Proofs, Security, and Computational Sciences

Jean-Jacques Lévy

December 3, 2010

Trento

msr-inria.inria.fr

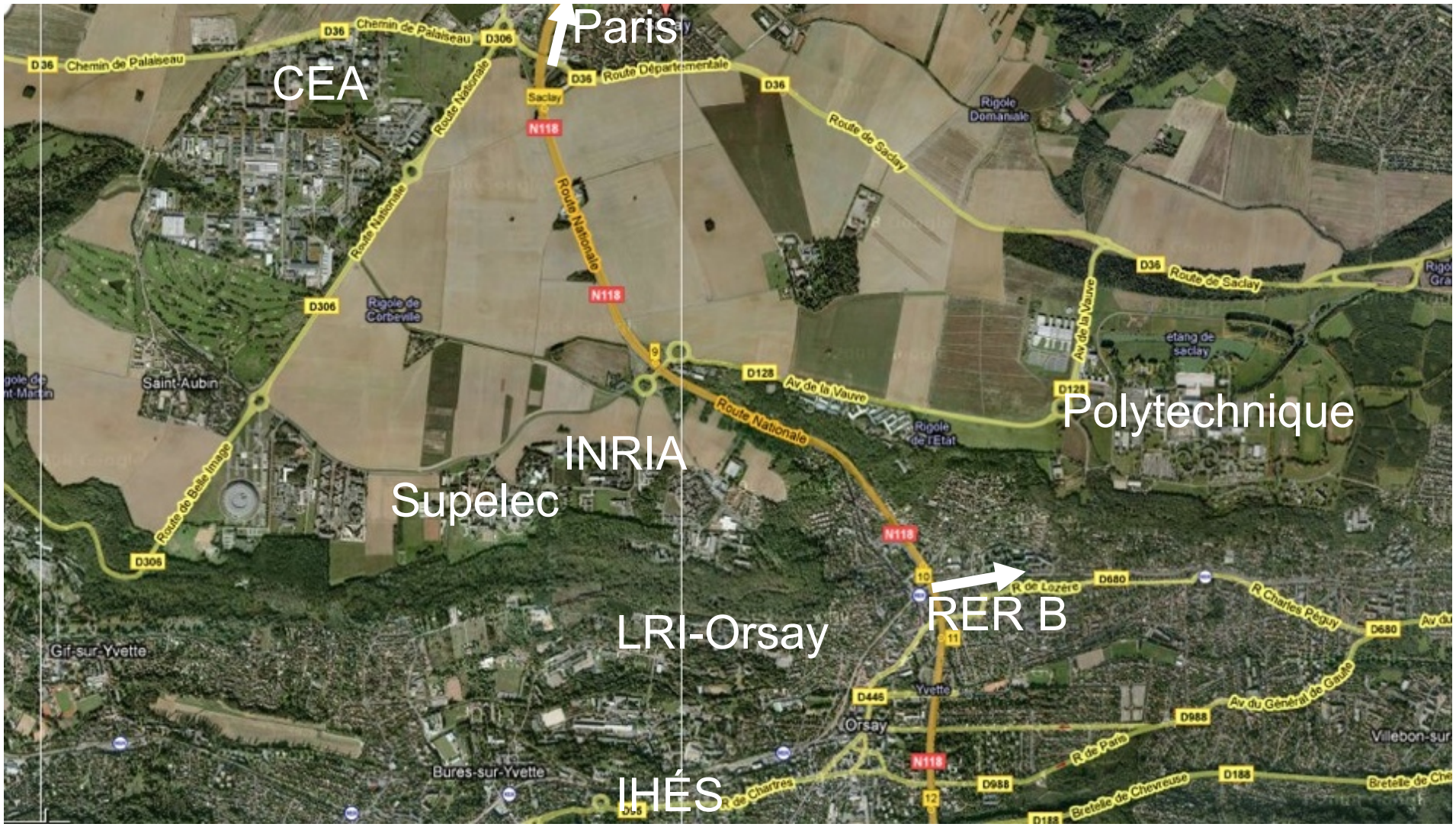
CENTRE DE RECHERCHE COMMUN
INRIA MICROSOFT RESEARCH


Trafic
Extras
Plan
Plateau de Saclay
Paris
Boulogne-Billancourt
Issy-les-Moulineaux
Versailles
Saint-Cloud
Suresnes
Rueil-Malmaison
Nanterre
Courbevoie
Asnières-sur-Seine
Clichy
Saint-Ouen
Aubervilliers
Montreuil
Vincennes
Saint-Maur-des-F
Champigny-sur-Marne
Créteil
Vitry-sur-Seine
Ivry-sur-Seine
Le Kremlin-Bicêtre
Montrouge
Meudon
Clamart
Châtillon
Fontenay-Aux-Roses
Bagneux
Antony
Fresnes
Châtenay-Malabry
Le Plessis-Robinson
Vélizy-Villacoublay
Jouy-en-Josas
Les Loges-en-Josas
Bièvres
Forêt Domaniale de Verrières
Massy
Saclay
Palaiseau
Orsay
Gif-sur-Yvette
Saint-Aubin
Châteaufort
Le Mesnil Blondel
Bures-sur-Yvette
Les Ulis
Villejust
Longjumeau
Champlan
Chilly-Mazarin
Athis-Mons
Montgeron
Crosne
Yerres
Brunoy
Savigny-sur-Orge
Draveil
Villeneuve-Saint-Georges
Limeil-Brévannes
Valenton
Villecresnes
Boissy-Saint-Léger
Bonneuil-sur-Marne
Sucy-en-Brie
Ormesson-sur-Marn
Noisy-le-Gra
Neuilly-sur-Marne
Nogent-sur-Marne
Villiers-sur-Marne
Rosny-sous-Bois
Gagny
Noisy-le-Sec
Villemomble
Bondy
Le Raincy
Clichy
Bobigny
Pantin
Les Lilas
Bagnolet
Fontenay-sous-Bois
Charenton-le-Pont
Maisons-Alfort
Coeuilly
Bellevue
Bois de Boulogne
Sèvres
Ville-d'Avray
Marnes-la-Coquette
Vaucresson
Bailly
La Celle-Saint-Cloud
Bougival
Marly-le-Roi
Croissy-sur-Seine
Le Vésinet
Chatou
Montesson
Carrières-sous-Bois
Viroflay
Chaville
Le Chesnay
Versailles
Buc
Châteaufort
Rungis
Orly
Choisy-le-Roi
Chevilly-Larue
L'Haÿ-les-Roses
Wissous
Draveil
Route Nationale
A86
A14
A3
A4
A6
A10
A6b
N3
N403
N13
N186
N12
N118
N305
N19
N6
N406
E05
E15
E54
A106

