II.2. Case Study: Unary and Binary Numbers
(after Vezzosi / Mörtberg / Abel '19)

Unary number $\mathbb{N}$

positive binary numbers Pos = inductive type with constructor
$pos1 : Pos$, $x0 : Pos \to Pos$, $x1 : Pos \to Pos$

binary number Bin = inductive type with constructors
$bin0 : Bin$, $binpos : Pos \to Bin$

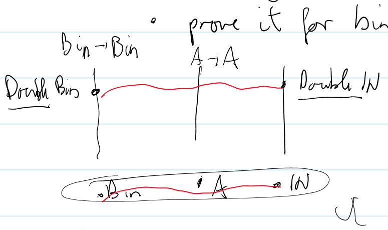
$\exists$ isomorphism $f : Bin \to \mathbb{N}$, $g : \mathbb{N} \to Bin$ with $f(g(n)) = n$, $g(f(b)) = b$ &
g preserves $+ \, (*, \ldots)$

$g(6) \equiv binpos(\underbrace{x0\,(x1\,(pos1))}_{Pos}) \equiv 110$

$0 \quad 1 \quad 1$

$\boxed{\mathbb{N} \text{ is good for definitions \& proofs}, \; Bin \text{ is good for effective calculation}}$

Challenge: Calculate $2^{20} = 2^5 \times 2^{15}$ in a proof using $\mathbb{N}$
- normalize unary representations to idpath: extremely ineffective
- use algebraic manipulation by hand: can get demanding
- prove it for binary numbers, transport the proof over $P : Bin = \mathbb{N}$



over which type family?

defined as Martin-Löf equality

from isomorphism, with $P_* b = f(b)$?
⇝ univalence!

$\underline{Double} : \Pi(A : U), A \to A$

$\underline{DoubleBin} : \underline{Double}\ Bin$ (easy to construct & effective for binary numbers)

$\underline{Double}\ Bin = Bin \to Bin$

P_*

$\underline{Double\mathbb{N}} : \underline{Double}\ \mathbb{N}$ (easy to show $Double\mathbb{N}\ m = 2 * m$)

$\underline{Double}\ \mathbb{N} = \mathbb{N} \to \mathbb{N}$

$\underline{doubles} : \Pi(A : U)(D : \underline{Double}\ A) \to \mathbb{N} \to A \to A$

Assume A, D, n: Do induction on n:
- $n \equiv 0 : \mapsto id_A$
- $n \equiv Sm : \mapsto D(\underline{doubles}\ A\ D\ m)$

type family $\underline{doubles}\ A\ D\ 20 = \underline{doubles}\ A\ D\ 5\ (\underline{doubles}\ A\ D\ 15)$

$A \equiv Bin,\ D = \underline{DoubleBin}$ $\qquad$ $A \equiv \mathbb{N}$ $D \equiv Double\mathbb{N}$

proof of $2^{20} = 2^5 \times 2^{15}$ $\longrightarrow$ proof of $2^{20} = 2^5 \times 2^{15}$

$A \equiv \mathrm{Bin}$, $D = \mathrm{DoubleBin}$ $\qquad$ $A \equiv \mathrm{UN}$ $\quad D \equiv \mathrm{DoubleUN}$

$$\text{proof of } 2^{20} = 2^5 \times 2^{15} \xrightarrow{\quad p_* \quad} \text{proof of } 2^{20} = 2^5 \times 2^{15}$$

(as binary numbers) $\qquad\qquad$ (as unary numbers)

Problem: The calculation will only happen "automagically" if $p_*(b) \equiv f(b)$

⇝ constructiveness of univalence ⇝ cubical type theory

- Why can't you do with the isomorphism? ⇝ More proof obligations! Not automagic!
- Is univalence only good for calculations? Localization: $(R[f^{-1}])[g^{-1}] \cong R[(fg)^{-1}]$

Localization in categories!

