Countability of Inductive Types Formalized in the Object-Logic Level

Qinxiang Cao   Xiwei Wu [*]

Abstract: The set of integer number lists with finite length, and the set of binary trees with integer labels are both countably infinite. Many inductively defined types also have countably many elements. In this paper, we formalize the syntax of first order inductive definitions in Coq and prove them countable, under some side conditions. Instead of writing a proof generator in a meta language, we develop an axiom-free proof in the Coq object logic. In other words, our proof is a dependently typed Coq function from the syntax of the inductive definition to the countability of the type. Based on this proof, we provide a Coq tactic to automatically prove the countability of concrete inductive types. We also developed Coq libraries for countability and for the syntax of inductive definitions, which have value on their own.

Keywords: countable, Coq, dependent type, inductive type, object logic, meta logic

1   Introduction

In type theory, a system supports inductive types if it allows users to define new types from constants and functions that create terms of objects of that type. The Calculus of Inductive Constructions (CIC) is a powerful language that aims to represent both functional programs in the style of the ML language and proofs in higher-order logic [16]. Its extensions are used as the kernel language of Coq [5] and Lean [14], both of which are widely used, and are widely considered to be a great success. In this paper, we focus on a common property, countability, of all first-order inductive types, and provide a general proof in Coq's object-logic. The techniques that we use in this formalization can be useful for formally proving other properties of inductive types in the future.

Here we show some examples of inductive types that we will use in this paper :

```
Inductive natlist :=  Cons : nat → natlist → natlist
                    | Nil  : natlist.
Inductive bintree :=  Node : nat → bintree → bintree → bintree
                    | Leaf : bintree.
Inductive expr := andp   : expr → expr → expr
                | orp    : expr → expr → expr
                | impp   : expr → expr → expr
                | falsep : expr
                | varp   : nat → expr.
```

As demonstrated above, `natlist` (list of natural numbers), `bintree` (binary trees with natural numbers as labels) and `expr` (the expressions of propositional language with `nat` as variable identifiers) can be defined inductively in the Coq proof assistant [5]. Here, the word "inductive" means that `natlist`, `bintree` and `expr` are the smallest of all sets that satisfy the above typing constraints. Specifically,

---

[*]Parallel authorship, equal contribution. Corresponding author: Qinxiang Cao.

`natlist` is defined as the smallest set containing "`Nil`" and closed by the "`Cons`" constructor, which allows us to define a recursive function `length` on `natlist` so that `length Nil = 0`, `length (Cons x l) = 1 + length l`, and to prove related properties by induction on the structure of `natlist`.

Countability is a basic property of sets. To state that a set is countable means that it has the same cardinality as some subset of the set of natural numbers. For example, in the Henkin style proof of FOL completeness [8], one important step is to construct a maximal consistent set Ψ by expanding a consistent set Φ of propositions:

$$
\begin{aligned}
\Psi_0 &:= \Phi \\
\Psi_{n+1} &:= \Psi_n \cup \{\phi_n\} \quad &&(\text{if } \Psi_n \cup \phi_n \text{ is consistent}) \\
\Psi_{n+1} &:= \Psi_n \quad &&(\text{if } \Psi_n \cup \phi_n \text{ is inconsistent}) \\
\Psi &:= \bigcup_n \Psi_n \quad &&\text{where } \phi_0, \phi_1, \dots \text{ are all FOL propositions.}
\end{aligned}
$$

In that proof, it is critical that the set of all FOL propositions is countable. The countability property allows us to enumerate all propositions as $\phi_0, \phi_1, \dots$. As another example, we can show the countability of computable functions by proving the countability of untyped lambda expressions. Since the set of all functions from natural numbers to natural numbers is uncountable, there must exist at least one uncomputable function. Like FO-propositions and lambda expressions, many sets can be formalized as inductive types, and we focus on the countability of the inductive types in this paper.

Proving `natlist` to be countable is straightforward. (1) The only `natlist` of length 0 is `Nil`. (2) The `natlist`s of length $(n+1)$ should be countable if those `natlist`s of length n are countable (because the former set is isomorphic with the Cartesian product of $\mathbb{N}$ and the latter set). (3) By induction, the set of `natlist`s of length n is countable for any n. (4) The set of all `natlist`s is a union of countably many countable sets, and thus is countable (because we can easily construct an bijection from $\mathbb{N}^2$ to $\mathbb{N}$: $f(x,y) = 2^x(2y+1) - 1$ and the construction does not even need the choice axiom). Similarly, natural number labeled binary trees with size n are countable for any n. Thus, the elements of `bintree` are countable. It is natural to apply the same proof idea to a more complex inductive type. We define a *rank* function to generalize the length function for `natlist` and the size function for binary trees (with some slight modification). For example, the `rank` function on `natlist` and `bintree` satisfies:

```
rank Nil = 1
rank (Cons n l) = rank l + 1
rank Leaf = 1
rank (Node n l r) = rank l + rank r + 1
```

We prove that given a fixed inductive type, its elements with rank less than n are countable[1]. Then, all elements of this type are also countable since the set is a union of countably many countable sets. One could write Coq tactics, which is a meta language, to describe our proof ideas above. In contrast, our target in this paper is to formally prove one single theorem in the object language for general inductive types' countability.

Handling general inductive types in Coq's object language is hard. Coq's object language, Gallina, has built-in support for recursive functions and inductive proofs, as long as they are about concrete inductive types. For general inductive types, we do not have such support, and even simple pattern match expressions are not easy to formalize. We choose to derive recursive functions and inductive proof

---

[1]In the general proof, we consider elements with rank less than n, not elements with rank equal to n

principles from general recursive functions. Using concrete inductive types as an example, `natlist`'s general recursive function is:

```
natlist_rect
   : forall P : natlist → Type,  P Nil →
     (forall (n : nat) (l : natlist), P l → P (Cons n l)) →
     forall l : natlist, P l
```

It satisfies, for any (maybe dependently typed) P and F_0, F_1,

```
natlist_rect P F₀ F₁ Nil = F_0
natlist_rect P F₀ F₁ (Cons n l) = F_1 n l (natlist_rect P F₀ F₁ l)
```

We generalize the combination of `natlist_rect` and the two equalities above, and develop our proofs based on them.

