Equivariant ZFA with Choice: a position paper

Murdoch J. Gabbay
Heriot-Watt University, Scotland, UK

Abstract: We propose Equivariant ZFA with Choice as a foundation for nominal techniques that is stronger than ZFC and weaker than FM, and why this may be particularly helpful in the context of automated reasoning.

1 Introduction

Nominal techniques assume a set $a, b, c, \ldots \in A$ of atoms; elements that can be compared for equality but which have few if any other properties. This deceptively simple foundational assumption has many applications—nominal abstract syntax (syntax-with-binding) [9, 11]; as implemented in Isabelle [12]; an open consistency problem [6]; a duality results [5, 8]; generalised finiteness for automata and regular languages [10, 1]; rewriting with binding [3]; and more.

So what is a foundation for nominal techniques?

Where this question is addressed in the nominal literature, the answer given is Fraenkel-Mostowski set theory (FM). In this position paper I will somewhat provocatively outline why this may have been a mistake, or at least a suboptimal choice. I will propose Equivariant ZFA with Choice (EZFAC) instead, and suggest why EZFAC may be especially suited to applications in automated reasoning and implementation. One standout point is that FM is inconsistent with the Axiom of Choice, whereas EZFA plus Choice (EZFAC) is consistent.

An expanded discussion of EZFAC is in [7].

2 Equivariant ZFA with Choice

Definition 2.1. The language of EZFAC is the language of sets with atoms—first-order logic with a binary predicate $\in$, and a single constant symbol $\lambda$ for the set of atoms, 1 Axioms are in Figure 1; notation is defined below.

Remark 2.2. Axioms (AtmEmp) to (Choice) are standard ZFAC (ZF with atoms and Choice). In rule (Choice), pset$^*$ is the nonempty powerset operator, since we cannot choose an element of the empty set.

Remark 2.3. ZF and ZFA are equally expressive: a model of ZFA embeds in one of ZF, 2 and vice-versa, and a predicate in ZFA can be translated (quite easily) to one in ZF.

Yet if the translation from ZFA to ZF leads to a quadratic increase in proof-size, or if ZFA is an environment which naturally lets us express native ZFA concepts, 3 then the gain from ZFA can be useful, as we will consider.

Definition 2.4. A permutation is a bijection on $A$. Define permutation action $\pi \cdot a$ by: $\pi \cdot a = \pi(a)$ if $a \in A$ and $\pi \cdot \emptyset = \emptyset$.

\begin{itemize}
  \item[(AtmEmp)] $t \in s \Rightarrow s \notin A$
  \item[(EmptySet)] $t \notin \emptyset$
  \item[(Ext)] $s, s' \notin A \Rightarrow (\forall t \cdot (b \in s \Leftrightarrow b \in s')) \Rightarrow s = s'$
  \item[(Pair)] $t \in \{ s, s' \} \Leftrightarrow (t = s \lor t = s')$
  \item[(Union)] $t \in \{ s \} \Leftrightarrow 3 a \cdot (t = a \land a \in s)$
  \item[(Pow)] $t \in \text{pset}(s) \Leftrightarrow t \subseteq s$
  \item[(Ind)] $(\forall s \cdot \{ y \in s. \phi(a = b) \}) \Rightarrow \phi \Rightarrow \forall s \cdot \phi(p\text{e}(\phi) = \{ a \})$
  \item[(Inf)] $\exists b \cdot \exists a \cdot c \in b \Rightarrow \exists a'.a' \in c \Rightarrow a \in \{ a \}$
  \item[(AtmInf)] $\neg (\exists a \cdot a \in A)$
  \item[(Replace)] $\exists b.\exists a \cdot a \in b \Rightarrow \exists a'.a' \in c \Leftrightarrow a = F(a')$
  \item[(Choice)] $\emptyset \neq \text{pset}^*(a) \Rightarrow \text{pset}^*$ nonempty powerset
  \item[(Equivar)] $\forall a \in \text{Perm}(\phi \Rightarrow a \notin a)$.
\end{itemize}

Figure 1: Axioms of EZFAC

Then given a predicate $\phi$ in the language of set theory with atoms, define $\pi \cdot \phi$ to be that predicate obtained by replacing every free variable $a$ with $\pi \cdot a$.

Remark 2.5. (Equivar) asserts that validity is preserved by permuting atoms in all parameters of a predicate. For instance if we have proved $\phi(a, b, c)$ for atoms $a, b, c \in A$ then taking $\pi = (a c)$ we have $\phi(c, b, a)$ and taking $\pi = (a b^i)(b^j)(c^j)$ we have $\phi(a^i, b^j, c^j)$. We do not have $\phi(a, b, a)$; this may still hold, but not by (Equivar) because no permutation takes $(a, b, c)$ to $(a, b, a)$.

