



HAL
open science

Deriving proved equality tests in Coq-elpi: Stronger induction principles for containers in Coq

Enrico Tassi

► **To cite this version:**

Enrico Tassi. Deriving proved equality tests in Coq-elpi: Stronger induction principles for containers in Coq. ITP 2019 - 10th International Conference on Interactive Theorem Proving, Sep 2019, Portland, United States. 10.4230/LIPIcs.CVIT.2016.23 . hal-01897468v2

HAL Id: hal-01897468

<https://inria.hal.science/hal-01897468v2>

Submitted on 8 Apr 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

1 Deriving proved equality tests in Coq-elpi: 2 Stronger induction principles for containers in Coq

3 Enrico Tassi

4 Université côte d'Azur - Inria

5 Enrico.Tassi@inria.fr

6 — Abstract —

7 We describe a procedure to derive equality tests and their correctness proofs from inductive type
8 declarations in Coq. Programs and proofs are derived compositionally, reusing code and proofs
9 derived previously.

10 The key steps are two. First, we design appropriate induction principles for data types defined
11 using parametric containers. Second, we develop a technique to work around the modularity limi-
12 tations imposed by the purely syntactic termination check Coq performs on recursive proofs. The
13 unary parametricity translation of inductive data types turns out to be the key to both steps.

14 Last but not least, we provide an implementation of the procedure for the Coq proof assistant
15 based on the Elpi [6] extension language.

16 **2012 ACM Subject Classification** Software and its engineering → General programming languages

17 **Keywords and phrases** Coq, Containers, Induction, Equality test, Parametricity translation

18 **Digital Object Identifier** 10.4230/LIPIcs.CVIT.2016.23

19 **1** Introduction

20 Modern typed programming languages come with the ability of generating boilerplate code
21 automatically. Typically when a data type is declared a substantial amount of code is made
22 available to the programmer at little cost, code such as an equality test, a printing function,
23 generic visitors etc. For example the `derive` directive of Haskell or the `ppx_deriving` OCaml
24 preprocessor provide these features for the respective programming language.

25 The situation is less than ideal in the Coq proof assistant. It is capable of synthesizing
26 the recursor of a data type, that, following the Curry-Howard isomorphism, implements the
27 induction principle associated to that data type. It supports all data types, containers such
28 as lists included, but generates a quite weak principle when a data type *uses* a container.
29 Take for example the data type rose tree (where `U` stands for a universe such as `Prop` or `Type`):

```
30 Inductive rtree A : U :=  
31 | Leaf (a : A)  
32 | Node (l : list (rtree A)).  
33
```

35 Its associated induction principle is the following one:

```
36 Lemma rtree_ind : ∀ A (P : rtree A → U),  
37   (∀ a : A, P (Leaf A a)) →  
38   (∀ l : list (rtree A), P (Node A l)) →  
39   ∀ r : rtree A, P r.  
40
```

42 Remark that the recursive step, line 3, lacks any induction hypotheses on (the elements
43 of) `l` while one would expect `P` to hold on each and every subtree. Even a very basic recursive
44 program such as an equality test cannot be proved correct using this induction principle. To
45 be honest, the Coq user is not even supposed to write equality tests by hand, nor to prove
46 them correct interactively. Coq provides two facilities to synthesize equality tests and their
47 correctness proofs called `Scheme Equality` and `decide equality`. The former is fully automatic



© Enrico Tassi;

licensed under Creative Commons License CC-BY

42nd Conference on Very Important Topics (CVIT 2016).

Editors: John Q. Open and Joan R. Access; Article No. 23; pp. 23:1–23:18

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

48 but is unfortunately very limited, for example it does not support containers. The latter
 49 requires human intervention and generates a single, large, term that mixes code and proofs.

50 As a consequence, users often need to manually write induction principles, equality tests
 51 and their correctness proofs. This situation is very unfortunate because the need for the
 52 automatic generation of boilerplate code such as equality tests is higher than ever in the Coq
 53 ecosystem. All modern formal libraries structure their contents in a hierarchy of interfaces
 54 and some machinery such as Type Classes [17] or Canonical Structures [8] are used to link
 55 the abstract library to the concrete instances the user is working on. For example the first
 56 interface one is required to implement in order to use the theorems in the Mathematical
 57 Components library [9] on a type T is the `eqType` one, requiring a correct equality test on T .

58 In this paper we use the framework for meta programming based on Elpi [6, 18] developed
 59 by the author and we focus on the derivation of equality tests. It turns out that generating
 60 equality tests is easy, while their correctness proofs are hard to synthesize, for two reasons.
 61 The first problem is that the standard induction principles generated by Coq, as shown
 62 before, are too weak. In order to strengthen them one needs quite some extra boilerplate,
 63 such as the derivation of the unary parametricity translation of the data types involved. The
 64 second reason is that termination checking is purely syntactic in Coq: in order to check that
 65 the induction hypothesis is applied to a smaller term, Coq may need to unfold all theorems
 66 involved in the proof. This forces proofs to be transparent that, in turn, breaks modularity:
 67 A statement is no more a contract, changing its proof may impact users.

68 In this paper we describe a derivation procedure for equality tests and their correctness
 69 proofs where programs and proofs are both derived compositionally, reusing code and proofs
 70 derived previously. This procedure also confines the termination check issue, allowing proofs
 71 to be mostly opaque. More precisely the contributions of this paper are the following ones:

- 72 ■ A technique to confine the issue stemming from the purely syntactic termination check
 73 implemented by Coq out of the main proofs. In this paper we apply it to the correctness
 74 proof of equality tests, but the technique is applicable to all proofs that proceed by
 75 structural induction.
- 76 ■ A modular and structured process to derive proved equality tests and, en passant,
 77 stronger induction principles for inductive types defined using containers.
- 78 ■ An implementation based on the Elpi extension language for the Coq proof assistant.

79 By installing the `coq-elpi` package¹ and issuing the command `Elpi derive rtree` one gets the
 80 following terms synthesized out of the type declaration for `rtree`:

```
81 Definition eq_axiom T f x := ∀ y, reflect (x = y) (f x y).
82
83 Definition rtree_eq : ∀ A, (A → A → bool) → rtree A → rtree A → bool.
84
85 Lemma rtree_eq_OK : ∀ A (A_eq : A → A → bool), (∀ a, eq_axiom A A_eq a) →
86   ∀ t, eq_axiom (rtree A) (rtree_eq A A_eq) t.
```

89 `reflect` is a predicate stating the equivalence between the proposition $(x = y)$ and the
 90 boolean test $(f\ x\ y)$; `rtree_eq` is a (transparent) equality test and `rtree_eq_OK` is its (opaque)
 91 correctness proof under the assumption that the equality test `A_eq` is correct.

92 The paper introduces the problem in section 2 by describing the shape of an equality
 93 test and of its correctness proof and explaining the modularity problem that stems for the
 94 termination checker of Coq. It then presents the main idea behind the modular derivation

¹ See <https://github.com/LPCIC/coq-elpi> for the installation instructions

95 procedure in section 3. Section 4 briefly introduces the Elpi extension language and section 5
 96 describes the full derivation.