II.3 Equivalences

How to obtain equalities in $A = B$ from isomorphisms between A and B?

homotopies $f \circ g \sim \mathrm{idmap}_B$ and $g \circ f \sim \mathrm{idmap}_A$

$$f : A \to B, \quad \underbrace{g : B \to A, \quad \eta : \prod_{b:B} f(g(b)) = b, \quad \varepsilon : \prod_{a:A} g(f(a)) = a}_{g \text{ is quasi-inverse to } f \ \rightsquigarrow\ (g, \eta, \varepsilon) : \mathrm{qinv}(f)}$$

$$\mathrm{idtoqinv} : \prod_{A,B:\mathcal{U}} A = B \longrightarrow \sum_{f:A\to B} \mathrm{qinv}(f) \quad :\equiv \quad \text{Assume } A, B, p : A = B.$$

Do path induction on p: Take $f \equiv g \equiv \mathrm{idmap}_A$,

$\eta \equiv \varepsilon \equiv (a : A \mapsto \mathrm{idpath}_a)$.

Theorem: There is no (quasi-) inverse $\mathrm{qinvtoid} : \prod_{A,B:\mathcal{U}} \sum_{f:A\to B} \mathrm{qinv}(f) \to A = B$ to $\mathrm{idtoqinv}$.

subtle - only fails when considering equalities of equalities, unique for many standard mathematical objects, but not for all: stacks resp. 2-categories, ...

Proof: Assume $\mathrm{qinvtoid}$ inverse to $\mathrm{idtoqinv}$ exists.

- Key observation: Quasi-isomorphisms $(f, g, \eta, \varepsilon)$ produced by $\mathrm{idtoqinv}$ are half-adjoint, i.e.

$$\boxed{\tau : \prod_{a:A} \underbrace{f(\varepsilon a)}_{f(g(f(a))) = f(a)} = \eta(fa) \quad \Big(\text{or equivalently, } \prod_{b:B} \underbrace{g(\eta b)}_{g(f(g(b))) = gb} = \varepsilon(gb)\Big)}$$

see (4) below.

Proof: By induction on $p : A = B$.

⇒ all quasi-isomorphisms must be half-adjoint, under the assumption.

⇝ Contradiction by constructing quasi-isomorphisms that are not half-adjoint.

Simplest choice of inverse maps between two types: $f :\equiv \mathrm{idmap}_A : A \to A$, $g :\equiv \mathrm{idmap}_A : A \to A$ ⇝ homotopies $\eta, \varepsilon : \prod_{a:A} a = a$ ⇝ half-adjointness $\tau : \prod_{a:A} \varepsilon a = \eta a$

$g :\equiv \mathrm{idmap}_A : A \to A$ $\quad a : A \quad a : A$

$\rightsquigarrow$ want to construct two non-equal objects in $\prod_{a:A} a = a$ for some type A.

- Key building block: nonequal equalities of inductive type $\mathbf{2}$, with constructors $0_{\mathbf{2}}, 1_{\mathbf{2}} : \mathbf{2}$.

  Inductively construct two functions $\mathrm{id}_{\mathbf{2}} : \mathbf{2} \to \mathbf{2} :\equiv 0_{\mathbf{2}} \mapsto 0_{\mathbf{2}},\ 1_{\mathbf{2}} \mapsto 1_{\mathbf{2}}$

  $\mathrm{nonid}_{\mathbf{2}} : \mathbf{2} \to \mathbf{2} :\equiv 0_{\mathbf{2}} \mapsto 1_{\mathbf{2}},\ 1_{\mathbf{2}} \mapsto 0_{\mathbf{2}}$

(1) Apply equality of functions on objects: $f, g : A \to B,\ p : f = g,\ a : A \mapsto p(a) : f(a) = g(a) :\equiv$ Do induction on p: Take $\mathrm{idpath}_{f(a)}$.

(2) $0_{\mathbf{2}} \neq 1_{\mathbf{2}}$: Construct $\mathrm{code}_{\mathbf{2}} : \mathbf{2} \to \mathbf{2} \to \mathcal{U} :\equiv \begin{cases} 0_{\mathbf{2}}, 0_{\mathbf{2}} \ \&\ 1_{\mathbf{2}}, 1_{\mathbf{2}} \mapsto \mathrm{True} \\ 0_{\mathbf{2}}, 1_{\mathbf{2}} \ \&\ 1_{\mathbf{2}}, 0_{\mathbf{2}} \mapsto \mathrm{False} \end{cases}$

$\boxed{\text{encode-decode method}}$

$\mathrm{encode}_{\mathbf{2}} : \prod_{a,b:\mathbf{2}} a = b \to \mathrm{code}_{\mathbf{2}}(a,b) :\equiv$ Do induction on $p : a = b$. Take $tt : \mathrm{True}$

$p : 0_{\mathbf{2}} = 1_{\mathbf{2}} \xrightarrow{\mathrm{encode}_{\mathbf{2}}(0_{\mathbf{2}}, 1_{\mathbf{2}})} pc : \mathrm{code}_{\mathbf{2}}(0_{\mathbf{2}}, 1_{\mathbf{2}}) \equiv \mathrm{False}$: contradiction.

