The Steenrod squares via unordered joins

Abstract—**The Steenrod squares are cohomology operations with important applications in algebraic topology. While these operations are well-understood classically, little is known about them in the setting of homotopy type theory. Although a definition of the Steenrod squares was put forward by Brunerie (2017), proofs of their characterising properties have remained elusive. In this paper, we revisit Brunerie's definition and provide proofs of these properties, including stability, Cartan's formula and the Adem relations. This is done by studying a higher inductive type called the unordered join. This approach is inherently synthetic and, consequently, many of our proofs differ significantly from their classical counterparts. Along the way we discuss upshots and limitations of homotopy type theory as a synthetic language for homotopy theory. The paper is accompanied by a computer formalisation in Cubical Agda.**

I. Introduction

Homotopy type theory (HoTT) is an extension of Martin-Löf type theory based on the idea of treating treating *types* as ∞-groupoids, or *spaces*. While HoTT only gained attention as recently as 2012, ∞-groupoids themselves are important mathematical objects and have long been fruitfully studied using the many tools of algebraic topology and homotopy theory. A key question is to what extent these tools can be made to work with the language of HoTT, and whether HoTT can provide new insights going beyond classical homotopy theory. By now there is an established line of research, dubbed *synthetic homotopy theory*, dedicated to answering these questions. The promises of synthetic homotopy theory include conceptual clarity, semantic generality (an argument expressed in HoTT automatically applies in many models, including arbitrary ∞-topoi), and amenability to computer formalisation, but it also comes with its own set of limitations.

A fundamental tool in homotopy theory is that of *cohomology*, and a fundamental tool in making sense of cohomology is that of *cohomology operations*. These are ways of constructing new cohomology classes from old ones, and they give the cohomology of any space a rich structure. The purpose of this paper is to study an important family of a cohomology operations, the *Steenrod squares*, in homotopy type theory. Although a good deal of work has been done setting up the foundations of cohomology in synthetic homotopy theory, from Eilenberg–MacLane spaces [1], cohomology groups [2], cup products [3], [4], and cellular cohomology [5], to Gysin sequences [6] and spectral sequences [7], the Steenrod squares have so far only been *defined* in HoTT in a short text by Brunerie [8]. The Steenrod squares are classically known to satisfy a list of properties that are not easily read off form their definition but are important for applications, and these properties have remained elusive in synthetic homotopy theory. In this work we will prove all these properties.

We have computer formalised a large part of the project (including all key technical results) in `Cubical Agda`, a proof assistant implementing a flavour of HoTT called cubical type theory. We emphasise, however, that this paper is agnostic with respect to HoTT flavour and is written in the implementation agnostic informal style of the HoTT book [9].

Two themes feature prominently in this work. The first theme is that of constructions which depend on an arbitrary 2-element type [8], [10]. Here, a type is said to be a 2-element type if it *merely* is equivalent to the standard 2-element type $\mathbb{Z}/2\mathbb{Z}$ (i.e. $\{0,1\}$). We denote the type of all 2-element types by $\mathbb{R}P^\infty$. Any construction that depends on an arbitrary 2-element type (i.e. indexed by $\mathbb{R}P^\infty$) is automatically $\mathbb{Z}/2\mathbb{Z}$-equivariant, and in this way we get a synthetic approach to equivariant homotopy theory. The second theme is that of higher inductive types; of particular importance to us are joins and smash products. The meat of our work consists of studying the interaction of these two themes: unordered joins and smash products and their properties.

To set the stage and state the main result of this paper, let us briefly revisit the work of Brunerie. Brunerie defines the nth Steenrod square, a map $H^m(X,\mathbb{Z}/2\mathbb{Z}) \to H^{m+n}(X,\mathbb{Z}/2\mathbb{Z})$, directly on Eilenberg–MacLane spaces: in HoTT, elements of $H^m(X,\mathbb{Z}/2\mathbb{Z})$ are represented by functions $X \to K_m$ where $K_m :\equiv K(\mathbb{Z}/2\mathbb{Z}, m)$ denotes the mth Eilenberg–MacLane space of $\mathbb{Z}/2\mathbb{Z}$, and so the Steenrod square is given by a map $\mathsf{Sq}^n : K_m \to K_{m+n}$. This map is defined as a composition:

$$K_m \to (\mathbb{R}P^\infty \to K_{2m}) \xrightarrow{\sim} \Pi_{i\leq 2m} K_i \xrightarrow{\mathsf{proj}_{m+n}} K_{m+n}. \quad (1)$$

Here the first map is defined using *unordered smash products*, and the second equivalence comes from the Thom isomorphism theorem. While this construction is elegant, it has turned out to be difficult to analyse. In particular, one would like to know that the Steenrod squares satisfy the properties listed below; proving these is the primary contribution of this paper.

Theorem 1 (The Steenrod squares, axiomatically)**.** *There is a set of pointed maps $\mathsf{Sq}^n : K_m \to_{\mathsf{pt}} K_{m+n}$ for $m,n \geq 0$, called the Steenrod squares, which satisfy the following identities.*

(I1) $\mathsf{Sq}^0(x) = x$

(I2) $\mathsf{Sq}^n(x) = 0$ *if* $n > m$

(I3) $\mathsf{Sq}^n(x) = x \smile x$ *if* $n = m$

(C) $\mathsf{Sq}^n(x \smile y) = \sum_{i+j=n} \mathsf{Sq}^i(x) \smile \mathsf{Sq}^j(y)$ *(the Cartan formula)*

In addition, the squares are stable and satisfy the Adem relations:

(Ω) *The nth square $\mathsf{Sq}^n : K_m \to_{\mathsf{pt}} K_{m+n}$ is also given by*

$$K_m \xrightarrow{\sim} \Omega(K_{m+1}) \xrightarrow{\Omega(\mathsf{Sq}^n)} \Omega(K_{(m+1)+n}) \xrightarrow{\sim} K_{m+n}.$$

(A) *The Adem relations are satisfied: for $n < 2k$, we have*

$$\mathsf{Sq}^n \circ \mathsf{Sq}^k = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{k-i-1}{n-2i} \mathsf{Sq}^{n+k-i} \circ \mathsf{Sq}^i.$$

A. Contributions and outline

The main contribution of this paper is a proof of the properties of Steenrod squares listed in Theorem 1. Before discussing Steenrod squares, in Section II we discuss some background material about $\mathbb{R}P^\infty$ and unordered pairs. Then in Section III we present a variant of Brunerie's definition of the Steenrod squares, via what we call unordered cup products. We prove all the properties of Steenrod squares listed in Theorem 1, modulo technicalities dealt with in later sections. In Section IV we discuss the easier of these technicalities, needed to prove that $\mathsf{Sq}^0(x) = x$. Section V concerns properties of unordered HITs and constitutes the technical core of this paper. In Section VI we discuss how a good theory of E_∞-monoids in type theory would have significantly simplified our work. In Section VII we showcase an application of Steenrod squares toward analysing $\pi_4(\mathbb{S}^3)$. Finally in Section VIII we mention some open questions.

B. Notation and basic definitions

Let us briefly introduce some notation while also recalling some basic constructions from HoTT which will be used in the paper. The reader familiar with HoTT should be able to safely skim or even skip this part.

a) Pi- and sigma-types: Let $B : A \to \mathcal{U}$ be a dependent type – here $\mathcal{U}$ denotes the universe of types (at some implicit universe level). We often use the notation $(a : A) \to B\,a$ and $(a : A) \times B\,a$ for $\Pi_{a:A} B(a)$ and $\Sigma_{a:A} B(a)$ respectively. We may sometimes write B^A for the non-dependent function type $A \to B$.

b) Equality: We write $x = y$ for the type of paths from x to y. We use $x :\equiv y$ for definitions. The constant path (reflexivity) is denoted by $\mathsf{refl}_x : x = x$. We use *path induction* to refer to the usual induction principle for identity types in MLTT.

c) Equivalences and univalence: A type X is said to be *contractible* if there is some $x : X$ s.t. for all $x' : X$, we have that $x' = x$. Given a map $f : A \to B$ we define its fibre over some point $b : B$ by $\mathsf{fib}_f(b) :\equiv (a : A) \times (f(a) = b)$. We say that f is an equivalence if $\mathsf{fib}_f(b)$ is contractible for each $b : B$. In this case, we simply write $f : A \simeq B$ and leave the contractibility proof implicit.

There is a canonical map $\mathsf{coe} : X = Y \to X \simeq Y$ defined by path induction, sending refl_X to the identity $\mathsf{id}_X : X \simeq X$. The univalence axiom says that coe itself is an equivalence. In particular, this means that if two types are equivalent, then they are equal.

d) Pointed structures: A pointed type (A, pt_A), i.e. a type A equipped with a basepoint $a_0 : A$, will often simply be written A, i.e. with the basepoint left implicit. We use the same convention for pointed functions and simply write $f : A \to_{\mathsf{pt}} B$ to mean a pair (f, pt_f) where $f : A \to B$ is a plain function and $\mathsf{pt}_f : f(\mathsf{pt}_A) = \mathsf{pt}_B$ is a proof that f is basepoint preserving.

e) Loop spaces: We define the *loop space* of a pointed type A by $\Omega(A) :\equiv (\mathsf{pt}_A = \mathsf{pt}_A)$. This construction is itself pointed by $\mathsf{refl}_{\mathsf{pt}_A}$ and can thus be iterated by inductively defining $\Omega^{n+1}(A) :\equiv \Omega^n(\Omega(A))$.

f) H-levels: We say that a type A is a (-2)*-type* if it is contractible and, inductively, that it is an n-type if $x = y$ is an $(n-1)$ type for all $x, y : A$. Apart from (-2)-types, special names are also given to (-1)-types and 0-types; these are, respectively, called *propositions* and *sets*.

g) Truncations: We write $\|A\|_n$ for the *n-truncation of A*, the canonical way of forcing A to become an n-type. This is a type equipped with an inclusion of points $|-| : A \to \|A\|_n$ whose induction principle say that the map $((x : \|A\|_n) \to B(x)) \to ((a : A) \to B\,|a|)$ is an equivalence whenever $B : \|A\|_n \to \mathcal{U}$ is a family of n-types. It is implemented using a recursive HIT [9, Section 7.3], but we do not need the implementation details here.

