Matita 0.99.1

Andrea Asperti
(Wilmer Ricciotti, Claudio Sacerdoti Coen)

Department of Computer Science, University of Bologna
Mura Anteo Zamboni 7, 40127, Bologna, ITALY
asperti@cs.unibo.it

Foundation of Mathematics for Computer-Aided Formalization

Padova, 9-11 January 2013

About Matita

Matita (pencil) is an implementation of the Calculus of Inductive Constructions alternative to Coq.

Distinctive features (already in version 0.5.2 [CADE '11])

- light
- completely functional
- native open terms [Matita team '09 (a)][1]
- strong disambiguation facilities
  [Sacerdoti Coen, Zacchiroli '04]
- small step execution of structured tactics (tinycals)
  [Sacerdoti Coen, Tassi, Zacchiroli '06]
- good documentation of system's internals

[1] Matita Team: Asperti, Ricciotti, Sacerdoti Coen, Tassi

Training and sperimentation

A good environment for

- learning the practice of formal development and the internals of interactive provers.
- experimenting innovative ideas

A Mature System

Some Matita developments:

- Number theory: Properties of Möbius μ, Euler φ and Chebyshev Θ functions; Bertrand's postulate [Asperti, Ricciotti '12 (b)]
- Constructive analysis: Lebesgue's dominated convergence theorem [Sacerdoti Coen, Tassi '08]
- Formal topology: elements of pointless topology [Sacerdoti Coen, Tassi '011]
- Programming languages metatheory: solution to the POPLmark challenge [Matita team '11]
- **Compilers verification**: EU Project CerCo (Certified Complexity) for the verification of a formally certified complexity preserving compiler for the C programming language [CerCo].
- Formal Complexity Formalization of aspects of Complexity Theory (reverse computational Complexity) [Asperti, Ricciotti '12].

Main novelties in version 0.99.1

Huge refactoring and simplification effort

- bidirectional type inference [Matita team '12]
- enhanced mechanism of unifications hints [Sacerdoti Coen, Tassi '011]
- a new type for tactics [Matita team '09 (b)]
- new "compact" syntax (partially inspired by SSReflect)

New Syntax

tactic	old syntax	new syntax
introduction	intro aaa	#aaa
application	apply aaa	@aaa
rewriting	rewrite > aaa	>aaa
constructor	constructor n	%n
automation	auto depth=n	/n/
proof leaves	reflexivity/assumption	//
anonymous elim.	intro H; elim H	*

* behaviour:

$$\Delta \vdash (\exists x : A.B) \to C \quad \Rightarrow \quad \Delta \vdash \forall x : A.B \to C$$
$$\Delta \vdash A \wedge B \to C \quad \Rightarrow \quad \Delta \vdash A \to B \to C$$

An example (old syntax)

```
theorem le_exp: ∀n,m,p:nat. O < p → n≤ m → p^n ≤ p^m.
apply nat_elim2
  [intros.
   apply lt_O_exp.assumption
  |intros.
   apply False_ind.
   apply ( le_to_not_lt  ? ? ? H1).
   apply le_O_n
  |intros.
   simplify.
   apply le_times
    [apply le_n
    |apply H[assumption|apply le_S_S_to_le.assumption]
    ]
  ]
qed.
```

An example (new syntax)

```
theorem le_exp: ∀n,m,p:nat. O < p → n≤m → p^n ≤ p^m.
@nat_elim2 #n #m
  [#ltm #len @lt_O_exp //
  |#_ #len @False_ind /2/
  |#Hind #p #posp #lenm normalize @le_times // @Hind /2/
  ]
qed.
```

compact and elegant

Size comparison

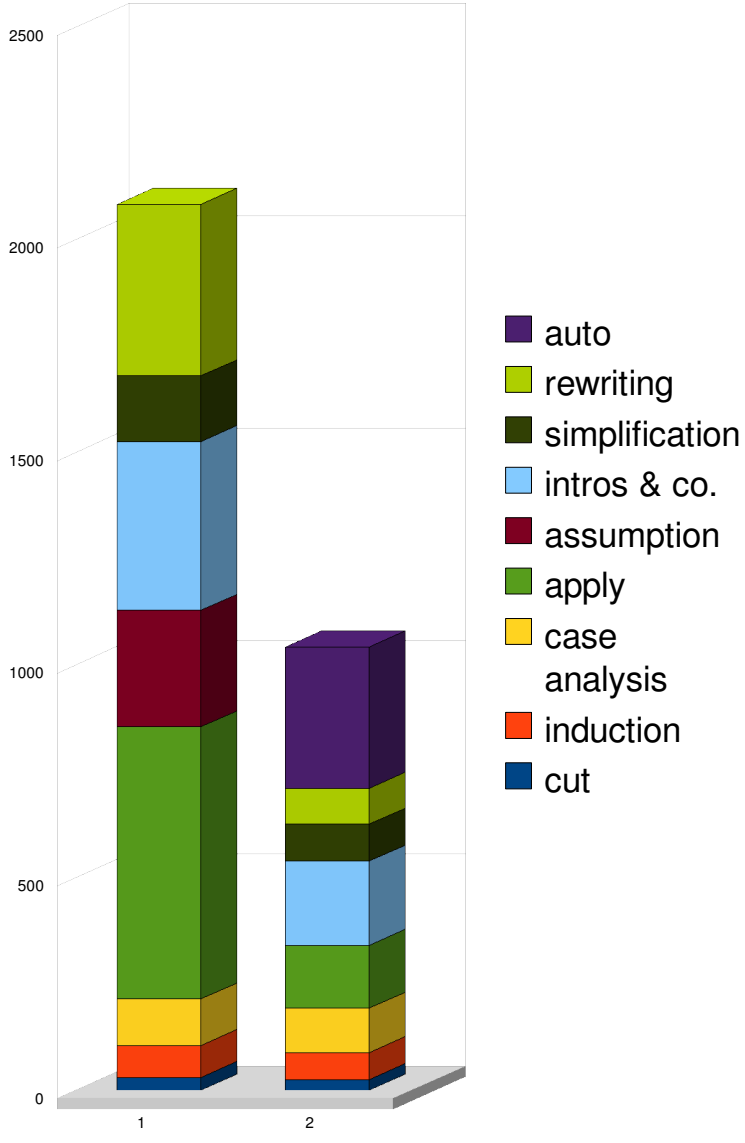
file	Matita 0.5.2		Matita 0.99	
logarithms	413	(20)	223	(21)
square root	217	(13)	221	(19)
binomial coeff.	259	(9)	192	(12)
order of primes	656	(33)	411	(37)
big operators	978	(30)	425	(27)
sigma and pi	526	(26)	188	(9)
factorial	325	(14)	145	(12)
chebyshev's theta	486	(13)	213	(13)
chebishev's psi	294	(11)	143	(13)
factorization	927	(25)	629	(32)
psi bounds	1123	(37)	507	(30)
bertrand (up)	683	(18)	446	(27)
bertrand (down)	526	(22)	240	(19)
total	7413	(271)	3983	(271)