97 **2 The problem: opaque proofs v.s. syntactic termination checking**

98 Recursors, or induction principles, are not primitive notions in Coq. The language provides
 99 constructors for fix point and pattern matching that work on any inductive data the user
 100 can declare. For example in order to test two lists `l1` and `l2` for equality one typically takes
 101 in input an equality test `A_eq` for the elements of type `A` and then performs the recursion:

```
102
103 Definition list_eq A (A_eq : A → A → bool) :=
104   fix rec (l1 l2 : list A) {struct l1} : bool :=
105     match l1, l2 with
106     | nil, nil => true
107     | x :: xs, y :: ys => A_eq x y && rec xs ys
108     | _, _ => false
109   end.
```

111 Coq accepts this definition because the recursive call is on `xs` that is a syntactically smaller
 112 term of the argument labelled as decreasing by the `{struct l1}` annotation.

113 We can define the equality test for `rtree` by reusing the equality test for lists:

```
114
115 Definition rtree_eq B (B_eq : B → B → bool) :=
116   fix rec (t1 t2 : rtree B) {struct t1} : bool :=
117     match t1, t2 with
118     | Leaf x, Leaf y => B_eq x y
119     | Node l1, Node l2 => list_eq (rtree B) rec l1 l2
120     | _, _ => false
121   end.
```

123 Note that `list_eq` is called passing as the `A_eq` argument the fixpoint `rec` itself (line 12). In
 124 order to check that the latter definition is sound, Coq looks at the body of `list_eq` to see
 125 whether its parameter `A_eq` is applied to a term smaller than `t1`. Since `l1` is a subterm of `t1`
 126 and since `x` is a subterm of `l1`, then the recursive call `(rec x y)` at line 5 is legit.

127 The fact that checking `rtree_eq` requires inspecting the body of `list_eq` is not very an-
 128 noying: we want both `list_eq` and `rtree_eq` to compute, hence their body matters to us.

129 On the contrary proof terms are typically hidden to the type checker once they have
 130 been validated, for both performance and modularity reasons. The desire is to make only
 131 the statement of theorems binding, and keep the freedom to clean, refactor, simplify proofs
 132 without breaking the rest of the formal development.

133 For example, let's assume that `list_eq_OK` is an opaque proof that `list_eq` is correct.

```
134
135 Lemma list_eq_OK : ∀ A (A_eq : A → A → bool),
136   (∀ a, eq_axiom A A_eq a) →
137   ∀ l, eq_axiom (list A) (list_eq A A_eq) l.
138 Proof. .. Qed. (* proof is opaque, hence hidden *)
```

140 It seems desirable to use this lemma in order to prove the correctness of `rtree_eq`, since it
 141 calls `list_eq`.

```
142
143 Lemma rtree_eq_OK B B_eq (HB: ∀ b, eq_axiom B B_eq b) :
144   ∀ t, eq_axiom (rtree B) (rtree_eq B B_eq) t
145 :=
146   fix IH (t1 t2 : rtree B) {struct t1} :=
147     match t1, t2 with
148     | Node l1, Node l2 => .. list_eq_OK (rtree B) (tree_eq B B_eq) IH l1 l2 ..
149     | Leaf b1, Leaf b2 => .. HB b1 b2 ..
150     | .. => ..
151   end.
```

23:4 Deriving proved equality tests in Coq-elpi

153 Unfortunately this term is rejected: we pass `IH`, the induction hypothesis, as the witness
154 that `(tree_eq B B_eq)` is a correct equality test (the argument at line 10 preceding `IH`) but
155 Coq does not know how `list_eq_OK` uses this argument, since its body is opaque.

156 The issue seems unfixable without changing Coq in order to use a more modular check
157 for termination, for example based on sized types [1]. We propose a less ambitious but more
158 practical approach here, that consists in putting the transparent terms that the termination
159 checker is going to inspect outside of the main proof bodies so that they can be kept opaque.

160 The intuition is to “reify” the property the termination checker wants to enforce. It can
161 be phrased as “`x` is a subterm of `t` and has the same type”. More in general we model “`x` is
162 a subterm of `t` with property `P`”.

163 3 The idea: put unary parametricity translation to good use

164 Given an inductive type `T` we name `is_T` an inductive predicate describing the type of the
165 inhabitants of `T`. This is the one for natural numbers:

```
166 Inductive is_nat : nat → U :=  
167 | is_0 : is_nat 0  
168 | is_S n (pn : is_nat n) : is_nat (S n).
```

171 The one for a container such as `list` is more interesting:

```
172 Inductive is_list A (PA : A → U) : list A → U :=  
173 | is_nil : is_list A PA nil  
174 | is_cons a (pa : PA a) l (pl : is_list A PA l) : is_list A PA (a :: l).
```

177 Remark that all the elements of the list validate `PA`.

178 When a type `T` is defined in terms of another type `C`, typically a container, the `is_C`
179 predicate shows up inside `is_T`. For example:

```
180 Inductive is_rtree A (PA : A → U) : rtree A → U :=  
181 | is_Leaf a (pa : PA a) : is_rtree A PA (Leaf A a)  
182 | is_Node l (pl : is_list (rtree A) (is_rtree A PA) l) : is_rtree A PA (Node A l).
```

185 Note how line 3 expresses the fact that all elements in the list `l` validate `(is_rtree A PA)`.

186 Our intuition is that these predicates reify the notion of being of a certain type, struc-
187 turally. What we typically write `(t : T)` can now be also phrased as `(is_T t)` as one would
188 do in a framework other than type theory, such as a mono-sorted logic.

189 It turns out that the inductive predicate `is_T` corresponds to the unary parametricity
190 translation [21] of the type `T`. Keller and Lasson in [7] give us an algorithm to synthesize
191 these predicates automatically. What we look for now is a way to synthesize a reasoning
192 principle for a term `t` when `(is_T t)` holds.

193 3.1 Stronger induction principles for containers

194 Let’s have a look at the standard induction principle of lists.

```
195 Lemma list_ind A (P : list A → U) :  
196 P nil →  
197 (∀ a l, P l → P (a :: l)) →  
198 ∀ l : list A, P l.
```

201 This principle is parametric on `A`: no knowledge on any term of type `A` such as `a` is ever
202 available. We want to synthesize a more powerful principle that lets us choose an invariant
203 for the subterms of type `A` (the differences are underlined):

```

204 Lemma list_induction A (PA: A → U) (P: list A → U):
205   P nil →
206   (∀ a (pa : PA a) l, P l → P (a :: l)) →
207   ∀ l, is_list A PA l → P l.
208
209

```

210 Note the extra premise (`is_list A PA l`): The implementation of this induction principle goes
 211 by recursion on the term of this type and finds as an argument of the `is_cons` constructor
 212 the proof evidence (`pa : PA a`) it feeds to the second premise (line 3). Intuitively all terms
 213 of type (`list A`) validate the property `P`, while all terms of type `A` validate the property `PA`.

214 More in general to each type we attach a property. For parameters we let the user choose
 215 (we take another parameter, `PA` here). For the type being analysed, `list A` here, we take the
 216 usual induction predicate `P`. For terms of other types we use their unary parametricity
 217 translation. Take for example the induction principle for `rtree`.

```

218 Lemma rtree_induction A PA (P : rtree A → U) :
219   (∀ a, PA a → P (Leaf A a)) →
220   (∀ l, is_list (rtree A) P l → P (Node A l)) →
221   ∀ t, is_rtree A PA t → P t.
222
223
224

```

224 Line 3 uses `is_list` to attach a property to `l`, and given that `l` has type (`list (rtree A)`) the
 225 property for the type parameter (`rtree A`) is exactly `P`. Note that this induction principle
 226 gives us access to `P`, the property one is proving, on the subtrees contained in `l`.

