Parametricity and excluded middle

Auke Booij

University of Birmingham

May 2016

Polymorphic functions

```
f :: forall x . x -> x
```

(Alternative notation: $f : \Pi_{X:\mathcal{U}} X \to X$ or $f_X : X \to X$.)
Must `f` be the identity function?
Parametricity says yes!
Parametricity gives *free theorems* about the terms of a language or logic $\mathcal{L}$.

Parametricity

Parametricity gives a property of the terms of a language.

But what can we say *internally*?
Can a logic say and/or prove that its own terms are well-behaved?

Parametricity and dependent type theory: known results

- There are parametric models of dependent type theory.
  Hence dependent type theory is parametric (as a metatheoretic claim).
  (e.g. Bernardy, Jansson, Paterson 2012)
- We can add internal parametricity to a type theory by extending the syntax.
  (e.g. Bernardy, Moulin 2012)
- Excluded middle is a non-parametric axiom.
  (e.g. Keller, Lasson 2012)
- There exist classical models of dependent type theory.
  So there is no hope of proving parametricity internally.
  (Such a proof would yield $\neg$LEM using the above.)

Can we obtain a constructive taboo from non-parametricity?

In some cases, yes!

Parametricity and dependent type theory: known results

- There are parametric models of dependent type theory.
  Hence dependent type theory is parametric (as a metatheoretic claim).
  (e.g. Bernardy, Jansson, Paterson 2012)
- We can add internal parametricity to a type theory by extending the syntax.
  (e.g. Bernardy, Moulin 2012)
- Excluded middle is a non-parametric axiom.
  (e.g. Keller, Lasson 2012)
- There exist classical models of dependent type theory.
  So there is no hope of proving parametricity internally.
  (Such a proof would yield $\neg$LEM using the above.)

Can we obtain a constructive taboo from non-parametricity?
In some cases, yes!

Homotopy Type Theory book

Exercise 6.9. Assuming LEM, construct a family $f : \Pi_{X:\mathcal{U}} X \to X$ such that $f_{\mathbf{2}} : \mathbf{2} \to \mathbf{2}$ is the non-identity automorphism.

Recall:

- LEM: law of excluded middle

$$\mathsf{LEM} :\equiv \Pi_{P:\mathsf{Prp}}\, P + \neg P$$

- Prp: type of propositions: those $P : \mathcal{U}$ with $x =_P y$ for all $x, y : P$
- non-identity automorphism on $\mathbf{2}$: boolean negation, a.k.a. flip
  Note: this map has no fixed points!

My contribution: This exercise has a converse!

Solution to exercise 6.9

Assuming LEM, construct a family $f : \Pi_{X:\mathcal{U}} X \to X$ such that $f_{\mathbf{2}} : \mathbf{2} \to \mathbf{2}$ is the non-identity automorphism.

- Notice that we can't simply do case analysis on whether the input type X is equivalent to $\mathbf{2}$, since this statement is not a proposition.
- Instead, take the $X : \mathcal{U}$ and $x : X$, and do case analysis on the existence of a unique point distinct from x.
- If such a point exists, return it.
  Otherwise return x.

Solution to exercise 6.9

Assuming LEM, construct a family $f : \Pi_{X:\mathcal{U}} X \to X$ such that $f_{\mathbf{2}} : \mathbf{2} \to \mathbf{2}$ is the non-identity automorphism.

- Notice that we can't simply do case analysis on whether the input type X is equivalent to $\mathbf{2}$, since this statement is not a proposition.
- Instead, take the $X : \mathcal{U}$ and $x : X$, and do case analysis on the existence of a unique point distinct from x.
- If such a point exists, return it.
  Otherwise return x.

Solution to exercise 6.9

Assuming LEM, construct a family $f : \Pi_{X:\mathcal{U}} X \to X$ such that $f_{\mathbf{2}} : \mathbf{2} \to \mathbf{2}$ is the non-identity automorphism.