Theoretically, it is more difficult to do something at the object-logic level than at the meta-logic level. Any proof formalized at the object-logic level is a Coq function from its assumptions to its conclusion, according to Curry-Howard correspondence. One can always develop a corresponding meta-language function that implements the "same" functionality. In contrast, some statements are only provable in a meta-logic, but are unprovable in the object logic. Martin Hofmann and Thomas Streicher showed that the principle of uniqueness of identity proofs is not derivable in the object logic itself [12].

Practically, our proof automation, which uses object-logic proofs, is more efficient than proof generators written in a meta-language. Our tool can prove `expr` countable in Coq in 0.089 seconds but a tactic-based proof will take 1.928 seconds to finish the proof[2] (see Coq development for more details). This result arises because our tool only requires Coq to typecheck one theorem with its arguments, but proofs, either proof scripts or proof terms, generated by a meta-language generator require Coq to type-check every single proof step.

In this paper, we formalize the general proof of countability theorem mentioned above, using Coq, and automate our proof to avoid repeating the long proof process. There are several ways in which this goal may be achieved. One is to use external tools to generate the operations and proofs of corresponding lemmas. For example, DBGen [17] generates single-variable substitution operations, and Autosubst2 [20] can generate substitution-related definitions and Coq proof terms. Another approach is to use the internal facility of theorem provers, which is written in a built-in meta language, to generate proof terms or proof scripts. Brian Huffman and Alexander Krauss (old datatype), and Jasmin Blanchette (BNF datatype) have developed tactics, which is a meta language, to prove datatypes countable [21] in Isabelle/HOL.

In comparison, an object logic proof of "for any possible T, $P(T)$ holds" is one singleton proof term of type $\forall T, P(T)$. A meta-logic proof is a meta-level program (with probably more expressiveness power) which takes T as its input and outputs a proof term of $P(T)$, which could be huge. Intuitively, the former one directly *states* that $\forall T, P(T)$ is true, while the latter one is an oracle which can *step-by-step explain* why $P(T)$ holds for a concrete T. Arthur Azevedo de Amorim's implementation [2] is the only object-level proof of countability before our paper. He used indices to number constructors of an inductive type. In other words, he formalized the syntax of inductive types and deeply embedded the syntax (in some sense, the meta language) in Coq's object language. As a consequence, his proof involves complicated reasoning about indices' equivalence, type's equivalence and dependent type issues—if two Coq types $T_1 = T_2$, T_1's elements are not automatically recognized as T_2's elements by Coq's type checker. Our formalization shows that such proof-reflection technique is not needed for a general countability proof.

---

[2]Processor: 2.3 GHz 8-Core Intel Core i9; Memory: 16 GB 2400 MHz DDR4.

Contributions. Our main contributions are a Coq formalized general countability proof for first order inductive types, and an automatic tactic for proving inductive types countable. We do not need any external tool to generate definitions, proof terms, or proof scripts, and our proof itself does not involve complicated dependently typed reasoning about type equalities. We also developed Coq libraries for countability and for a syntax of inductive definitions, which have values of their own. All of our proofs are formalized axiom-free, and our proof of countability theorem can be used in the completeness proof of separation logics, a Coq formalization for an early paper [6].

Outline. In Section 2, we will clarify our Coq definition of countability and our formalization of the syntax of first order inductive type definitions. In Section 3, we present our general countability theorem and our proof. In Section 4, we introduce our automatic tactic for proving concrete inductive types countable. We discuss related works in Section 5 and conclude in Section 6.

2 Preliminaries

In this section, we present our formal definition of countable (Section 2.1), the syntax of first order inductive types (Section 2.2), and general recursive functions (Section 2.3). We will also list their important properties, that we prove in our Coq library.

2.1 Countable

We define the type T to be countable if and only if there exists an injection from T to natural numbers, which means T is either finite or countably infinite. Here, an injection is a relation that keeps the injective property and functional property. This `Countable` is the definition used in our final theorem, but we use an auxiliary definition, `SetoidCountable`, in our proof. For the countability proof of inductive type T, we need to prove that $\{x : T \mid \mathsf{rank}(x) < n\}$ is countable for any n. In Coq, an element in $\{x : T \mid \mathsf{rank}(x) < n\}$ is a dependently typed tuple (x, p), where $x \in T$ and p is a proof of $\mathsf{rank}(x) < n$. Two such dependently typed tuples (x_1, p_1) and (x_2, p_2) are equal if $x_1 = x_2$, and p_1 and p_2 are identical proof terms. Proving $\{x : T \mid \mathsf{rank}(x) < n\}$ `Countable` requires us to show whether two proofs, p_1 and p_2, of $\mathsf{rank}(x) < n$ are identical. Using `SetoidCountable` avoids that kind of reasoning about proof terms, and avoids using the "proof-irrelevance" axiom in some sense[3]. The definition of $\{x : T \mid \mathsf{rank}(x) < n\}$ being `SetoidCountable` is straightforward: there exists a function f from $\{x : T \mid \mathsf{rank}(x) < n\}$ to natural numbers, so that if $f(x_1, p_1) = f(x_2, p_2)$ then $x1 = x2$.

```coq
Definition image_defined {A B} (R: A → B → Prop): Prop :=
    forall a, exists b, R a b.
Definition partial_functional {A B} (R: A → B → Prop): Prop :=
    forall a b1 b2, R a b1 → R a b2 → b1 = b2.
Definition injective {A B} (R: A → B → Prop): Prop :=
    forall a1 a2 b, R a1 b → R a2 b → a1 = a2.
Record injection (A B: Type): Type := {
    inj_R:> A → B → Prop;
    im_inj: image_defined inj_R;
    pf_inj: partial_functional inj_R;
    in_inj: injective inj_R }.
Definition Countable (T : Type) := injection T nat.
```