227 3.1.1 Synthesizing stronger induction principles

228 We postpone a detailed description of the synthesis to section 5.4, here we just sketch how
 229 to build the type on the induction principle.

230 It turns out that the types of the constructors of `is_T` give us a very good hint on the
 231 type of the induction principle. The type of the first premise

```

232 (∀ a, PA a → P (Leaf A a)) →
233

```

235 is exactly the type of the `is_Leaf` constructor

```

236 | is_Leaf a (pa : PA a) : is_rtree A PA (Leaf A a)
237
238

```

239 where (`is_rtree A PA`) is replaced by `P`. The same holds for the other premise: its type can
 240 be trivially obtained from the type of `is_Node`.

241 Our intuition is that the inductive predicate `is_T` provides the same information that
 242 typing provides. Induction principles give `P` on (smaller) terms of the same type, that would
 243 be terms for which `is_T` holds. Given their inductive nature, `is_T` predicates are able to
 244 propagate the desired property inside parametric containers.

245 3.2 Isolating the syntactic termination check problem

246 As one expects, it is possible to prove that `is_T` holds for terms of type `T`.

```

247 Definition nat_is_nat : ∀ n : nat, is_nat n :=
248   fix rec n : is_nat n :=
249     match n as i return (is_nat i) with
250     | 0 => is_0
251     | S p => is_S p (rec p)
252     end.
253
254

```

255 For containers (`T A`) we can prove (`is_T A PA`) when `PA` is trivial.

23:6 Deriving proved equality tests in Coq-elpi

```
256
257 Definition list_is_list : ∀ A (PA : A → U), (∀ a, PA a) → ∀ l, is_list A PA l.
```

```
258
259 Definition rtree_is_rtree : ∀ A (PA : A → U), (∀ a, PA a) → ∀ t, is_rtree A PA t.
```

261 These facts are then to be used in order to satisfy the premise of our induction principles.

262 Going back to our goal, we can build correctness proofs of equality tests in two steps.
263 For example, for natural numbers we can generate two lemmas:

```
264
265 Lemma nat_eq_correct : ∀ n, is_nat n → eq_axiom nat nat_eq n :=
266   nat_induction (eq_axiom nat nat_eq) P0 PS.
```

```
267
268 Lemma nat_eq_OK n : eq_axiom nat nat_eq n :=
269   nat_eq_correct n (nat_is_nat n).
```

271 where P0 and PS (line 2) stand for the two proof terms corresponding to the base case and
272 the inductive step of the proof. We omit them here for brevity.

273 For containers such as (list A) we can link the pieces in a similar way (at line 3 we omit
274 the proofs for nil and cons as before).

```
275
276 Lemma list_eq_correct A A_eq : ∀ l, is_list A (eq_axiom A A_eq) l →
277   eq_axiom list A (list_eq A A_eq) l :=
278   list_induction A (eq_axiom A A_eq) (eq_axiom (list A) (list_eq A A_eq)) Pnil Pcons.
```

```
279
280 Lemma list_eq_OK A A_eq (HA : ∀ a, eq_axiom A A_eq a) l :
281   eq_axiom (list A) (list_eq A A_eq) l :=
282   list_eq_correct A A_eq l (list_is_list A (eq_axiom A A_eq) HA l).
```

284 It is interesting to look at a data type that uses a container such as rtree: the induction
285 hypothesis P1 given by rtree_induction perfectly fits the premise of list_eq_correct (line 7).

```
286
287 Lemma rtree_eq_correct A A_eq : ∀ t, is_tree A (eq_axiom A A_eq) t →
288   eq_axiom (rtree A) (rtree_eq A A_eq)
289   :=
290   rtree_induction A (eq_axiom A A_eq) (eq_axiom (rtree A) (rtree_eq A A_eq))
291   PLeaf
292   (fun l (P1 : is_list (rtree A) (eq_axiom (rtree A) (rtree_eq A A_eq)) l) =>
293     .. list_eq_correct (rtree A) (rtree_eq A A_eq) l P1 ..).
```

```
294
295 Lemma rtree_eq_OK A A_eq (HA : ∀ a, eq_axiom A A_eq a) t :
296   eq_axiom (rtree A) (rtree_eq A A_eq) t :=
297   rtree_eq_correct A A_eq t (rtree_is_rtree A (eq_axiom A A_eq) HA t).
```

299 Type checking the terms above does not require any term to be transparent. Actually
300 they are applicative terms, there is no apparently recursive function involved.

301 Still there is no magic, we just swept the problem under the rug. In order to type check
302 the proof of rtree_is_rtree Coq needs to look at the proof term of list_is_list:

```
303
304 Definition rtree_is_rtree A PA (HPA : ∀ a, PA a) :=
305   fix IH t {struct t} : is_rtree A PA t :=
306     match t with
307     | Leaf a => is_Leaf A PA a (HPA a)
308     | Node l => is_Node A PA l (list_is_list (rtree A) (is_rtree A) IH l)
309     end.
```

311 As we explained in section 2 Coq would reject this term if the body of list_is_list was
312 opaque.

313 Even if we cannot make the problem disappear (without changing the way Coq checks
314 termination), we claim we confined the termination checking issue to the world of reified
315 type information. The transparent proofs of theorems such as T_is_T are separate from the
316 other, more relevant, proofs that can hence remain opaque as desired.

317 4 Elpi: an extension language for Coq

318 Elpi [6] is a dialect of λ Prolog [12], a higher order logic programming language. Elpi can
 319 be used as an extension language for Coq [18] in order to develop new commands in a
 320 programming language that has native support for bound variables.

321 Coq terms are represented in λ -tree syntax style [11] (sometimes also called Higher Order
 322 Abstract Syntax) reusing the binders of the programming language to represent the ones of
 323 Coq. For example, the term `(fun x => fact x)` is represented as `(lam (λ x, app["fact",x]))`.
 324 We say that `app` and `lam` are object level term constructors standing for iterated (n-ary)
 325 application and unary lambda abstraction; `"fact"` is a constant and `x` is a variable bound by
 326 λ x, that is the binder of the programming language.²

327 Programs are organized in clauses that represent both a data base of known facts and
 328 a set of rules to derive new facts out of known ones. For example one could use a relation
 329 named `eq-db` to link a type to its equality test.

```
330 eq-db "nat" "nat_eq".
331 eq-db (app["list", B]) (app["list_eq", B, B_eq]) :- eq-db B B_eq.
```

334 The first clause is a fact stating that `nat_eq` is the equality test for type `nat`. The second
 335 clause is an inference one and reads: the equality test for `(list B)` is `(list_eq B B_eq)` *if* `B_eq`
 336 is the equality test for `B`.

337 The `eq-db` data base can be queried for an equality test for, say, `(list nat)` by writing
 338 the goal `(eq-db (app["list", "nat"]) F)` where `F` is a variable to be filled in. By chaining the
 339 two clauses Elpi answers `(F = app["list_eq", "nat", "nat_eq"])` that reads back in the Coq
 340 syntax as `(list_eq nat nat_eq)`, the desired equality test for `(list nat)`.

