal to 1; or with all* a,b,c *being 1's contains a term* $(1,1,1,2^n-2)$.
2. (a,b,c,d) *with* $b=1$ *and* $d>1$ *odd; or with* $d=1$ *and* $b>1$ *odd contains a term* $(1,1,2,2^n-3)$.
3. (a,b,c,d) *with* $(a,b)=(1,odd)$*, or with* $(b,d)=(1,odd)$*, or with* $(c,b)=(1,odd)$ *contains a term* $(1,1,3,2^n-4)$ *unless* $(a,b,c)=(1,1,even)$ *or* $(a,b,c)=(even,1,1)$*, or* $(a,b,c)=(1,odd,1)$.
4. (a,b,c,d) *with* $(b,d)=(odd,1)$ *contains a term* $(1,1,2^n-2,1)$.
5. (a,b,c,d) *with* $(c,d)=(1,odd)$ *contains a term* $(1,2,1,2^n-3)$.
6. (a,b,c,d) *with* $(c,d)=(1,odd)$*; or with* $(c,d)=(odd,1)$*; or with* $(a,d)=(1,odd)$*; or with* $(b,d)=(1,odd)$ *contains a term* $(1,2,3,2^n-5)$ *unless* $(a,b,c,d)=(1,1,even,odd)$ *or* $(1,even,1,odd>1)$ *or* $(1,even,odd>1,1)$ *or* $(a>1,b>1,1,1)$ *or* $(even,1,odd>1,1)$ *or* $(even,1,1,odd>1)$.
7. (a,b,c,d) *with* $(c,d)=(odd,1)$ *contains a term* $(1,2,2^n-3,1)$.
8. (a,b,c,d) *with* $(a,b)=(1,odd)$ *and* $b>1$*; or with* $(b,a)=(1,odd)$ *and* $a>1$ *contains a term* $(1,3,1,2^n-4)$.

Monomials not listed here are all 0 in the quotient.

Dimension 5 has trivially $(1,1,1,2)$,$(1,1,2,1)$,$(1,2,1,1)$ *as a basis.*

The fourth result is about dimension 2^n+2.

Theorem 1.5. *In dimension* 2^n+2 *with* $n\geq 4$*,*

- $(1,1,1,2^n-1)$,
- $(1,1,3,2^n-3)$,

- $(1,1,2^n-1,1)$,
- $(1,3,1,2^n-3)$,
- $(1,3,2^n-3,1)$,
- $(1,2^n-1,1,1)$

form a basis of the quotient of $W^+(4)$ *by the divided differential operator algebra. Moreover, in terms of this basis,*

1. (a,b,c,d) *with* $(a,b,c)=(odd,1,1)$ *contains* $(1,1,1,2^n-1)$.
2. $(1,1,odd>1,d>1)$ *and* $(odd>1,1,1,d>1)$ *and* $(odd>1,1,c>1,1)$ *contain a term* $(1,1,3,2^n-3)$.
3. $(odd,1,odd,1)$ *contains a term* $(1,1,2^n-1,1)$.
4. $(1,odd>1,1,odd>1)$ *and* $(odd>1,1,1,odd>1)$ *and* $(odd>1,odd>1,1,1)$ *contain a term* $(1,3,1,2^n-3)$.
5. $(1,odd>1,odd>1,1)$ *and* $(odd>1,1,odd>1,1)$ *and* $(odd>1,odd>1,1,1)$ *contain a term* $(1,3,2^n-3,1)$.
6. $(odd,odd,1,1)$ *contains a term* $(1,2^n-1,1,1)$.

Monomials not listed here are 0 in the quotient.

For dimension 10, there is one more generator $(1,2,3,4)$*; all permutations of* $(1,2,3,4)$ *are equivalent to this monomial. The other conditions above are not changed.*

Dimension 6 has basis elements $(1,1,1,3)$,$(1,1,2,2)$,$(1,1,3,1)$,$(1,2,1,2)$,$(1,3,1,1)$.

The fifth result is about dimension 2^n+3.

Theorem 1.6. *In dimension* 2^n+3 *with* $n\geq 3$,

- $(1,1,2,2^n-1)$,
- $(1,1,2^n-1,2)$,
- $(1,2,1,2^n-1)$,

- $(1, 2, 3, 2^n - 3)$,
- $(1, 2, 2^n - 1, 1)$,
- $(1, 2^n - 1, 1, 2)$

form a basis of the quotient of $W^+(4)$ *by the divided differential operator algebra. Moreover, in terms of this basis, where* a, b, c, d *are all odd except one of them is 2,*

1. (a, b, c, d) *with* $a + c = 3$ *contains a term* $(1, 1, 2, 2^n - 1)$.
2. (a, b, c, d) *with* $a + d = 3$ *and* $c \neq a$; *or* $c + d = 3$ *and* $c \neq a$ *contains a term* $(1, 1, 2^n - 1, 2)$.
3. (a, b, c, d) *with* $a + c = 3$ *and* $b \neq a$; *or with* $b + c = 3$ *and* $b \neq a$ *contains a term* $(1, 2, 1, 2^n - 1)$.
4. (a, b, c, d) *with sum of two of them* 3 *and no two terms the same contains a term* $(1, 2, 3, 2^n - 3)$.
5. (a, b, c, d) *with* $a + d = 3$ *and* $a \neq b$ *and* $a \neq c$; *or* $b + d = 3$ *and* $b \neq a$ *and* $b \neq c$; *or* $c + d = 3$ *and* $c \neq a$ *and* $c \neq b$ *contains a term* $(1, 2, 2^n - 1, 1)$.
6. (a, b, c, d) *with* $c + d = 3$ *contains a term* $(1, 2^n - 1, 1, 2)$.

Those monomials not listed in the above are 0 in the quotient.

Dimension 7 has basis elements $(1, 1, 1, 4)$, $(1, 1, 2, 3)$, $(1, 1, 3, 2)$, $(1, 2, 1, 3)$, $(1, 2, 3, 1)$, $(1, 3, 1, 2)$.

The sixth result is about dimension $2^n + 4$.

Theorem 1.7. *In dimension* $2^n + 4$ *with* $n \geq 4$,

- $(1, 1, 3, 2^n - 1)$,
- $(1, 1, 2^n - 1, 3)$,
- $(1, 3, 1, 2^n - 1)$,
- $(1, 3, 5, 2^n - 5)$,

- $(1, 3, 2^n - 3, 3)$,
- $(1, 2^n - 1, 1, 3)$

form a basis of the quotient of $W^+(4)$ *by the divided differential operator algebra. Moreover, in terms of this basis, where* a, b, c, d *are all odd,*

1. (a, b, c, d) *with* $a + c = 4$ *contains a term* $(1, 1, 3, 2^n - 1)$.
2. (a, b, c, d) *with* $b + d = 4$ *contains a term* $(1, 1, 2^n - 1, 3)$.
3. (a, b, c, d) *with* $a + c = 4$ *and* $b \neq a$*; or with* $b + c = 4$ *and* $b \neq a$ *contains a term* $(1, 3, 1, 2^n - 1)$.
4. (a, b, c, d) *with no two of them the same and sum of two of them 4 contains a term* $(1, 3, 5, 2^n - 5)$.
5. (a, b, c, d) *with* $a + d = 4$ *and* $a \neq b$ *and* $a \neq c$*; or* $b + d = 4$ *and* $b \neq a$ *and* $b \neq c$*; or* $c + d = 4$ *and* $c \neq a$ *and* $c \neq b$ *contains a term* $(1, 3, 2^n - 3, 3)$.
6. (a, b, c, d) *with* $c + d = 4$ *contains a term* $(1, 2^n - 1, 1, 3)$.

All monomials in this dimension not listed above are 0 in the quotient.

For dimension 12*, the basis elements in* 4*) and* 5*) are the same* $(1, 3, 5, 3)$*; the elements containing* $(1, 3, 5, 3)$ *are* (a, b, c, d) *with* a, b, c *different from each other.*

The seventh result is about dimension $2^p + 2^q$ with $p > q > 2$.

Theorem 1.8. *In dimension* $2^p + 2^q$ *with* $p > q > 2$,

- $(1, 1, 2^q - 1, 2^p - 1)$,
- $(1, 1, 2^p - 1, 2^q - 1)$,
- $(1, 3, 2^q - 3, 2^p - 1)$,
- $(1, 3, 2^p - 3, 2^q - 1)$,
- $(1, 2^q - 1, 1, 2^p - 1)$,
- $(1, 2^p - 1, 1, 2^q - 1)$

form a basis of the quotient of $W^+(4)$ *by the divided differential operator algebra. Moreover, in terms of this basis, where* a, b, c, d *are all odd,*

1. (a, b, c, d) *with* $a + c = 2^q$ *contains a term* $(1, 1, 2^q - 1, 2^p - 1)$.
2. (a, b, c, d) *with* $b + d = 2^q$ *contains a term* $(1, 1, 2^p - 1, 2^q - 1)$.
3. (a, b, c, d) *with* $a + c = 2^q$ *and* $b \neq a$ *and* $b \neq c$*; or with* $b + c = 2^q$ *and* $a \neq b$ *and* $a \neq c$*; or with* $a + b = 2^q$ *and* $c \neq a$ *and* $c \neq b$ *contains a term* $(1, 3, 2^q - 3, 2^p - 1)$.
4. (a, b, c, d) *with* $a + d = 2^q$ *and* $a \neq b$ *and* $a \neq c$*; or* $b + d = 2^q$ *and* $b \neq a$ *and* $b \neq c$*; or* $c + d = 2^q$ *and* $c \neq a$ *and* $c \neq b$ *contain a term* $(1, 3, 2^p - 3, 2^q - 1)$.
5. (a, b, c, d) *with* $a + b = 2^q$ *contain a term* $(1, 2^q - 1, 1, 2^p - 1)$.
6. (a, b, c, d) *with* $c + d = 2^q$ *contain a term* $1, 2^p - 1, 1, 2^q - 1)$.

All monomials of this dimension not listed above are 0 in the quotient.

2 Some preliminary results.

Lemma 2.1.

$$(\mathrm{Sq}^{2^i}(a), b, c, d) \equiv (a, \mathrm{Sq}^{2^i}(b, c, d)).$$

Proof By the well known trick that $(\chi(\mathrm{Sq}^{2^i})x)y \equiv x\mathrm{Sq}^{2^i}y$, we only have to show $\chi(\mathrm{Sq}^{2^i})$ has the same effect as Sq^{2^i} on a monomial with only one variable. By the well known formula (see Proposition 7.1)

$$(\chi\mathrm{Sq}^j)x^n = \binom{n+2j}{j}x^{n+j},$$

since $\binom{n+2^{i+1}}{2^i} \equiv \binom{n}{2^i}$ mod 2 and $\mathrm{Sq}^{2^i}x^n = \binom{n}{2^i}x^{n+2^i}$, we are done.