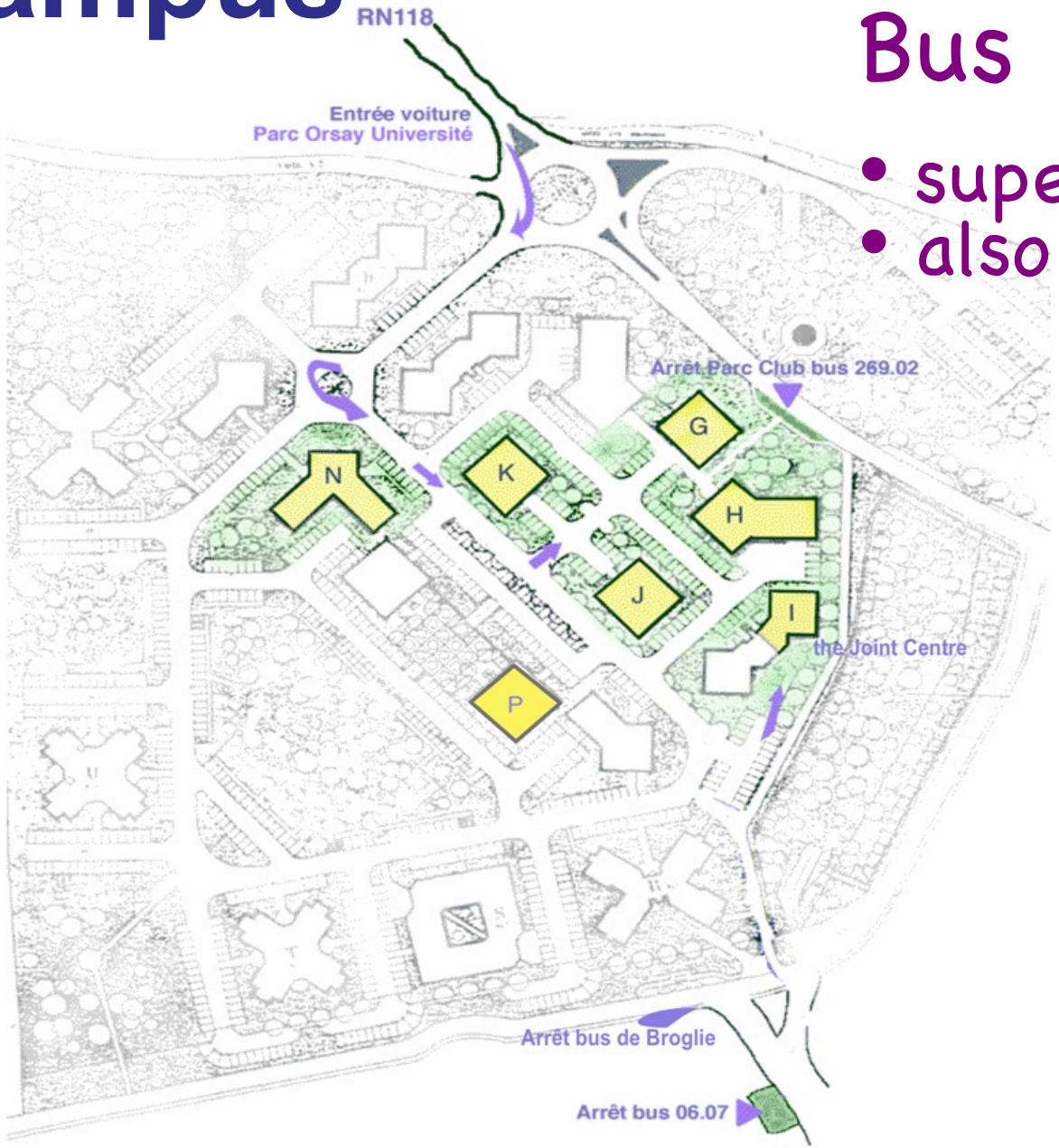
Localization

the plateau de Saclay

= long term investment



Campus



Bus 269-02

- super <= 10am
- also bus 06-07

6mn

Paris >= 30mn

Research

1. Track A
   - Math. Components (see Enrico Tassi's talk)
   - Security
   - TLA+
2. Track B
   - DDMF (see Frédéric Chyzak's talk)
   - ReActivity
   - Adaptative search
   - Image & video mining
   - Action Azure

Track A

Software Security

Trustworthy Computing

CENTRE DE RECHERCHE COMMUN

INRIA
MICROSOFT RESEARCH

Mathematical components

Georges Gonthier, MSRC
Assia Mahboubi, INRIA Saclay/LIX
Y. Bertot, L. Rideau, L. Théry, INRIA Sophia