(3) $\mathrm{id}_{\mathbf{2}} \neq \mathrm{nonid}_{\mathbf{2}}$: Apply $p : \mathrm{id}_{\mathbf{2}} = \mathrm{nonid}_{\mathbf{2}}$ on $0_{\mathbf{2}}$ as in (1) $\rightsquigarrow$ contradiction to (2)

(4) Applying a function on an equality of objects: $f : A \to B,\ p : a_1 =_A a_2 \mapsto f(p) : f(a_1) =_B f(a_2) :\equiv$ Do induction on p. Take $\mathrm{idpath}_{f(a)}$.

(5) $\mathrm{idp}_{\mathbf{2}} :\equiv \mathrm{quivtoid}(\mathrm{id}_{\mathbf{2}}) \overset{(3),(4)\ \&\ \mathrm{idtoquiv}\text{ inverse to quivtoid}}{\neq} \mathrm{quivtoid}(\mathrm{nonid}_{\mathbf{2}}) \equiv: \mathrm{nonidp}_{\mathbf{2}}$

Non-equal objects in $\prod_{a:A} a = a$: $\quad A :\equiv \mathcal{U}$ ($\rightsquigarrow a :\equiv \mathbf{2}$ possible)?

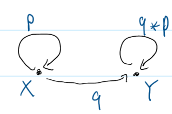
But how to construct equalities in $X = X$ for all $X : \mathcal{U}$ uniformly, such that $\mathbf{2}$ is mapped to $\mathrm{nonidp}_{\mathbf{2}}$?

Idea: Provide type $X : \mathcal{U}$ with equality $p : X = X \rightsquigarrow A :\equiv \sum_{X:\mathcal{U}} X = X$

$r : \prod_{A : \sum_{X:\mathcal{U}} X = X} A = A :\equiv (X, p) \mapsto (\mathrm{idpath}_X, \mathrm{idpath}_p : p = (\mathrm{idpath}_X)_* p) : (X,p) = (X,p)$

$\uparrow$ characterization of equality in Σ-types

$u : \prod_{A : \sum_{X:\mathcal{U}} X = X} A = A :\equiv (X, p) \mapsto (p, Q : p = p_* p)$



$\uparrow$ constructed by induction on $q : X = Y$: $q_* p = q^{-1} \bullet p \bullet q$;

$\uparrow \uparrow$ concatenation of equalities

set $q :\equiv p$: $p^{-1} \bullet p = \mathrm{idpath}$

$\mathrm{idpath} \bullet p = p$.

$r(\mathbf{2}, \mathrm{nonidp}_{\mathbf{2}}) \neq u(\mathbf{2}, \mathrm{nonidp}_{\mathbf{2}})$: project to the first component and use (5)

$\Longrightarrow (\mathrm{idmap}_{\sum_{X:\mathcal{U}} X = X}, \mathrm{idmap}_{\sum_{X:\mathcal{U}} X=X}, r, u)$ not half-adjoint $\Longrightarrow$ $\lightning$

<u>Definition</u>: $f : A \to B$ is called an equivalence if it has an inverse $g : B \to A$ checked by homotopies

Definition: $f : A \to B$ is called an equivalence if it has an inverse $g : B \to A$ checked by homotopies $\eta : b \mapsto f(g(b)) = b$ and $\varepsilon : a \mapsto g(f(a)) = a$ that are half-adjoint

$A \simeq B$: type of equivalences between A and B

Remark: The HoTT-Book presents 3 more, but equivalent definitions of equivalence.

Lemma: Adjointification

Quasi-inverses (g, η, ε) of a function $f : A \to B$ yields equivalences $(g, \eta', \varepsilon, \tau)$.

Proof: (1) $f, g : A \to B$, $H : f \sim g$, $p : a =_A b$ $\rightsquigarrow$

$$\begin{tikzcd} f(a) \arrow[r, equal, "Ha"] \arrow[d, equal, "f(p)"'] & g(a) \arrow[d, equal, "g(p)"] \\ f(b) \arrow[r, equal, "Hb"'] & g(b) \end{tikzcd} \quad \equiv \quad f(p) \cdot Hb = Ha \cdot g(p) : f(a) = g(b) :$$

Do induction on p.