- Notice that we can't simply do case analysis on whether the input type X is equivalent to $\mathbf{2}$, since this statement is not a proposition.
- Instead, take the $X : \mathcal{U}$ and $x : X$, and do case analysis on the existence of a unique point distinct from x.
- If such a point exists, return it.
  Otherwise return x.

Solution to exercise 6.9

Assuming LEM, construct a family $f : \Pi_{X:\mathcal{U}} X \to X$ such that $f_{\mathbf{2}} : \mathbf{2} \to \mathbf{2}$ is the non-identity automorphism.

- Notice that we can't simply do case analysis on whether the input type X is equivalent to $\mathbf{2}$, since this statement is not a proposition.
- Instead, take the $X : \mathcal{U}$ and $x : X$, and do case analysis on the existence of a unique point distinct from x.
- If such a point exists, return it.
  Otherwise return x.

Converse of exercise 6.9: statement

We will prove in intensional type theory:
Theorem. Suppose $f_X : X \to X$ is an *extensional* polymorphic function, such that $f_{\mathbf{2}} : \mathbf{2} \to \mathbf{2}$ is flip : $\mathbf{2} \to \mathbf{2}$. Then LEM holds.

A polymorphic function is *extensional* if it is invariant under isomorphisms. For $f_X : X \to X$, this means that whenever $e : X \to Y$ is an isomorphism, then for all $x : X$, it holds that $e(f_x(x)) = f_Y(e(x))$.

If $e : X \to Y$ is an isomorphism, then we write $X \simeq Y$, and we call X and Y *isomorphic*.

NB: For this talk, it is not important to distinguish between isomorphism and equivalence.

In particular, in univalent type theory, polymorphic functions are extensional. (But we will not restrict to this case.)

Converse of exercise 6.9, cont'd: proof idea

We'll work in a type theory with identity types.

Proving LEM means proving $P + \neg P$ for an arbitrary proposition P.

If P holds, then $\mathbf{1} + P \simeq \mathbf{2}$.
So f flips the elements of $\mathbf{1} + P$.
In particular, $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) \neq \mathsf{inl}(\star)$.

We'll decide P by looking at the action of f on the type $\mathbf{1} + P$.

Converse of exercise 6.9, cont'd: proof sketch

Suppose we are given $f : \Pi_{X:\mathcal{U}} X \to X$ with $f_{\mathbf{2}}$ boolean negation.

$$\mathsf{LEM} :\equiv \Pi_{P:\mathsf{Prp}}\, P + \neg P$$

We will prove LEM. So let $P : \mathsf{Prp}$ be an arbitrary proposition.
Consider $f_{\mathbf{1}+P}(\mathsf{inl}(\star))$: output is again in $\mathbf{1} + P$, so can do case analysis:

- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inr}(p)$ for some $p : P$: done
- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inl}(\star)$: Assume P. In that case, $\mathbf{1} + P \simeq \mathbf{2}$.
  Since we assumed that $f_{\mathbf{2}}$ was the flipping map, $\mathsf{inl}(\star)$ should not be a fixed point of $f_{\mathbf{1}+P}$! Contradiction.
  Hence $\neg P$.

Converse of exercise 6.9, cont'd: proof sketch

Suppose we are given $f : \Pi_{X:\mathcal{U}} X \to X$ with $f_{\mathbf{2}}$ boolean negation.

$$\mathsf{LEM} :\equiv \Pi_{P:\mathsf{Prp}}\, P + \neg P$$

We will prove LEM. So let $P : \mathsf{Prp}$ be an arbitrary proposition.

Consider $f_{\mathbf{1}+P}(\mathsf{inl}(\star))$: output is again in $\mathbf{1} + P$, so can do case analysis:

- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inr}(p)$ for some $p : P$: done
- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inl}(\star)$: Assume P. In that case, $\mathbf{1} + P \simeq \mathbf{2}$. Since we assumed that $f_{\mathbf{2}}$ was the flipping map, $\mathsf{inl}(\star)$ should not be a fixed point of $f_{\mathbf{1}+P}$! Contradiction. Hence $\neg P$.