---

[3] `Axiom proof_irrelevance : forall (P:Prop) (p1 p2:P), p1 = p2.`

```
Record Setoid_injection
  (A B: Type) (RA: A → A → Prop) (RB: B → B → Prop) := ...
    (* RA and RB are equivalence relations on A and B resp. *)
Definition SetoidCountable (A: Type) {RA: A → A → Prop}: Type :=
  @Setoid_injection A nat RA (@eq nat).
    (* RA is an equivalence relation on A *)
    (* @SetoidCountable A RA if the quotient set A/RA is countable. *)
```

In our countability library, we prove that products of two countable types and unions of countably many countable types are countable. We prove that the composition of two injections is still an injection (see `injective_compose` below), and if $f \circ g$ is an injection then f is an injection (see `injective_compose_rev` below). We also prove their setoid versions, but omit them here. We define "bijection" and prove some elementary properties about bijection and injection. For connections between `SetoidCountable` and `Countable`, we prove that any `Setoid_injection` on Coq's builtin equality is an `injection`, and thus any `SetoidCountable` type w.r.t. Coq's builtin equality is also `Countable`.

```
Lemma injective_compose {A B C} (R1: A → B → Prop) (R2: B → C → Prop):
    injective R1 → injective R2 → injective (compose R1 R2).
Lemma injective_compose_rev {A B C} (R1: A → B → Prop) (R2: B → C → Prop):
    image_defined R2 → injective (compose R1 R2) → injective R1.
Lemma SetoidCountable_Countable {A: Type}:
    SetoidCountable A (@eq A) → Countable A.
```

Here, we use a relation rather than a function to provide the definition of `Countable`, for better usability and extensibility. For example, if we have a bijection from *A* to *B* and we have `Countable B`, we want to show that *A* is also countable. We can do it easily by relation, but we cannot do it under the definition of function, because of the problem of computability.

2.2 Syntax of inductive definition

In our formalization, we only consider *first order inductive definitions*. Not all inductive types have only countably many elements. Thus we exclude definitions like the following:

```
Inductive inf_tree: Type :=
| inf_tree_leaf: inf_tree
| inf_tree_node: nat → (nat → inf_tree) → inf_tree.
```

However, we try to focus on techniques of building dependently type functions from inductive definitions to nontrivial proof terms in this work. Thus we choose to exclude mutually inductive definitions and nested inductive definitions from our formalization, although we believe that we can extend our work in the future to handle these cases.

Formally, a first-order inductive type *T* is defined by a list of constructors, each of which is a first-order function with result type *T*. The argument types of constructors should be constant base type[4] or *T* itself. So we formalize the syntax of an inductive definition *T* as a list of dependently typed pairs of typing rules and constructors: `list (sigT (fun arg ⇒ constr_type arg T))`, we will call it `Constrs_type` later in this paper. We usually call the "typing rule" part `arg`, with a type `list (option Type)`, and call a constructor `constr`, whose type depends on `arg` and is calculated

---

[4]Here, constant base type means other types which are countable.

by `constr_type`. For example, the definition of `natlist` has two branches. The type of `Cons` is: `nat → natlist → natlist`. It has two arguments, one of which is of type `nat` and the other is the inductive type `natlist` itself. Thus, this typing rule can be formalized as: `[Some nat; None]` (`Some` for a based type and `None` for the inductive type itself) and

```
constr_type [Some nat; None] natlist = nat → natlist → natlist
```

exactly describes the type of constructor `Cons`. Since the definition of `natlist` has two branches, this definition can be described by: `[ _[ [Some nat; None], Cons ]_; _[ [], Nil ]_ ]`.

2.3   General recursion

For an inductive type T, Coq generates `T_rect`, `T_ind`, `T_rec` and `T_sind`, which respectively correspond to elimination principles on `Type`, `Prop`, `Set` and `SProp`[5]. For our countability proof, `T_rect` is enough[5]. We define `rect_type` to compute the type of `T_rect` (we call it `rect` later in this paper) from an inductive definition. Similar to the definition of `Constrs_type`, we use `rect_clause_type` to compute each branch. Here we show the definitions of `rect_type` :

```
Fixpoint rect_type
         (T: Type) (constrs: Constrs_type) (P: T → Type): Type :=
  match constrs with
  | nil ⇒ forall x: T, P x
  | _[ arg, constr ]_ :: constrs0 ⇒
        rect_clause_type arg T P constr → rect_type T constrs0 P
  end.
```

For example, `natlist_rect` (which is generated by Coq) has type

```
forall P, rect_type natlist [ _[ [Some nat; None], Cons ]_; _[ [], Nil ]_ ] P
```

Knowledge of the type of general recursive function alone is not sufficient for building proofs. It is important that the computation result of a recursive function coincides with the definitions in its corresponding branch. For example, as mentioned in Section 1, `natlist_rect` satisfies:

```
natlist_rect P F₀ F₁ Nil = F_0
natlist_rect P F₀ F₁ (Cons n l) = F_1 n l (natlist_rect P F₀ F₁ l)
```

For general inductive types, we need to consider all possible ways of filling `rect`'s arguments. We introduce `apply_rect` so that `apply_rect T P constrs para (rect P) x` fills `rect`'s argument (like F_0 and F_1 above) in a parameterized way defined by `para` and calculates the result on $x : T$. Based on that, we define `rect_correct`:

```
rect_correct (T: Type) (constrs: Constrs_type)
   (rect: forall P, rect_type T constrs P): Prop
```

to be the following property: for any `para` and `x`, `apply_rect T P constrs para (rect P) x` equals to the recursive branch defined by `para` and `x` (and the recursive function `apply_rect T P constrs para rect` itself). Detailed definitions of `apply_rect` and `rect_correct` involve complicated dependent type issue, and we defer them to Section 3.

---

[5]The constant `T_ind` is always generated, whereas `T_rec` and `T_rect` may be impossible to derive, for example, when the sort is `Prop`. However, we only focus on the inductive type so no problems are encountered.

