UNIVALENT FOUNDATIONS AS A FOUNDATION FOR MATHEMATICAL PRACTICE

Abstract. I prove that invoking the univalence axiom is equivalent to arguing 'without loss of generality' within Propositional Univalent Foundations (PropUF), the fragment of Univalent Foundations (UF) in which all homotopy types are mere propositions. As a consequence, I argue that practicing mathematicians, in accepting 'without loss of generality' (WLOG) as a valid form of argument, implicitly accept the univalence axiom and that UF rightly serves as a Foundation for Mathematical Practice. By contrast, ZFC is inconsistent with WLOG as it is applied, and therefore cannot serve as a foundation for practice.

Introduction. It has been noted for some time that symmetry arguments, often signaled in a mathematical proof by the turn of phrase 'without loss of generality' or simply WLOG, are inconsistent with existing formal systems of mathematics. Quoting Barwise [Bar89, p. 849],

> "[C]urrent formal models of proof are severely impoverished [...]. For example, [...] proofs where one establishes one of several cases and then observes that the others follow by symmetry considerations [constitute] a perfectly valid (and ubiquitous) form of mathematical reasoning, but I know of no system of formal deduction that admits of such a general rule." [Daw15]

Along similar lines, Awodey writes,

> "Within a mathematical theory, theorem, or proof, it makes no practical difference which of two 'isomorphic copies' are used, and so they can be treated as the same mathematical object for all practical purposes. This common practice is even sometimes referred to light-heartedly as 'abuse of notation,' and mathematicians have developed a sort of systematic sloppiness to help them implement this principle, which is quite useful in practice, despite being literally false. It is, namely, incompatible with conventional foundations of mathematics in set theory." [Awo14, p. 2]

The kind of argument to which Barwise and Awodey allude is a staple of mathematical reasoning, even at the highest level. For example, the phrase "without loss of generality" appears twice in the proof of the Green–Tao theorem [GT08], once in Tao's proof of the Erdős discrepancy problem [Tao16], seven times in Hairer's work on regularity structures [Hai14], three times in Gowers's proof of the multidimensional Szemerédi theorem [Gow07], and twice in Zhang's proof of bounded gaps between primes [Zha14]. The list goes on. Any reader who has taken a college-level math course has likely encountered, and perhaps even produced, such an argument themselves. Could it really be that these celebrated achievements by well-respected mathematicians and many more mundane aspects of mathematical pedagogy are (in Awodey's parlance) "sloppy" and "literally false"?

In fact, such arguments are likely much more prevalent than would be apparent by a simple search for the phrase "without loss of generality" in mathematical papers. The form of argument can easily go unnoticed by generic appeal to an "obvious" symmetry without explicit use of the phrase 'without loss of generality'. For an easy example, consider the claim: Every set containing exactly 3 distinct elements can be ordered in exactly 6 ways. To prove, let $\{a_1, a_2, a_3\}$ be a generic set of 3 distinct elements. The possible orderings are

$$\begin{aligned} &a_1 < a_2 < a_3, \quad a_1 < a_3 < a_2, \quad a_2 < a_1 < a_3, \\ &a_2 < a_3 < a_1, \quad a_3 < a_1 < a_2, \quad a_3 < a_2 < a_1, \end{aligned} \tag{1}$$

for a total of 6. Since the elements of this set are arbitrary, the proof is complete.

No practicing mathematician would quibble with the validity of this argument. The claim is obvious and the proof is trivial. If ever a mathematical proof could be formally justified, it should be this one. But is the argument given formally valid?

In specializing from the generic claim "Every set containing exactly 3 distinct elements" to a specific set $\{a_1, a_2, a_3\}$ and then generalizing the result on the basis that these elements are "arbitrary", the proof makes an implicit (and apparently "sloppy") appeal to symmetry that is worth a closer look. The unspoken symmetry crops up when the elements of $\{a_1, a_2, a_3\}$ are declared as "arbitrary", which implies that any other distinct elements could be substituted for a_1, a_2, a_3 and the argument would go through *mutatis mutandis* (i.e., once the necessary changes have been made).[1] The validity of the argument requires first that $\{a_1, a_2, a_3\}$ is equivalent (as a set) to every other set containing 3 elements and second that the number of orderings of a set is an invariant property under set-theoretic equivalence. As long as these two criteria are met, the above argument holds. It is intuitively clear that these

[1] This step is itself ambiguous, leaving open the question as to what the "necessary changes" are in a given setting. The working mathematician gets away with such turns of phrase because the "necessary changes" are obvious to practitioners in the field, just as the "relevant symmetries" are meant to be obvious when one invokes "without loss of generality".

criteria are met in the above example, but to what extent do they need to be justified when giving a rigorous proof?