Matita 0.5.2 27 lines per theorem
Matita 0.99.1 15 lines per theorem

Tactic invocations

	Matita 0.5.2		Matita 0.99	
tactic	name	no.	name	no.
application	apply	2203	@	1792
	assumption	779		
rewriting	rewrite	1110	< / >	984
	reflexivity	244		
simplification	simplify	255	normalize	122
			whd	76
introduction	intro/intros	435	#	1904
elimination	cases	306	cases	190
	elim	131	elim	92
			*	62
cut	cut	89	cut	148
automation	auto	10	//	943

Pushing automation



Arithmetics with (2)
and without automation (1)
[Asperti, Sacerdoti Coen '09]

Philosophy

Representing a proof as a set of (possibly annotated, possibly structured) names (the *relevant* facts used in the proof).

Portable!?!

Exploit the interpretative capabilities of systems.
To be tested for scalability (it certainly works for small proofs).

Looking for partners to tets the idea.

Philosophy

Representing a proof as a set of (possibly annotated, possibly structured) names (the *relevant* facts used in the proof).

Portable!?!

Exploit the interpretative capabilities of systems.
To be tested for scalability (it certainly works for small proofs).

Looking for partners to tets the idea.

Matita Bibliography (1)


R. Amadio, A.Asperti, N.Ayache, B. Campbell, D. Mulligan, R. Pollack, Y.Régis-Gianas, C. Sacerdoti Coen, and I. Stark. *Certified complexity*. Procedia CS, 7:175–177, 2011.


A.Asperti, W.Ricciotti. *Formalizing Turing Machines* Wollic'12, LNCS 7456, pp 1–25, 2012.


A.Asperti, W.Ricciotti. *A proof of Bertrand's postulate* Journal of Formalized Reasoning, V.5, n.1, pp.37-57, 2012.


A.Asperti, C.Sacerdoti Coen. *Some Considerations on the Usability of Interactive Provers*. CICM'10, LNCS 6167, pp.147-156, 2010.


A.Asperti, W.Ricciotti, C.Sacerdoti Coen, E.Tassi. *A compact kernel for the Calculus of Inductive Constructions*. Sadhana 34(1):71–144, 2009.


A.Asperti, W.Ricciotti, C.Sacerdoti Coen, E.Tassi. *A new type for tactics*. Technical Report UBLCS-2009-14, University of Bologna, 2009.


A.Asperti, W.Ricciotti, C.Sacerdoti Coen, E.Tassi. *Formal metatheory of programming languages in the Matita interactive theorem prover*. Journal of Automated Reasoning: Special Issue on the Poplmark Challenge. Published online, May 2011.

Matita Bibliography (2)


A.Asperti, W.Ricciotti, C.Sacerdoti Coen, E.Tassi. *The Matita interactive theorem prover*. CADE-2011, Wroclaw, Poland, LNCS 6803, 2011.


A.Asperti, W.Ricciotti, C.Sacerdoti Coen, E.Tassi. *A bi-directional refinement algorithm for the calculus of (co)inductive constructions*. LMCS 8(1), 2012.


C.Sacerdoti Coen, E.Tassi. *A constructive and formal proof of Lebesgue's dominated convergence theorem in the interactive theorem prover Matita.* Journal of Formalized Reasoning, 1:51–89, 2008.


C.Sacerdoti Coen, E.Tassi. *Formalizing Overlap Algebras in Matita*. MSCS 21:1–31, 2011.


C.Sacerdoti Coen, E.Tassi. *Nonuniform Coercions via Unification Hints*. EPTCS 53:16–29, 2011.


C.Sacerdoti Coen, E.Tassi, S.Zacchiroli. *Tinycals: step by step tacticals*. UITP 2006, ENTCS 174, pp.125–142, 2006.


C. Sacerdoti Coen, S. Zacchiroli. *Efficient Ambiguous Parsing of Mathematical Formulae*. MKM 2004, LNCS 3119, pp.347–362, 2004.