Lemma 2.2. *Assume* $(a_1, a_2, a_3, a_4) \equiv (b_1, b_2, b_3, b_4)$, *where*

- *(a) Only the operations* Sq^j *and* Sq_2^j *with* $j < 2^n$ *are used; or*
- *(b) The dimension is at most* 2^{n+1}*; or*
- *(c) The dimension is* $2^{n+1}+1$ *or* $2^{n+1}+2$ *and greater than* 10.

Then for any k_1, k_2, k_3, $k_4 \geq 0$,

$$(a_1 + k_1 2^n, a_2 + k_2 2^n, a_3 + k_3 2^n, a_4 + k_4 2^n) \equiv (b_1 + k_1 2^n, b_2 + k_2 2^n, b_3 + k_3 2^n, b_4 + k_4 2^n)$$

Similarly, under the same conditions, if (a_1, a_2, a_3, a_4) *is hit, so is* $(a_1 + k_1 2^n, a_2 + k_2 2^n, a_3 + k_3 2^n, a_4 + k_4 2^n)$.

Proof Suppose

$$\sum \mathrm{Sq}^i(u, v, w, x) + \sum \mathrm{Sq}_2^j(m, t, o, p) = (a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4).$$

We only have to prove $\mathrm{Sq}^i(u, v, w, x) \cdot (k_1 2^n, k_2 2^n, k_3 2^n, k_4 2^n)$ and $\mathrm{Sq}_2^j(m, t, o, p) \cdot (k_1 2^n, k_2 2^n, k_3 2^n, k_4 2^n)$ are hit; the latter is obviously hit since we must have $j < 2^n$ and

$$\mathrm{Sq}_2^j((m, t, o, p) \cdot (k_1 2^n, k_2 2^n, k_3 2^n, k_4 2^n)) = \mathrm{Sq}_2^j(m, t, o, p) \cdot (k_1 2^n, k_2 2^n, k_3 2^n, k_4 2^n).$$

To see the former is hit, just notice that

$$\mathrm{Sq}^i((u,v,w,x)\cdot(k_1 2^n, k_2 2^n, k_3 2^n, k_4 2^n)) = \mathrm{Sq}^i(u,v,w,x)\cdot(k_1 2^n, k_2 2^n, k_3 2^n, k_4 2^n)$$

if $i < 2^n$. If $i = 2^n$, we have three cases.

Firstly, if the dimension is 2^{n+1}, then $\mathrm{Sq}^{2^n}(u,v,w,x) = (2u,2v,2w,2x)$ and $\mathrm{Sq}^i(u,v,w,x)\cdot(k_1 2^n, k_2 2^n, k_3 2^n, k_4 2^n)$ has 4 even components; but a monomial $(2a,2b,2c,2d)$ is hit since $\mathrm{Sq}^1(2a-1,2b,2c,2d) = (2a,2b,2c,2d)$. Secondly, if the dimension is $2^{n+1}+1$, every term of the expansion of $\mathrm{Sq}^{2^n}(u,v,w,x)$ with $u+v+w+x = 2^n+1$, must have at least 3 even numbers, so Lemma 2.4 applies. Thirdly, if the dimension is $2^{n+1}+2$, every term of the expansion of $\mathrm{Sq}^{2^n}(u,v,w,x)$ with $u+v+w+x = 2^n+2$, must have at least 2 even numbers, so Lemma 2.5 applies. Thus we have the Lemma.

This lemma will be repeatedly used to prove inductively the theorems of this paper.

Lemma 2.3. *Any (a,b,c,d) with a,b,c,d all positive is equivalent to a sum of (a_i,b_i,c_i,d_i) with (a_i,b_i,c_i) in the basis of Theorem 1.1.*

Proof: Write $(a,b,c) = \sum_i \theta_i(a_i,b_i,c_i)$, with each (a_i,b_i,c_i) as in Theorem 1.1 (where θ_i could be the identity operation). Then

$$(a,b,c,d) = \sum_i(\theta_i(a_i,b_i,c_i),d) \equiv \sum_i(a_i,b_i,c_i,\chi\theta(d)).$$

Lemma 2.4. *(a,b,c,d) with at least three of them even and a,b,c,d all positive is hit if $a+b+c+d > 7$.*

Proof This lemma can be found in [9]. If a,b,c,d are all even, then $(a,b,c,d) = \mathrm{Sq}^1(a-1,b,c,d)$. Otherwise, we can suppose a is odd and others are even. If $a > 1$, then $(a,b,c,d) = \mathrm{Sq}^1_2(a-2,b,c,d)$. If $a = 1$ then one of b,c,d is greater than 2; without loss of generality, suppose $b > 2$. We have $(a,b,c,d) \equiv (a+1,b-1,c,d)$ by expanding $\mathrm{Sq}^1(a,b-1,c,d)$. Now $(b-1,a+1,c,d)$ is hit since $b-1$ is odd and $b-1 > 1$, and the other three are even; so by permutation $(a+1,b-1,c,d)$ is hit, so (a,b,c,d) is hit.

Lemma 2.5. *(a,b,c,d) with a,b,c,d all positive and two of them even, two of them odd is hit if it is not in dimension 6 or 10 or 2^n for any n.*

Proof Again this can be found in [9]. The proof is our method.

For dimension no greater than 15, this has been proved by direct computation of our program; we only consider dimension greater than 15 in the following proof.

We may assume d even. In the proof of Lemma 2.3, $\chi\theta_i(d)$ has even degree whenever it is nonzero. Then (a_i, b_i, c_i) also has even degree, and must be one of $(1,1,2^k-2)$,$(1,2,2^k-3)$,$(1,2,3)$. So we only need to prove the following proposition:

Proposition 2.1. *In dimension other than 6, 10 and 2^n,with s even:*

1. $(1,2,3,s) \equiv 0$
2. $(1,1,2^k-2,s) \equiv 0$
3. $(1,2,2^k-3,s) \equiv 0.$

Part (1) holds for $s < 14$ by direct computation. Otherwise, suppose $s = 2^m + u$, with $0 \leq u < 2^m$.

If $u > 0$ and $u \neq 4$ and $u \neq 2^k - 6$, we conclude $(1,2,3,s) \equiv 0$ using Lemma 2.2 from $(1,2,3,u) \equiv 0$.

If $0 \leq u < 2^{m-1}$, we have $m \geq 4$, and by Lemma 2.1

$$\begin{aligned}(1,2,3,2^m+u) &= (1,2,3,\mathrm{Sq}^{2^{m-1}}(2^{m-1}+u)) \\ &\equiv (\mathrm{Sq}^{2^{m-1}}(1,2,3),2^{m-1}+u) = 0.\end{aligned}$$

Note that if $u = 2^k - 6$ and $u \geq 2^{m-1}$, we must have $k = m$. This makes the dimension 2^{m+1}, which is excluded.

This proves part (1); to prove parts (2) and (3), let's first prove the following proposition:

Proposition 2.2. *For $k \geq 3$,*

1. $(1,1,2^k-2,2^{k-1}) \equiv 0$
2. $(1,2,2^k-3,2^{k-1}) \equiv 0.$

Proof Using Lemma 2.1,

$$\begin{aligned}0 = (\mathrm{Sq}^{2^{k-2}}(1),1,2^k-2,2^{k-2}) &\equiv (1,\mathrm{Sq}^{2^{k-2}}(1,2^k-2,2^{k-2})) \\ &= (1,1,2^k+2^{k-2}-2,2^{k-2}) + (1,1,2^k-2,2^{k-1})\end{aligned}$$

for $k \geq 3$ and

$$\begin{aligned} 0 = (\mathrm{Sq}^{2^{k-1}}(1), 1, 2^{k-1} + 2^{k-2} - 2, 2^{k-2}) &\equiv (1, \mathrm{Sq}^{2^{k-1}}(1, 2^{k-1} + 2^{k-2} - 2, 2^{k-2})) \\ &= (1, 1, 2^k + 2^{k-2} - 2, 2^{k-2}). \end{aligned}$$

These give us the first result.

Similarly we have

$$\begin{aligned} 0 = (\mathrm{Sq}^{2^{k-2}}(2), 1, 2^k - 3, 2^{k-2}) &\equiv (2, \mathrm{Sq}^{2^{k-2}}(1, 2^k - 3, 2^{k-2})) \\ &= (2, 1, 2^k + 2^{k-2} - 3, 2^{k-2}) + (2, 1, 2^k - 3, 2^{k-1})) \end{aligned}$$

for $k \geq 4$ and

$$\begin{aligned} 0 = (\mathrm{Sq}^{2^{k-1}}(2), 1, 2^{k-1} + 2^{k-2} - 3, 2^{k-2}) &\equiv (2, \mathrm{Sq}^{2^{k-1}}(1, 2^{k-1} + 2^{k-2} - 3, 2^{k-2})) \\ &= (2, 1, 2^k + 2^{k-2} - 3, 2^{k-2}). \end{aligned}$$

These give us the second result. For $k = 3$, both results can be shown by direct computation.

Now we can prove part (2) and part (3) of Proposition 2.1 as part (1).

For part (2), suppose $s = 2^m + u$, with $0 \leq u < 2^m$.

If $k > m + 1$, where $m \geq 2$, $(1, 1, 2^k - 2, 2^m + u) \equiv 0$ follows by Lemma 2.2 from $(1, 1, 2^{m+1} - 2, 2^m + u) \equiv 0$, which is the case $k = m + 1$. if $u > 0$, the latter follows from $(1, 1, 2^m - 2, u) \equiv 0$ by Lemma 2.2 and induction, unless $m = u = 2$, in which case $(1, 1, 6, 6) \equiv 0$ by direct computation. If $u = 0$, it is Proposition 2.2. If $m = 1$, we must have $u = 0$, and the same method applies, except that induction starts at $k = 3$, where $(1, 1, 6, 2) \equiv 0$ by direct computation.

If $k \leq m$ and $u > 0$ and $u \neq 2^t - 2^k$, $(1, 1, 2^k - 2, 2^m + u) \equiv 0$ follows from $(1, 1, 2^k - 2, u) \equiv 0$, which is true by induction unless $k = u = 2$. If $k = u = 2$, we compute $(1, 1, 2, 2^m + 2) \equiv 0$ for $m = 2, 3$, and deduce that case $m \geq 4$ from the case $m = 3$ by Lemma 2.2.

Note that if $u = 0$, the dimension is $2^k + 2^m$ and we must have $k < m$. Also if $u = 2^t - 2^k$, the dimension is $2^m + 2^t$ and we must have $k < t < m$. So if $u = 0$ or $u = 2^t - 2^k$, we have by Lemma 2.1

$$\begin{aligned} (1, 1, 2^k - 2, 2^m + u) &= (1, 1, 2^k - 2, \mathrm{Sq}^{2^{m-1}}(2^{m-1} + u)) \\ &\equiv (\mathrm{Sq}^{2^{m-1}}(1, 1, 2^k - 2), 2^{m-1} + u). \end{aligned}$$

This is zero if $k \leq m-2$, and has all entries even if $k = m-1$.