Iona Pasca, INRIA Sophia

François Garillot, MSR-INRIA (PhD)
Cyril Cohen, ENS Cachan (PhD)
Enrico Tassi, MSR-INRIA (postdoc)
Benjamin Werner, INRIA Saclay/LIX

- **formal proofs** of math theorems with **long proofs**
  - 4 color theorem (3.5 Gonthier-years)
  - Feit-Thompson theorem (3 MathComp-years – under progress)
  - Hales theorem
- **computational** proofs
  - higher-order logic allows programming within it
  - Coq proof-assistant

4-color

Appel-Haken

finite groups

Feit-Thompson

Kepler

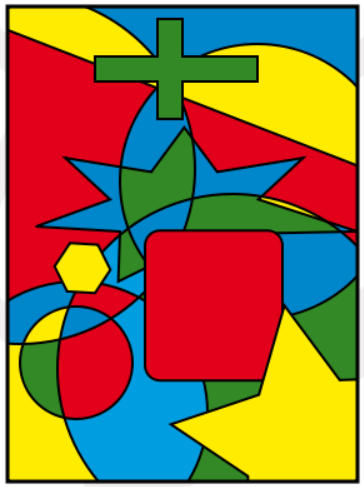
Hales

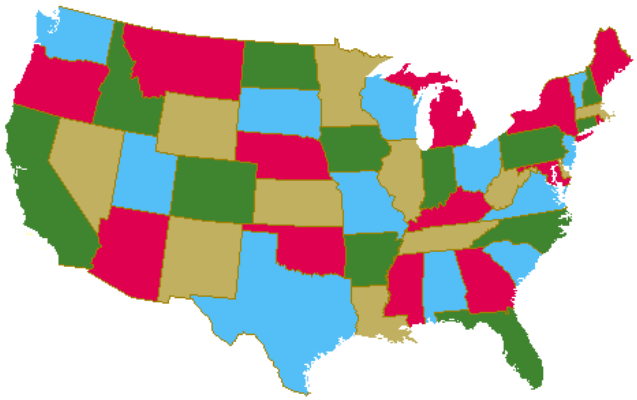
now also Formath EU project (Chalmers, Bologna, etc.)

???