h) Connectedness: We say that a type is n-connected if $\|A\|_n$ is contractible. We say that a function $f : A \to B$ is n-connected if all of its fibres are n-connected.

i) Pushouts: Given a span $Y \xleftarrow{f} X \xrightarrow{g} Z$, we define its (homotopy) pushout, $Y \sqcup^X Z$, to be the HIT generated by two point constructors $\mathsf{inl} : Y \to Y \sqcup^X Z$ and $\mathsf{inr} : Z \to Y \sqcup^X Z$, as well as one higher constructor $\mathsf{push} : (x : X) \to \mathsf{inl}(f\,x) = \mathsf{inr}(g, x)$. An important special case of pushouts is the *suspension* of a type X, written ΣX, which we define by $\Sigma X :\equiv \mathbb{1} \sqcup^X \mathbb{1}$. Another important construction is the *smash product* of two pointed types, denoted $X \wedge Y$. We define it here as the pushout $(\mathbb{1} + \mathbb{1}) \sqcup^{X+Y} X \times Y$. We write $\langle x, y \rangle$ for $\mathsf{inr}(x, y)$. We take all pushouts to by pointed, whenever possible, by $\mathsf{inl}(\mathsf{pt})$.

j) Eilenberg–MacLane spaces and cohomology: Given an abelian group G and a natural number n, we denote by $K(G, n)$ the nth *Eilenberg–MacLane space*, or *delooping*, of G [1]. It is characterised as the unique pointed $(n-1)$-connected n-type whose nth loop space $\Omega^n K(G, n)$ is isomorphic, as a group, to G. It follows that we have pointed equivalences $\sigma_n : K(G, n) \simeq \Omega K(G, n+1)$. In this way it is clear that $K(G, n)$ has an associative and commutative H-space structure (corresponding to path composition in $\Omega K(G, n+1)$), denoted $+ : K(G, n) \to K(G, n) \to K(G, n)$. If moreover G is a ring then we have a *cup product* $\smile : K(G, n) \to K(G, m) \to K(G, n+m)$ which is graded-commutative and associative.

The nth cohomology group of a type X with coefficients in an abelian group G is given by $H^n(X, G) :\equiv \|X \to K(G, n)\|_0$. The types $H^\bullet(X, G)$ are abelian groups by pointwise addition in $K(G, n)$, and moreover form a graded ring if G has the structure of a ring.

II. Unordered pairs and commutativity structures

One of the main themes in this paper, crucial for the treatment of Steenrod squares, is that of constructions that depend on 2-element type. We will write $\mathbb{Z}/2\mathbb{Z}$ for the standard 2-element type, with two distinct elements 0 and 1. A general type X is said to be a 2-element type if we have $\|X \simeq \mathbb{Z}/2\mathbb{Z}\|$. Thus any 2-element type is merely equivalent to $\mathbb{Z}/2\mathbb{Z}$, but it has no preferred enumeration. We write $\mathbb{R}P^\infty$ for the type of all 2-element types, or more explicitly

$$\mathbb{R}P^\infty :\equiv (X : \mathcal{U}) \times \|X \simeq \mathbb{Z}/2\mathbb{Z}\|.$$

We treat $\mathbb{R}P^\infty$ as a pointed type with basepoint $(\mathbb{Z}/2\mathbb{Z}, |\mathsf{id}_{\mathbb{Z}/2\mathbb{Z}}|)$. Buchholtz and Rijke [11] have shown that $\mathbb{R}P^\infty$ is the sequential colimit of the finite-dimensional real projective spaces $\mathbb{R}P^n$, hence the notation. Given a term $X : \mathbb{R}P^\infty$ we will conflate X with its underlying type $\mathsf{fst}(X) : \mathcal{U}$.

For us, $\mathbb{R}P^\infty$ is significant because it captures the idea of commutativity in a synthetic and homotopy coherent manner. Consider for example the symmetry of cartesian products, $A_0 \times A_1 \simeq A_1 \times A_0$. This can be explained as followed using $\mathbb{R}P^\infty$. The binary cartesian product can be seen as a $\mathbb{Z}/2\mathbb{Z}$-indexed dependent product, $\Pi_{i:\mathbb{Z}/2\mathbb{Z}}A(i)$ for $A : \mathbb{Z}/2\mathbb{Z} \to \mathcal{U}$. More generally, for any $X : \mathbb{R}P^\infty$ and $A : X \to \mathcal{U}$, we can consider the product $\Pi_{i:X}A(i)$. Clearly this reduces to the binary cartesian product if X is $\mathbb{Z}/2\mathbb{Z}$. Now $\mathbb{Z}/2\mathbb{Z}$ has a self-equivalence $\neg : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ which swaps 0 and 1, and by univalence this induces a loop $\mathsf{pt} = \mathsf{pt}$ of the corresponding basepoint of $\mathbb{Z}/2\mathbb{Z}$. By action on paths, this induces an equivalence $\Pi_{i:\mathbb{Z}/2\mathbb{Z}}A(i) \simeq \Pi_{i:\mathbb{Z}/2\mathbb{Z}}A(\neg i)$ for any $A : \mathbb{Z}/2\mathbb{Z} \to \mathcal{U}$, which reduces to commutativity of the cartesian product.

In general our usage of $\mathbb{R}P^\infty$ follows the same pattern. The point is to first generalise some construction which normally would operate on ordered pairs – like the cartesian product $A_0 \times A_1$ computed from the pair $(A_0, A_1) : \mathcal{U} \times \mathcal{U}$ – to a construction that depends on some 'unordered pair'. By an unordered pair (of elements of A), we mean a map $a : X \to A$ where $X : \mathbb{R}P^\infty$ and A is some arbitrary type. We often write A^X to emphasise that it should be thought of as a generalisation of A^2 – one might also say that A^X is a 'twisted' version of A^2.

The upshot is that whenever we write down a construction indexed by $\mathbb{R}P^\infty$, we automatically gain information about the symmetry of said construction. In the case of the cartesian product, this gives rise to the equivalence $\mathsf{swap}_{A_0,A_1} : A_0 \times A_1$, but this is not all. The fact that the self-equivalence $\neg : \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$ is involutive tells us that $\mathsf{swap}_{A_1,A_0} \circ \mathsf{swap}_{A_0,A_1} = \mathsf{id}$. This is only the start of an infinite tower of coherences, associated with the cell decomposition of $\mathbb{R}P^\infty$. The upshot of the synthetic approach is that we do not need to think explicitly about these coherences.

A. Basic facts about $\mathbb{R}P^\infty$

Let us now recall some elementary lemmas and constructions regarding $\mathbb{R}P^\infty$ and unordered pairs. The following lemma is a special case of a result due to Kraus [12, Proposition 8.1.2.] and the remaining ones can be found in Buchholtz and Rijke [11].

Lemma 2. *For $P : \mathbb{R}P^\infty \to \mathcal{U}$, the type of functions $(X : \mathbb{R}P^\infty) \to P(X)$ is equivalent to*

(a) $P(\mathbb{Z}/2\mathbb{Z})$ if P is proposition-valued.
(b) $(t : P(\mathbb{Z}/2\mathbb{Z})) \times (P(\neg)(t) = t)$ if P is set-valued.

Lemma 3. *All types $X : \mathbb{R}P^\infty$ are sets.*

Lemma 4. *For any $X : \mathbb{R}P^\infty$, there is an involution $\neg : X \simeq X$ agreeing with the usual $\mathbb{Z}/2\mathbb{Z}$-involution whenever $X :\equiv \mathbb{Z}/2\mathbb{Z}$.*

Although this lemma/definition is well-known, its proof illustrates a useful technique for defining operations over $\mathbb{R}P^\infty$, we we choose to include it.

Proof/construction of Lemma 4. For any $X : \mathbb{R}P^\infty$, consider the type $P(X) :\equiv (e : X \to X)((e \circ e = \mathsf{id}) \times e \neq \mathsf{id}_X)$. We claim that this type is contractible. Since this claim is a proposition, it suffices by Lemma 2 to show that $P(\mathbb{Z}/2\mathbb{Z})$ is contractible. This is trivial, as $P(\mathbb{Z}/2\mathbb{Z})$ is the type of non-identity involutions on $\mathbb{Z}/2\mathbb{Z}$ – a type uniquely pointed by $\mathbb{Z}/2\mathbb{Z}$-involution. So, $P(X)$ is contractible for any $X : \mathbb{R}P^\infty$ and we define $\neg$ to be the centre of contraction. □

Using Lemma 4, we may construct, for any $X : \mathbb{R}P^\infty$ and $x : X$, an equivalence $e^x : \mathbb{Z}/2\mathbb{Z} \simeq X$ defined by setting

$$e^x(0) :\equiv x \qquad e^x(1) := \neg x$$

To prove that this indeed is an equivalence, we note that this statement is a proposition and thus, by Lemma 2, it suffices to do so when X is $\mathbb{Z}/2\mathbb{Z}$. By case-splitting on $x : \mathbb{Z}/2\mathbb{Z}$, we see that the e^x is the identity when $x = 0$ and involution when $x = 1$. In particular, it is an equivalence. In fact, not only is e^x always an equivalence – the map $e^{(-)}$ is one itself:

Lemma 5. *For any $X : \mathbb{R}P^\infty$, the map $e^{(-)} : X \to (\mathbb{Z}/2\mathbb{Z} \simeq X)$ is an equivalence.*

Proof. The statement is a proposition, and thus it suffices to show it when $X = \mathbb{Z}/2\mathbb{Z}$. In this case, $e^{(-)}$ is the map sending 0 to the identity on $\mathbb{Z}/2\mathbb{Z}$ and sending 1 to the involution. As these are precisely the (two) $\mathbb{Z}/2\mathbb{Z}$-automorphisms, $e^{(-)}$ is clearly invertible and thus an equivalence. □

By univalence, Lemma 5 gives a characterisation of the based path types on $\mathbb{R}P^\infty$: it tells us that any based path type $(\mathsf{pt}_{\mathbb{R}P^\infty} = X)$ equivalent to the 'point' X itself. In particular, we get that unordered pairs (A^X) really corresponds to fibrations over the based path types of $\mathbb{R}P^\infty$, i.e. $(\mathsf{pt}_{\mathbb{R}P^\infty} = X \to A)$. This gives us a new way of interpreting path induction for $\mathbb{R}P^\infty$:

Lemma 6. *Let $A : (X : \mathbb{R}P^\infty) \times X \to \mathcal{U}$. Then the map*

$$(((X, x) : (\dots)) \to A(X, x)) \xrightarrow{f \mapsto f(\mathbb{Z}/2\mathbb{Z}, 0)} A(\mathbb{Z}/2\mathbb{Z}, 0)$$

is an equivalence.