Part (3) is entirely similar.

All the above shows that an element with at least two even entries is hit if it is not in dimension 2^n for some n or 6 or 10.

Lemma 2.6. $\binom{2^n-2r}{r} = 0$ *if* $r > 0$.

Proof If r is odd, this is 0 obviously; if $r = 2s$, then it equals $\binom{2^{n-1}-2s}{s}$; by induction this is 0.

Lemma 2.7. $\binom{2^n-1-r}{r} = 0$ *if* $r > 0$.

Proof Since $2^n - 1 - r$ and r have no common digits in the dyadic expansions, the result follows.

3 Proof of theorem 1.2

Lemma 3.1. *Elements in dimensions* $8n+5, 8n+6, 8n+7$ *for positive* n *are all hit.*

Proof This follows from the computation that all elements in dimension 13,14,15 are hit. An element of the form $(1, t, a, b)$ with $t \leq 3$ in these dimensions can be written as $(1, t, 8x+k, 8y+l)$ with $1 \leq k, l \leq 8$. So dimension of $(1, t, k, l)$ is ≤ 20, so it must be 13, or 14, or 15 or 5,6,7. If the dimension is $5, 6, 7$, we use $(1, t, k+8, l)$ or $(1, t, k, l+8)$ instead. Therefore by lemma 2.2, $(1, t, a, b)$ is hit. Similarly we can show $(1, t, a, b)$ with $a \leq 3$ is hit. But by Lemma 2.3 every element is a sum of elements $(1, t, a, b)$ with $t \leq 3$ or $a \leq 3$ in the quotient, hence the lemma.

Lemma 3.2. *All elements in dimensions* $2^{p+1} + 2^p + 1$*,* $2^{p+1} + 2^p + 2$*,* $2^{p+1} + 2^p + 3$*,* $2^{p+1} + 2^p + 4$ *are hit for* $p \geq 3$*.*

Lemma 3.3. *All elements in dimension* $2^p + 2^q + 2^r$ *with* $p > q > r \geq 3$ *are hit.*

We may freely permute the entries in any monomial here. By Lemma 2.3, we need only consider elements of the form $(1, t, a, b)$ with $1 \leq t \leq 3$. Further, Lemma 2.5 allows us to ignore all monomials with two or more even entries.

Proof of theorem 1.2

Assuming the above lemmas, suppose an element is in dimension $k2^{p+1} + 2^p + m$, with m among 1 to 4, $k \geq 1$, $p \geq 3$. If the element is of form $(1, t, a, b)$ with t among 1 to 3, we can find appropriate $x \geq 0, y \geq 0$ such that $(1, t, a - x2^{p+1}, b - y2^{p+1})$ is in dimension $2^{p+1}+2^p+m$. This is possible because if x, y are the greatest numbers that $a-x2^{p+1}, b-y2^{p+1}$ are still positive, then $(1, t, a - x2^{p+1}, b - y2^{p+1})$ is in dimension $\leq 2^{p+2} + 4$. So it must be in dimension $2^{p+1} + 2^p + m$ or $2^p + m$; if it is the second case, we just put back a 2^{p+1}, i.e. decrease x or y by 1 so as to have dimension $2^{p+1} + 2^p + m$. Now we can use lemma 3.2 and 2.2 to conclude that $(1, t, a, b)$ is hit.

Similarly we can prove elements in dimension $k2^p + 2^q + 2^r$ are hit for $p > q > r \geq 3$ if $k \geq 1$. Again we consider $(1, t, a, b)$; we can find $(1, t, a - x2^p, b - y2^p)$ in dimension $2^p + 2^q + 2^r$, and apply Lemma 2.2.

Consider monomials in dimension $8n + m$, with $0 \leq m \leq 7$.

Case $m = 5, 6, 7$ and $n \geq 1$: by lemma 3.1 they are hit.

Case $m = 1, 2, 3, 4$ and $\alpha(n) \geq 2$: write $8n = k2^{p+1} + 2^p$, $k \geq 1$, $p \geq 3$, this reduces to Lemma 3.2. Here and below we use $\alpha(n)$ to denote the number of 1's in the dyadic expansion of n.

Case $m = 0$, $\alpha(n) \geq 3$: write $8n = k2^p + 2^q + 2^r$, $p > q > r \geq 3$, this reduces to Lemma 3.3.

Since in Theorem 1.2 we only consider monomials in the above 3 cases, if we prove all the lemmas, then we are done.

Proof of Lemma 3.3 We show that if the result holds in dimension $2^p + 2^q + 2^r$, it holds in dimension $2^{p+1} + 2^q + 2^r$. After permutations, it is enough to consider elements of the form $(1, t, a, b)$ in dimension $2^{p+1} + 2^q + 2^r$ with $1 + t \leq 4$, so one of a, b must be greater than 2^p. Say $a > 2^p$, then $(1, t, a - 2^p, b)$ is hit, so by Lemma 2.2 $(1, t, a, b)$ is hit. This shows Lemma 3.3 is equivalent to the following lemma.

Lemma 3.4. *All elements in dimension* $2^{q+1} + 2^q + 2^r$ *with* $q > r \geq 2$ *are hit.*

Proof Let's consider elements of the form $(1, 1, 2^s - 1, 2^{q+1} + 2^q + 2^r - 2^s - 1)$ and $(1, 3, 2^s - 3, 2^{q+1} + 2^q + 2^r - 2^s - 1)$. By Lemma 2.5, we may ignore monomials with two or more even entries.

If $r \leq s \leq q$, then

$$0 \equiv (\mathrm{Sq}^{2^q}(1, 1, 2^s - 1), 2^{q+1} + 2^r - 2^s - 1) \equiv (1, 1, 2^s - 1, \mathrm{Sq}^{2^q}(2^{q+1} + 2^r - 2^s - 1))$$

by Lemma 2.1, so $(1, 1, 2^s - 1, 2^{q+1} + 2^q + 2^r - 2^s - 1)$ is hit; similarly $(1, 3, 2^s - 3, 2^{q+1} + 2^q + 2^r - 2^s - 1)$ is hit.

If $s < r$, we have

$$(1, 1, 2^s - 1, \mathrm{Sq}^{2^r}(2^{q+1} + 2^q - 2^s - 1)) \equiv (\mathrm{Sq}^{2^r}(1, 1, 2^s - 1), 2^{q+1} + 2^q - 2^s - 1) = 0.$$

So $(1, 1, 2^s - 1, 2^{q+1} + 2^q + 2^r - 2^s - 1)$ is hit; similarly $(1, 3, 2^s - 3, 2^{q+1} + 2^q + 2^r - 2^s - 1)$ is hit.

If $s = q + 1$, then we have $(1, 1, 2^{q+1} - 1, 2^q + 2^r - 1)$ and $(1, 3, 2^{q+1} - 3, 2^q + 2^r - 1)$. They are equivalent to $(1, 1, 2^{q+1} + 2^r - 1, 2^q - 1)$ and $(1, 3, 2^{q+1} + 2^r - 3, 2^q - 1)$ respectively by Lemma 2.1 using $(\mathrm{Sq}^{2^r}(1, 1, 2^{q+1} - 1), 2^q - 1) \equiv (1, 1, 2^{q+1} - 1, \mathrm{Sq}^{2^r}(2^q - 1))$ etc. Then

$$\begin{aligned} (1, 1, 2^{q+1} + 2^r - 1, 2^q - 1) &\equiv (\mathrm{Sq}^{2^q}(1, 1, 2^q + 2^r - 1), 2^q - 1) \\ &\equiv (1, 1, 2^q + 2^r - 1, \mathrm{Sq}^{2^q}(2^q - 1)) = 0 \end{aligned}$$

and similarly for $(1,3,2^{q+1}+2^r-3,2^q-1)$.

This finishes the proof of Lemma 3.4, thus that of Lemma 3.3.

Proof of Lemma 3.2

We deal with dimensions $2^{p+1}+2^p+1,2,3,4$ separately, here $p \geq 3$.

Proof of dimension $2^{p+1}+2^p+4$ with $p \geq 3$.

This is Lemma 3.4 with $r=2$.

Proof of dimension $2^{p+1}+2^p+2$ with $p \geq 3$.

We only have to show $(1,1,2^k-1,2^{p+1}+2^p-2^k+1)$ and $(1,3,2^k-3,2^{p+1}+2^p-2^k+1)$ are hit.

If $k \leq p$,

$$(1,1,2^k-1,\mathrm{Sq}^{2^p}(2^{p+1}-2^k+1)) \equiv (\mathrm{Sq}^{2^p}(1,1,2^k-1),2^{p+1}-2^k+1) \equiv 0.$$

This shows that $(1,1,2^k-1,2^{p+1}+2^p-2^k+1)$ is hit. Similarly $(1,3,2^k-3,2^{p+1}+2^p-2^k+1)$ is hit.

Now suppose $k=p+1$. We have $(1,1,2^{p+1}-1,2^p+1)$ and $(1,3,2^{p+1}-3,2^p+1)$. The former is equivalent to $(1,1,2^{p+1}+2^{p-1}-1,2^{p-1}+1)$ by lemma 2.1 applied to $(1,1,2^{p+1}-1,2^{p-1}+1)$. Then

$$\begin{aligned}(1,1,2^{p+1}+2^{p-1}-1,2^{p-1}+1) &\equiv (\mathrm{Sq}^{2^p}(1,1,2^p+2^{p-1}-1),2^{p-1}+1)\\ &\equiv (1,1,2^p+2^{p-1}-1,\mathrm{Sq}^{2^p}(2^{p-1}+1))=0\end{aligned}$$

and similarly for $(1,3,2^{p+1}-3,2^p+1)$.

Proof of dimension $2^{p+1}+2^p+3$ with $p \geq 3$.

This time we have to consider

$$\begin{gathered}(1,2,3,2^{p+1}+2^p-3)\\ (1,1,2^k-1,2^{p+1}+2^p-2^k+2)\\ (1,3,2^k-3,2^{p+1}+2^p-2^k+2)\\ (1,1,2^k-2,2^{p+1}+2^p-2^k+3)\\ (1,2,2^k-3,2^{p+1}+2^p-2^k+3)\end{gathered}$$

First,

$$(1,2,3,\mathrm{Sq}^{2^p}(2^{p+1}-3)) \equiv (\mathrm{Sq}^{2^p}(1,2,3),2^{p+1}-3)=0,$$

so $(1,2,3,2^{p+1}+2^p-3)$ is hit.

If $k=1$, $(1,1,1,2^{p+1}+2^p)$ is obviously hit by $\mathrm{Sq}^{2^{p-1}}$.