correct

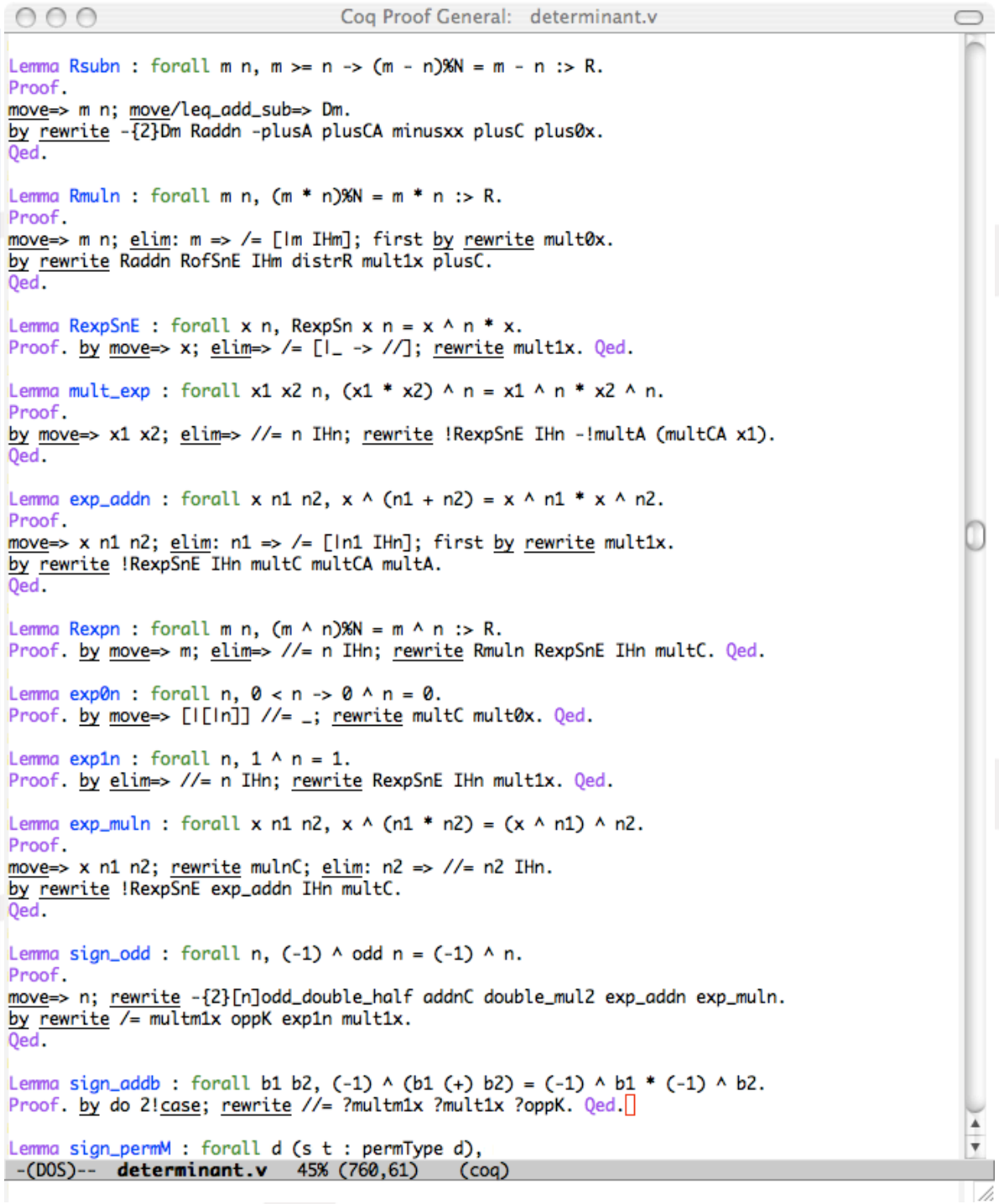
4 colors





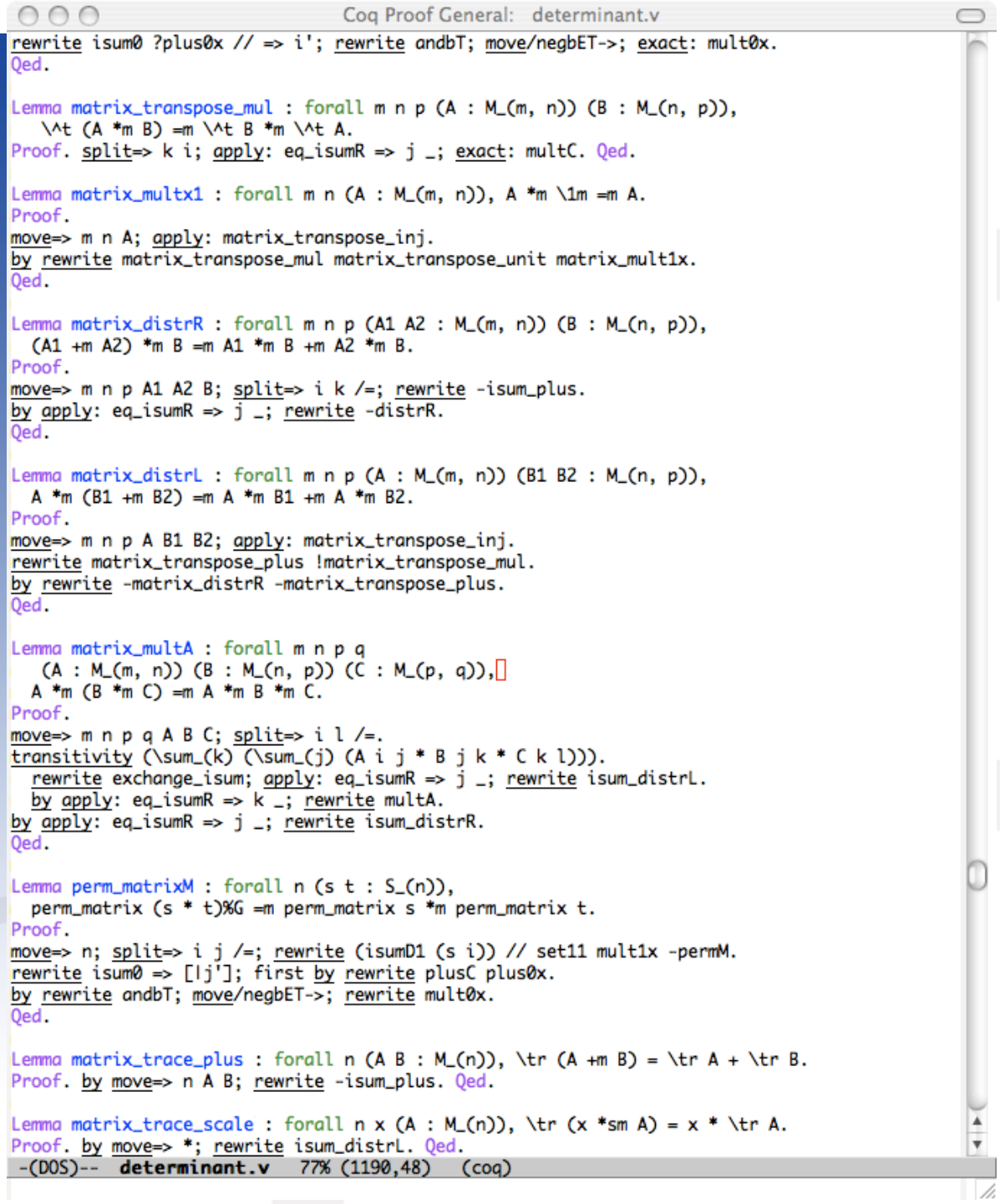
CENTRE DE RECHERCHE COMMUN
INRIA MICROSOFT RESEARCH

```
Section R_props.

(* The ring axioms, and some useful basic corollaries. *)

Hypothesis mult1x : forall x, 1 * x = x.
Hypothesis mult0x : forall x : R, 0 * x = 0.
Hypothesis plus0x : forall x : R, 0 + x = x.
Hypothesis minusxx : forall x : R, x - x = 0.
Hypothesis plusA : forall x1 x2 x3 : R, x1 + (x2 + x3) = x1 + x2 + x3.
Hypothesis plusC : forall x1 x2 : R, x1 + x2 = x2 + x1.
Hypothesis multA : forall x1 x2 x3 : R, x1 * (x2 * x3) = x1 * x2 * x3.
Hypothesis multC : forall x1 x2 : R, x1 * x2 = x2 * x1.
Hypothesis distrR : forall x1 x2 x3 : R, (x1 + x2) * x3 = x1 * x3 + x2 * x3.

Lemma plusCA : forall x1 x2 x3 : R, x1 + (x2 + x3) = x2 + (x1 + x3).
Proof. move=> *; rewrite !plusA; congr (_ + _); exact: plusC. Qed.

Lemma multCA : forall x1 x2 x3 : R, x1 * (x2 * x3) = x2 * (x1 * x3).
Proof. move=> *; rewrite !multA; congr (_ * _); exact: multC. Qed.

Lemma distrL : forall x1 x2 x3 : R, x1 * (x2 + x3) = x1 * x2 + x1 * x3.
Proof. by move=> x1 x2 x3; rewrite !(multC x1) distrR. Qed.

Lemma oppK : involutive opp.
Proof.
by move=> x; rewrite -{2}[x]plus0x -(minusxx (- x)) plusC plusA minusxx plus0x.
Qed.

Lemma multm1x : forall x, -1 * x = -x.
Proof.
move=> x; rewrite -[_ * x]plus0x -(minusxx x) -{1}[x]mult1x plusC plusCA plusA.
by rewrite -distrR minusxx mult0x plus0x.
Qed.
```