In summary, our proof about inductive type's countability depends on and only depends on the following arguments and hypothesis:

- the Coq type `T: Type`;

- the inductive definition `constrs: Constrs_type`;

- the general recursive function `rect: forall P, rect_type T constrs P`;

- the characteristic equations `rect_correctness: rect_correct constrs rect`.

We develop three automatic tactics `gen_constrs` , `gen_rect` , `apply_rect_correctness_gen` to get `constrs`, `rect` and `rect_correctness` above from T.

- In order to get `rect`, we build a virtual induction proof on T and analyze that proof term. For example, one can prove "`forall l: natlist, Type`" by the following tactic:

      intro l; induction l; exact bool.

  This tactic will generate the following proof term:

      fun l : natlist ⇒ natlist_rect (fun _ ⇒ Type) bool (fun _ _ _ ⇒ bool) l

  Then our tactic analyzes this proof term to get `natlist_rect`.

- In order to get `constrs`, we get `rect` first and analyze the syntax of its type. For example,

      natlist_rect:
          forall P : natlist → Type,
            (forall (n0 : nat) (l1 : natlist), P l1 → P (Cons n0 l1)) →
            (P Nil) →
            (forall l : natlist, P l)

  From its assumptions, our tactic can generate

      [_[[Some nat; None], Cons]_; _[[], Nil]_].

- In order to get `rect_correctness`, we only need to unfold the definitions of `rect_correct` and `apply_rect`, and prove the conclusion by reflexivity.

3   The countability theorem

As mentioned in Section 1, the main proof idea is to define a `rank` function from inductive type T to `nat`, and prove that $T_n \triangleq \{x : T \mid \text{rank}(x) < n\}$ is countable for any n. This conclusion can be proved by induction on n. Its induction step is to construct an injection from T_{n+1} to the union of different products of T_n, and the latter one is countable since T_n is countable by the induction hypothesis. Using `natlist` and `bintree` as examples, we can construct injections[6]:

    natlist_{n+1} →
      nat * (natlist_n * unit) + (unit + void)
    bintree_{n+1} →
      nat * (bintree_n * (bintree_n * unit)) + (unit + void)

---

[6]Here we choose not to present the correct `rank` function, for reasons of conciseness. The real general `rank` function takes more arguments to be specialized on `natlist` and `bintree`; see Section 3.1. Also, redundant "`* unit`" and "`+ void`" are introduced by a uniform recursive definition for convenience.

Using `natlist` as an example, this construction of injection takes three steps:

- Defining a function from `natlist` to `nat * (natlist * unit) + (unit + void)`:

```
pattern_match (l: natlist) :=
  match l with
  | Cons n0 l1 ⇒ inl (n0, (l1, tt))
                            (* inl chooses the left branch of sum type *)
                            (* tt is the only element of unit *)
  | Nil ⇒ inr (inl (tt))
                        (* inr chooses the right branch of sum type *)
  end.
```

- Well-definedness of `pattern_match`:
  We thus prove that if `rank l < S n` and `pattern_match l = inl (n0, (l1, tt))`, then
  `rank l1 < n`. Thus, we can define a dependently typed function of the type below based on
  `pattern_match`.

```
{l: natlist | rank l < S n} →
  nat * ({l: natlist | rank l < n} * unit) + (unit + void)
```

  In other words, we define

```
pattern_match_DT:
  natlist_{n+1} → nat * (natlist_n * unit) + (unit + void)
```

- Injective property:
  We prove that the `pattern_match` function we defined is an injection.

In Section 3.1, we introduce our general definition of `rank` and `pattern_match`. In Section 3.2 and
3.3, we establish the injective property above. Specifically, we first prove that `pattern_match` itself
is an injection (see Section 3.2) and use that conclusion to prove our final dependently typed version
injective (see Section 3.3). Finally, we summarize our main theorem in Section 3.4.

3.1   Definitions

We first define the function that calculates the union of different products named `normtype`. As shown
in the beginning of section 3, we want to project T_{n+1} into the union of different products of T_n. Also,
the non-dependent type version `pattern_match` is a function from T to the union of different products
of T. Thus, our definition of `normtype` is polymorphic. For example,

```
normtype natlist [ _[ [Some nat; None], Cons ]_; _[ [], Nil ]_ ] X
  = nat * (X * unit) + (unit + void)
normtype bintree [ _[ [Some nat; None; None], Node ]_; _[ [], Leaf ]_ ] X
  = nat * (X * (X * unit) + (unit + void)
```

In   our   definition   of   `normtype`,   we   analyze   the   inductive   definition   constrs
(which means `[ _[ [Some nat; None], cons ]_; _[ [], nil ]_ ]` for `natlist`), use product
types to represent each branch, and use sum types to connect them. For each branch, we use *A* when we
meet `Some A` and use *X* when we meet `None`. We can therefore generate all `normtype` types with the
same syntax tree as *T* like T_{n+1}.

As mentioned in Section 2, we need to define all recursive function (e.g. `rank`) and pattern match expressions (e.g. `pattern_match`) based on the general recursive function. Specifically, suppose `rect` is the general recursive function of type `T` with inductive definition `constrs`, we define `rank` and `pattern_match` by filling `rect`'s arguments through `apply_rect`.

When defining `rank`, each argument of `rect` is to add recursive calls' results together. For example, `size` (see Section 1) is the `rank` function of `bintree`. We can define it by filling `bintree`'s arguments:

```
size t = bintree_rect _ (fun n0 t1 r1 t2 r2 ⇒ r1 + r2 + 1) (1)
```

Here, in the recursive branch for constructor "Node", `n0` is the label, `t1` and `t2` are the left and right subtrees respectively, and `r1` and `r2` are the results of recursive calls: `size t1` and `size t2`; and in the recursive branch of constructor "Leaf", the return value is a constant 1. In general, we can define these arguments of `rect` based on the syntax of inductive definitions. Using the example above, the typing information of "Node" is described by [Some nat; None; None] since `Node` has type:

```
nat → bintree → bintree → bintree
```

The first element `Some nat` corresponds to `n0` above; the second element `None` corresponds to `t1` and `r1` above; and the element `None` corresponds to `t2` and `r2`.