Another way of understanding this is by the following induction rule for functions defined over $X : \mathbb{R}P^\infty$.

Lemma 7. *Let $X : \mathbb{R}P^\infty$, $B : X \to \mathcal{U}$ and $x : X$. Any pair of points $b_0 : B(x)$ and $b_1 : B(\neg x)$ induces a function*

$$\mathsf{Elim}^{x \mapsto b_0}_{\neg x \mapsto b_1} : (x : X) \to B(x)$$

satisfying $\mathsf{Elim}^{x\mapsto b_0}_{\neg x\mapsto b_1}(x) = b_0$ *and* $\mathsf{Elim}^{x\mapsto b_0}_{\neg x\mapsto b_1}(\neg x) = b_1$. *In fact, the map* $B(x) \times B(\neg x) \xrightarrow{(b_0,b_1)\mapsto \mathsf{Elim}^{x\mapsto b_0}_{\neg x\mapsto b_1}} \Pi_{x:X} B(x)$ *is an equivalence.*

B. Commutativity Structures

As discussed, significance of unordered pairs is that they allow us to capture the idea of an operation being homotopy commutative in an 'infinitely coherent' manner. This is captured by the following definition.

Definition 8 (Brunerie [8]). A *commutativity structure* for a binary operation $\diamond : A \times A \to B$ is a family of maps $\diamond_X : A^X \to B$ for each $X : \mathbb{R}P^\infty$ agreeing with $\diamond$ whenever $X = \mathbb{Z}/2\mathbb{Z}$.

By letting A and B be an Eilenberg-MacLane spaces in the above definition, a commutativity structure $\diamond_{(-)}$ will allow us to produce a cohomology classes in $H^*(\mathbb{R}P^\infty)$. Brunerie's construction of the Steenrod squares boils down to showing that the cup product $\smile : K_n \times K_n \to K_{2n}$ has a commutativity structure. Before we get there, however, let us give the following example in order to illustrate the general idea of how commutativity structures can be constructed. In fact, the following construction will be useful in its own right.

Example 9. For any commutative monoid $(M, +, 0)$, addition $+ : M \times M \to M$ has a commutativity structure. Since M is a monoid, it is a set and thus the type of maps $M^X \to M$ is a set for any X. We will define the commutativity structure, denoted by $\Sigma : M^X \to M$ for $X : \mathbb{R}P^\infty$, using Lemma 2(b). For $X :\equiv \mathbb{Z}/2\mathbb{Z}$, we define $\Sigma(f) := f(0)+f(1)$. We then need to check that this definition is invariant under $\mathbb{Z}/2\mathbb{Z}$-inversion. This corresponds to checking that $f(0) + f(1) = f(1) + f(0)$ which of course follows from commutativity of M.

The construction in Example 9 crucially relied on M being a set; when constructing commutativity structures in general, there are not that many other methods than this at hand. Fortunately, this argument can sometimes still be used in cases when the h-level of the type of commutativity structures is not 0.

Example 10. Addition on Eilenberg-MacLane spaces $+ : K_n \times K_n \to K_n$ has a commutativity structure. To see why, we consider the the the family of dependent types $P_X : (K_n^X \to K_n) \to \mathcal{U}$ defined by $P_X(f) :\equiv (f(\lambda x\,.0) = 0)$. We have

$$(f : K_n \times K_n \to K_n)(P_{\mathbb{Z}/2\mathbb{Z}}(f)) := (K_n \times K_n \to_{\mathsf{pt}} K_n)$$

which is a set [13, Corollary 9]. This means that Lemma 2(b) applies. It thus suffices to provide an element of $P_{\mathbb{Z}/2\mathbb{Z}}(+)$ and check that this choice is invariant w.r.t $\mathbb{Z}/2\mathbb{Z}$ involution. This boils down to verifying the commutativity of $+$.

This idea of defining a predicate over the function type of interest which forces it to become a set is present also in Brunerie's original definition of a commutativity structure for the cup product. Although he does not state it exactly this way, Brunerie implicitly considers the following predicate.

Definition 11. Let $X : \mathbb{R}P^\infty$, $A : X \to \mathcal{U}_{\mathsf{pt}}$ and $B : \mathcal{U}_{\mathsf{pt}}$, and $f : (\prod_{x:X} A(X)) \to B$. We define $\mathsf{isBiHom}_X(f) : \mathcal{U}$ to be the following type expressing that f is 'pointed in each argument':

$$(f(\lambda\, x\,.\,\mathsf{pt}) = \mathsf{pt}) \times (\mathsf{pts} : B^X)$$
$$\times \left(\left(a : \prod_{x:X} A(x)\right)(x : X) \to (a(x) = \mathsf{pt}) \to f(a) = \mathsf{pts}(x)\right)$$

We write $\mathsf{BiHom}_X(A, B)$ for $(f : \prod_{x:X} A(x) \to B) \times \mathsf{isBiHom}_X(f)$.

A straightforward rewriting shows that, for any proof of $\mathsf{isBiHom}_X(f)$, its pts component is constantly $\mathsf{pt} : B$, and we have

$$(f : A_0 \times A_1 \to B) \times \mathsf{isBiHom}_{\mathbb{Z}/2\mathbb{Z}}(f) \simeq (A_0 \wedge A_1 \to_{\mathsf{pt}} B).$$

By setting $A(x) = K_n$ and $B = K_{2n}$ in Definition 11, $\mathsf{isBiHom}_X$ is a predicate on the function type $K_n \times K_n \to K_{2n}$. Let us construct such a function. The key observation is that the type of such functions is equivalent to $K_n \wedge K_n \to_{\mathsf{pt}} K_{2n}$ whenever $X = \mathbb{Z}/2\mathbb{Z}$. This turns out to be a set [13, Corollary 9] and thus, the type of such function is a set for any $X : \mathbb{R}P^\infty$. Like in Examples 9 and 10, it is enough to give the construction when $X = \mathbb{Z}/2\mathbb{Z}$ and check that it commutative. Since the cup with coefficients mod 2 is commutative, it has a commutativity structure,.

This concludes (our take on) Brunerie's definition of the commutativity structure on the cup product. While it is certainly sufficient to construct the Steenrod squares, it has turned out to be rather hard to reason about. One simple but crucial reason for this is that Brunerie's definition does not quite capture a key fact about the cup product, namely that it is *graded*. The main issue we have is that our notion of a commutativity structure which does not allow for dependent types. To remedy this, we propose the following definition.

Definition 12. Let $A : I \to \mathcal{U}$ be a family of types where I is a commutative monoid (e.g. $I = \mathbb{N}$). A graded commutativity structure for a graded operation $\diamond : A_i \times A_j \to A_{i+j}$ is a family of maps $\diamond_{X,n} : (\Pi_{x:X} A_{n(x)}) \to A_{\Sigma n}$ for each $X : \mathbb{R}P^\infty$ and $n : X \to I$, which reduces to $\diamond$ for $X :\equiv \mathbb{Z}/2\mathbb{Z}$.

Remark 13. Since we work modulo 2 throughout, we have no reason to worry about the signs that normally show up when discussing graded commutativity of e.g the cup product, but let us make a comment about how they can be dealt with. For a group G and a finite type $\mathbf{n}$ of n elements, one can define a pointed type $K(G, \mathbf{n})$, which is like $K(G, n)$ but with a 'twist' relating odd permutations of $\mathbf{n}$ with the involution of $K(G, n)$ given by negation. If G then is a commutative ring, the corresponding graded commutativity structure on $K(G, -)$ would be given by maps $\Pi_{x:X} K(G, \mathbf{n}(x)) \to K(G, \sum_{x:X} \mathbf{n}(x))$ for $X : \mathbb{R}P^\infty$ and $\mathbf{n} : X \to \mathcal{U}$ a family of finite types. The key here is to index not by $\mathbb{N}$ but by the type of finite sets, or some other higher type which records information about twists.

Our construction of the commutativity structure on the cup product can be restated, word by word, to equip it with a graded commutativity structure. This slight generalisation of Brunerie's definition will be the one used in this paper. For this reason, let us finish this section by giving it a name.

Definition 14. The cup product has graded commutativity structure which we will refer to as the **unordered cup product**. For $X : \mathbb{R}P^\infty$, $n : X \to \mathbb{N}$ and $f : (x : X) \to K_{n(x)}$, we denote it by $\smile_{x:X} f(x) : K_{\Sigma n}$.

III. The Steenrod squares

We are now well-prepared to define the Steenrod squares. We follow Brunerie's approach, as laid out in (1). That is, we need to define two maps: one of type $K_m \to (\mathbb{R}P^\infty \to K_{2m})$ and one (equivalence) of type $(\mathbb{R}P^\infty \to K_{2m}) \to \prod_{i\leq 2m} K_i$. Let us start with the first map. Suppose we are given $a : K_m$ and $X : \mathbb{R}P^\infty$. We let $n : X \to \mathbb{N}$ and $\widehat{a} : (x : X) \to K_{n(x)}$ be the constant functions $n(x) :\equiv m$ and $\widehat{a}(x) := a$. We may now define $a^X : K_{2m}$ by

$$a^X :\equiv \smile_{x:X} \widehat{a}(x). \tag{2}$$

The notation is meant to suggest that we think of a^X as the cup product of X-many copies of a; traditionally this may also be written as $S(a, X)$.

The second map is given by the inverse equivalence in the following lemma.

Lemma 15. *For $n : \mathbb{N}$, we have an equivalence*

$$\mathsf{Gys}_n : \prod_{i\leq n} K_i \simeq (\mathbb{R}P^\infty \to K_n)$$
$$\mathsf{Gys}_n(b_0, \dots, b_n) :\equiv X \mapsto \sum_{i=0}^{n} b_i \smile t(X)^{n-i}.$$

Here t denotes the unique pointed equivalence $\mathbb{R}P^\infty \to K_1$, and $t(X)^{n-i}$ denotes iterated cup product of $t(X)$ with itself. One can think of Lemma 15 as describing the mod 2 cohomology of $\mathbb{R}P^\infty$, but more directly it says that every map $\mathbb{R}P^\infty \to K_n$ has a unique 'polynomial' representation. Before proving Lemma 15, we first have to state two simpler lemmas.