If $2 \leq k \leq p$,

$$0 \equiv (\mathrm{Sq}^{2^p}(1,1,2^k-1),2^{p+1}-2^k+2) \equiv (1,1,2^k-1,\mathrm{Sq}^{2^p}(2^{p+1}-2^k+2)),$$

so $(1,1,2^k-1,2^{p+1}+2^p-2^k+2)$ is hit. Similarly other cases follow.

Suppose $k=p+1$. We have by Lemma 2.1 twice

$$\begin{aligned}(1,1,2^{p+1}-1,2^p+2) &\equiv (1,1,2^{p+1}+2^{p-1}-1,2^{p-1}+2)\\ &\equiv \mathrm{Sq}^{2^p}(1,1,2^p+2^{p-1}-1),2^{p-1}+2)\\ &\equiv (1,1,2^p+2^{p-1}-1,\mathrm{Sq}^{2^p}(2^{p-1}+2))=0\end{aligned}$$

Proof of dimension $2^{p+1}+2^p+1$ with $p \geq 3$.

This time we have to consider

$$\begin{gathered}(1,2,3,2^{p+1}+2^p-5)\\ (1,1,2^k-1,2^{p+1}+2^p-2^k)\\ (1,3,2^k-3,2^{p+1}+2^p-2^k)\\ (1,1,2^k-2,2^{p+1}+2^p-2^k+1)\\ (1,2,2^k-3,2^{p+1}+2^p-2^k+1)\end{gathered}$$

The proof that they are hit is same as that of dimension $2^{p+1}+2^p+3$, except when $k=1$, where we get

$$(1,1,1,2^{p+1}+2^p-2) \equiv (\mathrm{Sq}^{2^p}(1,1,1),2^{p+1}-2)=0.$$

4 Linear functionals

To find a lower bound for the rank of the quotient in dimension q, we construct linear functionals $W(4)^q \to F_2$ that map all relations to 0. They are really homology classes. The symmetric group S_4 acts on these in the obvious way. If we find k linearly independent such functionals, the rank of the quotient must be at least k.

To specify a linear functional, we pick a set M of monomials in dimension q and take its characteristic function χ_M, which maps M to 1 and all other monomials to 0. To verify the condition, we take any integer $r > 0$ and monomial (x, y, z, t) in dimension $q - r$, and expand

$$\mathrm{Sq}^r(x, y, z, t) = \sum (a, b, c, d).$$

We have to show that the number of monomials (a, b, c, d) that lie in M is even. We have $\mathrm{Sq}_2^r(x, y, z, t)$ similarly, except that (x, y, z, t) lies in dimension $q - 2r$; this case is simpler, because a, b, c, d always have the same parity as x, y, z, t.

Lemma 4.1.

$$\sum_{i+j=k} \binom{x}{i}\binom{y}{j} = \binom{x+y}{k}.$$

Proof: This is the coefficient of u^k in $(1+u)^x(1+u)^y = (1+u)^{x+y}$.

4.1 Dimension 2^n

Case 1: Take $M=$ all monomials (a, b, c, d) with d odd.

There are no terms if t is even, so assume t is odd, $t = 2T + 1$. The number of terms in M is

$$\sum \binom{x}{i}\binom{y}{j}\binom{z}{k}\binom{t}{2L} = \sum_L \binom{x+y+z}{r-2L}\binom{2T+1}{2L} = \sum_L \binom{2^n - 2T - 1 - r}{r - 2L}\binom{2T+1}{2L},$$

summing over i, j, k, L such that $i + j + k + 2L = r$, by applying the lemma twice. If r is odd, $2^n - 2T - 1 - r$ is even and $\binom{2^n-2T-1-r}{r-2L} = 0$. If r is even, $r = 2R$, we have

$$\sum_L \binom{2^{n-1} - T - R - 1}{R - L}\binom{T}{L} = \binom{2^{n-1} - R - 1}{R} \equiv 0 \mod 2$$

by lemma 2.7.

For Sq_2^r, there are no terms unless t is odd, then all terms lie in M. We get

$$\sum \binom{x}{i}\binom{y}{j}\binom{z}{k}\binom{t}{l} = \binom{x+y+z+t}{r} = \binom{2^n-2r}{r} \equiv 0 \mod 2$$

by lemma 2.6, summing over all i, j, k, l such that $i+j+k+l=r$.

When we permute by S_4, we get four different linear functionals, of which only three are linearly independent, as their sum is zero.

Case 2: Take $M=$ all monomials (a,b,c,d) with all entries odd, $a+b=2^{n-1}$ (hence $c+d=2^{n-1}$ also).

For Sq^r, there are no terms in M unless x, y, z, t are all odd. Write $x=2X+1, y=2Y+1, z=2Z+1, t=2T+1$. Then $r=2R$ and $X+Y+Z+T+R+2=2^{n-1}$. The number of terms that lie in M is

$$\begin{aligned} & \sum \binom{2X+1}{2i}\binom{2Y+1}{2j}\binom{2Z+1}{2k}\binom{2T+1}{2l} \\ \equiv\ & \sum \binom{X}{i}\binom{Y}{j}\binom{Z}{k}\binom{T}{l} \\ =\ & \binom{X+Y}{2^{n-2}-1-X-Y}\binom{Z+T}{2^{n-2}-1-Z-T}, \end{aligned}$$

summing over all i, j, k, l such that $X+Y+i+j+1=2^{n-2}$ and $Z+T+k+l+1=2^{n-2}$. By Lemma 2.7, this is even unless $X+Y=2^{n-2}-1$ and $Z+T=2^{n-2}-1$, which implies $R=0$, which is not allowed.

For Sq_2^r there are no terms unless x, y, z, t are all odd, when we get

$$\sum \binom{2X+1}{i}\binom{2Y+1}{j}\binom{2Z+1}{k}\binom{2T+1}{l} = \binom{2X+2Y+2}{2^{n-2}-1-X-Y}\binom{2Z+2T+2}{2^{n-2}-1-Z-T},$$

summing over all i, j, k, l such that $X+Y+1+i+j=2^{n-2}$ and $Z+T+1+k+l=2^{n-2}$. This is even by lemma 2.6 unless $X+Y=Z+T=2^{n-2}-1$, which imply $r=0$.

When we permute, we find three linear functionals, all linearly independent, provided $n \geq 4$.

In all we have 6 linearly independent functionals. Every coefficient in Theorem 1.3 is a linear combination of these. (The coefficient of $(1, 3, 2^{n-1}-3, 2^{n-1}-1)$ is the sum of the three from case 2.)

4.2 Dimension $2^n + 1$

Take M=all (a, b, c, d) with $a = 1, b$ odd.

For Sq^r: No terms unless $x = 1, y$ odd. Put $y = 2Y+1$, then $1+2Y+1+z+t+r = 2^n+1$. We get

$$\sum \binom{y}{2j}\binom{z}{k}\binom{t}{l} = \sum_j \binom{y}{2j}\binom{z+t}{r-2j} \equiv \sum_j \binom{Y}{j}\binom{2^n-2Y-1-r}{r-2j}$$

summing over all j, k, l such that $2j + k + l = r$.

If r is odd, $2^n - 2Y - 1 - r$ is even and we get 0. If r is even, $r = 2R$, we get

$$\begin{aligned} &\sum_j \binom{Y}{j}\binom{2^n-2Y-1-2R}{2R-2j} \\ \equiv\ &\sum_j \binom{Y}{j}\binom{2^{n-1}-1-Y-R}{R-j} = \binom{2^{n-1}-1-R}{R} \mod 2, \end{aligned}$$

which is zero for $r > 0$ by Lemma 2.7.

For Sq_2^r: This time $1 + y + z + t + 2r = 2^n + 1$. No terms unless y is odd, then

$$\sum \binom{y}{j}\binom{z}{k}\binom{t}{l} = \binom{y+z+t}{r} = \binom{2^n-2r}{r} \equiv 0 \mod 2$$

summing over all j, k, l such that $j + k + l = r$.

If we permute b, c, d only, we get three linear functionals whose sum is zero, so only two of them are linearly independent. If we permute a as well, we get 12 functionals, of which 8 are linearly independent. Every coefficient in theorem 1.4 is a linear combinaation of these functionals.

4.3 Dimension $2^n + 3$

Take M = all (a, b, c, d) with $a + b = 3$, c odd, d odd.

For Sq^r: No terms unless $x + y \leq 3, z = 2Z + 1, t = 2T + 1$.

Case $x = y = 1$: $r = 2R + 1, Z + T + R = 2^{n-1} - 1$. Counting the terms (1,2,odd,odd), we get

$$\sum_{k+l=R} \binom{2Z+1}{2k}\binom{2T+1}{2l} \equiv \sum \binom{Z}{k}\binom{T}{l} = \binom{2^{n-1}-1-R}{R},$$

where $R = 0$ is possible. The count of terms (2,1,odd,odd), is the same, so the total number is even.

Case $x = 1, y = 2$: $r = 2R, Z + T + R = 2^{n-1} - 1$. The count is

$$\sum_{k+l=R} \binom{2Z+1}{2k}\binom{2T+1}{2l} \equiv \sum \binom{Z}{k}\binom{T}{l} = \binom{2^{n-1}-1-R}{R} \equiv 0 \mod 2$$

since $R > 0$.

The case $x = 2$, $y = 1$ is similar.

For Sq_2^r: No terms in M, unless x and y are 1 and 2 in either order, and $z = 2Z+1$ and $t = 2T + 1$. Then the count is

$$\sum_{k+l=r} \binom{2Z+1}{k}\binom{2T+1}{l} = \binom{2^n - 2r}{r} \equiv 0.$$

Permutation gives 6 linear functionals, all linearly independent. All coefficients in Theorem 1.6 are linear combinations of these.

4.4 Dimension $2^p + 2^q$ $(p > q \geq 1)$

Take M = all (a, b, c, d) with a, b, c, d all odd, $a + b = 2^q$.

For Sq^r: No terms unless x, y, z, t all odd. Write $x = 2X+1, y = 2Y+1, z = 2Z+1, t = 2T + 1$, then $r = 2R$, and $X + Y + Z + T + 2 + R = 2^{p-1} + 2^{q-1}$. The number of terms in M is

$$\begin{aligned}&\sum \binom{2X+1}{2i}\binom{2Y+1}{2j}\binom{2Z+1}{2k}\binom{2T+1}{2l}\\ \equiv\ &\sum \binom{X}{i}\binom{Y}{j}\binom{Z}{k}\binom{T}{l} = \binom{X+Y}{2^{q-1}-1-X-Y}\binom{Z+T}{2^{p-1}-1-Z-T} \mod 2,\end{aligned}$$

summing over all i, j, k, l such that $X+Y+i+j+1 = 2^{q-1}, Z+T+k+l+1 = 2^{p-1}$. This is even unless $X + Y = 2^{q-1} - 1$ and $Z + T = 2^{p-1} - 1$, which imply $r = 0$, which is not allowed.