This gives atoms a dual nature. Individually atoms point to themselves, 4 but collectively atoms have the flavour of variables ranging permutatively over $A$. 5

Remark 2.6. Equivariance is a native ZFA concept.

If our intuitions are ZF-shaped, then equivariance seems counterintuitive: “We can’t just permute elements. Suppose atoms are numbers: then are you claiming 1 < 2 if and only if 2 < 1?”. ZFA makes clear what is going on: the premise “Suppose atoms are numbers” makes no sense, because atoms are not numbers!

3 Equivariance, choice, and freshness

$\pi$ acts bijectively . . .

Lemma 3.1. Suppose $\mathfrak{M}$ is a model of ZFA$\langle C \rangle$. Then $\mathfrak{M} \vdash \pi y \in x$ if and only if $\mathfrak{M} \vdash y \in x$.

...so a model of ZFA or ZFAC already satisfies (Equivar) [4, Theorem 8.1.10]:

4In the Isabelle implementation of FM in my PhD thesis [4] this was literally so: I used Quine atoms such that $a = \{ a \}$. This removes the condition $a, b \notin A$ in (Ext), at a cost of some extremely mild nonwellfoundedness.

5To see this made precise see Subsection 2.6 and Lemma 4.17 of [2].
Theorem 3.2. If \( \mathcal{M} \) is a model of ZFA(C) then \( \mathcal{M} \) is also a model of EZFAC(C).

Proof. We prove \( \mathcal{M} \models \phi \iff \pi \cdot \phi \) by induction on \( \phi \). The case of \( \{ x \} \subseteq s \) is Lemma 3.1. The cases of \( \forall a, \phi \) and \( \mathcal{A} \) use the fact that \( \pi \) is bijective. Other cases are no harder. \( \square \)

Remark 3.3. Why do we need (Equivar)? While Theorem 3.2 shows how instances (Equivar) can be derived in ZFA, in practice the cost of proving them from first principles à la Theorem 3.2 scales with the complexity of the predicate \( \phi \). Instances of Theorem 3.2 can quadratically dominate development effort in a theorem-prover.\(^6\) This is the problem of \( \alpha \)-equivalence, come back to bite us. In contrast, axiom (Equivar) costs constant effort: namely, the cost of invoking the axiom.\(^7\) In this sense, equivariance is a natural axiom.

Remark 3.4. Choice compatible with equivariance. Surely arbitrary choices are inherently non-equivariant? Not if they are made inside \( \mathcal{M} \). Consider some choice-function \( f \in \text{pset}^*(x) \to y \). By Theorem 3.2 we immediately obtain \( \pi \cdot f \in \text{pset}^*(\pi \cdot y) \to \pi \cdot x \). In words: if \( f \) is a choice function for \( x \) in \( \mathcal{M} \) then by equivariance \( \pi \cdot f \) is a choice function for \( \pi \cdot x \) in \( \mathcal{M} \). We just permute atoms pointwise in the choice functions.

So the following are consistent with EZFA and derivable in EZFAC: “There exists a total ordering on \( \mathbb{A} \)”; “Every set can be well-ordered (even if the set mention atoms)”.

Remark 3.5. FM set theory has a finite support property for every \( x \) there exists \( A \subseteq \text{fin } \mathbb{A} \) such that if \( \forall a \in A. \pi(a) = a \) then \( \pi \cdot x = x \).

I argue that it is better to present freshness as a well-behavedness property in the larger EZFAC(C) universe. This is for several reasons:

1. Presenting (Fresh) as a well-behavedness property instead of an axiom eliminates the ‘But FM is inconsistent with Choice’ objection to nominal techniques. Anything we can do in FM, we can very easily do in EZFAC just by imposing finite support. Choice functions need not have finite support, but (unlike the case for FM) they still exist in the same EZFAC universe.

2. We sometimes specifically want non-supported elements; for example two recent papers \cite{7,8} are concerned with sets that have a notion of nominal support, but whose elements do not.

3. Support is not a hereditary property; e.g. ‘the set of all well-orderings of atoms’ is supported by \( \varnothing \), but no well-ordering of \( \mathbb{A} \) has finite support; or put another way, the FM universe is a proper subclass of the universe of finitely-supported elements.

4. Even if the reader’s next paper uses FM sets, it may be

\(^6\)This happened in the Isabelle/FM implementation in my thesis \cite{4}, and it was crippling. After my PhD I initiated a mark 2 development with an (Equivar) axiom-scheme (actually an Isabelle Oracle).

\(^7\)The modern nominal Isabelle implementation uses automated tactics to prove Theorem 3.2 for certain classes of \( \phi \), specialised to an application to nominal inductive datatypes. Nominal Isabelle good at what it does, but it is not (and never claimed to be) a universal nominal foundation.