What is a Foundation of Mathematical Practice? Before going any further, I should make clear what I mean by *Foundation of Mathematical Practice*. Among philosophers of mathematics, a *Foundation* is generally understood as an abstract "standard of rigor" in the sense that any mathematical statement that is claimed to be *true* could (in principle) be expressed and shown to hold in that Foundation. With this understanding, ZFC set theory has been adopted as the *de facto* Foundation of Mathematics by most philosophers. Importantly, the role of ZFC as a Foundation of Mathematics is to verify the truth of mathematical claims, irrespective of the validity of the argument given in support of those claims.

A Foundation of Mathematical Practice, on the other hand, deals with the latter issue of argumentation. As argumentation and proof are central to the *practice* of mathematics, I understand a *Foundation of Mathematical Practice* (FMP) to be a "standard of argument" in the sense that any argument that is regarded as *rigorous* could (in principle) be expressed and shown to be valid in that Foundation.

So whereas a Foundation of Mathematics deals with the *truth* of mathematical statements, a Foundation of Mathematical Practice deals with the *validity* of mathematical arguments. Regardless of whether the above argument can be translated into ZFC, the claim that any set with exactly 3 distinct elements can be ordered in exactly 6 ways can be shown to hold in ZFC. In fact, the argument given is not formally valid in ZFC, but it is valid in Univalent Foundations (UF), as I demonstrate below.

On this note, I ask if ZFC and/or UF can rightly be regarded as a Foundation for mathematics *as it is practiced*. In particular, I consider whether a given formal theory "permits [mathematicians] to do pretty much everything that it would come naturally for them to do" [Bur15, p. 117], which includes treating isomorphic objects as identical or distinct as they wish and applying standard rules of inference (WLOG, induction, proof by contradiction) as they deem appropriate. In the course of this discussion, I demonstrate, as the quotes by Awodey and Barwise already suggest, that WLOG is inconsistent with ZFC set theory, and therefore ZFC cannot serve as an FMP. I then prove that WLOG is (in a precise sense) equivalent to Voevodsky's axiom of univalence (UA) in the Univalent Foundations (UF) [Uni, APW13], from which I argue that UF is a suitable candidate for an FMP. Furthermore, the equivalence between WLOG and UA provides a non-structuralist justification for the univalence axiom, thus undermining prior attempts to level anti-structuralist criticisms, à la Burgess [Bur15], against UF; see, e.g., [BT18]. In short, since WLOG and UA are equivalent (see Theorem 1), and working mathematicians by and large accept WLOG as a valid form of argument, then working mathematicians also implicitly accept the univalence axiom. But because WLOG is not an overtly structuralist doctrine, the univalence axiom need not be regarded as a structuralist axiom, as has been argued previously in [Awo14], and thus UF (to the extent that it can be viewed as a Foundation of Mathematics) need not be viewed as a strictly "structuralist foundation" [Tse16].

Without Loss of Generality. WLOG is one of the most useful techniques in the working mathematician's toolkit, allowing a proof of one special case to stand in for perhaps infinitely many other 'practically identical' cases. For the sake of this discussion, I define WLOG to be an argument of the following form:

(WLOG) if P holds of A, then P holds of every B that is practically identical to A.

In our opening example concerning the orderings of a set with 3 elements, A is defined as $\{a_1, a_2, a_3\}$, $P(A)$ corresponds to "A can be ordered in exactly 6 ways", and "B is practically identical to A" means that "B is in bijective correspondence with A". Expressed in this way, the argument given above fits the structure of WLOG, and may be seen as justification for the conclusion that P holds for all 3-element sets.

More generally the meaning of 'practical identity' depends on the domain in which the argument is being applied, and thus requires special care in systems aiming to formalize all of mathematical practice. In number theory, 2/4, 3/6, and 4823/9646 can be treated as identical because they reduce to the same ratio when expressed in lowest terms, namely 1/2; in homotopy theory, $\mathbb{R}$ (with Euclidean topology) can be continuously deformed into $\bullet$ (with trivial topology), making the two homotopically identical (i.e., homotopy equivalent); in combinatorics, the set of directed graphs with n vertices is in bijective correspondence with, and thus is combinatorially identical to, the set of $\{0, 1\}$-valued $n \times n$ matrices with zero on the diagonal; and in group theory $(\{0, 1, 2\}, +(\text{mod } 3))$ is isomorphic (as a group) to any other representative of the cyclic group of order 3.

In general, the 'X theorist' (number theorist, homotopy theorist, combinatorialist, group theorist, etc.) has his own notion of 'X-theoretic equivalence' (e.g., numerical equivalence, equivalence up to continuous deformation, bijective correspondence, group isomorphism, etc.) which gives sense to the meaning of *practical identity* within 'X theory'. It is this notion of X-theoretic equivalence to which the mathematician appeals when arguing 'without loss of generality' within the context of 'X theory': for any (X-theoretic) property P and any (X-theoretic) structure A, if P holds of A then P holds of every other (X-theoretic) structure B that is equivalent to A (within X theory). This

X-theoretic implementation of WLOG can be expressed semi-formally as

$$\text{(2)} \qquad \mathrm{WLOG}_X \qquad \forall P\, \forall A\ (P(A) \to (\forall B\ (A \sim_X B) \to P(B))),$$

with $A \sim_X B$ indicating that A and B are 'X-theoretically equivalent' and the restriction of P, A, and B to X-theoretic properties/structures left implicit.