For Sq_2^r: Again x, y, z, t must all be odd, $x + y + z + t + 2r = 2^p + 2^q$. The number of terms in M is

$$\sum \binom{x}{i}\binom{y}{j}\binom{z}{k}\binom{t}{l} = \binom{x+y}{(2^q-x-y)/2}\binom{z+t}{(2^p-z-t)/2}$$

summing over all i, j, k, l such that $x + y + 2i + 2j = 2^q$,$z + t + 2k + 2l = 2^p$. This is even unless $x + y = 2^q$ and $z + t = 2^p$, which imply $r = 0$.

Permutation gives 6 functionals, all linearly independent. All coefficients appearing in Theorems 1.5,1.7,1.8 are linear combinations of these.

4.5 Dimension 10

Take M = all permutations of (1,2,3,4).

By direct calculation, this is an extra linear functional.

5 Proofs of theorems 1.3-1.8.

The linear functionals constructed in section 4 show that the proposed basis elements listed in Theorems 1.3-1.8 are linearly independent in $\bar{W}^+(4)$. To complete the proof, we have to show they span. But every element (a,b,c,d) is equivalent to a sum of (m,n,o,p) such that (m,n,o) is a basis element in $\bar{W}^+(3)$ by Lemma 2.3.

So we only have to consider elements (m,n,o,p) such that (m,n,o) is among $(1,1,2^p-1)$,$(1,2^p-1,1)$,$(1,3,2^p-3)$,$(1,2,2^p-3)$,$(1,2,3)$ and $(1,1,2^p-2)$. We show that all such elements can be written as sums of basis elements.

The proof below is by induction. We did not pay too much attention to the low dimension case, since we have a program which has worked out results up to dimension 100.

5.1 Dimension 2^n.

Case 1: Let's prove $(1,1,2l,2m) \equiv (1,1,2,2^n-4)$.

For $n=3$, this says only that $(1,1,4,2) \equiv (1,1,2,4)$, so assume $n \geq 4$. By induction, all monomials $(1,1,2a,2b)$ in dimension 2^{n-1} are equivalent. By Lemma 2.2, all monomials $(1,1,2^{n-1}+2a,2b)$ are equvalent, all monomials $(1,1,2^{n-2}+2a,2^{n-2}+2b)$ are equivalent, and all monomials $(1,1,2a,2^{n-1}+2b)$ are equivalent. But these ranges overlap for $n \geq 5$. For $n=4$ we compute $(1,1,6,8) \equiv (1,1,2,12)$, hence by permutation $(1,1,8,6) \equiv (1,1,12,2)$ and we get the same result.

Case 2: $(1,2,2^p-3,2^n-2^p) = (1,2,1,2^n-4)$.

If $p < n-1$, then $(1,2,2^p-3,2^{n-1}-2^p) \equiv (1,2,1,2^{n-1}-4)$, and we easily get what we want by applying Lemma 2.2.

If $p = n-1$, then we have $(1,2,2^{n-1}-3,2^{n-1})$. Since $(1,2,2^{n-2}-3,2^{n-2}) \equiv (1,2,1,2^{n-1}-4)$, we get $(1,2,2^{n-2}+1,2^{n-1}+2^{n-2}-4)$. Now $(1,2,2^{n-2}+1,2^{n-2}-4) \equiv (1,2,1,2^{n-1}-4)$, assuming $n \geq 5$, and we get what we want.

Case 3: $(1,1,2^p-1,2^n-2^p-1) \equiv (1,1,1,2^n-3)$ if $p \neq n-1$.

If $p < n-2$, then $(1,1,2^p-1,2^{n-1}-2^p-1) \equiv (1,1,1,2^{n-1}-3)$, we get what we want easily. If $p = n-2$, then we have

$$\begin{aligned}
& (1,1,2^{n-2}-1,2^{n-1}+2^{n-2}-1) \\
\equiv\; & (2,2,2^{n-1}-3,2^{n-1}-1)+(1,2,2^{n-1}-2,2^{n-1}-1) \\
& +(2,1,2^{n-1}-2,2^{n-1}-1) \\
\equiv\; & (1,1,\mathrm{Sq}^2(2^{n-1}-3,2^{n-1}-1))+(1,1,\mathrm{Sq}^1(2^{n-1}-2,2^{n-1}-1)) \\
=\; & (1,1,2^{n-1}-3,2^{n-1}+1) \\
\equiv\; & (1,1,1,2^n-3)
\end{aligned}$$

In the first equality we use Lemma 2.1 and $\mathrm{Sq}^{2^{n-2}}(1,1,2^{n-2}-1,2^{n-1}-1)$. In the last equality we have used $(1,1,2^{n-1}-3,2^{n-1}+1) \equiv (1,1,1,2^n-3)$, since the induction hypothesis $(1,1,2^{n-1}-3,1) \equiv (1,1,1,2^{n-1}-3)$ in dimension 2^{n-1}.

Case 4: $(1,2^p-1,1,2^n-2^p-1) \equiv (1,1,1,2^n-3)$ if $p \neq n-1$.

But this is a permutation of case 3.

Case 5: $(1,2,3,2^n-6) \equiv (1,2,1,2^n-4)$

Since in dimension 2^{n-1} we have $(1,2,3,2^{n-1}-6) \equiv (1,2,1,2^{n-1}-4)$, assuming $n \geq 5$, it follows easily from Lemma 2.2.

Case 6: $(1,3,2^p-3,2^n-2^p-1) \equiv (1,1,1,2^n-3)$ if $p \neq n-1$.

If $p < n-2$, since $(1,3,2^p-3,2^{n-1}-2^p-1) \equiv (1,1,1,2^{n-1}-3)$, this is easy. If $p = n-2$, we have

$$\begin{aligned}
& (1,3,2^{n-2}-3,2^{n-1}+2^{n-2}-1) \\
\equiv\; & (2,6,2^{n-1}-7,2^{n-1}-1)+(1,6,2^{n-1}-6,2^{n-1}-1) \\
& +(2,5,2^{n-1}-6,2^{n-1}-1) \\
\equiv\; & (1,5,\mathrm{Sq}^2(2^{n-1}-7,2^{n-1}-1))+(1,5,\mathrm{Sq}^1(2^{n-1}-6,2^{n-1}-1)) \\
=\; & (1,5,2^{n-1}-7,2^{n-1}+1) \\
\equiv\; & (1,1,1,2^n-3)
\end{aligned}$$

The reasoning is like case 3.

5.2 Dimension 2^n+1

The result is easy for $n = 3$ and can be computed directly for $n = 4$, so assume $n \geq 5$.

Case 1: $(1,1,2^p-2,2^n-2^p+1) \equiv (1,1,2,2^n-3)$ if $p<n$, else it is $(1,1,2^n-2,1)$.

If $p < n-1$, then $(1,1,2^p-2,2^{n-1}-2^p+1) \equiv (1,1,2,2^{n-1}-3)$, and the result follows easily. If $p=n-1$, we have $(1,1,2^{n-2}-2,2^{n-2}+1) \equiv (1,1,2,2^{n-1}-3)$, so we have $(1,1,2+2^{n-2},2^{n-1}+2^{n-2}-3)$. This is equivalent to $(1,1,2,2^n-3)$ since $(1,1,2+2^{n-2},2^{n-2}-3) \equiv (1,1,2,2^{n-1}-3)$.

Case 2: $(1,2,3,2^n-5)$, this is a basis element.

Case 3: $(1,2,2^p-3,2^n-2^p+1) \equiv (1,2,3,2^n-5)$ if $n>p>2$, else it is $(1,2,1,2^n-3)$ or $(1,2,2^n-3,1)$.

If $2<p<n-1$, then $(1,2,2^p-3,2^{n-1}-2^p+1) \equiv (1,2,3,2^{n-1}-5)$, and the result follows easily. If $p=n-1$, we have $(1,2,2^{n-2}-3,2^{n-2}+1) \equiv (1,2,3,2^{n-1}-5)$, so by Lemma 2.2

$$\begin{aligned}(1,2,2^{n-1}-3,2^{n-1}+1) &\equiv (1,2,3+2^{n-2},2^{n-1}+2^{n-2}-5)\\ &\equiv (1,2,3,2^n-5)\end{aligned}$$

using $(1,2,3+2^{n-2},2^{n-2}-5) \equiv (1,2,3,2^{n-1}-5)$.

Case 4: $(1,1,2^p-1,2^n-2^p) \equiv (1,1,3,2^n-4)$ if $n>p>1$; if $p=1$, $(1,1,1,2^n-2)$ is a basis element.

If $1<p<n-1$, then $(1,1,2^p-1,2^{n-1}-2^p) \equiv (1,1,3,2^{n-1}-4)$, and the result follows. If $p=n-1$, we have by Lemma 2.2,

$$(1,1,2^{n-1}-1,2^{n-1}) \equiv (1,1,2^{n-1}-3,2^{n-1}+2) \equiv (1,1,3,2^n-4).$$

Case 5: $(1,2^p-1,1,2^n-2^p) \equiv (1,3,1,2^n-4)$ for $n>p>1$.

This is just a permutation of case 4.

Case 6: $(1,3,2^p-3,2^n-2^p) \equiv (1,1,1,2^n-2)+(1,1,3,2^n-4)+(1,3,1,2^n-4)$ for $n>p>2$.

Again if $2<p<n-1$, the result follows easily from

$$(1,3,2^p-3,2^{n-1}-2^p) \equiv (1,1,1,2^{n-1}-2)+(1,1,3,2^{n-1}-4)+(1,3,1,2^{n-1}-4).$$

If $p=n-1$, we have $(1,3,2^{n-1}-3,2^{n-1})$. By using

$$(1,3,2^{n-2}-3,2^{n-2}) \equiv (1,1,1,2^{n-1}-2)+(1,1,3,2^{n-1}-4)+(1,3,1,2^{n-1}-4)$$

we get

$$\begin{aligned} & (1,1,1+2^{n-2},2^{n-1}+2^{n-2}-2)+(1,1,3+2^{n-2},2^{n-1}+2^{n-2}-4) \\ + \quad & (1,3,1+2^{n-2},2^{n-1}+2^{n-2}-4). \end{aligned}$$

But the first two terms cancel out since $(1,1,2^{n-2}+1,2^{n-2}-2) \equiv (1,1,2^{n-2}+3,2^{n-2}-4)$ in dimension $2^{n-1}+1$; since $(1,3,\mathit{odd}>1,\mathit{even})$ in dimension 2^{n-1} is equavalent to $(1,1,1,2^{n-1}-2)+(1,1,3,2^{n-1}-4)+(1,3,1,2^{n-1}-4)$, the result follows.

5.3 Dimension 2^n+2

This time we only have to consider elements made up of odd numbers, by Lemma 2.5.

Case 1: $(1,1,2^p-1,2^n-2^p+1) \equiv (1,1,3,2^n-3)$ if $n>p>1$, else it is $(1,1,1,2^n-1)$ or $(1,1,2^n-1,1)$, a basis element.