Defining `pattern_match` is more complicated. Here is how we define the `pattern_match` function for `natlist` (see the beginning of Section 3) by filling `rect`'s arguments.

```
pattern_match t =
  natlist_rect _ (fun n0 l1 r1 ⇒ inl (n0, (l1, tt))) (inr (inl tt))
```

Here, we put `inl` in the Cons branch since it is the first branch, and we put `inr ∘ inl` in the Nil branch since it is the second branch. That means we cannot define these two arguments of `natlist_rect` based only on Cons's and Nil's typing information. Specifically, if `constrs` can be decomposed into: `constrs1 ++ _[arg2,constr2]_ :: constrs3`, then `rect`'s arguments for the arg2-constr2-branch also depend on the length of `constrs1` and `constrs3`. For this reason, the definition of `apply_rect` must allow `para` (the parameterized way of filling `rect`'s arguments) to take `constrs1` and `constrs3` as its arguments.

In our real definition, `apply_rect`'s type is:

```
apply_rect T constrs P para rect_P : forall (t: T), P constrs t.
```

where (we omit `para`'s type first and introduce it later)

```
P: Constrs_type → T → Type;
rect_P: rect_type T constrs (P constrs)
```

Here `P` defines the dependently typed result type and `rect_P` is a specialized `rect` for computing results of "type" `P`. The most important parameter of `apply_rect` is `para`. Its type is:

```
para: forall constrs1 arg2 constr2 constrs3,
  let constrs := rev_append constrs1 (_[arg2, constr2]_ :: constrs3) in
  rect_clause_type arg2 T (P constrs) constr2
```

That is: if `constrs`, all branches of inductive definitions, can be decomposed into (rev constrs1), `_[arg2, constr2]_`, and `constrs3`, then `para` computes `rect_P`'s argument for the branch of `arg2` and `constr2`. Here, the function `rev_append` is the auxiliary function for defining a tail-recursive list reverse provided by Coq's standard library:

```
rev_append {A} (l l' : list A) : list A :=
  match l with
  | [] ⇒ l'
  | a :: l0 ⇒ rev_append l0 (a :: l')
  end.
```

It ensures that for any `l` and `l'`, `rev_append l l' = rev l ++ l`. It is critical for us to use

```
rev_append constrs1 (_[arg2, constr2]_ :: constrs3)
```

instead of

```
constrs1 ++ _[arg2, constr2]_ :: constrs3
```

because it is much more convenient for building dependently typed inductive proofs and dependently typed recursive functions. When we apply an inductive proof on the structure of `constrs`, we can easily transform

```
        rev_append constrs1 (_[arg2, constr2]_ :: constrs3)
```
to `rev_append (_[arg2, constr2]_ :: constrs1) constrs3`
because they are $\beta\eta\iota$-reduction to each other, and so can pass Coq's unification checking. But it is not the case for

```
        constrs1 ++ (_[arg2, constr2]_ :: constrs3)
```
and `(constrs1 ++ [ _[arg2, constr2]_ ]) ++ constrs3`
which are equal, and can be proved equal, but they cannot pass Coq's unification checking.

   In the end, we define `paras` for `rank` and `pattern_match`, and define these two functions for generic inductive types based on corresponding `paras` and `apply_rect`.

3.2   Injective property: the simple typed version

We have defined `pattern_match`, a function from `T` to `normtype T constrs T` (which is a union type of different product types). We prove it to be an injection in this subsection. Later, we will use this simplified conclusion to establish our ultimate goal: a `Setoid_injection` from T_{n+1} to `normtype T constrs T_n`.

   To prove `pattern_match` to be injective (formalized as `PM_inj` below), we need to perform case analysis over both *a* and *b*.

```
Definition PM_inj T constrs rect: Prop :=
  forall a b: T, pattern_match a = pattern_match b → a = b.
```

Again, case analysis proofs is nontrivial since we are now reasoning about a generic inductive type, not a concrete one. We use a specialized `rect` to solve the problem:

```
Definition rect_PM_inj:
  rect_type T constrs
    (fun a ⇒ forall b, pattern_match a = pattern_match b → a = b)
:=  rect _.
```

Here, `rect_PM_inj` is a proof of a big implication proposition, whose conclusion is exactly `PM_inj` and whose assumptions are those case analysis branches. Thus, the proof of the injective property can be built by filling all those arguments of `rect_PM_inj`. Specifically, we decompose `constrs` into a form of `rev_append constrs1 constrs2` (at first `constrs1 = []` and `constrs2 = constrs`) and fill those

arguments by an induction over `constrs2`. We successfully avoid dependently typed type-casting since we use `rev_append` in this proof and in `apply_rect`'s types. We omit proof details here.

We now finish the definition of a "simple" typed function, `pattern_match`, and the proof of its injective property. During the proof process, we encounter some problems regarding dependent types and solve them with the help of `rev_append`. To construct an injection from T_{n+1} (defined as $\{x : T \mid \text{rank } x < S \text{ } n\}$) to `normtype T constrs` T_n, we need to prove linear arithmetic properties about `rank`. We could prove that dependently typed injective property in a similar way, but the dependent types with irrelevant proofs will trouble us much more. So we choose a different proof strategy.