Given the liberty with which mathematicians appeal to WLOG in their native disciplines, and the ubiquity with which arguments along these lines appear in proofs accepted as rigorous, a Foundation of Mathematical Practice should thus provide a formal basis in which WLOG_X can be consistently employed across all mathematical disciplines. In symbols, a Foundation of Mathematical Practice should be a formal model for WLOG_X for every conceivable instantiation of X:

$$\text{(3)} \qquad \mathrm{FMP} \models \forall X\ \mathrm{WLOG}_X.$$

Below I assess the merits of ZFC set theory and Univalent Foundations with respect to their ability to satisfy (3).

ZFC is not a Foundation of Mathematical Practice. When formalized in set theory, with all mathematical objects represented as (structured) sets, the relevant version of 'X-theoretic equivalence' is given by ZFC's axiom of extensionality,

$$\text{(Ext)} \qquad (A =_{\mathbf{ZFC}} B) \leftrightarrow \forall x\ ((x \in A) \leftrightarrow (x \in B)).$$

In words, (Ext) states that two sets are identical only if they contain the same elements, which in turn makes two mathematical structures (formalized as sets in ZFC) 'practically identical' only if their set-theoretic representations are identical *as sets*. With this definition of equivalence, WLOG_X is expressed formally as a second-order statement (not internal to ZFC) by

$$\mathrm{WLOG}_{\mathbf{ZFC}} \qquad \forall P\, \forall A\ \left(P(A) \to (\forall B\ (A =_{\mathbf{ZFC}} B) \to P(B))\right),$$

where P is quantified over all set-theoretic properties. As written, $\mathrm{WLOG}_{\mathbf{ZFC}}$ is valid in ZFC—a predicate applied to equal inputs ($A =_{\mathbf{ZFC}} B$) produces equal outputs—but its scope is too narrow to capture the spirit of 'without loss of generality' as it is usually applied in practice.

Consider the following example from homotopy theory, with $\mathbb{R}$ equipped with the Euclidean topology and $\bullet$ (the point) equipped with the trivial topology. Homotopically, $\mathbb{R}$ and $\bullet$ (with respective topologies) are equivalent, since each can be continuously deformed into the other, and thus any homotopical properties proven of $\mathbb{R}$ can be transferred 'without loss of generality' to $\bullet$. Strictly speaking, however, the formal representatives of $\mathbb{R}$ and $\bullet$ in ZFC are not identical *as sets*, i.e., $\mathbb{R} \neq_{\mathbf{ZFC}} \bullet$, and therefore $\mathrm{WLOG}_{\mathbf{ZFC}}$ cannot be formally applied to transfer properties between the two. So even though $\mathbb{R}$ and $\bullet$

are homotopy equivalent, the quantification over set-theoretic properties P in $\text{WLOG}_{\mathbf{ZFC}}$ allows them to be distinguished within ZFC (e.g., the property 'π is an element of the base set' holds of $\mathbb{R}$ but not $\bullet$), making it "literally false", as Awodey [Awo14] notes, to transfer properties between two equivalent representatives unless those representatives are themselves set-theoretically identical.

On the one hand, the concept of equality in ZFC is too strict to account for the homotopy equivalence between $\mathbb{R}$ and $\bullet$. On the other hand, the syntax of ZFC is too loose in allowing one to state non-homotopical properties (such as 'π is an element of the base set') that are not preserved under homotopy equivalence. Similar observations can be made about the formalization of combinatorial, topological, number theoretic, algebraic, etc. properties in ZFC. For example, in our running example about the orderings of a set with 3 elements, the "arbitrary" set $\{a_1, a_2, a_3\}$ is *not* identical to any other "arbitrary" set $\{a'_1, a'_2, a'_3\}$. Therefore, while the argument $\text{WLOG}_{\mathbf{ZFC}}$ can be applied, its application does not generalize to give the number of orderings of any set other than that whose orderings are listed in (1). The conclusion that every 3 element set can be ordered in exactly 6 ways does not follow from the application of $\text{WLOG}_{\mathbf{ZFC}}$. With these observations we see that $\text{WLOG}_{\mathbf{ZFC}}$ is not consistent with $\forall X\ \text{WLOG}_X$ as it is used in practice, and therefore ZFC is not a Foundation of Mathematical Practice in the sense of (3).