If $p<n-1$, since $(1,1,2^p-1,2^{n-1}-2^p+1) \equiv (1,1,3,2^{n-1}-3)$, the result follows; if $p=n-1$, then we have $(1,1,2^{n-1}-1,2^{n-1}+1)$. Considering $(1,1,2^{n-2}-1,2^{n-2}+1) \equiv (1,1,3,2^{n-1}-3)$ (assuming $n>3$), we get $(1,1,2^{n-2}+3,2^{n-1}+2^{n-2}-3)$. We get the result since $(1,1,2^{n-2}+3,2^{n-2}-3) \equiv (1,1,3,2^{n-1}-3)$.

Case 2: $(1,2^p-1,1,2^n-2^p+1) \equiv (1,3,1,2^n-3)$ if $n>p>1$, else is $(1,1,1,2^n-1)$ or $(1,2^n-1,1,1)$, a basis element.

This is a permutation of case 1.

Case 3: $(1,3,2^p-3,2^n-2^p+1) \equiv 0$ if $n>p>2$, else we get $(1,3,1,2^n-3)$ or $(1,3,2^n-3,1)$, a basis element.

If $n-1>p>2$, since $(1,3,2^p-3,2^{n-1}-2^p+1) \equiv 0$, we have the result; if $p=n-1$, we have $(1,3,2^{n-1}-3,2^{n-1}+1)$. Since $(1,3,2^{n-2}-3,2^{n-2}+1) \equiv 0$ for $n \geq 5$, we have the result. For $n=4$, we compute directly that $(1,3,5,9) \equiv 0$.

5.4 Dimension 2^n+3

We assume $n \geq 5$. For $n<5$ we have direct computation.

Case 1: $(1,1,2^p-1,2^n-2^p+2) \equiv 0$ if $n>p \geq 1$, else we have $(1,1,2^n-1,2)$.

If $p<n-1$, this follows easily since $(1,1,2^p-1,2^{n-1}-2^p+2) \equiv 0$; if $p=n-1$, we have $(1,1,2^{n-1}-1,2^{n-1}+2)$. Since

$$(1,1,3,6)=\mathrm{Sq}_2^2(1,1,3,2)+\mathrm{Sq}_2^1(1,1,5,2)+\mathrm{Sq}_2^3(1,1,1,2)+\mathrm{Sq}_2^1(1,1,1,6),$$

Lemma 2.2 gives $(0,0,2^{n-1}-4,2^{n-1}-4)\cdot(1,1,3,6)\equiv 0$, and the result also follows.

Case 2: $(1,2^p-1,1,2^n-2^p+2)\equiv 0$ if $n>p\geq 1$, else we have $(1,2^n-1,1,2)$. This is a permutation of case 1.

Case 3: $(1,3,2^p-3,2^n-2^p+2)\equiv 0$ if $n>p>1$, else we have $(1,3,2^n-3,2)$.

If $p<n-1$, since $(1,3,2^p-3,2^{n-1}-2^p+2)\equiv 0$, the result follows; else if $p=n-1$ we have $(1,3,2^{n-1}-3,2^{n-1}+2)$. Since $(0,0,2^{n-1}-4,2^{n-1}-4)\cdot(1,3,1,6)\equiv 0$ by the computation in case 1, we have the result.

But we also have to show

$$(1,3,2^n-3,2)\equiv(1,1,2^n-1,2)+(1,2,3,2^n-3)+(1,2,2^n-1,1).$$

Since by induction and Lemma 2.2 we can show

$$(1,3,2^n-3,2)\equiv(1,1,2^n-1,2)+(1,2,3+2^{n-1},2^{n-1}-3)+(1,2,2^n-1,1),$$

we have to show

$$(1,2,2^{n-1}+3,2^{n-1}-3)\equiv(1,2,3,2^n-3).$$

By Lemma 2.1

$$\begin{aligned}0 &= (\mathrm{Sq}^8(1),2,2^{n-1}-5,2^{n-1}-3)\equiv(1,\mathrm{Sq}^8(2,2^{n-1}-5,2^{n-1}-3))\\ &= (1,2,2^{n-1}-5,2^{n-1}+5)+(1,2,2^{n-1}-2,2^{n-1}+2)+(1,2,2^{n-1}+3,2^{n-1}-3)\\ &\quad +(1,4,2^{n-1}-4,2^{n-1}+2)+(1,4,2^{n-1}-3,2^{n-1}+1)\end{aligned}$$

We may neglect the terms with 3 even entries. By Lemma 2.2, $(1,4,2^{n-1}-3,2^{n-1}+1)\equiv 0$ since $(1,4,2^{n-1}-3,1)\equiv 0$, $(1,2,2^{n-1}-5,2^{n-1}+5)\equiv(1,2,3,2^n-3)$ since $(1,2,2^{n-1}-5,5)\equiv(1,2,3,2^{n-1}-3)$.

Case 4: $(1,2,3,2^n-3)$, this is a basis element.

Case 5: $(1,1,2^p-2,2^n-2^p+3)\equiv 0$ if $n\geq p>2$, else if $p=2$, we have $(1,1,2,2^n-1)$.

If $p=n$, this follows from dimension $2^{n-1}+3$ using $(1,1,2^{n-1}-2,3)\equiv 0$. If $n>p>2$, it follows from $(1,1,2^p-2,2^{n-1}-2^p+3)\equiv 0$ in dimension $2^{n-1}+3$.

Case 6: $(1,2,2^p-3,2^n-2^p+3)\equiv(1,2,3,2^n-3)$ if $p>2$, else if $p=2$, we have $(1,2,1,2^n-1)$.

If $n-1 \geq p > 2$, the result follows easily. If $p = n$, we have $(1, 2, 2^n - 3, 3)$. By Lemma 2.2, $(1, 2, 2^n - 3, 3) \equiv (1, 2, 2^{n-1} + 3, 2^{n-1} - 3)$, since $(1, 2, 2^{n-1} - 3, 3) \equiv (1, 2, 3, 2^{n-1} - 3)$. We have already shown that $(1, 2, 2^{n-1} + 3, 2^{n-1} - 3) \equiv (1, 2, 3, 2^n - 3)$.

5.5 Dimension $2^n + 4$.

We assume $n \geq 5$.

Case 1: $(1, 1, 2^p - 1, 2^n - 2^p + 3) \equiv 0$ if $n > p$ and $p \neq 2$. Else we get $(1, 1, 2^n - 1, 3)$ or $(1, 1, 3, 2^n - 1)$.

If $p = 1$ or $n - 1 > p > 2$, since $(1, 1, 1, 2^{n-1} + 1) \equiv 0$ and $(1, 1, 2^p - 1, 2^{n-1} - 2^p + 3) \equiv 0$, the result follows.

If $p = n - 1$, we have $(1, 1, 2^{n-1} - 1, 2^{n-1} + 3)$. We use

$$\begin{aligned} 0 &= (\mathrm{Sq}_2^4(1,1), 2^{n-1} - 1, 2^{n-1} - 5) \equiv (1, 1, \chi\mathrm{Sq}_2^4(2^{n-1} - 1, 2^{n-1} - 5)) \\ &= (1, 1, 2^{n-1} - 1, 2^{n-1} + 3) + (1, 1, 2^{n-1} + 1, 2^{n-1} + 1) + (1, 1, 2^{n-1} + 5, 2^{n-1} - 3). \end{aligned}$$

But the latter two terms are hit by $\mathrm{Sq}^2(1, 1, 2^{n-1} - 1, 2^{n-1} + 1)$ and $\mathrm{Sq}^2(1, 1, 2^{n-1} + 5, 2^{n-1} - 5)$.

Case 2: $(1, 2^p - 1, 1, 2^n - 2^p + 3) \equiv 0$ if $n > p$ and $p \neq 2$. Else we get $(1, 2^n - 1, 1, 3)$ or $(1, 3, 1, 2^n - 1)$.

This is a permutation of case 1.

Case 3: $(1, 3, 2^p - 3, 2^n - 2^p + 3) \equiv (1, 3, 5, 2^n - 5)$ if $n > p > 2$, else we get $(1, 3, 1, 2^n - 1)$ or $(1, 3, 2^n - 3, 3)$.

Again if $p < n - 1$, this follows from $(1, 3, 2^p - 3, 2^{n-1} - 2^p + 3) \equiv (1, 3, 5, 2^{n-1} - 5)$.

We have to show

$$(1, 3, 2^{n-1} - 3, 2^{n-1} + 3) \equiv (1, 3, 5, 2^n - 5).$$

ignoring monomials with even entries, we expand

$$\begin{aligned} 0 &= (\mathrm{Sq}^8(3), 1, 2^{n-1} - 3, 2^{n-1} - 5) \equiv (3, \mathrm{Sq}^8(1, 2^{n-1} - 3, 2^{n-1} - 5)) \\ &= (3, 1, 2^{n-1} - 3, 2^{n-1} + 3) + (3, 1, 2^{n-1} + 5, 2^{n-1} - 5). \end{aligned}$$

thus by permutation, $(1, 3, 2^{n-1} - 3, 2^{n-1} + 3) \equiv (1, 3, 2^{n-1} + 5, 2^{n-1} - 5)$.

Next we use Proposition 7.2 to expand

$$\begin{aligned} 0 &= (\mathrm{Sq}_2^8(1,3), 2^{n-1} - 11, 2^{n-1} - 5) \equiv (1, 3, \chi\mathrm{Sq}_2^8(2^{n-1} - 11, 2^{n-1} - 5)) \\ &= (1, 3, 2^{n-1} + 5, 2^{n-1} - 5) + (1, 3, 2^{n-1} - 9, 2^{n-1} + 9) \end{aligned}$$

So $(1,3,2^{n-1}+5,2^{n-1}-5) \equiv (1,3,2^{n-1}-9,2^{n-1}+9)$.

Finally, $(1,3,2^{n-1}-9,2^{n-1}+9) \equiv (1,3,5,2^n-5)$ follows by Lemma 2.2 from $(1,3,2^{n-1}-9,9) \equiv (1,3,5,2^{n-1}-5)$ in dimension $2^{n-1}+4$.

5.6 Dimension $2^m + 2^n$ with $m > n+1 \geq 4$

Lemma 5.1. $(1,9,2^k+2^n-9,2^k-1) \equiv 0$ *in dimension* $2^{k+1}+2^n$*, for any* $k \geq n+1, n \geq 3$.

Proof Expand

$$(\mathrm{Sq}_2^{2^n}(1,3,2^k-2^n-3),2^k-1) \equiv (1,3,2^k-2^n-3,(\chi\mathrm{Sq}_2^{2^n})(2^k-1))$$

On the left, there are only three terms,

$$(1,9,2^k+2^n-9,2^k-1)+(3,7,2^k+2^n-9,2^k-1)+(3,9,2^k+2^n-11,2^k-1)$$

The second and third terms are trivial by Lemma 2.2, since $(3,7,2^n-9,2^k-1) \equiv 0$ and $(3,9,2^n-11,2^k-1) \equiv 0$ in dimension 2^k+2^n.