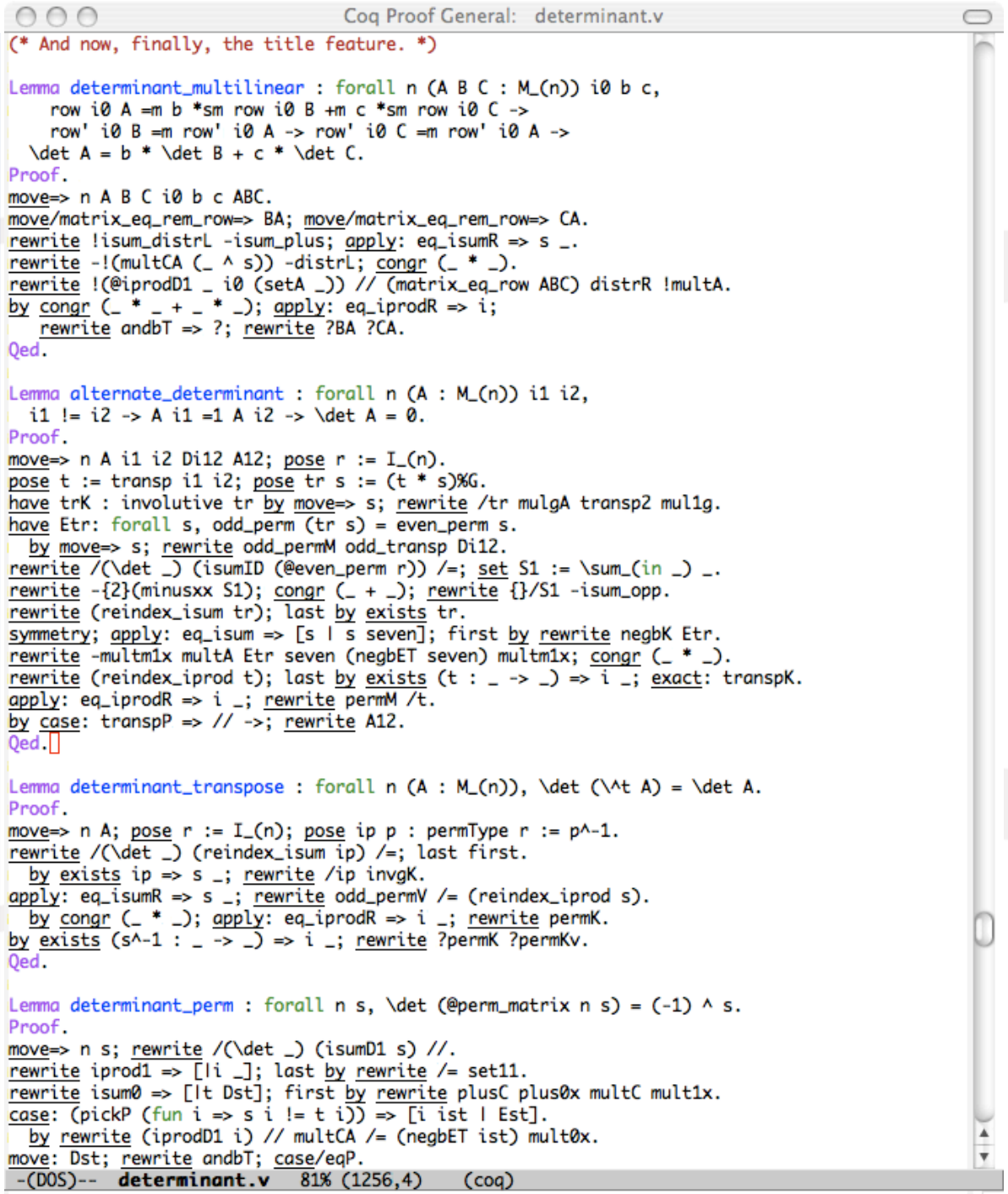
linear algebra

CENTRE DE RECHERCHE COMMUN
INRIA
MICROSOFT RESEARCH



linear algebra

CENTRE DE RECHERCHE COMMUN
INRIA
MICROSOFT RESEARCH



linear algebra

CENTRE DE RECHERCHE COMMUN
INRIA
MICROSOFT RESEARCH

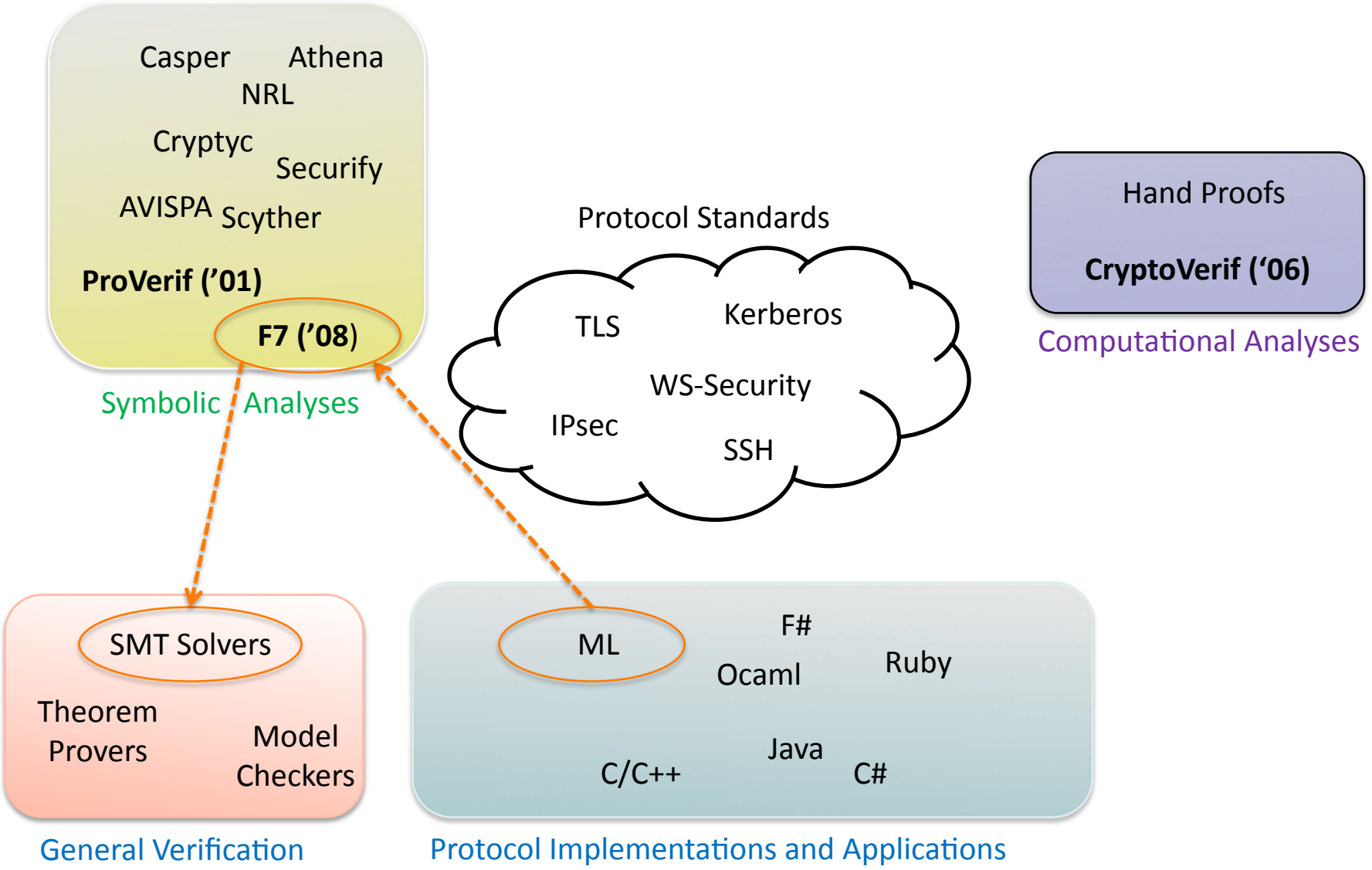
```
Lemma determinant1 : forall n, \det (unit_matrix n) = 1.
Proof.
move=> n; have:= @determinant_perm n 1%G; rewrite odd_perm1 => /= <-.
apply: determinant_extensional; symmetry; exact: perm_matrix1.
Qed.

Lemma determinant_scale : forall n x (A : M_(n)),
  \det (x *sm A) = x ^ n * \det A.
Proof.
move=> n x A; rewrite isum_distrL; apply: eq_isumR => s _.
by rewrite multCA iprod_mult iprod_id card_ordinal.
Qed.

Lemma determinantM : forall n (A B : M_(n)), \det (A *m B) = \det A * \det B.
Proof.
move=> n A B; rewrite isum_distrR.
pose AB (f : F_(n)) (s : S_(n)) i := A i (f i) * B (f i) (s i).
transitivity (\sum_(f) \sum_(s : S_(n)) (-1) ^ s * \prod_(i) AB f s i).
  rewrite exchange_isum; apply: eq_isumR => s _.