Structuralist foundations. This conflict between the norms of ZFC and the mores of mathematical practice fly in the face of set-theoretic orthodoxy, and in particular Burgess's assessment of ZFC's standing among mathematicians:

> "Mathematicians acquiesced in the set-theoretic framework, mostly without enthusiasm, doubtless in large part because the standard axiom system ZFC permits them to do pretty much everything that it would come naturally for them to do in the way of constructing new structures out of old, and permits the deduction of all the familiar principles of traditional mathematics that had been put on any sort of rigorous basis over the preceding century. [...] In short, it permits the mathematician to *stop thinking about* foundational questions." [Bur15, p. 117]

Sure, mathematicians may not think about foundations—they're too busy doing math—but is this because they have *stopped* thinking about foundations, or because they never started? In a random survey of mathematicians, of whom I mean geometers, algebraists, probabilists, number theorists, topologists, combinatorialists, analysts, etc., one is likely to encounter few who know the axiom of extensionality by name, fewer who can identify any connection between set-theoretic foundations and their day-to-day work as mathematicians, fewer still who do not make regular use of WLOG in what they consider to be rigorous arguments, and almost nobody who is concerned by the fact that WLOG is incompatible with the set-theoretic framework. In short, it is not the case that the set-theoretic framework "permits [mathematicians] to do pretty much everything that it would come naturally for them to do", and mathematicians couldn't care less.

The discrepancy between set-theoretic foundations and mathematical practice has motivated calls for structuralist foundations, as in Lawvere's Elementary Theory of the Category of Sets [Law05] and the more recently proposed Univalent Foundations [Uni]. Arguments for mathematical structuralism take root in Benacerraf's famous "antinomy" [TH17] of von Neumann's and Zermelo's construction of the natural numbers. As Benacerraf [Ben65] observed, there are set-theoretic differences between the two constructions, e.g., $0 \in 2$ when $2 = \{0, 1\}$ but $0 \notin 2$ when $2 = \{1\}$. Thus, if expressed in set theory, there is no formal way to reconcile the Zermelodist (who formalizes the ordinal numbers as $0 = \emptyset$, $1 = \{0\}$, $2 = \{1\}$, $\ldots$) to the Neumannian (who formalizes the ordinals instead as $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, $\ldots$), even though the difference between the two has no bearing on what the natural numbers are meant to represent in practice. To dispense with this formalistic conflict between Zermelodists and Neumannians, of which practicing mathematicians are neither, Tsementzis [Tse16] argues for a structuralist foundation of mathematics whose formal system makes it literally impossible to express "nonsensical" properties that have nothing to do with the structures being formalized, such as the set-theoretic statement '$1 \in 2$'. The Univalent Foundations achieves precisely this, first by formalizing all mathematical objects as homotopy types in homotopy type theory (HoTT) and then by postulating the univalence axiom, which asserts

$$\underbrace{(A \simeq B)}_{\text{(homotopy) equivalence}} \quad \underbrace{\simeq}_{\text{is (homotopy) equivalent to}} \quad \underbrace{(A =_{\mathbf{UF}} B)}_{\text{identity}}, \tag{4}$$

where $A =_{\mathbf{UF}} B$ indicates that A and B are identical for the purpose of practicing mathematics internally to UF.[2]

In making the statement 'has the same structure as' (formalized as $A \simeq B$) itself have the same structure as ($\simeq$) the statement 'is identical to' (written $A =_{\mathbf{UF}} B$), the univalence axiom is seen by some as a formal embodiment of the structuralist philosophy, e.g., [Awo14, Tse16], and a resolution to Benacerraf's conundrum. But critics of the Univalent Foundations, and mathematical structuralism more generally, note that practicing mathematicians sometimes

[2]Formally, the univalence axiom asserts that a specific map $(A =_{\mathbf{UF}} B) \to (A \simeq B)$ is a homotopy equivalence, as in [Uni, Axiom 2.10.3]. But these additional technicalities are not needed when working in the fragment of UF relevant to the present discussion.

behave as structuralists, and sometimes don't, putting any hardline structuralist framework, and in particular structuralist arguments for UF, at odds with mathematical practice. *Contra* structuralism, Burgess spins Benacerraf's observation instead as an indifference of mathematicians to the identification of mathematical structures:

> "The number theorist, even in a first course, wants to take certain background material for granted, and is generally indifferent as to where the background notions and results came from. Moreover, Benacerraf is right that included in the scope of this indifference is indifference as to the *identity* of the natural numbers, to which of the many isomorphic progressions is 'the' natural number system." [Bur15, p. 145]

Burgess continues, "Structuralism errs in generalizing too far from [Benacerraf's] initial correct observations [...]."