Lemma 16. *For $n : \mathbb{N}$, we have an equivalence*

$$(\mathbb{R}P^\infty \to K_n) \simeq (\mathbb{R}P^\infty \to_{\mathsf{pt}} K_{n+1})$$
$$f \mapsto X \mapsto t(X) \smile f(X)$$

Lemma 16 is proved using the Thom isomorphism [6, Section 6.1]. For details, see [4, Section 5.5].

Lemma 17. *For any invertible H-space B and pointed A, we have an equivalence*

$$B \times (A \to_{\mathsf{pt}} B) \simeq A \to B$$
$$(b, f) \mapsto a \mapsto b + f(a)$$

Proof. We have

$$\begin{aligned} B \times (A \to_{\mathsf{pt}} B) &\simeq (b : B) \times (A \to_{\mathsf{pt}} (B, b)) \\ &\simeq (f : A \to B) \times (b : B) \times (f(a) = b) \\ &\simeq (A \to B) \end{aligned}$$

where the first step comes from the fact that B is an H-space (and hence homogeneous) and the second is contractibility of singletons. This equivalence agrees with the proposed one by construction. ☐

We are now ready to prove Lemma 15.

Proof of Lemma 15. By induction. For $n = 0$ this is simply the statement that any map $\mathbb{R}P^\infty \to K_0$ is constant, which follows from connectedness of $\mathbb{R}P^\infty$. Now suppose the lemma holds for some $n \geq 0$. Then

$$\begin{aligned} \Pi_{i\leq n+1} K_i &\simeq K_{n+1} \times \Pi_{i\leq n} \\ &\simeq K_{n+1} \times (\mathbb{R}P^\infty \to K_n) \\ &\simeq K_{n+1} \times (\mathbb{R}P^\infty \to_{\mathsf{pt}} K_{n+1}) \\ &\simeq \mathbb{R}P^\infty \to K_{n+1}. \end{aligned}$$

Here the second line is by inductive hypothesis, the third by Lemma 16, and the final line is by Lemma 17. It is direct to see that the forward composite is the desired one. ☐

Finally, we are ready to define the Steenrod squares.

Definition 18 (Steenrod squares)**.** We define the total square $\widehat{\mathsf{Sq}} : K_m \to \prod_{i\leq 2m} K_i$ by $\widehat{\mathsf{Sq}}(a) :\equiv \mathsf{Gys}_{2m}^{-1}(a^{(-)})$.We define the nth Steenrod square $\mathsf{Sq}^n : K_m \to K_{m+n}$ by

$$\mathsf{Sq}^n(a) :\equiv \begin{cases} \mathsf{proj}_{m+n}(\widehat{\mathsf{Sq}}(a)) & \text{if } n \leq m \\ 0 & \text{otherwise} \end{cases}$$

Unpacking the definition, we get the following characterisation of $\mathsf{Sq}^n(a)$ for a given $a : K_m$: they are the unique collection of terms such that for every $X : \mathbb{R}P^\infty$ we have[1]

$$a^X = \sum_{i=0}^{m} \mathsf{Sq}^m(a) \smile t(X)^{m-i}. \tag{3}$$

Note that (I2) holds by construction with this definition of Sq^n.

A. Proving the main theorem

Now that we have a definition of the Steenrod squares (following Brunerie), in this section we work our way towards a proof of Theorem 1. The idea is to use Equation (3) to reduce properties of Sq^n to properties of $(-)^X$, and hence of the unordered cup product. The following is a simple example.

Lemma 19. *The Steenrod squares are pointed, i.e.* $\mathsf{Sq}^n(0) = 0$.

Proof. We have $0^X = 0$ for any $X : \mathbb{R}P^\infty$ since the unordered cup product is a bihom by construction. Thus Equation (3)

[1]Formally we should include terms i from 0 to $2m$ in the equation. But the corresponding maps $\mathsf{Sq}^n : K_m \to K_{m+n}$ with $n < 0$ are zero for connectedness reasons; they are pointed by Lemma 19.

gives $0 = \sum_{i=0}^{n} \mathsf{Sq}^n(a) \smile t(X)^{n-i}$ for all $X : \mathbb{R}P^\infty$. By Lemma 15, we must have $\mathsf{Sq}^n(a) = 0$ for all n. $\square$

Perhaps more interestingly, the Cartan formula is equivalent to the following innocuous equation:

$$(a \smile b)^X = a^X \smile b^X. \tag{4}$$

We will prove the above equation via the following generalisation, which can be thought of as a type of Fubini interchange law and will also give rise to the Adem relations.

Theorem 20. *For any $X, Y : \mathbb{R}P^\infty$, $n : X \times Y \to \mathbb{N}$ and $f : \prod_{x:X} \prod_{y:Y} K_{n(x,y)}$, we have*

$$\smile_{x:X} \smile_{y:Y} f(x,y) = \smile_{y:Y} \smile_{x:X} f(x,y).$$

While easy to state, proving Theorem 20 is far more difficult than anything we have done so far. Its proof, which we assume for now but which will be discussed at length later in the paper, forces us develop the theory of unordered joins and constitutes the technical core of this paper. Before we are faced with reality, let us reap its fruits prematurely and prove the characterising properties of the Steenrod squares laid out in Theorem 1.

Proposition 21. *The Steenrod squares satisfy the Cartan formula (C).*

Proof. Consider Theorem 20 in these case where Y is $\mathbb{Z}/2\mathbb{Z}$, and n, f depend only their second arguments, so that they are given simply by $i, j : \mathbb{N}$ and $a : K_i$, $b : K_j$. In this case $\mathbb{Z}/2\mathbb{Z}$-indexed 'unordered' cup product reduces to the ordinary cup product, and the X-indexed cup product reduces to $(-)^X$, so that we end up with Equation (4), $(a \smile b)^X = a^X \smile b^X$. Combined with Equation (3), this gives the following:

$$\begin{aligned}
&\sum_{k=0}^{i+j} \mathsf{Sq}^k(a \smile b) \smile t(X)^{i+j-k} \\
&= \left(\sum_{l=0}^{i} \mathsf{Sq}^l(a) \smile t(X)^{i-l} \right) \smile \left(\sum_{m=0}^{h} \mathsf{Sq}^m(b) \smile t(X)^{j-m} \right) \\
&= \sum_{l=0}^{i} \sum_{m=0}^{j} \mathsf{Sq}^l(a) \smile \mathsf{Sq}^m(b) \smile t(X)^{i+j-l-m}.
\end{aligned}$$

Since, for given a, b, the above identity holds in $K_{2(i+j)}$ for *all* $X : \mathbb{R}P^\infty$, we may by Lemma 15 formally identify coefficients of the polynomials. This concludes the proof. $\square$

Proposition 22. *The Steenrod squares satisfy (I3): for $x : K_n$ we have $\mathsf{Sq}^n(x) = x \smile x$.*

Proof. Taking X to be $\mathbb{Z}/2\mathbb{Z}$ in Equation (3), we have $t(X) = 0$ and so only term in the sum remains: $a^{\mathbb{Z}/2\mathbb{Z}} = \mathsf{Sq}^n(a)$. We have $a^{\mathbb{Z}/2\mathbb{Z}} = a^2$ since the unordered cup product generalises the ordinary cup product. This concludes the proof. $\square$

An important fact about Steenrod squares not listed in Theorem 1 is that they are additive: $\mathsf{Sq}^n(a+b) = \mathsf{Sq}^n(a) + \mathsf{Sq}^n(b)$. This is a consequence of (Ω), essentially because the action of any function on paths respects path composition. But there is also a more direct proof.

Lemma 23. *The Steenrod squares are additive: for $a, b : K_m$ we have $\mathsf{Sq}^n(a+b) = \mathsf{Sq}^n(a) + \mathsf{Sq}^n(b)$.*

Proof. By Equation (3), it suffices to prove that $(a+b)^X = a^X + b^X$. In fact one can show a stronger statement, that $(-)^X : K_m \to K_{2m}$ has a unique delooping. Since this is a proposition, we may suppose that X is $\mathbb{Z}/2\mathbb{Z}$, i.e. it suffices to show that $(-)^2 : K_m \to K_{2m}$ has a unique delooping. By [14, Corollary 12], the delooping is unique if it exists, and it exists if and only if $(a+b)^2 = a^2 + b^2$. This holds by distributivity and commutativity since we are working mod 2. $\square$

Remark 24. Related to Lemma 23, we remark that an alternative, simpler definition of Sq^n is possible. The stability axiom Theorem 1 tells us that the map $\mathsf{Sq}^n : K_m \to_{\mathrm{pt}} K_{m+n}$ should be a delooping of $\mathsf{Sq}^n : K_{m-1} \to_{\mathrm{pt}} K_{m+n-1}$. By [14, Corollary 12] and the fact that $(a+b)^2 = a^2 + b^2$, the delooping exists and is unique so we could take this as a recursive definition of Sq^n, starting from the definition of $\mathsf{Sq}^n : K_n \to K_{2n}$ as $x \mapsto x \smile x$. In this way one would immediately get a stable cohomology operation, which is sufficient for some purposes, but this definition seems to give no insight toward proving the Cartan formula or Adem relations.

Before we continue with the remaining axioms, we will need the following computation of the action of the Steenrod squares on the map $e : \mathbb{S}^1 \to K_1$ defined by letting $e(\mathsf{base}) :\equiv \mathrm{pt}$ and $\mathsf{ap}_e(\mathsf{loop}) := \sigma(1)$ where, recall, $\sigma : \mathbb{Z}/2\mathbb{Z} \simeq \Omega(K_1)$. Like Theorem 20, the statement looks deceptively easy but turns out to be quite technical. For now, we admit the result; its proof will be discussed in more detail in Section IV.

Lemma 25. *Let $x : \mathbb{S}^1$. We have*

$$\mathsf{Sq}^n(e(x)) = \begin{cases} e(x) & \text{if } n = 0 \\ 0 & \text{otherwise} \end{cases}$$

The following result is easier to prove and explains why e is relevant to us.