  by rewrite -isum_distrL distr_iprodA_isumA.
rewrite (isumID (fun f => uniq (fval f))) plusC isum0 ?plus0x => /= [|f Uf].
  rewrite (reindex_isum (fun s => val (pval s))); last first.
    have s0 : S_(n) := 1%G; pose uf (f : F_(n)) := uniq (fval f).
    pose pf f := if insub uf f is Some s then Perm s else s0.
    exists pf => /= f Uf; rewrite /pf (insubT uf Uf) //; exact: eq_fun_of_perm.
  apply: eq_isum => [s|s _]; rewrite ?(valP (pval s)) // isum_distrL.
  rewrite (reindex_isum (mulg s)); last first.
    by exists (mulg s^-1) => t; rewrite ?mulKgv ?mulKg.
  apply: eq_isumR => t _; rewrite iprod_mult multA multCA multA multCA multA.
```

Secure Distributed Comp.

Cédric Fournet, MSRC
Karthik Bhargavan, INRIA Rocq.
G. Barthe, IMDEA, Bruno Blanchet, INRIA/ENS
B. Grégoire, S. Zanella, INRIA Sophia
James Leifer, INRIA Rocq.
Jean-Jacques Lévy, INRIA Rocq.
Tamara Rezk, INRIA Sophia
Francesco Zappa Nardelli, INRIA Rocq.
Nataliya Guts, MSR-INRIA (PhD)
Jérémy Planul, MSR-INRIA (PhD)