With respect to mathematical practice, Burgess has a point. While there are times when the working mathematician is indifferent to how a particular class of mathematical objects is identified (e.g., the Cauchy reals versus the Dedekind reals, Zermelo's versus von Neumann's construction of the natural numbers, the number $2/4$ versus the number $1/2$), there are others when it is desirable to distinguish isomorphic structures (e.g., when counting the number of distinct 2-element subgroups of the Klein group). So while devoutly non-structuralist arguments in favor of set-theoretic foundations are incongruous with the practice of mathematicians (from college freshmen to Fields medalists) who routinely appeal to structuralist rationale whenever they treat isomorphic objects as identical or otherwise argue 'by symmetry', arguments for the Univalent Foundations as a structuralist foundation [Tse16, Awo14] are out of step with the thought process of mathematicians who may wish to distinguish isomorphic structures from time to time [BT18]. On this point, the structuralist attitude underlying Awodey's and Tsementzis's support for the Univalent Foundations, regardless of how well UF deals with Benacerraf's and similar problems, risks putting off practicing mathematicians who neither know nor care about 'structuralism' but have grown comfortable with set-theoretic notation and jargon ('element', 'subset', $\in$, $\subset$) in their own practice.

To make the case for Univalent Foundations on practical grounds, I argue that the univalence axiom need not be interpreted as a structuralist axiom at all, and thus the Univalent Foundations need not be regarded as a structuralist foundation. To this end, I prove that for all practical purposes invoking the univalence axiom is equivalent to arguing 'without loss of generality' (WLOG), which both establishes UF as a Foundation of Mathematical Practice, in the sense of (3), and offers a non-structuralist justification for UF that differs from the earlier structuralist arguments in [Awo14, Tse16].

Univalent Foundations as a Foundation of Mathematical Practice. I prove here that the univalence axiom and WLOG are identical within *Propositional Univalent Foundations* (or PropUF for short), which is the fragment of UF with homotopy types restricted to mere propositions [Uni, Chapter 3]. Whereas UF takes a universe $\mathcal{U}$ of homotopy types as its basic objects, which in full generality can have the structure of an ∞-groupoid (containing objects, paths between objects, paths between paths, paths between paths between paths, and so on all the way 'up to ∞'), Propositional UF contains only homotopy types with at most a single unique inhabitant up to homotopy. The universe of objects in PropUF is thus the subset $\mathrm{Prop}_{\mathcal{U}} :\equiv \sum_{A:\mathcal{U}} \mathtt{isProp}(A)$ of all $A : \mathcal{U}$ satisfying

$$\mathtt{isProp}(A) :\equiv \prod_{x,y:A} (x =_A y).$$[3]

Because current mathematical practice is primarily concerned with whether or not a mathematical statement is true or false, the restriction here to Propositional UF is most relevant for assessing the role of UF as a foundation for mathematical practice.[4]

Since all mathematical objects are interpreted as homotopy types in PropUF, the relevant interpretation of 'X-theoretic equivalence' is given by *homotopy equivalence*, denoted $A \simeq B$ and defined formally as

$$A \simeq B :\equiv \sum_{f:A\to B} \left(\sum_{g:B\to A} (f \circ g \sim \mathtt{id}_B) \right) \times \left(\sum_{h:B\to A} (h \circ f \sim \mathtt{id}_A) \right). \tag{5}$$

According to (5), a homotopy equivalence between A and B is established by producing a triple of maps (f, g, h) with $f : A \to B$ and $g, h : B \to A$ together with proofs that $f \circ g$ is homotopic to the identity on B and

[3]In the syntax of HoTT, a term of $\mathtt{isProp}(A)$ is a map which takes a pair $x, y : A$ to a proof that x and y are identical (or, homotopically, points x and y in A to a path between them). The terms of $\mathrm{Prop}_{\mathcal{U}}$ are pairs $\langle A, p\rangle$ consisting of a type $A : \mathcal{U}$ and a proof $p : \mathtt{isProp}(A)$ that A is a proposition. Since $\mathtt{isProp}$ is itself a proposition, and thus has just one unique inhabitant, all proofs of $\mathtt{isProp}(A)$ are identical, permitting the interpretation of $\mathrm{Prop}_{\mathcal{U}}$ as the *subset* of all $A : \mathcal{U}$ satisfying $\mathtt{isProp}(A)$.

[4]It is perhaps also notable that although HoTT does not assume the law of excluded middle (LEM), and in fact is inconsistent with asserting LEM over the entire universe ($\mathtt{LEM}_\infty : \prod_{A:\mathcal{U}}(A + \neg A)$), it is consistent with assuming LEM for mere propositions. In particular, PropUF is consistent with the additional axiom

$$\mathtt{LEM}_{-1} : \prod_{A:\mathrm{Prop}_{\mathcal{U}}} (A + \neg A),$$

so that proof by contradiction is a valid form of argument in PropUF.

