Lemma 1. *Taken as elements of $L(k)_{-\infty}$ as a module over $\mathcal{A}(n) \otimes_{\mathcal{A}(n-k)} \mathbb{F}_2$, the set*

$$\{X_n X_{n-1} \cdots X_{n-k+1} \mathrm{Sq}^I \mid I = (2^{n+1} m_1, 2^n m_2, \ldots, 2^{n-k+2} m_k), m_1 \geq m_2 \geq \cdots \geq m_{n-k}\}$$

is linearly independent.

Proof. Note that by the commutation relation we have shown, the element $s = X_n X_{n-1} \cdots X_{n-k+1} \mathrm{Sq}^I$ may be rewritten as

$$X_n \mathrm{Sq}^{2^{n+1} m_1} X_{n-1} \mathrm{Sq}^{2^n m_2} \cdots X_{n-k+1} \mathrm{Sq}^{2^{n-k+2} m_k}.$$

Let $M_{k,n}$ be the subspace of $\mathcal{A}$ which is spanned by elements of the form yz where $y \in L(k)$ and $z \in \mathcal{A}(n)$ with the degree of z at least 1. If $b \in \mathcal{A}$, we will write $b + M_{k,n}$ for the subset of $\mathcal{A}$ consisting of elements of the form $b + m$ for $m \in M_{k,n}$.

Proposition 1. *The element*

$$X_n \mathrm{Sq}^{2^{n+1} m_n} X_{n-1} \mathrm{Sq}^{2^n m_{n-1}} \cdots X_{n-k+1} \mathrm{Sq}^{2^{n-k+2} m_{n-k+1}}$$

is in

$$\mathrm{Sq}^{2^{n+1}(m_n+n)+1} \mathrm{Sq}^{2^n(m_{n-1}+n-1)+1} \cdots \mathrm{Sq}^{2^{n-k+2}(m_{n-k+1}+n-k+1)+1} + M_{k,n-k}.$$

Proof. We proceed by induction on k for fixed n. If $k = 1$, we know that $X_n \in M_{1,n-1} + \mathrm{Sq}^{n2^{n+1}+1}$, since the latter term is the only element of $L(1)$ in the right dimension. Then since, as an $\mathcal{A}(n)$-module, $L(1)$ is periodic in degrees modulo 2^{n+1}, $X_n \mathrm{Sq}^{2^{n+1} m} \in M_{1,n-1} + \mathrm{Sq}^{2^{n+1}(n+m)+1}$.

Now suppose the proposition holds for some k; we will show it for $k+1$. Let

$$t = X_n \mathrm{Sq}^{2^{n+1} m_n} X_{n-1} \mathrm{Sq}^{2^n m_{n-1}} \cdots X_{n-k+1} \mathrm{Sq}^{2^{n-k+2} m_{n-k+1}},$$

let $t' = X_{n-k} \mathrm{Sq}^{2^{n-k+1} m_{n-k}}$, let

$$b = \mathrm{Sq}^{2^{n+1}(m_n+n)+1} \mathrm{Sq}^{2^n(m_{n-1}+n-1)+1} \cdots \mathrm{Sq}^{2^{n-k+2}(m_{n-k+1}+n-k+1)+1},$$

and let $b' = \mathrm{Sq}^{2^{n-k+1}(m_{n-k}+n-k)+1}$. Then by inductive hypothesis we know that $t \in b + M_{k,n-k}$ and by the base case we know that $t' \in b' + M_{1,n-k-1}$; we wish to show that $tt' \in bb' + M_{k+1,n-k-1}$. To do this, it suffices to show that $bM_{1,n-k-1}$ and $M_{k,n-k} t'$ are contained in $M_{k+1,n-k-1}$; for simplicity we will show that this is true of the spanning sets we have constructed.

First, let $y \in L(1)$, $z \in \mathcal{A}(n-k-1)$ with z not in degree 0, so that $yz \in M_{1,n-k-1}$. Then by looking at degrees, by is already in admissible form, so it is in $L(k+1)$, so $byz \in M_{k+1,n-k-1}$ as desired. Since elements of the form yz span $M_{1,n-k-1}$, we get that $bM_{1,n-k-1} \subset M_{k+1,n-k-1}$.

Second, let $y \in L(k)$, $z \in \mathcal{A}(n-k)$ with z not in degree 0, so that $yz \in M_{k,n-k}$. If $z \notin \mathcal{A}(n-k-1)$, then zX_{n-k} must be zero in $\mathcal{A}(n-k)$. Then we may assume $z \in \mathcal{A}(n-k-1)$; we will show that both yzb' and $yzM_{1,n-k-1}$ are contained in $M_{k+1,n-k-1}$. Now if we write zb' in admissible form, multiplying by y will give an element already in admissible form by looking at degrees, so we need only show that $zb' \in M_{1,n-k-1}$. If we multiply out using the Adem relations, this is clearly true, modulo showing that zb' contains no terms of length 1. This is easy to show; by the Milnor basis, z cannot end in a Steenrod square with degree a multiple of 2^{n-k}, but b' is a Steenrod square in a degree which is 1 modulo 2^{n-k}, so on multiplying the two, the length 1 term must vanish, as desired.

Finally, then, we must show that $yzM_{1,n-k-1} \subset M_{k+1,n-k-1}$; let $y' \in L(1)$ and $z' \in \mathcal{A}(n-k-1)$, so we must show that $yzy'z' \in M_{k+1,n-k-1}$. Again looking at the Adem relations, we may write zy' in the form $y''z''$ where $y'' \in L(1)$ and $z'' \in \mathcal{A}(n-k-1)$. Then $z''z' \in \mathcal{A}(n-k-1)$ and is not in degree zero, and $yy'' \in L(k+1)$, so $yy''z''z' \in M_{k+1,n-k-1}$.

Then the induction is complete; all terms of $tt' - bb'$ are in $M_{k+1,n-k-1}$ as desired. $\square$

Then since the elements in question may be written in the given form, their shortest terms are unique and distinct, so the terms are linearly independent. $\square$