The right side is 0, since $\binom{2^k-1+3\cdot 2^n-1}{2^n} = \binom{2^k+2^{n+1}+2^n-2}{2^n} = 0$.

Case 1: $(1,1,2^p-1,2^n+2^m-2^p-1) \equiv 0$ if $p < n$ or $m > p > n$, else we have $(1,1,2^m-1,2^n-1)$ or $(1,1,2^n-1,2^m-1)$.

If $p \neq m-1$, since $(1,1,2^p-1,2^{m-1}-2^p+2^n-1) \equiv 0$ in dimension $2^{m-1}+2^n$, the result follows. If $p = m-1$, since $m-2 \geq n$, in dimension $2^{m-1}+2^n$, we have

$$(1,1,2^{m-1}-1,2^n-1) \equiv (9,1,2^{m-1}-1,2^n-9)+(1,9,2^{m-1}-1,2^n-9).$$

By Lemma 2.2,

$$\begin{aligned} & (1,1,2^{m-1}-1,2^{m-1}+2^n-1) \\ \equiv\ & (9,1,2^{m-1}-1,2^{m-1}+2^n-9)+(1,9,2^{m-1}-1,2^{m-1}+2^n-9) \\ \equiv\ & 0 \end{aligned}$$

since each term on the right is a permutation of the term in the Lemma.

Case 2: $(1,2^p-1,1,2^m+2^n-2^p-1) \equiv 0$ if $n > p$ or $m \geq p \geq n$, else we get $(1,2^n-1,1,2^m-1)$ or $(1,2^m-1,1,2^n-1)$.

This is a permutation of case 1.

Case 3: $(1,3,2^p-3,2^m+2^n-2^p-1)\equiv 0$ if $n>p>1$ or $m>p>n$; else if $p=n$ or $p=m$, we get $(1,3,2^n-3,2^m-1)$ or $(1,3,2^m-3,2^n-1)$, which are basis elements.

If $p\neq m-1$, since $(1,3,2^p-3,2^{m-1}-2^p+2^n-1)\equiv 0$ in dimension $2^{m-1}+2^n$, the result follows by Lemma 2.2.

If $p=m-1$ and $m\geq n+2$, in dimension $2^{m-1}+2^n$,

$$(1,3,2^{m-1}-3,2^n-1)\equiv(9,1,2^{m-1}-1,2^n-9)$$

By Lemma 2.2 and Lemma 5.1,

$$(1,3,2^{m-1}-3,2^{m-1}+2^n-1)\equiv(9,1,2^{m-1}-1,2^{m-1}+2^n-9)\equiv 0.$$

We are done.

5.7 Dimension $2^{n+1}+2^n$ with $n\geq 3$.

Case 1: $(1,1,2^p-1,2^{n+1}+2^n-2^p-1)\equiv 0$ if $1\leq p<n$; if $p=n$, we get $(1,1,2^n-1,2^{n+1}-1)$; if $p=n+1$, we get $(1,1,2^{n+1}-1,2^n-1)$; both are basis elements.

If $p\leq n-1$, by Lemma 2.1,

$$\begin{aligned}(1,1,2^p-1,2^{n+1}+2^n-2^p-1) &= (1,1,2^p-1,\mathrm{Sq}^{2^n}(2^{n+1}-2^p-1))\\ &\equiv (\mathrm{Sq}^{2^n}(1,1,2^p-1),2^{n+1}-2^p-1)\\ &= 0\end{aligned}$$

Case 2: $(1,2^p-1,1,2^{n+1}+2^n-2^p-1)\equiv 0$ if $1\leq p<n$; if $p=n$, we get $(1,2^n-1,1,2^{n+1}-1)$; if $p=n+1$, we get $(1,2^{n+1}-1,1,2^n-1)$, both are basis elements.

This is a permutation of case 1.

Case 3: $(1,3,2^p-3,2^{n+1}+2^n-2^p-1)\equiv 0$ if $1<p<n$; if $p=n$, we get $(1,3,2^n-3,2^{n+1}-1)$; if $p=n+1$, we get $(1,3,2^{n+1}-3,2^n-1)$; both are basis elements.

If $p\leq n-1$, by Lemma 2.1,

$$(1,3,2^p-3,\mathrm{Sq}^{2^n}(2^{n+1}-2^p-1))\equiv(\mathrm{Sq}^{2^n}(1,3,2^p-3),2^{n+1}-2^p-1)=0$$

.

6 The action of S_4.

We shall use P_{i_1,i_2} to mean the permutation that swaps i_1 and i_2, and leaves other elements unchanged. It is well known that the group is generated by P_{12}, P_{13}, P_{14}. We give the action of S_4 on $\bar{W}^+(4)$.

6.1 Dimension 2^n for $n \geq 4$.

Denote $(1,1,1,2^n-3)$, $(1,1,2,2^n-4)$, $(1,1,2^{n-1}-1,2^{n-1}-1)$, $(1,2,1,2^n-4)$, $(1,3,2^{n-1}-3,2^{n-1}-1)$, $(1,2^{n-1}-1,1,2^{n-1}-1)$ by v_1, v_2, v_3, v_4, v_5, v_6 respectively. The action is as follows:

1. $P_{12}v_1 = v_1$, $P_{13}v_1 = v_1$, $P_{14}v_1 = v_1$;
2. $P_{12}v_2 = v_2$, $P_{13}v_2 = v_2 + v_4$, $P_{14}v_2 = v_1 + v_4$;
3. $P_{12}v_3 = v_3$, $P_{13}v_3 = v_1 + v_3 + v_6$, $P_{14}v_3 = v_6$;
4. $P_{12}v_4 = v_2 + v_4$, $P_{13}v_4 = v_4$, $P_{14}v_4 = v_1 + v_2$;
5. $P_{12}v_5 = v_1 + v_3 + v_5$, $P_{13}v_5 = v_1 + v_6 + v_5$, $P_{14}v_5 = v_5$;
6. $P_{12}v_6 = v_1 + v_3 + v_6$, $P_{13}v_6 = v_6$, $P_{14}v_6 = v_3$

These can be read off very easily from theorem 1.3.

6.2 Dimension $2^n + 1$ for $n \geq 3$.

Denote $(1,1,1,2^n-2)$, $(1,1,2,2^n-3)$, $(1,1,3,2^n-4)$, $(1,1,2^n-2,1)$, $(1,2,1,2^n-3)$, $(1,2,3,2^n-5)$, $(1,2,2^n-3,1)$, $(1,3,1,2^n-4)$ by v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8 respectively. The action is as follows:

1. $P_{12}v_1 = v_1$, $P_{13}v_1 = v_1$, $P_{14}v_1 = v_1 + v_4 + v_5 + v_6 + v_7$;
2. $P_{12}v_2 = v_2$, $P_{13}v_2 = v_1 + v_2 + v_5$, $P_{14}v_2 = v_1 + v_3 + v_4 + v_6 + v_8$;
3. $P_{12}v_3 = v_3$, $P_{13}v_3 = v_3 + v_8$, $P_{14}v_3 = v_3 + v_4 + v_7$;
4. $P_{12}v_4 = v_4$, $P_{13}v_4 = v_1 + v_4 + v_5 + v_6 + v_7$, $P_{14}v_4 = v_4$;
5. $P_{12}v_5 = v_1 + v_2 + v_5$, $P_{13}v_5 = v_5$, $P_{14}v_5 = v_5 + v_7$;

6. $P_{12}v_6 = v_2 + v_3 + v_6$, $P_{13}v_6 = v_5 + v_6$, $P_{14}v_6 = v_6 + v_7$;

7. $P_{12}v_7 = v_3 + v_4 + v_7$, $P_{13}v_7 = v_5 + v_7$, $P_{14}v_7 = v_7$;

8. $P_{12}v_8 = v_3 + v_8$, $P_{13}v_8 = v_8$, $P_{14}v_8 = v_1 + v_2 + v_3 + v_4 + v_5 + v_7$

Again this can be read off very easily from theorem 1.4.

6.3 Dimension $2^n + 2$ for $n \geq 4$.

Denote $(1,1,1,2^n-1)$, $(1,1,3,2^n-3)$, $(1,1,2^n-1,1)$, $(1,3,1,2^n-3)$, $(1,3,2^n-3,1)$, $(1,2^n-1,1,1)$ by v_1, v_2, v_3, v_4, v_5, v_6 respectively. The action is as follows:

1. $P_{12}v_1 = v_1$, $P_{13}v_1 = v_1$, $P_{14}v_1 = v_1 + v_3 + v_6$;

2. $P_{12}v_2 = v_2$, $P_{13}v_2 = v_1 + v_2 + v_4$, $P_{14}v_2 = v_2 + v_3 + v_5$;

3. $P_{12}v_3 = v_3$, $P_{13}v_3 = v_1 + v_3 + v_6$, $P_{14}v_3 = v_3$;

4. $P_{12}v_4 = v_1 + v_2 + v_4$, $P_{13}v_4 = v_4$, $P_{14}v_4 = v_4 + v_5 + v_6$;

5. $P_{12}v_5 = v_2 + v_3 + v_5$, $P_{13}v_5 = v_4 + v_5 + v_6$, $P_{14}v_5 = v_5$;

6. $P_{12}v_6 = v_1 + v_3 + v_6$, $P_{13}v_6 = v_6$, $P_{14}v_6 = v_6$

6.4 Dimension $2^n + 3$ for $n \geq 3$.

Denote $(1,1,2,2^n-1)$, $(1,1,2^n-1,2)$, $(1,2,1,2^n-1)$, $(1,2,3,2^n-3)$, $(1,2,2^n-1,1)$, $(1,2^n-1,1,2)$ by v_1, v_2, v_3, v_4, v_5, v_6 respectively. The action is as follows:

1. $P_{12}v_1 = v_1$, $P_{13}v_1 = v_1 + v_3$, $P_{14}v_1 = v_2 + v_3 + v_5 + v_6$;

2. $P_{12}v_2 = v_2$, $P_{13}v_2 = v_2 + v_6$, $P_{14}v_2 = v_2 + v_5$;

3. $P_{12}v_3 = v_1 + v_3$, $P_{13}v_3 = v_3$, $P_{14}v_3 = v_3 + v_5$;

4. $P_{12}v_4 = v_4$, $P_{13}v_4 = v_3 + v_4$, $P_{14}v_4 = v_4 + v_5$;

5. $P_{12}v_5 = v_2 + v_5$, $P_{13}v_5 = v_3 + v_5$, $P_{14}v_5 = v_5$;

6. $P_{12}v_6 = v_2 + v_6$, $P_{13}v_6 = v_6$, $P_{14}v_6 = v_1 + v_2 + v_3 + v_5$