$h \circ f$ is homotopic to the identity on A.[5] To aid the proof, I define here the *Propositional Univalence Axiom* (PropUA) in PropUF, which states that homotopy equivalence is logically equivalent to identity for types that are mere propositions:

(6) $$\underset{\text{homotopy equivalence}}{(A \simeq B)} \quad \underset{\text{is logically equivalent to}}{\leftrightarrow} \quad \underset{\text{identity,}}{(A =_{\mathbf{PropUF}} B)}$$

where in HoTT the expression '$P \leftrightarrow Q$' is shorthand for the homotopy type

$$P \leftrightarrow Q :\equiv (P \to Q) \times (Q \to P)$$

whose inhabitants are pairs of maps, one from P to Q and one from Q to P.

In general, homotopy equivalence implies logical equivalence, i.e., $(A \simeq B) \to (A \leftrightarrow B)$, making PropUA appear weaker than the univalence axiom (4). But since all types in PropUF are mere propositions, and $A \simeq B$ and $A \leftrightarrow B$ are mere propositions whenever A and B are mere propositions, it readily follows (cf. [Uni, Lemma 3.3.3]) that logical equivalence of A and B is logically equivalent to equivalence of their homotopy types in PropUF, giving an inhabitant of

(7) $$\prod_{A,B:\mathrm{Prop}_{\mathcal{U}}} (A \simeq B) \leftrightarrow (A \leftrightarrow B).$$

From this it is immediate that PropUA in (6) is homotopy equivalent (hence, also logically equivalent) to the ostensibly stronger Univalence Axiom in (4).

The major claim here in establishing UF as a (not necessarily structuralist) FMP is that WLOG (suitably expressed in PropUF) is equivalent to the Propositional Univalence Axiom, or equivalently the Univalence Axiom. Within PropUF (where 'X theory' is homotopy type theory and 'X-theoretic equivalence' is homotopy equivalence), WLOG_X in (2) can be expressed internally as

(8)

$$\mathrm{WLOG}_{\mathbf{PropUF}} :\equiv \prod_{P:\mathrm{Prop}_{\mathcal{U}} \to \mathrm{Prop}_{\mathcal{U}}} \prod_{A:\mathrm{Prop}_{\mathcal{U}}} \left(P(A) \to \prod_{B:\mathrm{Prop}_{\mathcal{U}}} ((A \simeq B) \to P(B)) \right).$$

The formal assertion, from which I argue (3) for UF, is detailed in the following.

Theorem 1. WLOG and UA are equivalent in Propositional UF. In particular,

(9) $$\mathrm{WLOG}_{\mathbf{PropUF}} \;\simeq\; \mathrm{PropUA}.$$

[5] In HoTT, the statement $f \sim f'$ that two functions $f, f' : A \to B$ are *homotopic* is shorthand for the type

$$f \sim f' :\equiv \prod_{a:A} (f(a) =_B f'(a)).$$

Proof. First, since $\mathrm{WLOG}_{\mathbf{PropUF}}$ and PropUA are themselves mere propositions in PropUF, (7) implies the logical equivalence between (9) and

$$\mathrm{WLOG}_{\mathbf{PropUF}} \leftrightarrow \mathrm{PropUA}.$$

Second, by applying (7) to $A \simeq B$ in (6), we derive the logical equivalence between

$$\begin{aligned} \mathrm{PropUA} &:\equiv \ (A \simeq B) \quad \leftrightarrow \quad (A =_{\mathbf{PropUF}} B) \quad \text{and} \\ \mathrm{PropUA}_{\leftrightarrow} &:\equiv (A \leftrightarrow B) \quad \leftrightarrow \quad (A =_{\mathbf{PropUF}} B). \end{aligned}$$

Also by (7), $\mathrm{WLOG}_{\mathbf{PropUF}}$ is logically equivalent to the statement of WLOG with $A \simeq B$ replaced by $A \leftrightarrow B$:

$$\mathrm{WLOG}_{\leftrightarrow} :\equiv \prod_{P:\mathrm{Prop}_{\mathcal{U}} \to \mathrm{Prop}_{\mathcal{U}}} \prod_{A:\mathrm{Prop}_{\mathcal{U}}} \left(P(A) \to \prod_{B:\mathrm{Prop}_{\mathcal{U}}} (A \leftrightarrow B) \to P(B) \right).$$

Thus, to prove the claim it suffices to prove the logically equivalent claim that $\mathrm{WLOG}_{\leftrightarrow} \leftrightarrow \mathrm{PropUA}_{\leftrightarrow}$ holds in PropUF.