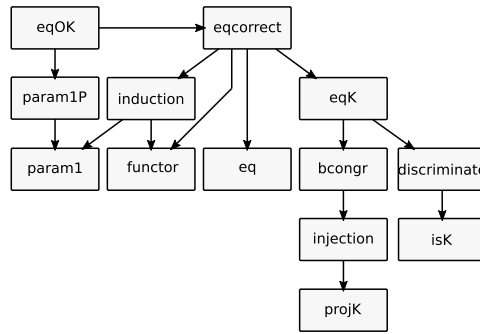
341 It is worth pointing out that in λ Prolog the set of clauses is dynamic: a program is
 342 allowed to add clauses inside a specific scope (typically the one of a binder) and the runtime
 343 collects them when the scope ends. As we will see, this feature is useful when a derivation
 344 takes place under an hypothetical context, e.g. when one assumes a parameter `A` and an
 345 equality test `A_eq`. No other feature of the Elpi language is relevant to this paper.

346 Finally, the integration of Elpi in Coq exposes to the extension language primitives to
 347 access the logical environment, e.g. to read an inductive data type declaration; to declare a
 348 new inductive type; to define a new constant; etc.

349 5 Anatomy of the derivation

350 The structure of the derivation is depicted in the following diagram. Each box represents
 351 a component deriving a complete term. An arrow from component A to component B tells
 352 that the terms generated by B are used by the terms generated by A. The interfaces between
 353 these components are indeed types: one can replace the work done by each component with
 354 a few hand written terms, if necessary.

² Here we simplify a little the embedding and use strings to represent named terms, omitting their nodes:
 For example `nat`, an inductive type, is actually written `(indt "Coq.Init.Datatypes.nat")`, while
`fact`, a defined constant, is written `(const "Coq.Arith.Factorial.fact")`.



355

356 The *eq* component is in charge of synthesizing the program performing the equality test.
 357 The correctness proof generated by *eqcorrect* goes by induction on the first term of the two
 358 being compared and then goes on in a different branch for each constructor *K*. The property
 359 being proved by induction is expressed using *eq_axiom* that, as we will detail in section 5.6
 360 is equivalent to a double implication. The *bcongr* component proves that the property is
 361 preserved by equal contexts, that is when the two terms are built using the same constructor.
 362 When they are not the program must return false and the equality be false as well: this is
 363 shown by *eqK*, that performs the case split on the second term. The no confusion property
 364 of constructor is key to this contextual reasoning. *projK* and *isK* generate utility functions
 365 that are then used by *injection* and *discriminate* to prove that constructors are injective
 366 and different. As we sketched in the previous sections the unary parametricity translation
 367 plays a key role in expressing the induction principle. The inductive predicate *is_T* for an
 368 inductive type *T* is generated by *param1* while *param1P* shows that terms of type *T* validate
 369 *is_T*. *functor* shows that *is_T* is a functor when *T* has parameters. This property is both used
 370 to synthesize induction principles and also to combine the pieces together in the correctness
 371 proof. The *eqOK* component hides the *is_T* relation from the theorems proved by *eqcorrect*
 372 by using the lemmas *T_is_T* proved by *param1P*.

373 5.1 Equality test

374 Synthesizing the equality test for a type *T* proceeds as follows. First the test takes in input
 375 each type parameter *A* together with an equality test *A_eq*. Then the recursive function takes
 376 in input two terms of type *T* and inspects both via pattern matching. Outside the diagonal,
 377 where constructors are different, it says *false*. On the diagonal it composes the calls on the
 378 arguments of the constructors using boolean conjunction. The code called to compare two
 379 arguments depends on their type: If it is *T* then it is a recursive call; if it is a type parameter
 380 *A* then we use *A_eq*; if it is another type it uses the corresponding equality test.

381 Let us take for example the equality test for rose trees:

```

382 Definition rtree_eq A (A_eq : A → A → bool) :=
383   fix rec (t1 t2 : rtree A) {struct t1} : bool :=
384     match t1, t2 with
385     | Leaf a, Leaf b => A_eq a b
386     | Node l, Node s => list_eq (rtree A) rec l s
387     | _, _ => false
388   end.
  
```

391 Line 5 calls *list_eq* since the type of *l* and *s* is *(list (rtree A))* and it passes to it *rec* since
 392 the type parameter of *list* is *(rtree A)*.

Here is an excerpt of Elpi code used to synthesize the body of the branches:

```

393
394 eq-db "A" "A_eq".
395 eq-db (app["rtree","A"]) "rec".
396 eq-db (app["list", B]) (app["list_eq", B, B_eq]) :- eq-db B B_eq.
397

```

The first clause says that `A_eq` is the equality test for type `A`, and is used to build the branch at line 4. The third clause, chained with the second one, combines `list_eq` with `rec` building the branch at line 5. The first two clauses are present only during the derivation of the body of the fixpoint, under the context formed by the type parameter `A`, its equality test `A_eq`, and the recursive call `rec` itself. Once the derivation is complete both clauses are removed from the data base and the following one is permanently added.

```

405 eq-db (app["rtree", B]) (app["rtree_eq", B, B_eq]) :- eq-db B_eq.
406

```

5.2 Parametricity

The `param1` component is able to generate the unary parametricity translation of types and terms following [7]. We already gave many examples in section 3. The `param1P` component synthesizes proofs that terms of type `T` validate `is_T` by a trivial structural recursion: constructor `K` is mapped to `is_K`. When `T` is a container we assume the triviality of the property on the type parameter. For example:

```

414 Definition rtree_is_rtree A (PA : A → U) : (∀x, PA x) → ∀t, is_rtree A PA t.
415

```

5.3 Functoriality

The `functor` component implements a double service. For non-indexed containers it synthesizes a simple map:

```

420 Definition list_map A B : (A → B) → list A → list AB.
421

```

The derivation becomes more interesting when the container has indexes, e.g. when the container is a `is_T` inductive predicate. On indexed data types the derivation avoids to map the indexes and consequently all type variables occurring in the types of the indexes. For example, mapping the `is_list` inductive predicate gives:

```

427 Lemma is_list_funct A P Q : (∀a, P a → Q a) → ∀l, is_list A P l → is_list A Q l.
428

```

This property corresponds to the functoriality of `is_list` over the property about the type parameter. Note that parameters of arity one, such as `P`, are mapped point wise.

As we did for the `eq-db` data base of equality tests, we can store these maps as clauses and use the data base later on in the *induction* and *ecorrect* derivations. Here is an excerpt of Elpi code for this data base, that we call `funct-db`:

```

435 funct-db (app["is_list",A,P]) (app["is_list",A,Q]) (app["is_list_funct",A,P,Q,F]) :-
436   funct-db P Q F.
437

```

Note that the terms involved are “point free”, i.e. the first two arguments are terms of arity one, while the third term is of arity two. The identity is written as follows:

```

441 funct-db P P (lam (λa, lam (λp, p))).
442

```

This means that when one has a term `a` and a term `(p : P a)`, in order to obtain a term `(q : Q a)` he can query `funct-db` by asking Elpi to fill in `M` in `(funct-db "P" "Q" M)`. If the answer is `(M = f)` then the desired term is obtained by passing `a` and `p` to `f`, that is `(f a p : Q a)`.

447 **5.4 Induction**

448 In order to derive the induction principle for type T we first derive its unary parametricity
 449 translation is_T . The is_T inductive predicate has one constructor is_K for each constructor
 450 K of the type T . The type of is_K relates to the type of K in the following way. For each
 451 argument $(a : A)$ of K , is_K takes two arguments: $(a : A)$ and $(pa : \text{is}_A a)$. Finally the
 452 type of $(\text{is}_K a_1 pa_1 \dots a_n pa_n)$ is $(\text{is}_T (K a_1 \dots a_n))$.