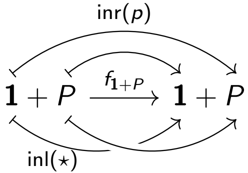
Converse of exercise 6.9, cont'd: proof sketch

Suppose we are given $f : \Pi_{X:\mathcal{U}} X \to X$ with $f_{\mathbf{2}}$ boolean negation.

$$\mathsf{LEM} :\equiv \Pi_{P:\mathsf{Prp}}\, P + \neg P$$

We will prove LEM. So let $P : \mathsf{Prp}$ be an arbitrary proposition.
Consider $f_{\mathbf{1}+P}(\mathsf{inl}(\star))$: output is again in $\mathbf{1} + P$, so can do case analysis:

- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inr}(p)$ for some $p : P$: done
- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inl}(\star)$: Assume P. In that case, $\mathbf{1} + P \simeq \mathbf{2}$. Since we assumed that $f_{\mathbf{2}}$ was the flipping map, $\mathsf{inl}(\star)$ should not be a fixed point of $f_{\mathbf{1}+P}$! Contradiction.
  Hence $\neg P$.



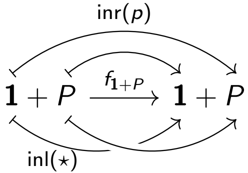
Converse of exercise 6.9, cont'd: proof sketch

Suppose we are given $f : \Pi_{X:\mathcal{U}} X \to X$ with $f_{\mathbf{2}}$ boolean negation.

$$\mathsf{LEM} :\equiv \Pi_{P:\mathsf{Prp}}\, P + \neg P$$

We will prove LEM. So let $P : \mathsf{Prp}$ be an arbitrary proposition.
Consider $f_{\mathbf{1}+P}(\mathsf{inl}(\star))$: output is again in $\mathbf{1} + P$, so can do case analysis:

- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inr}(p)$ for some $p : P$: done
- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inl}(\star)$: Assume P. In that case, $\mathbf{1} + P \simeq \mathbf{2}$. Since we assumed that $f_{\mathbf{2}}$ was the flipping map, $\mathsf{inl}(\star)$ should not be a fixed point of $f_{\mathbf{1}+P}$! Contradiction. Hence $\neg P$.



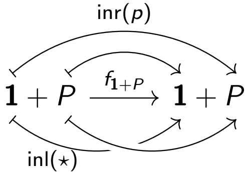
Converse of exercise 6.9, cont'd: proof sketch

Suppose we are given $f : \Pi_{X:\mathcal{U}} X \to X$ with $f_{\mathbf{2}}$ boolean negation.

$$\mathsf{LEM} :\equiv \Pi_{P:\mathsf{Prp}}\, P + \neg P$$

We will prove LEM. So let $P : \mathsf{Prp}$ be an arbitrary proposition.
Consider $f_{\mathbf{1}+P}(\mathsf{inl}(\star))$: output is again in $\mathbf{1} + P$, so can do case analysis:

- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inr}(p)$ for some $p : P$: done
- $f_{\mathbf{1}+P}(\mathsf{inl}(\star)) = \mathsf{inl}(\star)$: Assume P. In that case, $\mathbf{1} + P \simeq \mathbf{2}$.
  Since we assumed that $f_{\mathbf{2}}$ was the flipping map, $\mathsf{inl}(\star)$ should not be a fixed point of $f_{\mathbf{1}+P}$! Contradiction.
  Hence $\neg P$.



Conclusions, questions

- Non-parametricity can be seen as a constructive taboo.
- “If you build in sufficient reflection that you can pattern-match on your types, you’ve already built in LEM.” (Jacques Carette)

- Are there more instances of this? (yes)
- Can we find a general framework for deriving constructive taboos from (certain) non-parametricity?

Conclusions, questions

- Non-parametricity can be seen as a constructive taboo.
- "If you build in sufficient reflection that you can pattern-match on your types, you've already built in LEM." (Jacques Carette)

- Are there more instances of this? (yes)
- Can we find a general framework for deriving constructive taboos from (certain) non-parametricity?