Lemma 26. *For $n : \mathbb{N}$, the map $f_n : K_n \to (S^1 \to_{\mathrm{pt}} K_{n+1})$ given by $a \mapsto x \mapsto e(x) \smile a$ is an equivalence.*

Proof. By definition of the cup product, we have that f_{n+1} is a delooping of f_n. Thus if f_n is an equivalence, then so is f_{n+1}. So it suffices to consider $n = 0$, which is direct. $\square$

Proposition 27. *The Steenrod squares satisfy the stability axiom (Ω).*

Proof. Given $m, n : \mathbb{N}$, we would like to show that $\sigma_{m+n}^{-1} \circ \Omega \mathsf{Sq}^n_{m+1} \circ \sigma_m = \mathsf{Sq}^n_m$, where Sq^n_m denotes the Steenrod square $K_m \to K_{m+n}$. Let τ_X denote the canonical equivalence $\Omega X \xrightarrow{\sim} (\mathbb{S}^1 \to_{\mathrm{pt}} X)$. It suffices to show

$$\tau_{K_{m+n+1}} \Omega \mathsf{Sq}^n_{m+1} \tau_{K_{m+1}}^{-1} \circ \tau_{K_{m+1}} \sigma_m = \tau_{K_{m+n+1}} \sigma_{m+n} \circ \mathsf{Sq}^n_m.$$

The upshot is that the composites above admit simpler descriptions. First, it is direct that the map $\tau_{K_{m+n+1}} \circ \Omega \mathsf{Sq}^n_{m+1} \circ \tau^{-1}_{K_{m+1}} : (\mathbb{S}^1 \to_{\mathrm{pt}} K_{m+1}) \to (\mathbb{S}^1 \to_{\mathrm{pt}} K_{m+n+1})$ is simply $l \mapsto x \mapsto \mathsf{Sq}^n_{m+1}(l(x))$. Secondly, the map $\tau_{K_{m+1}} \circ \sigma_m : K_m \to (\mathbb{S}^1 \to_{\mathrm{pt}} K_{m+1})$ is simply $a \mapsto x \mapsto e(x) \smile a$. To see this, note that both maps are pointed equivalences, by Lemma 26, and note any pointed self-equivalence of K_m is the identity. By symmetry, $\tau_{K_{m+n+1}} \circ \sigma_{m+n}$ admits a similar description. Thus it suffices to show that for every $a : K_m$ and $x : \mathbb{S}^1$, we have

$$\mathsf{Sq}^n(e(x) \smile a) = e(x) \smile \mathsf{Sq}^n(a).$$

By the Cartan formula, the left hand side computes to $\mathsf{Sq}^0(e(x)) \smile \mathsf{Sq}^n(a) + \mathsf{Sq}^1(e(x)) \smile \mathsf{Sq}^{n-1}(a)$. We are done by Lemma 25. ☐

Proposition 28. *The Steenrod squares satisfy axiom (I1), i.e.* $\mathsf{Sq}^0 = \mathsf{id}$.

Proof. The zeroth square lives in the type of pointed functions $K_n \to_{\mathrm{pt}} K_n$ – a type which we understand well: looping $(K_n \to_{\mathrm{pt}} K_n) \to (K_{n-1} \to_{\mathrm{pt}} K_{n-1})$ is an equivalence for each $n \geq 0$. Since looping preserves the identity function, it is thus, by (Ω), enough to show that $\mathsf{Sq}^0_0 : K_0 \to K_0$ is the identity. By (I3), we have $\mathsf{Sq}^0_0(x) = x \smile x$. However, since $K_0 :\equiv \mathbb{Z}/2\mathbb{Z}$, the cup product here is simply $\mathbb{F}_2$-multiplication and thus $\mathsf{Sq}^0_0(x) = x \smile x = x$. ☐

Proposition 29. *The Steenrod squares satisfy the Adem relations (A).*

Proof. Given $m : \mathbb{N}$ and $a : K_m$, consider Theorem 20 in the case where n and f are constantly m, a. In this case we get that, for any $X, Y : \mathbb{R}P^\infty$, we have

$$(a^X)^Y = (a^Y)^X.$$

The idea is now simply to expand each side using Equation (3). We also make use of Lemma 23, the Cartan formula, and the fact that $t(X)^Y = t(X)^2 + t(X) \smile t(Y)$, which follows from (I3). In this way we get the following.

$$\begin{aligned}
(a^X)^Y &= \left(\sum_i \mathsf{Sq}^i(a) \smile t(X)^{n-i} \right)^Y \\
&= \sum_i \mathsf{Sq}^i(a)^Y \smile (t(X)^2 + t(X)t(Y))^{n-i} \\
&= \sum_{i,j,k} \binom{n-i}{k} \mathsf{Sq}^j \mathsf{Sq}^i(a) t(Y)^{2n-j-k} t(X)^{n+k-i}
\end{aligned}$$

In the same way one can express $(a^Y)^X$ as a polynomial in $t(X)$ and $t(Y)$. Since we have $(a^X)^Y = (a^Y)^X$, we can formally identify coefficients in these polynomials, by repeated application of Lemma 15. The steps required to go from here to the Adem relations are the same as in the classical case; see [15, Page 345] for details. ☐

This concludes the proof of Theorem 1.

A natural question to ask after seeing the short and snappy proofs in this section is whether, perhaps, the setting of HoTT makes working with cohomology operations like the Steenrod squares 'easier' than in a more traditional setting. Although there are aspects of our setup here which certainly seem to speak in favour of HoTT, we wish to use this section to emphasise that *a lot* of the heavy lifting is done by Theorem 20 and Lemma 25 which we have, thus far, only assumed. Thus, this question entirely hinges on the difficulty of proving these statements. For this reason we will now devote the remainder of the paper to proofs. They are interesting in their own right, as they force us to develop a fair bit of novel machinery; in the case of Theorem 20, we develop the theory of unordered joins; in the case of Lemma 25, we provide a more general characterisation of commutator homotopies. Interestingly, Lemma 25 turns out to be quite a bit easier than Theorem 20 – in most classical expositions, the situation is reversed [16]. For this reason, we will change the order of these two results and begin with the proof of Lemma 25. As the results tend to be technical, we do not go into all of the proofs in detail and emphasise instead that the coming sections have been computer formalised.

IV. The Zeroth Square

Although Lemma 25 (which, recall, states that $\mathsf{Sq}^n \circ e : \mathbb{S}^1 \to K_n$ is non-trivial only for $n = 0$) may look simple, it turns out to require rather general observations regarding the interplay between certain null-homotopies and commutativity proofs. To make this precise, we start by considering, for any pointed type A, the diagonal map $\Delta : \Sigma A \to_{\mathrm{pt}} \Sigma A \wedge \Sigma A$. We can easily show that this map is null. This null-homotopy is important for two reasons. First, it shows that $\mathsf{Sq}^1 \circ e : \mathbb{S}^1 \to K_2$ vanishes: indeed, we have $\mathsf{Sq}^1(e(x)) = e(x) \smile e(x)$ and this map factors as

$$\mathbb{S}^1 \xrightarrow{\Delta} \mathbb{S}^1 \wedge \mathbb{S}^1 \to K_1 \wedge K_1 \xrightarrow{\smile} K_2$$

which our null-homotopy shows must vanish. We can also use it in the following construction which generalises certain Steenrod squares. Let $F : \Sigma A \wedge \Sigma A \to_{\mathrm{pt}} B$ and suppose that F is commutative, i.e. we are given an identification $F = F \circ \mathsf{swap}$ of pointed maps. This data fits into a commutative diagram

$$\begin{tikzcd}
\Sigma A \arrow[rrr] \arrow[rr] \arrow[dr] \arrow[ddd] & & & 1 \arrow[ddd] \\
& & \Sigma A \wedge \Sigma A \arrow[dr, "F"] & \\
& \Sigma A \wedge \Sigma A \arrow[ur, "\mathsf{swap}"] \arrow[drr, "F"] & & \\
1 \arrow[rrr] & & & B
\end{tikzcd} \tag{5}$$

where the bottom right triangle is given by the commutativity of F. When $A = \mathbb{S}^0$ and F is the cup product $\mathbb{S}^1 \wedge \mathbb{S}^1 \to K_2$, the parallelogram describe the commutator of the cup product, something we see gives rise to Sq^0, simply by unfolding its definition. Explicitly, this means that, for any $x : \mathbb{S}^1$ the square $\mathsf{Sq}^0(e(x))$ is the element in K_1 obtained via the equivalence $\Omega K_2 \simeq K_1$ applied to the loop

$$\mathrm{pt} \rightsquigarrow e(x) \smile e(x) \xrightarrow{\mathsf{comm}_\smile(e(x), e(x))} e(x) \smile e(x) \rightsquigarrow \mathrm{pt}$$

Thus, we are done if we can show that the middle parallelogram is non-trivial, as a self-identification of $\smile \circ \Delta : \mathbb{S}^1 \to K_2$.

Let us show this by proving a more general fact concerning the situation in diagram (5). By the universal property of suspensions, any F fitting into this diagram induces a map $S_F : \Sigma^2 A \to_{\mathsf{pt}} B$. Let us define another such map, written $F_\Delta : \Sigma^2 A \to_{\mathsf{pt}} B$, by the following composition.

$$\Sigma^2 A \xrightarrow{\Sigma^2 \Delta} \Sigma^2 (A \wedge A) \xrightarrow{\sim} \Sigma A \wedge \Sigma A \xrightarrow{F} B$$

A natural question is to ask how these two functions are related. Perhaps surprisingly, regardless of the choice of commutator homotopy used to define S_F, they turn out to be the same.