453 The induction principle is synthesized by following these steps:

- 454 1. take in input each parameter $A_1 PA_1 \dots A_n PAn$ of is_T .
- 455 2. take in input a predicate $(P : T A_1 \dots A_n \rightarrow U)$.
- 456 3. for each constructor is_K of type
 457 $(\forall A_1 PA_1 \dots A_n PAn, \forall a_1 pa_1 \dots a_n pa_n, \text{is}_T A_1 PA_1 \dots A_n PAn (K a_1 \dots a_n))$
 458 take in input an assumption HK of type $(\forall a_1 pa_1 \dots a_n pa_n, P (K a_1 \dots a_n))$.
- 459 4. take in input $(t : T A_1 \dots A_n)$.
- 460 5. take in input $(x : \text{is}_T A_1 PA_1 \dots A_n PAn t)$.
- 461 6. perform recursion on x and a case split. Then in each branch
 462 a. bind all arguments of is_K , namely
 463 $(a_1 : A_1) (pa_1 : \text{is}_A_1 a_1) \dots (a_n : A_n) (pa_n : \text{is}_A_n a_n)$
 464 b. obtain qai by *mapping* the corresponding pai (as in `funct-db`, see below).
 465 c. return $(HK a_1 qai \dots a_n qan)$

466 Lets take for example the induction principle for rose trees:

```
467 Definition rtree_induction A PA P
468 (HLeaf : ∀ a, PA a → P (Leaf A a))
469 (HNode : ∀ l, is_list (rtree A) P l → P (Node A l)) :
470 ∀ t, is_rtree A PA t → P t
471 :=
472 fix IH (t: rtree A) (x: is_rtree A PA t) {struct x}: P t :=
473   match x with
474   | is_Leaf a pa => HLeaf a pa
475   | is_Node l pl => (* pl: is_list (rtree A) (is_rtree A PA) l *)
476     HNode l (is_list_funct (rtree A) (is_rtree A PA) P IH l pl)
477   end.
```

480 Note how, intuitively, the type of $HLeaf$ can be obtained from the type of is_Leaf by
 481 replacing $(\text{is}_rtree A PA)$ with P .

482 Finally let us see how the second argument to $HNode$ is synthesized. We take advantage of
 483 the fact that Elpi is a logic programming language and we query the data base `funct-db` as
 484 follows. First we temporarily register the fact that IH maps $(\text{is}_rtree A PA)$ to P obtaining,
 485 among others, the following clauses.

```
486 funct-db (app["is_rtree", "A", "PA"]) "P" "IH".
487 funct-db (app["is_list", A, P]) (app["is_list", A, Q]) (app["is_list_funct", A, P, Q, F]) :-
488   funct-db P Q F.
```

491 Then we query `funct-db` as follows:

```
492 funct-db (app["is_list", app["rtree", "A"], app["is_rtree", "A", "PA"]])
493   (app["is_list", app["rtree", "A"], "P"])
494   Q.
```

497 The answer $(Q = \text{app}["is_list_funct", \text{app}["rtree", "A"], \text{app}["is_rtree", "A", "PA"], "P", "IH"])$
 498 is exactly the second term we need to pass to $HNode$ (once applied to l and pl , line 10 above).

499 It is worth pointing out that, for the term to be accepted by the termination checker the
 500 map over is_list must be transparent.

501 To sum up the unary parametricity translation gives us the type of the induction principle,
 502 up to a trivial substitution. The functoriality property of the inductive predicates obtained
 503 by parametricity gives us a way to prove the branches.

504 5.5 No confusion property

505 In order to prove that an equality test is correct one has to show the so called “no confusion”
 506 property, that is that constructors are injective and disjoint (see for example [10]).

507 The simplest form of the property of being disjoint is expressed on `bool`:

```
508 Lemma bool_discr : true = false → ∀T : U, T.
```

511 This lemma is proved by hand once and for all. What the *isK* component synthesizes is a
 512 per-constructor test to be used in order to reduce a discrimination problem on type `T` to a
 513 discrimination problem on `bool`. For the rose tree data type *isK* generates:

```
514 Definition is_Node A (t : rtree A) := match t with Node _ => true | _ => false end.  

    515 Definition is_Leaf A (t : rtree A) := match t with Leaf _ => true | _ => false end.
```

518 The *discriminate* components uses one more trivial fact, `eq_f`, in order to assemble these
 519 tests together with `bool_discr`.

```
520 Lemma eq_f T1 T2 (f : T1 → T2) : ∀a b, a = b → f a = f b.
```

523 From a term `H` of type `(Node l = Leaf a)` the *discriminate* procedure synthesizes:

```
524 (bool_discr (eq_f (rtree A) (rtree A) (is_Node A) H)) : ∀T : U, T
```

527 Note that the type of the term `(eq_f .. H)` is `(is_Node A (Node l) = is_Node A (Leaf a))` that
 528 is convertible to `(true = false)`, the premise of `bool_discr`.

530 In order to prove the injectivity of constructors the *projK* component synthesizes a
 531 projector for each argument of each constructor. For the `cons` constructor of `list` we get:

```
532 Definition get_cons1 A (d1 : A) (d2 : list A) (l : list A) : A :=  

    533   match l with nil => d1 | x :: _ => x end.  

    534 Definition get_cons2 A (d1 : A) (d2 : list A) (l : list A) : list A :=  

    535   match l with nil => d2 | _ :: xs => xs end.
```

539 Each projector takes in input default values for each and every argument of the constructor.
 540 It is designed to be used by the *injection* procedure as follows. Given a term `H` of type
 541 `(x :: xs = y :: ys)` it synthesizes:

```
542 (eq_f (list A) A (get_cons1 A x xs) (x :: xs) (y :: ys) H) : x = y  

    543 (eq_f (list A) (list A) (get_cons2 A x xs) (x :: xs) (y :: ys) H) : xs = ys
```

546 These terms are easy to build given that the type of `H` contains the default values to be
 547 passed to the projectors. Note that the type of the second term is actually:

```
548 get_cons2 A x xs (cons x xs) = get_cons2 A x xs (cons y ys)
```

551 that is convertible to the desired type `(xs = ys)`.

552 5.6 Congruence

553 In the definition of `eq_axiom` we use the `reflect` predicate [9]. It is a sort of if-and-only-if
 554 specialized to link a proposition and a boolean test. It is defined as follows:

23:12 Deriving proved equality tests in Coq-elpi

```

555 Inductive reflect (P : U) : bool → U :=
556 | ReflectT (p : P) : reflect P true
557 | ReflectF (np : P → False) : reflect P false.
558

```

In our case the shape of P is always an equation between two terms of an inductive type, i.e. constructors. When the same constructor occurs in both sides, as in $(k\ x1 \dots xn = k\ y1 \dots y2)$, the equality test discards k and proceeds on each $(xi = yi)$. The *bcongr* component synthesizes lemmas helping to prove the correctness of this step. For example:

```

564 Lemma list_bcongr_cons A :
565   ∀ (x y : A) b, reflect (x = y) b →
566   ∀ (xs ys : list A) c, reflect (xs = ys) c →
567   reflect (x :: xs = y :: ys) (b && c)
568
569 Lemma rtree_bcongr_Leaf A (x y : A) b :
570   reflect (x = y) b → reflect (Leaf A x = Leaf A y) b
571
572 Lemma rtree_bcongr_Node A (l1 l2 : list (rtree A)) b :
573   reflect (l1 = l2) b → reflect (Node A l1 = Node A l2) b
574

```

Note that these lemmas are not related to the equality test specific to the inductive type. Indeed they deal with the `reflect` predicate, but not with the `eq_axiom` predicate that we use every time we talk about equality tests.

