ABSTRACT. Let $\chi$ be the canonical conjugation in the Steenrod algebra $\mathfrak{A}_2$. I prove the identity

$$Sq^{2n} + \chi(Sq^n) = Sq^{2n-1} \chi(Sq^{n-1})$$

and generalizations of this identity both in $\mathfrak{A}_2$ and in $\mathfrak{A}_p$ where $p$ is an odd prime.

The canonical conjugation $\chi$ in the mod 2 Steenrod algebra $\mathfrak{A}_2$ can be defined by Thom's recursion formula

$$\sum_{i=0}^{n} Sq^i \chi(Sq^{n-i}) = 0$$

together with the stipulation that $\chi: \mathfrak{A}_2 \to \mathfrak{A}_2$ be an anti-isomorphism [3]. Since the elements $Sq^{2n}$ multiplicatively generate $\mathfrak{A}_2$, we can calculate $\chi$ if we can calculate $\chi(Sq^{2n})$ for all $n$. The above recursion formula is unnecessarily cumbersome for this goal. In fact, the recursion can be shortened considerably by use of the following interesting

Identity. $Sq^{2n} + \chi(Sq^n) = Sq^{2n-1} \chi(Sq^{2n-1})$ for all positive integers $n$.

Applying the identity recursively we obtain the

Formula.

$$\chi(Sq^{2n}) = Sq^{2n} + \sum_{i=1}^{n-1} \left( \prod_{j=1}^{i} Sq^{2n-j} \right) Sq^{2n-i}.$$ 

For example,

$$\chi(Sq^{16}) = Sq^{16} + Sq^8 Sq^8 + Sq^8 Sq^4 Sq^4 + Sq^8 Sq^4 Sq^2 Sq^2.$$ 

In this paper, I will prove a theorem which will imply the above identity, and which also yields results about the mod $p$ Steenrod algebra $\mathfrak{A}_p$ when $p$ is an odd prime. The technique is to use Milnor's calculation of $\chi$ in the
Milnor basis for $\mathcal{G}_p$ [2], together with properties of binomial coefficients mod $p$. This technique was noticed independently by Donald Davis, who used it to prove other identities involving $\chi$ in $\mathcal{G}_p$ [1].

Let $p$ be a fixed prime. Let $R = (r_1, r_2, \ldots)$ be a sequence of non-negative integers with only a finite number of nonzero terms. For each such $R$ there is an element $\mathcal{P}^R$ in the Milnor basis for $\mathcal{G}_p$, of degree $\sum_{i \geq 1} 2(p^i - 1)r_i$ (if $p = 2$, the element is written $Sq^R$ and its degree is $\sum_{i \geq 1} (2^i - 1)r_i$). We define $|R| = \sum_{i \geq 1} p^{i-1}r_i$. Then Davis’ main proposition can be written.

**Proposition 1.** $\mathcal{P}^m \chi(\mathcal{P}^n) = (-1)^n \sum_{R \in \mathcal{P}} (\frac{|R|}{m})^R$ where the sum is taken over all $R$ such that $\mathcal{P}^R$ has the proper degree, i.e. over all $R$ such that

$$\sum_{i \geq 1} (p^i - 1)r_i = (p - 1)(m + n).$$

If $p = 2$, the only necessary modification is to write $Sq$ for $\mathcal{P}$. The binomial coefficient is, of course, to be interpreted mod $p$.

**Proof.** See [1]. □

The one additional fact about binomial coefficients which we will need is

**Proposition 2.** Let $a$ and $b$ be integers. If $p^a \leq r < p^ab$, then

$$\sum_{k=0}^{b} (-1)^k \binom{r}{p^ak} \equiv 0 \pmod{p}.$$

**Proof.** Write $r = p^as + t$, with $1 \leq s \leq b$ and $0 \leq t < p^a$.

Then

$$\binom{p^as + t}{p^ak} \equiv \binom{s}{k} \pmod{p},$$

as is easily seen by comparing the coefficients of $x^{p^ak}$ in the congruence

$$(1 + x)^{p^as + t} \equiv (1 + x^{p^a})^s(1 + x)^t \pmod{p}.$$

Hence the proposition follows from the well-known identity $\sum_{k=0}^{b} (-1)^k \binom{s}{k} = 0$ for $1 \leq s \leq b$. □

We can now prove our main

**Theorem.** Let $a \geq 0$ and $b > 1$ be integers. Then

$$\sum_{k=0}^{b} \mathcal{P}^{p^ak} \chi(\mathcal{P}^{p^a(b-k)}) = 0.$$

**Examples.** (1) If $a = 0$, we get Thom’s original recursion formula in $\mathcal{G}_p$.

(2) If $p = 2$, $a = n - 1$, $b = 2$, we get the identity at the beginning of this paper.
(3) If $p = 2$, $a = 2$, $b = 3$, we get
\[ \chi(Sq^{12}) + Sq^4\chi(Sq^8) + Sq^8\chi(Sq^4) + Sq^{12} = 0. \]

(4) If $p = 3$, $a = 2$, $b = 3$, we get
\[ \chi(P^{27}) + P^9\chi(P^{18}) + P^{18}\chi(P^9) + P^{27} = 0. \]

Proof of Theorem. Consider any $\beta = (\beta_1, \beta_2, \ldots)$ such that $\beta \geq 1$.

The coefficient of $\bar{P}^R$ in the Milnor base expansion of the sum in the Theorem is, by Proposition 1,
\[ \sum_{k=0}^{b} (-1)^b \bar{P}^{a(b-k)} \left( \frac{|R|}{p^{a_k}} \right) = (-1)^b \sum_{k=0}^{b} (-1)^k \left( \frac{|R|}{p^{a_k}} \right). \]

By Proposition 2, this coefficient is zero if $p^a \leq |R| \leq p^{ab}$. But (*) gives that
\[ |R| = \sum_{i \geq 1} p^{i-1} r_i = \frac{1}{p} \left[ (p - 1)p^{ab} + \sum_{i \geq 1} r_i \right] \]
and we also have
\[ 0 \leq \sum_{i \geq 1} r_i \leq \frac{1}{p - 1} \sum_{i \geq 1} (p^i - 1)r_i = p^ab. \]

Hence $((p - 1)/p)p^{ab} \leq |R| \leq p^{ab}$; and since $b > 1$, the required inequality holds. \(\Box\)

BIBLIOGRAPHY