Theorem 30. *Let A and B be pointed types. For any map $F : \Sigma A \wedge \Sigma A \to_{\mathsf{pt}} B$ and any choice of commutator $F = F \circ \mathsf{swap}$, we have that $S_F = F_\Delta$.*

Proof. The proof follows easily by considering the general diagram of pointed maps

$$\begin{tikzcd}
X \arrow[rrr] \arrow[drr, "h"] \arrow[ddr, "k"'] \arrow[dddd] & & & 1 \arrow[dl] \arrow[dddd] \\
& & Y \arrow[ddr, "f"] & \\
& Z \arrow[ur, "\sim"] \arrow[ddrr, "g"] & & \\
& & & \\
1 \arrow[uur] \arrow[rrr] & & & W
\end{tikzcd}$$

where the composition of the top triangle with the upper part of the parallelogram is assumed to give the leftmost triangle. We also assume that all areas enclosed in solid lines commute (as pointed maps), with the lowest and rightmost triangles having fillers witnessing the pointedness of g and f. By the universal property of suspension, we obtain maps $h' : \Sigma X \to Y$ and $w : \Sigma X \to W$. It follows by path induction that $h' \circ f = w$. Instantiating the diagram with $X = \Sigma A$, $Y = Z = \Sigma A \wedge \Sigma A$ and $g = f = F$, we obtain the desired statement.

One can also show that $S_F(x) = F_\Delta(x)$ by simply carrying out an induction on $x : \Sigma A$ and doing some technical but straightforward path algebra. This is what we did in the formalisation. $\square$

This result is interesting in its own right. Roughly, it says that, under the right circumstances, commutators of non-trivial multiplications are homotopically non-trivial. We are, however, particularly interested in a special case of the statement: the case when F is the cup product $\smile : \mathbb{S}^1 \wedge \mathbb{S}^1 \to K_2$. As remarked before, the non-vanishing of S_F in this case corresponds to the non-vanishing of $\mathsf{Sq}^0 \circ e$. Hence, with Theorem 30 at our disposal, we are done if we can verify that F_Δ is non-trivial – something which is immediate in this case as it describes the generator of $H^2(\mathbb{S}^2) \cong \mathbb{Z}/2\mathbb{Z}$. This concludes the proof of Lemma 25.

Remark 31 (Another Brunerie number)**.** The non-trivial case of Lemma 25 is that of $n = 0$. This case should, however, not be difficult. Both e and $\mathsf{Sq}^0 \circ e : \mathbb{S}^1 \to_{\mathsf{pt}} K_1$ define elements of $\mathbb{Z}/2\mathbb{Z}$ under the equivalence $F : (\mathbb{S}^1 \to_{\mathsf{pt}} K_1) \simeq \Omega K_1 \simeq \mathbb{Z}/2\mathbb{Z}$. As we are working constructively, we should in principle just have to plug the values $F(e), F(\mathsf{Sq}^0 \circ e) : \mathbb{Z}/2\mathbb{Z}$ into a proof assistant like `Cubical Agda` and normalise them. Unfortunately, our attempts at this have been unsuccessful (we simply run out of memory).

V. Unordered joins and their Fubini theorem

We now set out to prove Theorem 20. This theorem states that our unordered cup product satisfies a certain 'Fubini theorem'. Recall from the definition of the unordered cup product $\smile_X : \Pi_{x:X} K_{n(x)} \to K_{\sum n}$ that it has the structure of a bihom, i.e. it is pointed in each argument, and that it is non-trivial. This characterises $\smile_X$ up to contractible choice, and so anything we prove about $\smile_X$ should come from this characterisation. In order to prove Theorem 20, we would like to have a similar characterisation of the iterated cup product

$$\smile_X \smile_Y : \Pi_{x:X} \Pi_{y:Y} K_{n(x,y)} \to K_{\sum n}.$$

In other words we would like to find a way to uniquely characterise $\smile_X \smile_Y$, that is symmetric in X and Y. Morally, this characterisation is that $\smile_X \smile_Y$ is coherently pointed in each of its $X \times Y$-many arguments. Thus we are lead to consider a generalisation of $\mathsf{isBiHom}$ to the 4-element type $X \times Y$. Already defining such a generalisation is rather complicated; it involves the combinatorics of all non-empty (decidable) subsets of $X \times Y$ and their inclusions. So it will be helpful to have another perspective on $\mathsf{isBiHom}$. In fact Brunerie [8] never considered $\mathsf{isBiHom}$, instead working with its corepresenting object, the unordered smash product.

Definition 32. Let $X : \mathbb{R}P^\infty$ and $A : X \to \mathcal{U}_{\mathsf{pt}}$ be a family of pointed types. We define the unordered smash product of A, denoted $\bigwedge_{x:X} A(x)$ by the following pushout

$$\begin{tikzcd}
(x : X) \times A(x) \arrow[rr, "(x,a) \mapsto \mathsf{Elim}^{x \mapsto a}_{\neg x \mapsto \mathsf{pt}}"] \arrow[d, "\mathsf{fst}"'] & & \prod_{x:X} A(x) \arrow[d] \\
X \arrow[rr] & & \bigwedge_{x:X} A(x) \arrow[ul, phantom, very near start, "\ulcorner"]
\end{tikzcd}$$

We take this type to be pointed by $\mathsf{inr}(\lambda x\,.\mathsf{pt})$.

It is easy to see that $\mathsf{isBiHom}(f)$ is equivalent to asking that f factors through $\mathsf{inr} : \Pi_{x:X} A(x) \to \bigwedge_{x:X} A(x)$ via a pointed map $\bigwedge_{x:X} A(x) \to_{\mathsf{pt}} B$, and that $\mathsf{BiHom}_X(A, B)$ is equivalent to the type of all such pointed maps $\bigwedge_{x:X} A(x) \to_{\mathsf{pt}} B$. In this way, one can see that $\smile_X \smile_Y$ is given by the composite of the map $\Pi_{x:X} \Pi_y K_{n(x,y)} \to \bigwedge_{x:X} \bigwedge_{y:Y} K_{n(x,y)}$, given by $f \mapsto \mathsf{inr}\,(x \mapsto \mathsf{inr}(y \mapsto f(x,y)))$, with the unique non-trivial map $\bigwedge_{x:X} \bigwedge_{y:Y} K_{n(x,y)} \to_{\mathsf{pt}} K_{\sum n}$. What remains to be shown is that we have a pointed equivalence $e : \bigwedge_{x:X} \bigwedge_{y:Y} A(x,y) \simeq \bigwedge_{y:Y} \bigwedge_{x:X} A(x,y)$ such that the following diagram commutes.

$$\begin{tikzcd}
\Pi_{x:X} \Pi_{y:Y} A(x,y) \arrow[r, "\mathsf{swap}"] \arrow[d] & \Pi_{y:Y} \Pi_{x:X} A(x,y) \arrow[d] \\
\bigwedge_{x:X} \bigwedge_{y:Y} A(x,y) \arrow[r, "e"'] & \bigwedge_{y:Y} \bigwedge_{x:X} A(x,y)
\end{tikzcd}$$

Again this turns out to be rather complicated, and we need another simplifying device.

Definition 33. Let $X : \mathbb{R}P^\infty$ and $A : X \to \mathcal{U}$. We define the unordered join of A, denoted $\ast_{x:X} A(x)$, by the following pushout.

$$\begin{tikzcd}
X \times \Pi_{x:X} A(x) \arrow[r, "\mathsf{snd}"] \arrow[d, "(x,f)\mapsto(x,f(x))"'] & \Pi_{x:X} A(x) \arrow[d] \\
(x : X) \times A(x) \arrow[r] & \ast_{x:X} A(x) \arrow[ul, phantom, "\ulcorner", very near start]
\end{tikzcd}$$

This construction agrees with the usual definition of joins whenever $X = \mathbb{Z}/2\mathbb{Z}$:

Lemma 34. *Given two types A_0 and A_1, we have $\ast_{x:\mathbb{Z}/2\mathbb{Z}} A_x \simeq A_0 * A_1$.*

Proof. By the 3×3 lemma applied to the following diagram.

$$\begin{tikzcd}
A_0 & \varnothing \arrow[l] \arrow[r] & A_1 \\
A_0 \times A_1 \arrow[u, "\mathsf{fst}"] \arrow[d, "\mathsf{id}"] & \varnothing \arrow[l] \arrow[r] \arrow[u] \arrow[d] & A_0 \times A_1 \arrow[u, "\mathsf{snd}"'] \arrow[d, "\mathsf{id}"'] \\
A_0 \times A_1 & A_0 \times A_1 \arrow[l, "\mathsf{id}"'] \arrow[r, "\mathsf{id}"] & A_0 \times A_1
\end{tikzcd}$$

□

The unordered join is relevant for us because $\mathsf{isBiHom}(f)$ is easily seen to be equivalent to

$$(a : \Pi_{x:X} A(x)) \to \ast_{x:X} (a(x) = \mathrm{pt}) \to (f(a) = \mathrm{pt}).$$

An equivalent way to phrase this (which we will not use) is that $\bigwedge_{x:X} A(x)$ is the cofibre of the projection

$$(a : \Pi_{x:X} A(x)) \times \ast_{x:X} (a(x) = \mathrm{pt}) \to \Pi_{x:X} A(x)$$

onto the first component; this map might be called an *unordered wedge inclusion*.

Given this characterisation of $\mathsf{isBiHom}(f)$ in terms of the unordered join, the proof of Theorem 20 will eventually reduce to the following lemma.

Lemma 35. *For any $X, Y : \mathbb{R}P^\infty$ and $A : X \times Y \to \mathcal{U}$, we have a function*

$$\ast_{x:X} \ast_{y:Y} A(x,y) \to \ast_{y:Y} \ast_{x:X} A(x,y)$$

Interestingly, we do not need to ask for any properties of this function, although it is important that we *construct* a function as opposed to proving its mere existence. Since the proof of Lemma 35 is rather technical, we postpone it for the moment and turn to the main result promised at the beginning of this section.

Proof of Theorem 20. Suppose given $X, Y : \mathbb{R}P^\infty$, $n : X \times Y \to \mathbb{N}$, fixed throughout the proof; we'd like to show that $\smile_X \smile_Y = \smile_Y \smile_X$. Given $f : \Pi_{x:X} \Pi_{y:Y} K_{n(x,y)}$, we claim that we have a map

$$\ast_{x:X} \ast_{y:Y} (f(x,y) = 0) \to (\smile_{x:X} \smile_{y:Y} f(x,y) = 0). \qquad (6)$$

Indeed we have a map $\ast_{x:X} \ast_{y:Y} (f(x,y) = 0) \to \ast_{x:X} \smile_{y:Y} f(x,y) = 0$ by functoriality of the unordered join together with the fact that $\smile_Y$ is a bihom, and a map $(\ast_{x:X} \smile_{y:Y} f(x,y) = 0) \to (\smile_{x:X} \smile_{y:Y} f(x,y) = 0)$ since $\smile_X$ is a bihom.