The derivation goes as follows: if any of the premises is false, then the result is proved by `ReflectF` and the injectivity of constructors. If all premises are `ReflectT` their argument, an equation, can be used to rewrite the conclusion.

```

582 Lemma list_bcongr_cons A
583 (x y : A) b (hb : reflect (x = y) b)
584 (xs ys : list A) c (hc : reflect (xs = ys) c) :
585 reflect (x :: xs = y :: ys) (b && c) :=
586 match hb, hc with
587 | ReflectT eq_refl, ReflectT eq_refl => ReflectT eq_refl
588 | ReflectF (e : x = y → False), _ =>
589   ReflectF (fun H : x :: xs = y :: ys =>
590     e (eq_f (list A) A (get_cons1 A x xs) (x :: xs) (y :: ys) H))
591 | _, ReflectF e =>
592   ReflectF .. (e (eq_f .. (get_cons2 ..) ..) ..) ..
593 end.
594

```

The elimination of `hb` and `hc` substitutes `b` and `c` by either `true` or `false`. In the branch at line 6 the boolean expression is hence `(true && true)` while the proposition is `(x :: xs = x :: xs)` given that the two equations `(x = y)` and `(xs = ys)` were eliminated as well.

The argument of `e` at line 9 is the term generated by the *injection* component. The branch at line 11, covering the case where the heads are equal but the tails different, is very close to lines 8 and 9 but for the fact that the projector for the second argument of `cons` is used, instead of the projection for the first one.

There are other ways one could have expressed these lemmas, for example by not mentioning the `cons` constructor explicitly but rather an abstract function `k` known to be injective on the first and second argument. Even if we find this presentation more appealing on paper, in practice we found no advantage and we hence opted for the current approach.

bcongr gives us lemmas to propagate equality and inequality only under the same constructor. *eqK* complements this work by proving `eq_axiom` also when the constructors differ.

Recall that the induction principle does a case split on one term, the first one of the two being compared. *eqK* generates a lemma for each constructor, to be used in the corresponding branch of the induction, that performs the case split on the second term being compared. This is the lemma generated for `Node`:

```

613
614 Lemma rtree_eq_axiom_Node A (A_eq : A → A → bool) l1 :
615   eq_axiom (list (rtree A)) (list_eq (rtree A) (rtree_eq A A_eq)) l1 →
616   eq_axiom (rtree A) (rtree_eq A A_eq) (Node A l1)
617 :=
618   fun H (t2 : rtree A) =>
619   match t2 with
620   | Leaf n =>
621     ReflectF (fun abs : Node A l1 = Leaf A n =>
622       bool_discr (eq_f (rtree A) bool (is_Node A) (Node A l1) (Leaf A n) abs) False)
623   | Node l2 =>
624     rtree_bcongr_Node A l1 l2 (list_eq (rtree A) (rtree_eq A A_eq) l1 l2) (H l2)
625 end.
626

```

627 Note that the code for the first branch is what *discriminate* synthesizes; while the code in
 628 the second branch is what *bcongr* generates.

629 5.7 Correctness

630 The *eqcorrect* component combines the induction principle generated by *induction* with the
 631 case split on the second term provided by *eqK*.

632 Let's recall the type of the correctness lemma for *list_eq*, of the induction principle and
 633 then let's analyse the proof of *rtree_eq_correct*:

```

634
635 Lemma list_eq_correct A (fa : A → A → bool) l,
636   is_list A (eq_axiom A fa) l →
637   eq_axiom (list A) (list_eq A fa) l.
638
639 Definition rtree_induction A PA P
640   (HLeaf : ∀y, PA y → P (Leaf A y))
641   (HNode : ∀l, is_list (rtree A) P l → P (Node A l)) :
642   ∀t, is_rtree A PA t → P t.
643
644 Lemma rtree_eq_axiom_Node A (f : A → A → bool) l1 :
645   eq_axiom (list (rtree A)) (list_eq (rtree A) (rtree_eq A f)) l1 →
646   eq_axiom (rtree A) (rtree_eq A f) (Node A l1).

```

648 The proof is a rather straightforward application of the induction principle to the property

```

649 eq_axiom (rtree A) (rtree_eq A fa)
650
651

```

652 Each branch is then proved by the corresponding lemma generated by *eqK* with only one
 653 caveat: one may need to adapt the induction hypothesis, *P1* here, in order to make it fit the
 654 premise of the lemma generated by *eqK*. In this specific case the "adaptor" is *list_eq_correct*.

```

655
656 Lemma rtree_eq_correct A (fa : A → A → bool) :=
657   rtree_induction A (eq_axiom A fa)
658   (*P*) (eq_axiom (rtree A) (rtree_eq A fa))
659   (*HLeaf*) (rtree_eq_axiom_Leaf A fa)
660   (*HNode*) (fun l (P1 : is_list (rtree A) (eq_axiom (rtree A) (rtree_eq A fa)) l) =>
661     rtree_eq_axiom_Node A fa l (list_eq_correct (rtree A) (rtree_eq A fa) l P1)).

```

663 Logic programming provides a natural way to synthesize the adaptor. We load in the
 664 data base all the correctness proofs synthesized so far, as follows:

```

665
666 funct-db (app["is_list", A, PA])
667   (app["eq_axiom", app["list", A], app["list_eq", A, A_eq]]) R :-
668   R = (app["list_eq_correct", A, A_eq]),
669   funct-db PA (app["eq_axiom", A, A_eq]).
670

```

671 This clause simply gives an operational reading to the type of *list_eq_correct*: the conclusion
 672 is true if the premise is. The only cleverness is to separate the premise in two parts, being a

23:14 Deriving proved equality tests in Coq-elpi

673 (list A) with property PA and have PA be a sufficient condition to prove that A_eq is correct.
674 In this way clauses compose better: Search peels off just one type constructor at a time.
675 Indeed we extend the `funct-db` predicate, instead of building a new one just for correctness
676 lemmas, because functoriality lemmas are sometimes needed in addition to the correctness
677 ones. Take for example this simple data type of a histogram.

```
678 Inductive histogram := Columns (bars : list nat).  
679  
680  
681 Lemma histogram_induction (P : histogram → Type) :  
682   (∀ l, is_list nat is_nat l → P (Columns l)) →  
683   ∀ h, is_histogram h → P h.
```

685 Now look at the lemma synthesized by `eqK` for the `Columns` constructor.

```
686 Lemma histogram_eq_axiom_Columns l :  
687   eq_axiom (list nat) (list_eq nat nat_eq) l →  
688   ∀ h, eq_axiom_at histogram histogram_eq (Columns l) h.
```

```
691 Lemma histogram_eq_correct h : eq_axiom histogram histogram_eq h :=  
692   histogram_induction  
693     (eq_axiom histogram histogram_eq)  
694     (fun l (P1 : is_list nat is_nat l) =>  
695       histogram_eq_axiom_Columns  
696         l (list_eq_correct nat nat_eq  
697           l (is_list_func nat is_nat (eq_axiom nat nat_eq) nat_eq_correct l P1))).  
698
```

700 Note that the type of P1 is (is_list nat is_nat) and that it needs to be adapted to match
701 (is_list nat (eq_axiom nat nat_eq)). The correctness lemma for nat_eq, namely `nat_eq_correct`
702 of type (∀ n, is_nat n → eq_axiom nat nat_eq n), cannot be used directly but must undergo
703 the `is_list_func` functor.