6.5 Dimension $2^n + 4$ for $n \geq 4$.

Denote $(1,1,3,2^n-1)$, $(1,1,2^n-1,3)$, $(1,3,1,2^n-1)$, $(1,3,5,2^n-5)$, $(1,3,2^n-3,3)$, $(1,2^n-1,1,3)$ by v_1, v_2, v_3, v_4, v_5, v_6 respectively. The action is as follows:

1. $P_{12}v_1 = v_1$, $P_{13}v_1 = v_1 + v_3$, $P_{14}v_1 = v_3 + v_5 + v_6$;
2. $P_{12}v_2 = v_2$, $P_{13}v_2 = v_2 + v_6$, $P_{14}v_2 = v_5$;
3. $P_{12}v_3 = v_1 + v_3$, $P_{13}v_3 = v_3$, $P_{14}v_3 = v_2 + v_3 + v_5$;
4. $P_{12}v_4 = v_4$, $P_{13}v_4 = v_3 + v_4$, $P_{14}v_4 = v_2 + v_4 + v_5$;
5. $P_{12}v_5 = v_2 + v_5$, $P_{13}v_5 = v_3 + v_5 + v_6$, $P_{14}v_5 = v_2$;
6. $P_{12}v_6 = v_2 + v_6$, $P_{13}v_6 = v_6$, $P_{14}v_6 = v_1 + v_3 + v_5$

6.6 Dimension $2^p + 2^q$ for $p > q \geq 3$.

Denote $(1,1,2^q-1,2^p-1)$, $(1,1,2^p-1,2^q-1)$, $(1,3,2^q-3,2^p-1)$, $(1,3,2^p-3,2^q-1)$, $(1,2^q-1,1,2^p-1)$, $(1,2^p-1,1,2^q-1)$ by v_1, v_2, v_3, v_4, v_5, v_6 respectively. The action is as follows:

1. $P_{12}v_1 = v_1$, $P_{13}v_1 = v_1 + v_5$, $P_{14}v_1 = v_3 + v_4 + v_6$;
2. $P_{12}v_2 = v_2$, $P_{13}v_2 = v_2 + v_6$, $P_{14}v_2 = v_3 + v_4 + v_5$;
3. $P_{12}v_3 = v_1 + v_3$, $P_{13}v_3 = v_3 + v_5$, $P_{14}v_3 = v_3$;
4. $P_{12}v_4 = v_2 + v_4$, $P_{13}v_4 = v_4 + v_6$, $P_{14}v_4 = v_4$;
5. $P_{12}v_5 = v_1 + v_5$, $P_{13}v_5 = v_5$, $P_{14}v_5 = v_2 + v_3 + v_4$;
6. $P_{12}v_6 = v_2 + v_6$, $P_{13}v_6 = v_6$, $P_{14}v_6 = v_1 + v_3 + v_4$

7 Appendix: two formulae about $\chi\mathrm{Sq}^i$ and $\chi\mathrm{Sq}_2^i$.

Proposition 7.1. *For x in dimension 1,*

$$(\chi\mathrm{Sq}^i)x^t = \binom{t+2i}{i} x^{t+i} \mod 2$$

This is a well known result, but we feel it is still necessary to give a proof here. We provide two proofs, the first one is algebraic, and the second one is more geometric, and is provided by Prof. Boardman. By definition of χ,

$$\chi\mathrm{Sq}^{i+1} = \sum_{k=1}^{i+1} (\chi\mathrm{Sq}^{i+1-k})\mathrm{Sq}^k.$$

Proof 1: When $i = 1$, the proposition is obvious, since $\chi\mathrm{Sq}^1 = \mathrm{Sq}^1$ and $\binom{t+2}{1} = \binom{t}{1}$.

We suppose the proposition is correct for i and lower values, and use induction to prove it is correct for $i+1$. By the above formula we get

$$\begin{aligned}
(\chi\mathrm{Sq}^{i+1})x^t &= \sum_{k=1}^{i+1} (\chi\mathrm{Sq}^{i+1-k})\mathrm{Sq}^k x^t \\
&= \sum_{k=1}^{i+1} \binom{t+k+2i+2-2k}{i+1-k} \binom{t}{k} x^{t+i+1} \\
&= \sum_{k=1}^{t} \binom{t+2i+2-k}{t+i+1} \binom{t}{k} x^{t+i+1}
\end{aligned}$$

All the above computation is mod 2. Consider

$$\sum_{k=0}^{t} \binom{t}{k} (1+x)^{t+2i+2-k} = (1+1+x)^t(1+x)^{2i+2} = x^t(1+x)^{2i+2}.$$

The coefficient of x^{t+i+1} on the right side is $\binom{2i+2}{i+1}$, which is 0 mod 2; but the coefficient on the left side is $\sum_{k=0}^{t} \binom{t+2i+2-k}{t+i+1}\binom{t}{k}$, so we get

$$\binom{t+2i+2}{t+i+1} = \sum_{k=1}^{t} \binom{t+2i+2-k}{t+i+1} \binom{t}{k}.$$

Since $\binom{t+2i+2}{t+i+1} = \binom{t+2i+2}{i+1}$, this shows

$$(\chi\mathrm{Sq}^{i+1})x^t = \binom{t+2i+2}{i+1} x^{t+i+1}.$$

This finishes the induction proof of the proposition.

Proof 2: Recall that Poincaré duality in RP^{2^l-1}, $H^*(RP^{2^l-1}) \cong H_*(RP^{2^l-1})$ is an isomorphism of $\mathcal{A}$-modules. Take $x \in H^1(RP^{2^l-1})$, $z_i \in H_i(RP^{2^l-1})$ dual to x^i, and compute $(\chi\mathrm{Sq}^i)x^n$ in $H^*(RP^{2^l-1})$.

Since x^n corresponds to z_{2^l-1-n} and x^{n+i} corresponds to $z_{2^l-1-n-i}$, $(\chi\mathrm{Sq}^i)(x^n)$ corresponds to $(\chi\mathrm{Sq}^i)z_{2^l-1-n} = (?)z_{2^l-1-n-i}$, here "?" is the coefficient we want to know, and

$$\begin{aligned}
\left\langle x^{2^l-1-n-i}, (\chi\mathrm{Sq}^i)z_{2^l-1-n})\right\rangle &= \left\langle \mathrm{Sq}^i x^{2^l-1-n-i}, z_{2^l-1-n}\right\rangle \\
&= \left\langle \binom{2^l-1-n-i}{i} x^{2^l-1-n}, z_{2^l-1-n}\right\rangle \\
&= \binom{2^l-1-n-i}{i}
\end{aligned}$$

We only have to show $\binom{2^l-1-n-i}{i} = \binom{n+2i}{i}$ mod 2 for l large enough. Since

$$\binom{2^l-1-n-i}{i} = \binom{2^l-1-n-i}{2^l-1-n-2i} = \binom{n+2i}{n+i} = \binom{n+2i}{i},$$

we are done.

Proposition 7.2. *For x in dimension 1,*

$$(\chi\mathrm{Sq}_2^i)x^t = \binom{t+3i-1}{i} x^{t+2i}$$

By definition,

$$\chi\mathrm{Sq}_2^{i+1} = \sum_{k=1}^{i+1} (\chi\mathrm{Sq}_2^{i+1-k})\mathrm{Sq}_2^k.$$

Another lemma we will use is

Lemma 7.1.

$$\binom{3i+2}{i+1} = 0 \mod 2$$

Proof: If i is even, the equality is obvious. Suppose the lemma is true for $k < i$. If $i = 2j+1$,

$$\binom{3i+2}{i+1} = \binom{6j+5}{2j+2} = \binom{3j+2}{j+1}$$

By induction, the right side is 0 mod 2, so we are done.

Proof of the proposition: When $i = 1$, $\chi \mathrm{Sq}_2^1 = \mathrm{Sq}_2^1$, and $\binom{t+2}{1} = \binom{t}{1}$, so the proposition is true. Using the formula, we get

$$\begin{aligned}
(\chi \mathrm{Sq}_2^{i+1})x^t &= \sum_{k=1}^{i+1} (\chi \mathrm{Sq}_2^{i+1-k}) \mathrm{Sq}_2^k x^t \\
&= \sum_{k=1}^{i+1} \binom{t+2k+3i+2-3k}{i+1-k} \binom{t}{k} x^{t+2i+2} \\
&= \sum_{k=1}^{t} \binom{t+3i+2-k}{t+2i+1} \binom{t}{k} x^{t+2i+2}
\end{aligned}$$

All the above computation is mod 2. Consider

$$\sum_{k=0}^{t} \binom{t}{k} (1+x)^{t+3i+2-k} = (1+1+x)^t (1+x)^{3i+2} = x^t (1+x)^{3i+2}.$$

The coefficient of x^{t+2i+1} on the right side is $\binom{3i+2}{2i+1} = \binom{3i+2}{i+1}$, which is 0 mod 2; but the coefficient on the left side is $\sum_{k=0}^{t} \binom{t+3i+2-k}{t+2i+1} \binom{t}{k}$, so we get

$$\binom{t+3i+2}{t+2i+1} = \sum_{k=1}^{t} \binom{t+3i+2-k}{t+2i+1} \binom{t}{k}.$$

Since $\binom{t+3i+2}{t+2i+1} = \binom{t+3i+2}{i+1}$, this shows

$$(\chi \mathrm{Sq}_2^{i+1})x^t = \binom{t+3i+2}{i+1} x^{t+2i+2}.$$

References

[1] M. Boardman, Modular representations on the homology of powers of real projective space, Contemporary Mathematics, Vol. 146, 1993.

[2] M. Kameko, Product of projective spaces as Steenrod modules, Ph.D. thesis, Johns Hopkins University, 1990.

[3] I. Kozma, Irreducibles in the Landweber-Novikov algebra, Proc. Amer. Math. Soc. 55(1976)453-456.

[4] F. Peterson, $\mathcal{A}$-generators for certain polynomial algebras, Math. Proc. Cambridge Philos. Soc. 105(1989)311-312.

[5] W. M. Singer, On the action of Steenrod squares on polynomial algebras, Proc. Amer. Math. Soc. 111(1991)577-583.

[6] R. M. W. Wood, Problems in the Steenrod algebra, Bull. London Math. Soc. 30(1998), 449-517.

[7] R. M. W. Wood, Steenrod squares of polynomials and the Peterson conjecture, Math. Proc. Cambridge Philos. Soc. 105(1989)307-309.

[8] R. M. W. Wood, Differential operators and the Steenrod algebra, Proc. London Math. Soc. 75 (1997)194-220.

[9] Suo Xiao, Ph.D. thesis, 1998, Manchester University.

Vitae

Hemin Yang was born in Sichuan province, P.R. China in Jan. 1970. He has spent 11 years in Nankai University, Tianjin, China. He began his graduate study in Johns Hopkins University in 1998.