of course done. Otherwise, $f(n), f(m)$ cannot both be smaller than N, as $g(n) = g(m)$. In both remaining cases, $f(n) = g(n) = g(m) = f(N+1)$ and $f(N+1) = g(n) = g(m) = f(m)$, we are done. □

We can now rule out the existence of equivalences between finite sets of different size.

cor:Fin-n-injective

Corollary 2.17.7. *If $m < n$, then $(\sum_{k:\mathbb{N}} k < m) \neq (\sum_{k:\mathbb{N}} k < n)$.*

Another application of Definition 2.17.4 is a short proof of Euclidean division.

lem:euclid-div

Lemma 2.17.8. *For all $n, m : \mathbb{N}$ with $m > 0$ there exist $q, r : \mathbb{N}$ such that $r < m$ and $n = qm + r$.*

Proof. Define $P(k) :\equiv (n \leq km)$. Since $m > 0$ we have $P(n)$. Now set $k :\equiv \mu_P(n)$ as in Definition 2.17.4. If $n = km$ and we set $q :\equiv k$ and $r :\equiv 0$. If $n < km$, then $k > 0$ and we set $q :\equiv k - 1$. By minimality we have $qm < n < km$ and hence $n = qm + r$ for some $r < m$. □

2.18 *The type of finite types*

sec:typeFin

Recall from Section 2.6.1 the types False, True and Bool containing zero, one and two elements, respectively. We now define generally the type of n elements for any $n : \mathbb{N}$.

def:finiteset

Definition 2.18.1. For any type X define $\mathrm{succ}(X) :\equiv X \amalg \mathrm{True}$. Define inductively the type family $F(n)$, for each $n : \mathbb{N}$, by setting $F(0) :\equiv \emptyset$ and $F(S(n)) :\equiv \mathrm{succ}(F(n))$. Now abbreviate $\mathbb{n} :\equiv F(n)$. The type $\mathbb{n}$ is called the type with n elements, and we denote its elements by $0, 1, \ldots, n-1$ rather than by the corresponding expressions using inl and inr.

xca:finite-types

Exercise 2.18.2.

(1) Denote in full all elements of ~~$\emptyset$,~~ $\mathbb{1}$, and $\mathbb{2}$. Bbb 0 here

(2) Show (using ~~UA~~) that $\mathbb{1} = \mathrm{True}$, $\mathbb{2} = \mathrm{Bool}$. univalence

(3) Show (using ~~UA~~) that $\mathbb{n} = \sum_{k:\mathbb{N}} k < n$ for all $n : \mathbb{N}$. univalence

(4) Show that ~~$n = m$~~ if $\mathbb{m} = \mathbb{n}$. m = n

lem:maxonefinitetype

Lemma 2.18.3.

(1) $\sum_{n:\mathbb{N}} \|X = \mathbb{n}\|$ *is a proposition, for all types X.* It would be useful to call this proposition "being finite" now and to introduce notation "isFinite"

(2) $\sum_{X:\mathcal{U}} \sum_{n:\mathbb{N}} \|X = \mathbb{n}\| = \sum_{X:\mathcal{U}} \|\sum_{n:\mathbb{N}} X = \mathbb{n}\|$.

Proof. (1) Assume $(n, p), (m, q) : \sum_{n:\mathbb{N}} \|X = \mathbb{n}\|$. Then we have $\|\mathbb{n} = \mathbb{m}\|$, so $\|n = m\|$ by Exercise 2.18.2. But $\mathbb{N}$ is a set by Theorem 2.16.2, so $\|n = m\| = (n = m)$. It follows that $(n, p) = (m, q)$.

(2) Follows from $\sum_{n:\mathbb{N}} \|X = \mathbb{n}\| = \|\sum_{n:\mathbb{N}} X = \mathbb{n}\|$, which is easily proved by giving functions in both directions and using UA. □

The above lemma remains ~~of course~~ true if X ranges over Set. If a set S is in the same component in Set as $\mathbb{n}$ we say that *S has cardinality n* or that *the cardinality of S is n*.

def:groupoidFin

DEFINITION 2.18.4. The *groupoid of finite sets* is defined by

$$\mathrm{fin} :\equiv \sum_{S:\mathrm{Set}} \|\sum_{n:\mathbb{N}} S = \mathbb{n}\|.$$

use "isFinite" here

For $n : \mathbb{N}$, the *groupoid of sets of cardinality n* is defined by

$$\mathrm{fin}_n :\equiv \sum_{S:\mathrm{Set}} \|S = \mathbb{n}\|.$$

Observe that $\mathrm{fin}_0 = \mathrm{fin}_1 = \mathbb{1}$ and $\mathrm{fin} = \sum_{n:\mathbb{N}} \mathrm{fin}_n$ by Lemma 2.18.3.

Note that fin is the image of the map $F : \mathbb{N} \to \mathcal{U}$ from Definition 2.18.1, and is hence essentially $\mathcal{U}$-small (for any universe $\mathcal{U}$), by Principle 2.15.6.

2.19 *More equivalences*

sec:more-on-equivalences

In this section we collect a number of useful results on equivalences.

lem:ap-equivalence

LEMMA 2.19.1. *If $f : A \to B$ is an equivalence, then so is each $\mathrm{ap}_f : (a = a') \to (f(a) = f(a'))$ for all $a, a' : A$.*

Proof. Let $f^{-1} : B \to A$ be the inverse of f, then we have $\mathrm{ap}_{f^{-1}} : (b = b') \to (f^{-1}(b) = f^{-1}(b'))$ for all $b, b' : B$. Consider $\mathrm{ap}_{f^{-1}}$ for $b :\equiv f(a)$ and $b' :\equiv f(a')$. Then the codomain is $f^{-1}(f(a)) = f^{-1}(f(a'))$, and not $a = a'$. However, we have $h(x) : f^{-1}(f(x)) = x$ for every $x : A$, so the codomain of $\mathrm{ap}_{f^{-1}}$ is equivalent to the domain of ap_f.

We apply Lemma 2.7.8. We take the inverse of ap_f to map $q : f(a) = f(a')$ to $h(a') \cdot \mathrm{ap}_{f^{-1}}(q) \cdot h(a)^{-1} : a = a'$. We then have to prove $h(a') \cdot \mathrm{ap}_{f^{-1}}(\mathrm{ap}_f(p)) \cdot h(a)^{-1} = p$ for all $p : a = a'$, as well as $\mathrm{ap}_f(h(a')) \cdot \mathrm{ap}_{f^{-1}}(q) \cdot h(a)^{-1}) = q$ for all $q : f(a) = f(a')$.

The first roundtrip is easy by induction on p. The reader may also recognize a naturality square as in Definition 2.4.4 based on the homotopy h. The second roundtrip also uses the other homotopy $i(y) : f(f^{-1}(y)) = y$ for all $y : B$. This case is more involved and uses several applications of Definition 2.4.4. We refrain from giving all details.[41] □

[41] A short proof can be obtained from Lemma 2.19.8.

The converse of Lemma 2.19.1 is not true: $f : \mathbb{1} \to \mathbb{2}$ sending 0 to 0 is not an equivalence. As a function between sets, f is an injection (one-to-one), but not a surjection. We need these important concepts for types in general. We define them as close as possible to their usual meaning in set theory: a function from A to B is surjective if the preimage of any $b : B$ is non-empty, and injective if such preimages contain at most one element.

def:injection

DEFINITION 2.19.2. A function $f : A \to B$ is an *injection*, or *injective*, if $f^{-1}(b)$ is a proposition for all $b : B$. A function $f : A \to B$ is a *surjection*,