Now let T be the sigma-type consisting of functions $\mu : \Pi_{x:X} \Pi_{y:Y} K_{n(x,y)} \to K_{\sum n}$ together with a proof that for all $f : \Pi_{x:X} \Pi_{y:Y} K_{n(x,y)}$, we have $\ast_{x:X} \ast_{y:Y} f(x,y) = \mathrm{pt} \to \mu(f) = \mathrm{pt}$. We can construct two elements of T: on the one hand we have $\smile_X \smile_Y$ together with the argument above that we have a map as in Equation (6). By symmetry and using Lemma 35, we can similarly construct an element of T whose first component is $\smile_Y \smile_X$. Now we claim that these two elements of T are equal; in fact we claim there is a unique identification between them. This will finish the proof, since if two pairs are equal then so are their first components.

Since our claim is now a proposition, we may assume that X and Y are both $\mathbb{Z}/2\mathbb{Z}$. In this case, we have that T is the set of pointed maps

$$K_{n(0,0)} \wedge K_{n(0,1)} \wedge K_{n(1,0)} \wedge K_{n(1,1)} \to_{\mathrm{pt}} K_{\sum n}.$$

By [17, Lemma 15], two pointed maps out of an iterated smash product are equal if they are equal when restricted to the product, in this case $\Pi_{i,j\in\{0,1\}} K_{n(i,j)}$. Our two elements of T correspond to the maps

$$(a_{00}, a_{01}, a_{10}, a_{11}) \mapsto (a_{00} \smile a_{01}) \smile (a_{10} \smile a_{11})$$

and

$$(a_{00}, a_{01}, a_{10}, a_{11}) \mapsto (a_{00} \smile a_{10}) \smile (a_{01} \smile a_{11}).$$

Indeed these are equal by commutativity and associativity of the cup product. This concludes the proof. □

A. Proving Lemma 35

No result used in this project has turned out to be quite as problematic as Lemma 35 – the result is highly technical and its the computer formalisation was only completed after a year's worth of failed attempts. While we would be very happy to see a more conceptual proof of this statement, we are sceptical to the existence of such a proof. To illustrate why, note that the pushout describing the unordered join $\ast_{x:X} A(x)$ in no way requires X to be a two-element type – the definition makes sense for arbitrary X, although in this case we might write it with an apostrophe $\ast'$ to remind ourselves that it is no longer a good generalisation of the usual join. Thus, we may ask whether it is true, for *any* two types X and Y and family $A : X \times Y \to \mathcal{U}$ whether the map

$$\mathcal{F} : \ast'_{x:X} \ast'_{y:Y} A(x,y) \to \ast'_{y:Y} \ast'_{x:X} A(x,y)$$

exists. This seems difficult (if not impossible) to do in general, as we cannot prove in general that the domain and codomain are equivalent. For instance, if we set $X = \mathbb{Z}/2\mathbb{Z}$ and $Y = \mathsf{hProp}$, $A(0, P) :\equiv \neg P$ and $A(1, P) := P$, then the LHS becomes contractible whereas the RHS is equivalent to the suspension of LEM – a type whose contractibility is independent of HoTT .

So, let us try to define $\mathcal{F}$ for $X, Y : \mathbb{R}P^\infty$. The function will be described by the following data:

$$\mathcal{F}_l : \left(\prod_{x:X} \bigast_{y:Y} A(x,y)\right) \to \bigast_{y:Y} \bigast_{x:X} A(x,y)$$
$$\mathcal{F}_r : (x : X) \times \bigast_{y:Y} A(x,y) \to \bigast_{y:Y} \bigast_{x:X} A(x,y)$$
$$\mathcal{F}_{lr} : (x : X) \left(f : \prod_{x:X} \bigast_{y:Y} A(x,y)\right) \to F_l(f) = F_r(x, f(x))$$

The key problem here is defining F_l – its codomain is a Π-type and thus does not automatically come equipped with an elimination rule. Consequently, we need to understand the type $\prod_{x:X} \bigast_{y:Y} A(x,y)$. Luckily, it turns out that we can describe this Π-type using a rather involved construction. To give it a (somewhat) more concise definition, let us define, for any two types B, C and family $R : B \to C \to \mathcal{U}$, the *relational* pushout, $P(B, C, R)$ to simply be the pushout of the span $B \leftarrow (b : B) \times (c : C) \times R(b, c) \to C$. Any pushout $B \xleftarrow{f} D \xrightarrow{g} C$ can be written as a relational pushout by setting $R(b, c) :\equiv (d : D) \times (f(d) = b) \times (g(d) = c)$ (and vice versa).

Lemma 36. *Let $X : \mathbb{R}P^\infty$, $B, C : X \to \mathcal{U}$, and $R : B(x) \times C(x) \to \mathcal{U}$ (with $x : X$ an implicit argument). Then $\prod_{x:X} P(B(x), C(x), R(x))$ is equivalent to the HIT T with the following constructors:*

- bb : $(\prod_{x:X} B(x)) \to T$
- cc : $(\prod_{x:X} C(x)) \to T$
- bc : $(x : X) \times B(x) \times C(\neg x) \to T$
- rr : $(b : \prod_{x:X} B(x))(c : \prod_{x:X} C(x))(r : \prod_{x:X} R(b(x), c(x))) \to bb(b) = cc(c)$
- br : $(x : X)(b : \prod_{k:X} B(k))(c : C(\neg x))(r : R(b(\neg x), c)) \to bb(a) = bc(b(x), c)$
- cr : $(x : X)(b : B(x))(c : \prod_{k:X} C(k))(r : R(b, c(x))) \to bc(b, c(\neg x)) = cc(c)$
- rr' : $(b : \prod_{x:X} B(x))\,(c : \prod_{x:X} C(x))\,(r : \prod_{x:X} R(b(x), c(x)))\,(x : X) \to rr(b, c, r) = br(x, \neg x, b, c(\neg x), r(\neg x)) \cdot cr(x, \neg x, b(x), c, r(x))$

Proof sketch. It is straightforward to define a map $w_X : T \to \Pi_{x:X} P(B(x), C(x), R(x))$ by T-induction. By Lemma 2(a) it is sufficient to show that w_X is an equivalence when $X = \mathbb{Z}/2\mathbb{Z}$. This is somewhat technical but can be done with relative ease. □

If we instantiate the above with $B(x) :\equiv (y : Y) \times A(x, y)$, $C(x) := \prod_{y:Y} A(x, y)$ and $R((y, a), f) := (f(y) = a)$, we have $P(B(x), C(x), R(x)) \simeq \bigast_{y:Y} A(x, y)$ and thus Lemma 36 tells us that there is an equivalence $w : T \simeq \prod_{x:X} \bigast_{y:Y} A(x, y)$. Hence, in order to construct $\mathcal{F}_l$, it is enough to define a map $T \to \bigast_{y:Y} \bigast_{x:X} A(x, y)$.

Mapping out of T is, in general, not much easier than mapping out of $\prod_{x:X} \bigast_{y:Y} A(x, y)$: a map out of T must be defined over $\Pi_{x:X} B(x)$ and $\Pi_{x:X} C(x)$. which again forces us to map out of Π-types. The type $\Pi_{x:X} C(x)$ is unproblematic: it is simply $\Pi_{x:X}\Pi_{y:Y} A(x, y)$ and defines an element of $\bigast_{y:Y} \bigast_{x:X} A(x, y)$ by simply swapping the arguments. However, $\prod_{x:X} B(x) :\equiv \Pi_{x:X}((y : Y) \times A(x, y))$ is more complicated – where we send an element f of this type depends on the behaviour of $\mathsf{fst} \circ f : X \to Y$. Fortunately, we can understand this type.

Lemma 37. *For any $X, Y : \mathbb{R}P^\infty$, the map $((X \simeq Y) + Y) \to (X \to Y)$ sending equivalences to their underlying functions and $y : Y$ to the constant map $\lambda\, x \,.\, y$ is an equivalence.*

Proof. Since the statement is a proposition, it suffices to show it when $X = Y = \mathbb{Z}/2\mathbb{Z}$. In this case, the statement is simply the trivial observation that any function $(\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z})$ is either an equivalence or constant. □

Using Lemma 37, we can replace each occurrence of $\Pi_{x:X}((y : Y) \times A(x, y))$ in T with the equivalent type

$$((e : X \simeq Y) \times A(x, e(x))) + ((y : Y) \times A(x, y))$$

which has a more well-behaved elimination principle. After this rewriting, it is possible to define, by pattern-matching, a map $\psi_{X,Y} : T \to \bigast_{y:Y} \bigast_{x:X} A(x, y)$, which allows us to define $\mathcal{F}_l = \psi_{X,Y} \circ \phi^{-1}_{X,T}$. We then need define, for each $x : X$, the function $\mathcal{F}_r(x, -)$ and the homotopy $\mathcal{F}_{lr}(x, -)$. In theory, this is somewhat easier: as we have $x : X$ in context, we may apply Lemma 6. In practice, we have to deal with a large number of difficult coherence problems which we completely sweep under the rug here.

VI. Joins and E_∞-monoids

Much progress in synthetic homotopy type theory is held back by what is known as the *problem of infinite objects* [18]. This problem appears in many guises, and is traditionally explained in terms of semi-simplicial types. In this work we brush against instances of this problem in many places where we would like to talk about higher commutative, more precisely E_∞, monoids.

The idea of E_∞-monoids is remarkably natural from a type-theoretic perspective. An E_∞-monoid should consist of a type A and for *any finite type* X a 'multiplication' map

$$\mu_X : A^X \to A.$$

These multiplication maps express that any finite collection of elements of A can be multiplied, and that their order is irrelevant in a homotopy coherent sense. The unary multiplication $\mu_1 : A^1 \to A$ should be the canonical equivalence. These multiplication maps are subject to certain coherences, starting with the following: given a finite type $X : \mathcal{U}$ and a family of finite types $Y : \mathcal{U}$ indexed by X, the two maps $A^{(x:X)\times Y(x)} \to A$ given respectively by $\mu_{(x:X)\times Y(x)}$ and

$$a \mapsto \mu_X(x \mapsto \mu_Y(y \mapsto a(x,y)))$$

are identified. This expresses a kind of generalised associativity.