3.3   Injective property: the dependent type version

Instead of developing a similar (but more complicated) proof of the injective property for the dependently typed version of `pattern_match`, we choose to *use* our injective proof above to build our dependently typed injective proof. In order to prove `pattern_match_DT` (the dependently typed version of `pattern_match`, a mapping from T_{n+1} to `normtype T constrs` T_n) to be injective, it is sufficient to show (Fig. 1 illustrates this proof strategy):

- `pattern_match ∘ proj1_sig = (normtype_map proj1_sig) ∘ pattern_match_DT`;
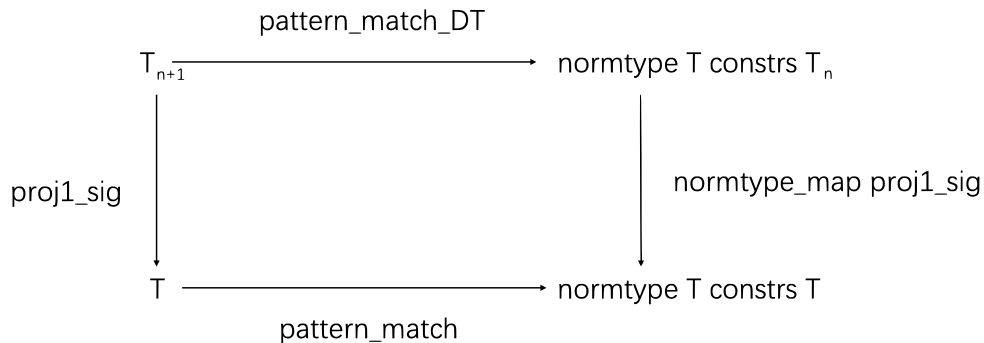- `pattern_match` is injective;
- `proj1_sig` is injective.

Figure 1: Proof strategy

Here, `proj1_sig` (defined by Coq standard library) removes the proof part of Coq's sigma types:

```
proj1_sig {A} {P: A → Prop} (e : sig P): A :=
   match e with exist _ a _ ⇒ a end
```

and we define `normtype_map` to apply `proj1_sig` on each part of `normtype T constrs` T_n.

The reasoning behind this proof strategy is straightforward. By the second and the third condition (`pattern_match` and `proj1_sig` are injective), we know that `pattern_match ∘ proj1_sig` is injective using theorem `injective_compose` (see Section 2.1). Thus, `(normtype_map proj1_sig) ∘ pattern_match_DT` is also injective according to the first condition (the diagram in Fig. 1 commutes). In the end, `pattern_match_DT` must be an injection due to theorem `injective_compose_rev` (see Section 2.1).

We proved `pattern_match` to be injective in Section 3.3 and `proj1_sig` is obviously an injection; thus we only need to prove `pattern_match ∘ proj1_sig = (normtype_map proj1_sig) ∘ pattern_match_DT`, based on our definition of `pattern_match_DT` and `normtype_map`.

In our Coq formalization, the real type of `pattern_match_DT` is:

```
Definition pattern_match_DT n:
    forall t:T, rank t < S n → normtype T constrs T_n.
```

given type `T`, its inductive definition `constrs` and its general recursive function `rect` and `rect_correctness`. Using `natlist` as an example,

```
pattern_match_DT n (l: natlist):
    length l < S n → nat * (natlist_n * unit) + (unit + void)
:= match l with
    | Cons n0 l1 ⇒
        fun H: length (Cons n0 l1) < S n ⇒
          inl (n0, (exist _ l1 SomeProof, tt))
    | Nil ⇒
        fun H: length Nil < S n ⇒
          inr (inl (tt))
    end.
```

The function above may be hard to read. It is equivalent to the following one, which is written in a less dependently typed way.

```
pattern_match_DT_demo n (l: natlist) (H: length l < S n) :=
    match l with
    | Cons n0 l1 ⇒ inl (n0, (exist _ l1 SomeProof, tt))
    | Nil ⇒ inr (inl (tt))
    end.
```

In their `Cons` branches, we need to provide a proof of `length l1 < n` at the place of `SomeProof` given `H: length l < S n`.

In order to define such a `pattern_match_DT` function for a generic inductive type `T`, we build its definition based on `apply_rect` and a "para" of the following type:

```
Definition pattern_match_para_DT n T constrs1 arg2 constr2 constrs3:
    let constrs := rev_append constrs1 (_[arg2, constr2]_ :: constrs3) in
    rect_clause_type arg2 T
        (fun t ⇒ rank t < S n → normtype T constrs T_n)
        constr2.
```

That is, we define `pattern_match_DT` by filling arguments of `T`'s general recursive function `rect`. Given that `constrs` is decomposed into `rev_append constrs1 (_[arg2, constr2]_ :: constrs3)`, this `para` above computes the `arg2`-`constr2`-argument of `rect`. Again, using the `Cons` argument of `natlist_rect` as an example, this `para` should have the following type:

```
forall n0 l1,
    length (Cons n0 l1) < S n →
    normtype natlist constrs_natlist natlist_n
```

In the definition of `pattern_match_para_DT` and the proof of `pattern_match ∘ proj1_sig = (normtype_map proj1_sig) ∘ pattern_match_DT`, we repeatedly use `rect_correctness` to reason about `rank`. For the sake of space, we omit details here.

3.4 Main theorem

We have constructed the injection from T_{n+1} to `normtype T constrs` T_n in Coq. The definition of `apply_rect` helps us define most of the functions we need, and most of the intermediate lemmas can be reduced to properties of `apply_rect` and the corresponding `para`, which greatly simplifies our proof. We use `rev_append` to avoid type casting.

In summary, we use `SetoidCountable` as an auxiliary definition to prove the countability theorem. Specifically, we prove `SetoidCountable` T_n by induction over *n* and by the injection we just constructed. In the end, our main theorem is:

```
Variable (T: Type).
Variable (constrs: Constrs_type).
Variable (rect: forall P, rect_type T constrs P).
Variable (rect_correctness : rect_correct T constrs rect).
Hypothesis base_countable :
  Forall_type (fun s ⇒ (Forall_type option_Countable) (projT1 s)) constrs.
Theorem Countable_T : Countable T.
```

where the function `Forall_type` (provided by Coq's standard library) defines the universal predicates over lists

```
Inductive Forall_type {A : Type} (P : A → Type) : list A → Type :=
    | Forall_type_nil : Forall_type P nil
    | Forall_type_cons : forall (x : A) (l : list A),
              P x → Forall_type P l → Forall_type P (x :: l).
```

and the hypothesis `base_countable` says that all base types used in the inductive definition are countable. For example, this theorem proves that `natlist` is countable, as long as `nat` is countable.