Proof of $\mathit{PropUA}_{\leftrightarrow} \to \mathit{WLOG}_{\leftrightarrow}$. This follows by combining $\mathrm{PropUA}_{\leftrightarrow}$ with HoTT's induction principle [Uni, Chapter 1.12]. In particular, the induction principle automatically implies

$$\begin{aligned} &\mathrm{WLOG}_{=} :\equiv \\ &\quad :\equiv \prod_{P:\mathrm{Prop}_{\mathcal{U}} \to \mathrm{Prop}_{\mathcal{U}}} \prod_{A:\mathrm{Prop}_{\mathcal{U}}} \left(P(A) \to \prod_{B:\mathrm{Prop}_{\mathcal{U}}} (A =_{\mathbf{PropUF}} B) \to P(B) \right). \end{aligned}$$

(To see this, note that for fixed $A : \mathrm{Prop}_{\mathcal{U}}$, if $P(A)$ holds of $A : \mathrm{Prop}_{\mathcal{U}}$, i.e., if there is an inhabitant $a : P(A)$, then defining

$$\begin{aligned} C &: \prod_{B:\mathrm{Prop}_{\mathcal{U}}} (A =_{\mathbf{PropUF}} B) \to \mathrm{Prop}_{\mathcal{U}} \\ C(B,p) &:\equiv P(B), \end{aligned}$$

and taking $a : C(A, \mathtt{refl}_A) \equiv P(A)$ allows us to apply based path induction to obtain an inhabitant of

$$\prod_{B:\mathrm{Prop}_{\mathcal{U}}} \prod_{p:A =_{\mathbf{PropUF}} B} C(B,p) \equiv \prod_{B:\mathrm{Prop}_{\mathcal{U}}} (A =_{\mathbf{PropUF}} B) \to P(B),$$

as claimed.) By $\mathrm{PropUA}_{\leftrightarrow}$, we have $(A \leftrightarrow B) \leftrightarrow (A =_{\mathbf{PropUF}} B)$, so that $\mathrm{WLOG}_{=} \leftrightarrow \mathrm{WLOG}_{\leftrightarrow}$, yielding $\mathrm{PropUA}_{\leftrightarrow} \to (\mathrm{WLOG}_{=} \leftrightarrow \mathrm{WLOG}_{\leftrightarrow})$. ☐

Proof of $\mathit{WLOG}_{\leftrightarrow} \to \mathit{PropUA}_{\leftrightarrow}$. Fix $A : \mathrm{Prop}_{\mathcal{U}}$. To show the direction $(A \leftrightarrow B) \to (A =_{\mathbf{PropUF}} B)$ in $\mathrm{PropUA}_{\leftrightarrow}$, define $P(B) :\equiv (A =_{\mathbf{PropUF}} B)$. The result follows automatically by $\mathrm{WLOG}_{\leftrightarrow}$ because $P(A) \equiv (A =_{\mathbf{PropUF}} A)$

holds trivially by $\mathtt{refl}_A$. The converse $(A =_{\mathbf{PropUF}} B) \to (A \leftrightarrow B)$ holds by based path induction at fixed $A : \mathrm{Prop}_{\mathcal{U}}$ for $P(B) :\equiv (A \leftrightarrow B)$. □

We have shown

$$\mathrm{WLOG}_{\mathbf{PropUF}} \leftrightarrow \mathrm{WLOG}_{\leftrightarrow} \leftrightarrow \mathrm{PropUA}_{\leftrightarrow} \leftrightarrow \mathrm{PropUA},$$

completing the proof. □

Concluding remarks. In the context of our running example, (8) is a rule for constructing a proof that "Every set with exactly 3 distinct elements can be ordered in exactly 6 distinct ways" from a proof that this statement is true of a specific 3-element set. In particular, let A be the set $\{a_1, a_2, a_3\}$ and P encode the property "can be ordered in exactly 6 ways", so that $P(A)$ asserts that "A can be ordered in exactly 6 ways". With this interpretation, the second half of (8), expressed formally as

$$\prod_{B:\mathrm{Prop}_{\mathcal{U}}} (A \simeq B) \to P(B),$$

translates to "For every B that is equivalent to A (i.e., for every B that is a set with exactly 3 elements), the elements of B can be ordered in exactly 6 ways". To obtain this conclusion, it is enough to prove $P(A)$, which we have done by exhaustively listing all of the possibilities in (1). The formal expression of $\mathrm{WLOG}_{\mathbf{PropUF}}$ in (8) thus makes the intuitive and obvious argument formally rigorous in a way that cannot be achieved in ZFC.

A remaining open question regarding UF's ability to satisfy (3) is whether its internal notion of equivalence, given by homotopy equivalence, can serve in the role of 'X-theoretic equivalence' for all practical instances of X. Tsementzis took up this question in [Tse16, Section 5], noting that while there is a way to make sense of $\sim_X$ in specific instances of 'X' (e.g., number theory, group theory, category theory), and that this formalization of $\sim_X$ in UF does coincide with $\simeq$, there is no general algorithm to prove this for general 'X'. Quoting [Tse16] (with $\sim_X$ and $\simeq$ substituted to be consistent with notation used here),

> "It might now appear that the relevant question to ask is whether $\simeq$ captures the *meaning* of our original informal notion $\sim_X$, whatever that may be. In one sense, this question is impossible to settle. There will always be room for a persistent skeptic to doubt that this has been achieved: 'Has the meaning of group isomorphism as mathematicians understand it really been captured by the appropriate instance of homotopy equivalence in UF?' [...] And in another sense, the question has a trivial answer. After all, the identity types in UF only 'see' those features of the terms being considered that were used to define these terms to begin with. And if we agree that the terms of [our

> formalization of the structure] adequately capture the features of objects of the class [of structures] that we are interested in (e.g. that they are sets, that they have a multiplicative operation etc.) then the identity type will 'see' all those features and thus preserve them."