Other instances: generalizations

Theorem. Suppose $f_X : X \to X$ is an *extensional* polymorphic function. Suppose we are given $X, Y : \mathcal{U}$, and an element $x : X$, and we assume that f_{X+Y} sends every element of X to Y (in other words, $f_{X+Y} \circ \mathsf{inl} : X \to X + Y$ factors through $\mathsf{inr} : Y \to X + Y$)

Then LEM holds.

This reduces to the previous case by taking $X = Y = \mathbf{1}$.

Other instances: Church numerals

Metatheoretically, the parametric terms of type

$$\Pi_{X:\mathcal{U}}(X \to X) \to (X \to X)$$

are Church numerals, namely $\lambda X.\lambda g.g^n$ for some natural number n.

Theorem. Suppose $f : \Pi_{X:\mathcal{U}}(X \to X) \to (X \to X)$ is extensional, and has $f_{\mathbf{2}}(\mathrm{id}_{\mathbf{2}}) = \mathrm{flip}$.
Then LEM holds.
Proof: Do case analysis on $f_{\mathbf{1}+P}(\mathrm{id}_{\mathbf{1}+P})(\mathrm{inl}(\star))$, as in the previous case.

Other instances: Boolean-valued functions

Metatheoretically, the parametric terms of type

$$\Pi_{X:\mathcal{U}} X \to \mathbf{2}$$

are constantly true or false.

Theorem. Suppose there is $X : \mathcal{U}$, and $x, y : X$, with $f_X(x) = \mathsf{tt}$ and $f_X(y) = \mathsf{ff}$, and that there is $e : X \simeq X$ with $e(x) = y$.
Then f cannot be extensional.

(But what about $X, Y : \mathcal{U}$, $x : X$, $y : Y$, $f_X(x) \neq f_Y(y)$ with X, Y not necessarily equivalent?)

Other instances: Rice's theorem for the universe

Theorem. Suppose $f : \mathcal{U} \to \mathbf{2}$ is extensional in the sense that if $X \simeq Y$ then $f(X) = f(Y)$
Further suppose that there are $X, Y : \mathcal{U}$ (not necessarily equivalent) with $f(X) = \mathtt{tt}$ and $f(Y) = \mathtt{ff}$.
Then we obtain the weak limited principle of omniscience.

(Escardó 2012)

(Recall Rice's theorem in computability theory: no non-trivial property of partial functions is decidable.)

Acknowledgements and references

The simplified proof for polymorphic identity I presented is due to my supervisor Martín Escardó.
Thanks to Uday Reddy for giving the talk on parametricity that inspired me to think about this.

HoTT book: `https://homotopytypetheory.org/`

Original proof is described in the extended abstract: *Parametricity and excluded middle* (April 2016)
(This proof was formalized in Agda using the HoTT-Agda library.)
`http://www.cs.bham.ac.uk/~abb538/`

Appendices

Univalence refresher

If $g : X \to Y$ is an isomorphism (i.e. g has a two-sided inverse h), then g is an equivalence. Write:

$$g : X \simeq Y$$

Univalence axiom: from an equivalence $g : X \simeq Y$ we may derive an identity $\mathrm{ua}(g) : X =_{\mathcal{U}} Y$.

Recall Prp: those $P : \mathcal{U}$ with $x =_P y$ for all $x, y : P$.

Given $p : P$, can define equivalence $P \simeq \mathbf{1}$ (by mapping everything in P to $\star : \mathbf{1}$, and mapping everything in $\mathbf{1}$ to $p : P$).
($\mathbf{1}$ is the type whose only point is $\star : \mathbf{1}$)

Contractible types and propositions

$$\mathrm{isContr}(A) :\equiv \Sigma_{a:A}\Pi_{x:A} a =_A x$$

$$\mathrm{isProp}(A) :\equiv \Pi_{x,y:A} x =_A y$$

In A is a proposition, inhabited $a : A$, we can take a to be the center of contraction.

$\mathbf{1}$ is contractible. If A is contractible, then $A \simeq \mathbf{1}$.