4   Automatic proof systems

To make our result more practical and accessible, we developed Coq tactics to automatically prove inductive types countable. We define three tactics `gen_constrs`, `gen_rect`, `apply_rect_correctness_gen` to get `constrs`, `rect` and `rect_correctness` from `T` (previously mentioned in Section 2, see Coq development for more details). According to the list of conditions and hypothesis, we need in proof (as shown above in Section 3.4), the last thing that needs to be done is to prove `base_countable`, which means that all base types used in the definition of `T` are countable. This is done using a library of proved countability results and Coq assumptions. Here are two typical applications of our tactic `Countable_solver`:

```
Theorem Countable_expr : Countable expr.
Proof. intros. Countable_solver. Qed.
Theorem Countable_list : forall A: Type, Countable A → Countable (list A).
Proof. intros. Countable_solver. Qed.
```

5   Related work

We discuss three related studies in proving relevant properties for inductive types in Coq and one in Isabelle/HOL. What sets our formalization apart from this work is our proof at Coq's object logic level; only Deriving [2] develops object logic proofs like us. As a result, our proofs and automation instructions do not need other additional axioms, libraries, or tools, and can run with high efficiency.

- Theory Countable[1] : These researchers also used injection to represent the `Countable` relation. Their main idea was to construct an injection from data types to old data types which are countable. They could automatically prove the countability of data types which had nested and mutual recursion, and used other data types. However, the process and automatic tactics were formalized in a meta language.

- Autosubst[19] & Autosubst2[20] : Autosubst can automatically generate the substitution operations for a custom inductive type of terms, and prove the corresponding substitution lemmas. The library gives the enumerability of De Brujin substitution algebra[18]. Autosubst offers tactics that implement the normalization and decision procedure. They believe that it is hard to maintain or extend Ltac code, so that they proposed a new implementation of Autosubst which comes in the form of a code generator to generate Coq proof terms, and at the same time extends Autosubst's input language to mutual inductive sorts with multiple sorts of variables. Autosubst and Autosubst2 develop formalized proofs as tactics and external proof term generators, respectively, which can be treated as meta-level mappings from the syntax of inductive definitions to countability proof terms. In comparison, our proof is a Coq object-level mapping from inductive definitions to countability, but we do not support mutually inductive types at present.

- Undecidability[9] : Forster et. al. formalized the computational undecidability of the validity, satisfiability, and provability of first-order formulas following a synthetic approach based on the computation native to Coq's constructive type theory. They extended the library in 2020, to present a comprehensive analysis of the computational content of completeness theorems for first-order logic, considering various semantics and deduction systems[10]. They proved first-order logic's propositions countable in their completeness proof. They also formalized the syntax of inductive definitions[7], as we did, but they do not provide a general theorem of countability.

- Deriving [2] : Deriving proved inductive types countable in Coq. Deriving uses `countType` in the MathComp library, which provides a different definition of injection and `Countable`. Although this alternative definition requires injections to be Coq-computable functions, it is not a significant drawback comparing with our definitions when applying inductive type's countability. Deriving supports the proof of countability for mutually inductive types and nested inductive types. Their proof strategy is different from ours: they built an injection from every inductive type *T* to *finite-width trees*, which they defined as a Coq type and proved countable. More significantly, they provided two formalization of inductive definitions. One is like ours:

  ```
  constrs: list (sigT (fun arg ⇒ constr_type arg T));
  ```

  the other uses indices to number the constructors. In other words, the latter formalization is a deep embedding of the meta language (the syntax of inductive types) into Coq's object language. They

---

[7]This general formalization appears in their Coq development but they do not mention that in their paper.

carefully used computable functions over the deeply embedded meta language (since natural numbers' equality tests are computable, but types' equality tests are not computable) in their definitions and used the connection between these two formalizations to compute their final proof term. In their proofs, they need to reason about indices' equalities, types' equalities and relevant dependent type issues—if two Coq types $T_1 = T_2$, T_1's elements are not automatically recognized as T_2's elements by Coq's type checker. In comparison, our work shows that inductions over constructor lists do prove the conclusion using the "`rev-append trick`", and we do not need number-indexing and heavy-weighted proof reflection to bypass related difficulties in dependently type proofs.

6   Conclusions

We proved in Coq that a first-order inductive type is countable as long as all base types used in the definition are countable. Our definitions and proofs are all axiom-free. We provide an alternative way of thinking about solving dependent types at the object level. We developed very efficient tactics which use this countability theorem to prove concrete inductive types to be countable. Our formalization and automatic tactic still have room for expansion in the future. For example, our tactics do not work when applied to mutually recursive types. We believe that it is plausible to transform the mutually recursive types into primitive recursive types [11] and enhance our tactics. Our Coq development can be found at:

`https://github.com/QinxiangCao/Countable_PaperSubmission`

References

[1] Jasmin Blanchette Alexander Krauss, Brian Huffman: *This is a library of Countable Theory in Isabelle/HOL.* `https://devel.isa-afp.org/browser_info/current/HOL/HOL-Library/Countable.html`.

[2] A. A. de Amorim (2020): *Deriving Instances with Dependent Types. CoqPL 2020.*

[3] Abhishek Anand & Vincent Rahli (2014): *A Generic Approach to Proofs about Substitution*. In Amy P. Felty & Brigitte Pientka, editors: *Proceedings of the 2014 International Workshop on Logical Frameworks and Meta-languages: Theory and Practice, LFMTP '14, Vienna, Austria, July 17, 2014*, ACM, pp. 5: 1–5: 8, doi:10.1145/2631172.2631177.

[4] Brian Aydemir & Stephanie Weirich (2010): *LNgen: Tool support for locally nameless representations*.