So while we can never know for certain that all of mathematics can be suitably encoded in UF, cf. [Tse16], several instances have already been demonstrated without any clearcut examples in which the notion of identity implied by univalence fails to coincide with what should be intuitively expected. From this perspective, UF certainly provides a (little 'f') foundation of mathematical practice, in the sense of encoding specific instances of WLOG_X, when 'X' is homotopy theory, category theory, set theory, number theory, group theory, or graph theory [Uni, Tse16]. When combined with Theorem 1, these observations should inspire cautious optimism that UF can serve as a Foundation of Mathematical Practice, both in the sense of (3) and in the broader sense of "[permitting mathematicians] to do pretty much everything that [comes] naturally for them to do."

In making this latter assertion, I do not mean to suggest that mathematicians want to argue using the notation or terminology of homotopy type theory, or that such argumentation "comes naturally" to them. My point instead is that the proof system of UF allows practicing mathematicians to do whatever comes naturally without having to worry about it—as in the argument given above for the number of orderings of a 3 element set or more generally by appealing to "without loss of generality" when deemed appropriate.

By Theorem 1, the practitioner who argues WLOG could equivalently invoke the "structuralist" univalence axiom, and the structuralist who appeals to univalence could just as well argue without loss of generality, as the practitioner does. As such, practicing mathematicians face no dilemma between "acquiescing" in the formalism of ZFC (and having to abandon WLOG) and abandoning ZFC (and continuing to do what comes naturally). But a crisis looms for the dogmatic set theorist who, by Theorem 1 and Burgess's principle of indifference to identification quoted above, should be *indifferent* between the identical identifications of the 'structuralist' axiom of univalence and the 'pragmatist' method of proof WLOG. Neither one is consistent with ZFC, but the latter (and thus also the former) is ubiquitous in mathematical practice and is handled seamlessly by the Univalent Foundations. On pain of hypocrisy and logical inconsistency, the devout set theorist must either renounce WLOG, and render himself hopeless for solving many mathematical problems, or else acknowledge that the *practice* of mathematics is more consistent with the formalism of UF, and its "structuralist" axiom of univalence, than with that of ZFC.

References

[APW13] S. Awodey, A. Pelayo, and M.A. Warren, *Voevodsky's Univalence Axiom in Homotopy Type Theory*, Notices of the AMS **60** (2013), no. 9, 1164–1167.

[Awo14] S. Awodey, *Structuralism, Invariance, and Univalence*, Philosophia Mathematica **22** (2014), no. 1, 1–11.

[Bar89] J. Barwise, *Mathematical proofs of computer system correctness*, Notices Amer. Math. Soc. **36** (1989), no. 7, 844–851.

[Ben65] P. Benacerraf, *What numbers could not be*, The Philosophical Review **74** (1965), no. 1, 47–73.

[BT18] J. Burgess and D. Tsementzis, *Structuralism and Fidelity to Practice*, Unpublished manuscript (2018).

[Bur15] J.P. Burgess, *Rigor and Structure*, Oxford Press, 2015.

[Daw15] J.W. Dawson, *Why Prove it Again?: Alternative Proofs in Mathematical Practice*, 2015.

[Gow07] W.T. Gowers, *Hypergraph regularity and the multidimensional Szemerédi theorem*, Annals of Mathematics **166** (2007), 897–946.

[GT08] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167** (2008), 481–547.

[Hai14] M. Hairer, *A theory of regularity structures*, Invent. Math. **198** (2014), no. 2, 269–504.

[Law05] W. Lawvere, *An elementary theory of the category of sets*, Reprints in Theory and Applications of Categories **12** (2005), 1–35.

[Tao16] T. Tao, *The Erdős discrepancy problem*, Discrete Analysis **1** (2016). Accessed at arXiv:1509.05363 on April 12, 2018.

[TH17] D. Tsementzis and H. Halvorson, *Foundations and Philosophy*, Philosopher's Imprint (2017).

[Tse16] D. Tsementzis, *Univalent Foundations as Structuralist Foundations*, Synthese (2016).

[Uni] Univalent Foundations Program, The, *Homotopy Type Theory: Univalent Foundations of Mathematics.*

[Zha14] Y. Zhang, *Bounded gaps between primes*, Annals of Mathematics **179** (2014), 1121–1174. Accessed at http://valleytalk.org/wp-content/uploads/2013/05/YitangZhang.pdf.