(2) $\underset{A \to A}{H : f \sim id_A}$, $a : A$ $\rightsquigarrow$

$$\begin{tikzcd} ffa \arrow[r, equal, "Hfa"] \arrow[d, equal, "f(Ha)"'] & f(a) \arrow[d, equal, "Ha"] \\ fa \arrow[r, equal, "Ha"'] & a \end{tikzcd} \quad \equiv \quad f(Ha) \cdot Ha = Hfa \cdot Ha : ffa = a$$

apply (1) with $g :\equiv id_A$, $p :\equiv Ha$

$\Rightarrow$ $fHa = Hfa : ffa = fa$: cancel Ha

Set $\eta'(b) :\equiv \eta(f(g(b)))^{-1} \cdot f(\varepsilon(g(b))) \cdot \eta(b)$

$\Rightarrow$ $\tau(a) : f(\varepsilon(a)) = \eta(f(g(f(a))))^{-1} \cdot \eta(f(g(f(a)))) \cdot f(\varepsilon a)$

$f(g(f(g(f(a)\ldots) = f(g(f(a))) = f(a)$

$\|$ (1) with $H :\equiv \eta : f \circ g \sim id_B$, $p :\equiv f(\varepsilon a)$

$\quad - \; " \; - \cdot f(g(f(\varepsilon a))) \cdot \eta(f(a))$

$f(g(f(g(f(a)\ldots) = f(g(f(a)))$

$\|$ (2) with $H :\equiv \varepsilon : g \circ f \sim id_A$, $a :\equiv a$

$\quad - \; " \; - \cdot f(\varepsilon(g(f(a)\ldots) \cdot - \; " \; - \; = \eta'(f(a))$

II.4. Univalence

idtoequiv : $A = B \to A \simeq B$ Do induction on $p : A = B$

$\text{idpath } A \mapsto (\text{idmap}_A, \text{idmap}_A, \lambda(a:A), \text{idpath } A, \lambda(a:A), \text{idpath } A, \lambda(a:A), \text{idpath}(\text{idpath } A))$

Univalence Axiom: idtoequiv is an equivalence

$$\Pi(A, B : \mathcal{U}), \boxed{(A = B) \simeq (A \simeq B)}$$

Theorem (Voevodsky '06) HoTT with Univalence is (at least) as consistent as ZF(C).

Idea of Proof: Construct model of HoTT in category of simplicial sets, using a universal Kan fibration

Emily Riehl: On the ∞-topos semantics of HoTT arXiv 2024

Idea of Proof: Construct model of HoTT in category of simplicial sets, using a universal Kan fibration

Emily Riehl: On the ∞-topos semantics of HoTT, arXiv 2024

Alternative characterisation of univalence

Definition: $A : \mathcal{U}$ is called contractible if there is a base $a_0 : A$ and an equality $a_0 = a$ for all $a : A$.

Lemma 1: Two contractible types A, B are equivalent.

Proof: $f :\equiv a \mapsto b_0 : A \to B$ and $g :\equiv b \mapsto a_0$ are inverse to each other.

Lemma 2: A type A is contractible if it can be retracted to a contractible type B i.e., there are $f : A \to B$, $g : B \to A$ such that $g(f(a)) = a$ for all $a : A$.

Proof: $f(a) = b_0$, hence $a = g(f(a)) = g(b_0) \equiv: a_0$ for all $a : A$.

Proposition 1: Assume univalence. Then: The fibers $f^{-1}(b) :\equiv \sum_{a:A} f(a) = b$ of an equivalence $f : A \to B$ are contractible, for all $a : A$.

Proof: Univalence $\Rightarrow$ $f = \mathrm{idtoequiv}(p)$ for some $p : A = B$. Do induction on p:
$\mathrm{idpath}\ A : A = A \rightsquigarrow f \equiv \mathrm{idmap}_A \rightsquigarrow f^{-1}(b) \equiv \sum_{a:A} a = b$, contractible to $\langle b, \mathrm{idpath}\ b \rangle$.

Remark: The inverse also holds, see [HoTT-Book, Thm. 4.4.3]