[5] Bruno Barras, Samuel Boutin, Cristina Cornes, Judicaël Courant, Yann Coscoy, David Delahaye, Daniel de Rauglaudre, Jean-Christophe Filliâtre, Eduardo Giménez, Hugo Herbelin et al. (1999): *The Coq proof assistant reference manual. INRIA, version* 6(11).

[6] Qinxiang Cao, Santiago Cuellar & Andrew W. Appel (2017): *Bringing Order to the Separation Logic Jungle*. In Bor-Yuh Evan Chang, editor: *Programming Languages and Systems - 15th Asian Symposium, APLAS 2017, Suzhou, China, November 27-29, 2017, Proceedings, Lecture Notes in Computer Science* 10695, Springer, pp. 190–211, doi:10.1007/978-3-319-71237-6_10.

[7] Adam Chlipala (2008): *Parametric higher-order abstract syntax for mechanized semantics*. In James Hook & Peter Thiemann, editors: *Proceeding of the 13th ACM SIGPLAN international conference on Functional programming, ICFP 2008, Victoria, BC, Canada, September 20-28, 2008*, ACM, pp. 143–156, doi:10.1145/1411204.1411226.

[8] Heinz-Dieter Ebbinghaus, Jörg Flum & Wolfgang Thomas (1994): *Mathematical logic (2. ed.)*. Undergraduate texts in mathematics, Springer, doi:10.1007/978-1-4757-2355-7.

[9]   Yannick Forster, Dominik Kirst & Gert Smolka (2019): *On synthetic undecidability in coq, with an application to the entscheidungsproblem*. In Assia Mahboubi & Magnus O. Myreen, editors: *Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2019, Cascais, Portugal, January 14-15, 2019*, ACM, pp. 38–51, doi:10.1145/3293880.3294091.

[10] Yannick Forster, Dominik Kirst & Dominik Wehr (2020): *Completeness Theorems for First-Order Logic Analysed in Constructive Type Theory*. In Sergei N. Artëmov & Anil Nerode, editors: *Logical Foundations of Computer Science - International Symposium, LFCS 2020, Deerfield Beach, FL, USA, January 4-7, 2020, Proceedings*, Lecture Notes in Computer Science 11972, Springer, pp. 47–74, doi:10.1007/978-3-030-36755-8_4.

[11] Peter Freyd (1990): *Recursive types reduced to inductive types*. In: *[1990] Proceedings. Fifth Annual IEEE Symposium on Logic in Computer Science*, pp. 498–507, doi:10.1109/LICS.1990.113772.

[12] M. Hofmann & T. Streicher (1994): *The groupoid model refutes uniqueness of identity proofs*. In: *Proceedings Ninth Annual IEEE Symposium on Logic in Computer Science*, pp. 208–212, doi:10.1109/LICS.1994.316071.

[13] Gyesik Lee, Bruno C. d. S. Oliveira, Sungkeun Cho & Kwangkeun Yi (2012): *GMeta: A Generic Formal Metatheory Framework for First-Order Representations*. In Helmut Seidl, editor: *Programming Languages and Systems - 21st European Symposium on Programming, ESOP 2012, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2012, Tallinn, Estonia, March 24 - April 1, 2012. Proceedings*, Lecture Notes in Computer Science 7211, Springer, pp. 436–455, doi:10.1007/978-3-642-28869-2_22.

[14] Leonardo Mendonça de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn & Jakob von Raumer (2015): *The Lean Theorem Prover (System Description)*. In Amy P. Felty & Aart Middeldorp, editors: *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings*, Lecture Notes in Computer Science 9195, Springer, pp. 378–388, doi:10.1007/978-3-319-21401-6_26.

[15] Rob Nederpelt & Herman Geuvers (2014): *Type theory and formal proof: an introduction*. Cambridge University Press, doi:10.1017/CBO9781139567725.

[16] Christine Paulin-Mohring (2015): *Introduction to the Calculus of Inductive Constructions*. In Bruno Woltzenlogel Paleo & David Delahaye, editors: *All about Proofs, Proofs for All, Studies in Logic (Mathematical logic and foundations)* 55, College Publications. Available at `https://hal.inria.fr/hal-01094195`.

[17] Emmanuel Polonowski (2013): *Automatically Generated Infrastructure for De Bruijn Syntaxes*. In Sandrine Blazy, Christine Paulin-Mohring & David Pichardie, editors: *Interactive Theorem Proving - 4th International Conference, ITP 2013, Rennes, France, July 22-26, 2013. Proceedings*, Lecture Notes in Computer Science 7998, Springer, pp. 402–417, doi:10.1007/978-3-642-39634-2_29.

[18] Steven Schäfer, Gert Smolka & Tobias Tebbi (2015): *Completeness and Decidability of de Bruijn Substitution Algebra in Coq*. In Xavier Leroy & Alwen Tiu, editors: *Proceedings of the 2015 Conference on Certified Programs and Proofs, CPP 2015, Mumbai, India, January 15-17, 2015*, ACM, pp. 67–73, doi:10.1145/2676724.2693163.

[19] Steven Schäfer, Tobias Tebbi & Gert Smolka (2015): *Autosubst: Reasoning with de Bruijn Terms and Parallel Substitutions*. In Christian Urban & Xingyuan Zhang, editors: *Interactive Theorem Proving - 6th International Conference, ITP 2015, Nanjing, China, August 24-27, 2015, Proceedings*, Lecture Notes in Computer Science 9236, Springer, pp. 359–374, doi:10.1007/978-3-319-22102-1_24.

[20] Kathrin Stark, Steven Schäfer & Jonas Kaiser (2019): *Autosubst 2: reasoning with multi-sorted de Bruijn terms and vector substitutions*. In Assia Mahboubi & Magnus O. Myreen, editors: *Proceedings of the 8th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2019, Cascais, Portugal, January 14-15, 2019*, ACM, pp. 166–180, doi:10.1145/3293880.3294101.

[21] Christian Sternagel & René Thiemann (2015): *Deriving class instances for datatypes*. Arch. Formal Proofs 2015. Available at `https://www.isa-afp.org/entries/Deriving.shtml`.