704 5.8 eqOK

705 The last derivation hides the `is_T` predicate to the final user by combining the output of
706 `eqcorrect` and `param1P`.

```
707 Lemma list_eq_correct A A_eq :  
708   ∀ l, is_list A (eq_axiom A A_eq) l → eq_axiom (list A) (list_eq A A_eq) l.  
709  
710  
711 Lemma list_eq_OK A A_eq A_eq_OK l : eq_axiom (list A) (list_eq A A_eq) l :=  
712   list_eq_correct A A_eq l (list_is_list A (eq_axiom A A_eq) A_eq_OK).  
713
```

714 Both lemmas are needed. The former composes well and is needed if one defines a type
715 using lists as a container. The latter is what the user needs in order to work with lists.

716 5.9 Assessment

717 The code is quite compact thanks to the fact that the programming language is very high
718 level and that its programming paradigm is a good fit for this application.

719 On the average each components is about 200 lines of code. Simpler derivations like
720 `projK`, `isK` or even `param1P` are under 100 lines.

721 Debugging this kind of code did not pose particular difficulties. The typical error results
722 in the generated term being ill-typed. In that case the Coq type checker could be used to
723 identify the culprit. Given how small the derivations are, it was simple to identify the lines
724 generating the offending subterm.

725 The time required to design and develop the entire procedure amounts to approximately
726 six months, but spanned over more than one and a half year: most of the time has been

727 spent improving the integration of Elpi in Coq in response to the experience gathered on this
 728 work. At the time of writing the Elpi integration in Coq does not support mutual inductive
 729 types, universe polymorphic definitions and primitive projections.

730 All derivations support polynomial types. Some derivations also support index data, eg
 731 *eq* is able to synthesize an equality test for vectors. Most of the derivations for contextual
 732 reasoning, such as *eqK* and *bcongr* do not support indexes.

733 6 Related work

734 Systems similar to Coq [19], e.g. Matita [2], Lean [5], Agda [14] and Isabelle [13] all generate
 735 induction principles automatically, and some of them also the no confusion properties.

736 To our knowledge Isabelle is the only system that generates sensible induction principles
 737 and proved equality tests when containers are involved. As described in [4] the (co)datatype
 738 package is built on top of Bounded Natural Functors [20], a notion that makes the con-
 739 struction of (co)datatypes in Higher Order Logic compositional. Our starting point is very
 740 different since Coq, and type theory in general, internalizes the definitional mechanism for
 741 (co)datatypes. As a consequence a package like the one described in this paper cannot
 742 change it but only work around its eventual limitations. In particular the way Coq checks
 743 recursive functions for termination is a fixed, syntactic, non modular, criteria for which some
 744 alternatives have been studied (see for example [3, 15]) but never implemented. The non
 745 modular criteria applies to induction principles as well, since they are proved using recursion.
 746 It is a strength of the construction described in this paper to recover some modularity and
 747 hence be able to synthesize mechanically most of what [4] is able to synthesize.

748 Most Interactive Theorem Provers come with simple forms of Prolog-like automation,
 749 usually in the form of Type Classes. The user typically resorts to that in order to perform
 750 some of the inductive reasoning one needs in order to synthesize code in a type directed way.
 751 To our knowledge no ready-to-use package to synthesize equality tests and their proofs was
 752 written this way.

753 Some systems, notably Lean, come with a whole round meta programming framework.
 754 Still, to our knowledge, the primary application is the development of proof commands, not
 755 program/proof synthesis, in spite of the stunning similarity.

756 Coq provides two mechanisms strictly related to this work. The `Scheme Equality` com-
 757 mand generates for a type τ the code for the equality test (`T_eqb`) and a proof that equality
 758 is decidable on τ . The proof internally uses the equality test, but its type does not:

```
759 T_eq_dec : ∀ x y : T, {x = y} + {x <> y}
```

762 By unfolding the proof term, that is transparent, it should be possible to recover the fact
 763 that `T_eqb` is a correct equality test. Data types defined using containers are not supported.
 764 The `decide equality` tactic requires the user to start a lemma with a statement as the one
 765 depicted above. The tactic only performs one (case split) step and has to be iterated by
 766 hand. It does not remember which equalities were proved decidable before, it is up to the
 767 user to eventually share code. The proof term generated is, in a type theoretic sense, a
 768 program even if its code mixes the comparison test with its correctness proof. This proof
 769 is fully transparent, and inlines all the contextual reasoning steps such as injection and
 770 discrimination. As a result the term is very large and computationally heavy when run
 771 within Coq.

772 In the programming language world derivation is much more developed. The dominant
 773 approach is to provide some meta programming facilities, e.g. by providing a syntax to the
 774 declaration of types and then use the programming language itself to write derivations [16]

775 that run at compile time as compiler plugins. Our approach is similar in a sense, since we
 776 work at the meta level on the syntax of types (and terms), but it is also very different since
 777 we pick a different programming language for meta programming. In particular we choose a
 778 very high level one that makes our derivations very concise and hides uninteresting details
 779 such as the representation of bound variables. The derivation described in the paper is the
 780 result of many failed attempts and we believe that the high level nature of the programming
 781 language we chose played an important role in the exploratory phase.

782 **7 Conclusion**

783 We described a technique to derive stronger induction principles for Coq data types built
 784 using containers. We use the unary parametricity translation of a data type in order to
 785 fuel its induction principle, to thread an invariant on the contained when used as a con-
 786 tainer and finally to confine the modularity problems stemming from the termination check
 787 implemented in Coq. Finally we provide a Coq package deriving correct equality tests for
 788 polynomial inductive data types.

789 It is work in progress to extend the derivation to inductive types with decidable indexes.
 790 Preliminary work hints that indexes of base types such as `nat` pose no problem. On the
 791 contrary when indexes mention containers, that admit a decidable equality only if their
 792 contained does, the *param1P* component gets substantially more complex. In particular
 793 some notions of Homotopy Type Theory come in to play. For example the notion of being
 794 provable on the entire domain such as $(\forall a : A, P a) \rightarrow (\forall t : T A, \text{is_T A P } t)$ seems to
 795 require to be strengthened using the notion of contractibility (that is, the property should
 796 hold and its proof be unique), in order for the construction to compose well.

797 We also look forward to let the user tune the derivation process by annotating the type
 798 declarations. For example the user may want to skip certain arguments when generating
 799 the equality test, such as the integer describing the length of a sub vector in the `cons`
 800 constructor. The resulting equality test surely requires some user intervention in order to
 801 be proved correct, but it features a better computational complexity.

802 Finally, adding other derivations to the package seems appealing. For example the
 803 interface next to `eqType` in the hierarchy used in the Mathematical Component library is the
 804 one of countable types, i.e. types in bijection with natural numbers. The interface requires,
 805 roughly, a serialization function to another countable type, a tedious task that could be
 806 made automatic.

807 We are grateful to Maxime Denes and Cyril Cohen for the many discussions shedding light
 808 on the subject. We thank Cyril Cohen for writing the code of *param2* (binary parametricity
 809 translation), out of which *param1* was easily obtained. We also thank Damien Rouhling,
 810 Laurent Théry and Laurence Rideau for proofreading the paper. Finally we are indebted to
 811 Luc Chabassier for working on an early prototype of Elpi on the synthesis of equality tests:
 812 an experiment that convinced the author it was actually doable.