This is not a complete definition of E_∞-monoids – it is missing an infinite tower of higher coherences – but we can get far with just the data above.

For example, we would like to know that the universe of types $\mathcal{U}$ forms an E_∞-monoid where the multiplication is given by unordered join of types. The unordered binary join would be a special case, and the Fubini map (indeed, equivalence) of Lemma 35 – our main technical result – would be a consequence of generalised associativity, since $\mu_{X\times Y}$ and $\mu_{Y\times X}$ are related by the path $X \times Y = Y \times X$ obtained from univalence. In this way the technical burden of this paper would be much lighter if we simply had access to this E_∞-monoid structure!

The problems associated with this appear at three different levels. At the first level, we cannot even define whole the infinite tower of E_∞-coherences in type theory. This is a well-known instance of the problem of infinite objects, but not so relevant for us. At the second level, it is not clear how to define the unordered join of a general finite family of types. We have seen how to do it given a finite family of size 2, and it is clear how to do it for 3 and 4, but the complexity grows very quickly, and we run into the problem of infinite objects in trying to define a general pattern.

At the third level, consider what happens when we try to reason about unordered joins of just a few spaces – for example as in Lemma 35. At this level, our problems are finitary and in principle surmountable. But they are also remarkably difficult since we lack a systematic way to approach these problems. This story can be compared with that of coherences for the smash product [17].

VII. Steenrod Squares and $\pi_4(\mathbb{S}^3)$

The Steenrod squares are not only an esoteric construction: they have several crucial applications in algebraic algebraic topology. One typical example is the computation of $\pi_4(\mathbb{S}^3)$, the 4th homotopy group of the 3-sphere, i.e $\|\mathbb{S}^4 \to_{\mathsf{pt}} \mathbb{S}^3\|_0$. Although the fact that $\pi_4(\mathbb{S}^3) \cong \mathbb{Z}/2\mathbb{Z}$ is well-known in HoTT, due to Brunerie [6], it was shown by Ljungström and Mörtberg [19] that this can be shown in a very direct way under the assumption that $\pi_4(\mathbb{S}^3)$ is non-trivial. We can now complete this proof by giving a new (in HoTT) argument for why $\pi_4(\mathbb{S}^3)$ does not vanish. Let $h : \mathbb{S}^3 \to \mathbb{S}^2$ be the *Hopf map*, i.e. the generator of $\pi_3(\mathbb{S}^2)$. If we can show that its suspension $\Sigma h : \mathbb{S}^4 \to \mathbb{S}^3$ is non-trivial, we are done. In HoTT, we define $\mathbb{C}P^2 :\!- C_h$ to be the cofibre of h. Since suspensions commute with cofibres, we get $C_{\Sigma h} \simeq \Sigma\mathbb{C}P^2$. On the other hand, the cofibre of the constant pointed map $\mathsf{const} : \mathbb{S}^4 \to \mathbb{S}^3$ is equivalent to $\mathbb{S}^5 \vee \mathbb{S}^3$, i.e. the pushout of the span $\mathbb{S}^5 \leftarrow \mathbb{1} \to \mathbb{S}^3$. Thus, we are done if we can show the following.

Theorem 38. $\Sigma\mathbb{C}P^2 \not\simeq \mathbb{S}^5 \vee \mathbb{S}^3$

Proof. Both spaces in questions are suspensions, with $\mathbb{S}^5 \vee \mathbb{S}^3 \simeq \Sigma\mathbb{S}^4 \vee \mathbb{S}^2$. We consider the following diagram (where, we remark, all cohomology groups are equivalent to $\mathbb{Z}/2\mathbb{Z}$) where $A \in \{\mathbb{C}P^2, \mathbb{S}^4 \vee \mathbb{S}^2\}$

$$\begin{tikzcd} H^2(A,\mathbb{Z}/2\mathbb{Z}) \arrow[r, "(-)^2"] \arrow[d, "\sim"'] & H^4(A,\mathbb{Z}/2\mathbb{Z}) \arrow[d] \\ H^3(\Sigma A,\mathbb{Z}/2\mathbb{Z}) \arrow[r, "\mathsf{Sq}^2"'] & H^5(A,\mathbb{Z}/2\mathbb{Z}) \end{tikzcd}$$

This diagram is an instance of the suspension property for the Steenrod squares. When $A = \mathbb{C}P^2$, the squaring map is non-trivial (this was proved in HoTT by Brunerie [6] using $\mathbb{Z}$-coefficients but the proof works fine also for $\mathbb{Z}/2\mathbb{Z}$-coefficients). When $A = \mathbb{S}^4 \vee \mathbb{S}^2$, the squaring map is trivial since wedge sums have trivial cup-products. So $\Sigma\mathbb{C}P^2$ has non-trivial Sq^2 whereas for $\mathbb{S}^5 \vee \mathbb{S}^3$ it is trivial and thus we may conclude that these types cannot be equivalent. □

Corollary 39. $\pi_4(\mathbb{S}^3) \neq 0$

VIII. Conclusions and Future Work

In this paper we have proved important properties of the Steenrod squares in homotopy type theory, following a definition of Brunerie. This has necessitated the development of a substantial theory of unordered HITs, and we hope that our paper can serve as an illustration of the current state of synthetic homotopy theory – its power and its limitation.

This work suggests a number of further questions. Regarding Steenrod squares, one would like to know that they generate all maps $K(\mathbb{Z}/2\mathbb{Z}, n) \to K(\mathbb{Z}/2\mathbb{Z}, m)$ in an appropriate sense. Can this be proved in homotopy type theory? What about the assertion that the equations listed in Theorem 1 generate all possible relations between the Steenrod squares?

More generally, for any odd prime p there should be an analogue of the Steenrod square, namely the Steenrod reduced pth power $P^n : K(\mathbb{Z}/p\mathbb{Z}, m) \to_{\mathsf{pt}} K(\mathbb{Z}/p\mathbb{Z}, m + 2n(p-1))$. Can this even be studied in homotopy type theory? It is not clear how to even define it without running into the problem of infinite objects.

Let us also highlight the problems discussed in Section VI. Is it possible to define the unordered join of a general finite family of type? And is it possible to prove things like Lemma 35 more efficiently and systematically?

References

[1] D. R. Licata and E. Finster, “Eilenberg-MacLane Spaces in Homotopy Type Theory,” in *Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, ser. CSL-LICS ’14. New York, NY, USA: Association for Computing Machinery, 2014. [Online]. Available: https://doi.org/10.1145/2603088.2603153

[2] G. Brunerie, A. Ljungström, and A. Mörtberg, “Synthetic Integral Cohomology in Cubical Agda,” in *30th EACSL Annual Conference on Computer Science Logic (CSL 2022)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), F. Manea and A. Simpson, Eds., vol. 216. Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, pp. 11:1–11:19. [Online]. Available: https://drops.dagstuhl.de/opus/volltexte/2022/15731

[3] T. Lamiaux, A. Ljungström, and A. Mörtberg, “Computing cohomology rings in cubical agda,” in *Proceedings of the 12th ACM SIGPLAN International Conference on Certified Programs and Proofs*, ser. CPP 2023. New York, NY, USA: Association for Computing Machinery, 2023, p. 239–252. [Online]. Available: https://doi.org/10.1145/3573105.3575677

[4] A. Ljungström and A. Mörtberg, “Computational synthetic cohomology theory in homotopy type theory,” 2024. [Online]. Available: https://arxiv.org/abs/2401.16336

[5] U. Buchholtz and K.-B. Hou Favonia, “Cellular Cohomology in Homotopy Type Theory,” in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, ser. LICS ’18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 521–529. [Online]. Available: https://doi.org/10.1145/3209108.3209188

[6] G. Brunerie, “On the homotopy groups of spheres in homotopy type theory,” Ph.D. dissertation, Université Nice Sophia Antipolis, 2016. [Online]. Available: http://arxiv.org/abs/1606.05916

[7] F. van Doorn, “On the Formalization of Higher Inductive Types and Synthetic Homotopy Theory,” Ph.D. dissertation, Carnegie Mellon University, May 2018. [Online]. Available: https://arxiv.org/abs/1808.10690

[8] G. Brunerie, “The steenrod squares in homotopy type theory,” 2016, abstract at *23rd International Conference on Types for Proofs and Programs (TYPES 2017)*. [Online]. Available: https://types2017.elte.hu/proc.pdf#page=45

[9] The Univalent Foundations Program, *Homotopy Type Theory: Univalent Foundations of Mathematics*. Institute for Advanced Study: Self-published, 2013. [Online]. Available: https://homotopytypetheory.org/book/

[10] U. Buchholtz, “Unordered pairs in homotopy type theory,” 2023, preprint. [Online]. Available: https://ulrikbuchholtz.dk/pairs.pdf

[11] U. Buchholtz and E. Rijke, “The real projective spaces in homotopy type theory,” in *2017 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, 2017, pp. 1–8.

[12] N. Kraus, “Truncation levels in homotopy type theory,” July 2015. [Online]. Available: https://eprints.nottingham.ac.uk/28986/

[13] U. Buchholtz, F. van Doorn, and E. Rijke, “Higher Groups in Homotopy Type Theory,” in *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, ser. LICS ’18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 205–214. [Online]. Available: https://doi.org/10.1145/3209108.3209150

[14] D. Wärn, “Eilenberg–maclane spaces and stabilisation in homotopy type theory,” *Journal of Homotopy and Related Structures*, vol. 18, no. 2, pp. 357–368, Sep 2023.

[15] J.-C. Hausmann, *Mod two homology and cohomology*. Springer, 2014, vol. 10.

[16] H. Miller, *Lectures on Algebraic Topology*. WORLD SCIENTIFIC, 2021. [Online]. Available: https://www.worldscientific.com/doi/abs/10.1142/12132

[17] A. Ljungström, “Symmetric monoidal smash products in homotopy type theory,” *Mathematical Structures in Computer Science*, p. 1–23, 2024.

[18] U. Buchholtz, *Higher Structures in Homotopy Type Theory*, 2019, pp. 151–172.

[19] A. Ljungström and A. Mörtberg, “Formalising and computing the fourth homotopy group of the 3-sphere in cubical agda,” 2024. [Online]. Available: https://arxiv.org/abs/2302.00151