813 **References**

-
- 814 1 Andreas Abel. Semi-continuous sized types and termination. *Logical Methods in Com-*
 815 *puter Science*, 4(2), 2008. URL: [https://doi.org/10.2168/LMCS-4\(2:3\)2008](https://doi.org/10.2168/LMCS-4(2:3)2008), doi:10.2168/
 816 LMCS-4(2:3)2008.
- 817 2 Andrea Asperti, Wilmer Ricciotti, Claudio Sacerdoti Coen, and Enrico Tassi. The Matita
 818 interactive theorem prover. In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors,

- 819 *Automated Deduction – CADE-23*, pages 64–69, Berlin, Heidelberg, 2011. Springer Berlin
820 Heidelberg.
- 821 **3** Gilles Barthe, Benjamin Grégoire, and Fernando Pastawski. Cic^{\wedge} : type-based termination
822 of recursive definitions in the calculus of inductive constructions. In *Logic for Programming,*
823 *Artificial Intelligence, and Reasoning, 13th International Conference, LPAR 2006, Phnom*
824 *Penh, Cambodia, November 13-17, 2006, Proceedings*, pages 257–271, 2006. URL: https://doi.org/10.1007/11916277_18, doi:10.1007/11916277_18.
- 826 **4** Jasmin Christian Blanchette, Johannes Hölzl, Andreas Lochbihler, Lorenz Panny, Andrei
827 Popescu, and Dmitriy Traytel. Truly modular (co)datatypes for isabelle/hol. In Gerwin
828 Klein and Ruben Gamboa, editors, *Interactive Theorem Proving*, pages 93–110, Cham, 2014.
829 Springer International Publishing.
- 830 **5** Leonardo de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer.
831 The lean theorem prover (system description). In Amy P. Felty and Aart Middeldorp, edi-
832 tors, *Automated Deduction - CADE-25*, pages 378–388, Cham, 2015. Springer International
833 Publishing.
- 834 **6** Cvetan Dunchev, Ferruccio Guidi, Claudio Sacerdoti Coen, and Enrico Tassi. ELPI: fast,
835 Embeddable, λ Prolog Interpreter. In *Proceedings of LPAR*, Suva, Fiji, November 2015. URL:
836 <https://hal.inria.fr/hal-01176856>.
- 837 **7** Chantal Keller and Marc Lasson. Parametricity in an Impredicative Sort. In Patrick Cégielski
838 and Arnaud Durand, editors, *CSL - 26th International Workshop/21st Annual Conference of*
839 *the EACSL - 2012*, volume 16 of *CSL*, pages 381–395, Fontainebleau, France, September
840 2012. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. URL: [https://hal.inria.fr/](https://hal.inria.fr/hal-00730913)
841 [hal-00730913](https://hal.inria.fr/hal-00730913), doi:10.4230/LIPIcs.CSL.2012.399.
- 842 **8** Assia Mahboubi and Enrico Tassi. Canonical Structures for the Working Coq User. In
843 Sandrine Blazy, Christine Paulin-Mohring, and David Pichardie, editors, *Interactive Theorem*
844 *Proving*, pages 19–34, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
- 845 **9** Assia Mahboubi and Enrico Tassi. *Mathematical Components*. draft, v1-183-gb37ad7, 2018.
- 846 **10** Conor McBride, Healfdene Goguen, and James McKinna. A few constructions on constructors.
847 In Jean-Christophe Filliâtre, Christine Paulin-Mohring, and Benjamin Werner, editors, *Types*
848 *for Proofs and Programs*, pages 186–200, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
- 849 **11** Dale Miller. Abstract syntax for variable binders: An overview. In John Lloyd, Veronica
850 Dahl, Ulrich Furbach, Manfred Kerber, Kung-Kiu Lau, Catuscia Palamidessi, Luís Moniz
851 Pereira, Yehoshua Sagiv, and Peter J. Stuckey, editors, *Computational Logic — CL 2000*,
852 pages 239–253, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.
- 853 **12** Dale Miller and Gopalan Nadathur. *Programming with Higher-Order Logic*. Cambridge Uni-
854 versity Press, 2012. doi:10.1017/CB09781139021326.
- 855 **13** Tobias Nipkow, Markus Wenzel, and Lawrence C. Paulson. *Isabelle/HOL: A Proof Assistant*
856 *for Higher-order Logic*. Springer-Verlag, Berlin, Heidelberg, 2002.
- 857 **14** Ulf Norell. *Towards a practical programming language based on dependent type theory*. PhD
858 thesis, Department of Computer Science and Engineering, Chalmers University of Technology,
859 SE-412 96 Göteborg, Sweden, September 2007.
- 860 **15** Jorge Luis Sacchini. *On type-based termination and dependent pattern matching in the calculus*
861 *of inductive constructions*. Theses, École Nationale Supérieure des Mines de Paris, June 2011.
862 URL: <https://pastel.archives-ouvertes.fr/pastel1-00622429>.
- 863 **16** Tim Sheard and Simon Peyton Jones. Template meta-programming for haskell. *SIGPLAN*
864 *Not.*, 37(12):60–75, December 2002. URL: <http://doi.acm.org/10.1145/636517.636528>,
865 doi:10.1145/636517.636528.
- 866 **17** Matthieu Sozeau and Nicolas Oury. First-class type classes. In *Proceedings of the 21st In-*
867 *ternational Conference on Theorem Proving in Higher Order Logics*, TPHOLs '08, pages
868 278–293, Berlin, Heidelberg, 2008. Springer-Verlag. URL: [http://dx.doi.org/10.1007/](http://dx.doi.org/10.1007/978-3-540-71067-7_23)
869 [978-3-540-71067-7_23](http://dx.doi.org/10.1007/978-3-540-71067-7_23), doi:10.1007/978-3-540-71067-7_23.

23:18 Deriving proved equality tests in Coq-elpi

- 870 **18** Enrico Tassi. Elpi: an extension language for Coq (Metaprogramming Coq in the Elpi λ Prolog
871 dialect). CoqPL, January 2018. URL: <https://hal.inria.fr/hal-01637063>.
- 872 **19** The Coq Development Team. The coq proof assistant, version 8.8.0, April 2018. URL:
873 <https://doi.org/10.5281/zenodo.1219885>, doi:10.5281/zenodo.1219885.
- 874 **20** Dmitry Traytel, Andrei Popescu, and Jasmin C. Blanchette. Foundational, compositional
875 (co)datatypes for higher-order logic: Category theory applied to theorem proving. In *Pro-*
876 *ceedings of the 2012 27th Annual IEEE/ACM Symposium on Logic in Computer Science,*
877 *LICS '12*, pages 596–605, Washington, DC, USA, 2012. IEEE Computer Society. URL:
878 <https://doi.org/10.1109/LICS.2012.75>, doi:10.1109/LICS.2012.75.
- 879 **21** Philip Wadler. Theorems for free! In *Proceedings of the Fourth International Conference*
880 *on Functional Programming Languages and Computer Architecture, FPCA '89*, pages 347–
881 359, New York, NY, USA, 1989. ACM. URL: <http://doi.acm.org/10.1145/99370.99404>,
882 doi:10.1145/99370.99404.