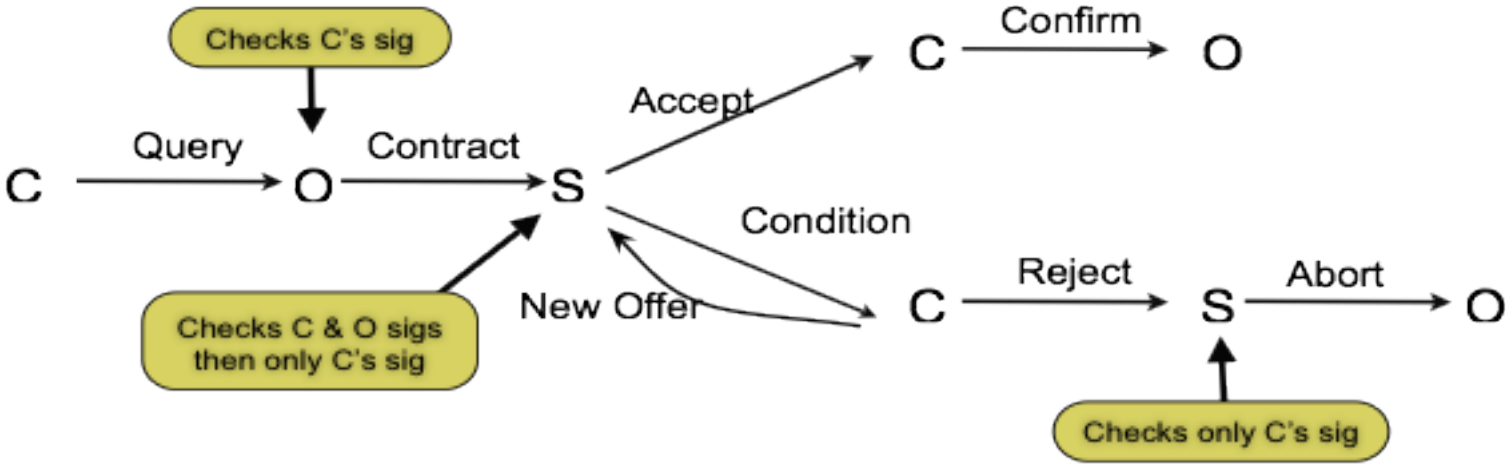
- **programming** with secured communications
- **certified compiler** from high-level primitives to low-level crypto-protocols
- formal proofs of **probabilistic protocols**

Specs, Code, and Formal Tools

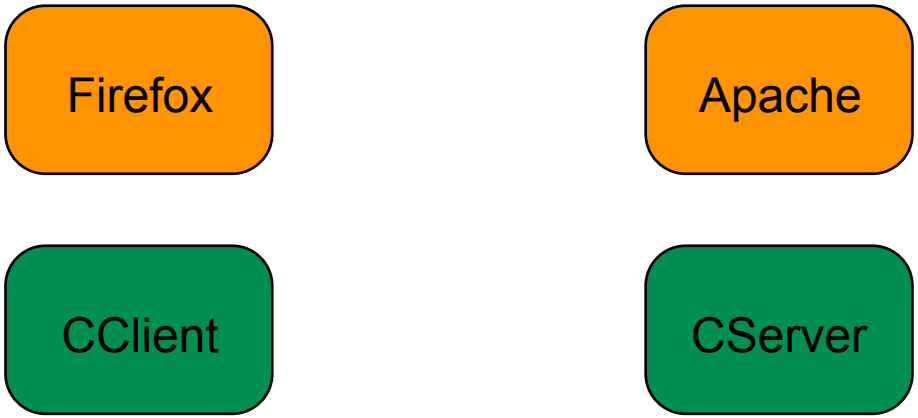


Secure Distributed Comp.

- secure implementations for typed session abstractions (v1 and v2)
- cryptographic enforcement of information-flow security
- secure Audit Logs
- automated verifications of protocol implementations (TLS)
- CertiCrypt: Formal Proofs for Computational Cryptography



Verification of TLS implementation

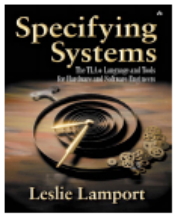


- Firefox + Apache
- certified client CClient + certified server CServer
- Test functional features of Firefox + CServer and CClient + Apache
- Prove security property of CC + CS
- by translation to CryptoVerif [Bruno Blanchet]
- automatic translation from Caml + assertion to CryptoVerif (fs2cv)

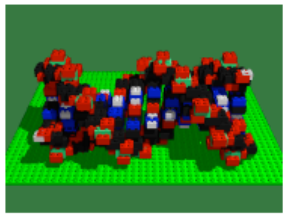
Tools for Formal Proofs

Damien Doligez, INRIA Rocq.
Denis Cousineau, MSR-INRIA (postdoc)
Leslie Lamport, MSRSV
Stephan Merz, INRIA Lorraine

- **Natural proofs**
  - **First-order** temporal logic
  - specification/verification of **concurrent** programs
  - tools for **automatic** theorem proving



TLA+



tools for proofs

Zenon

```
---------------------------- MODULE Peterson6 ----------------------------

Not(i) == IF i = 0 THEN 1 ELSE 0

(*******
--algorithm Peterson {
   variables flag = [i \in {0, 1} |-> FALSE], turn = 0;
   process (proc \in {0,1}) {
     a0: while (TRUE) {
     a1:   flag[self] := TRUE;
     a2:   turn := Not(self);
     a3a:  if (flag[Not(self)]) {goto a3b} else {goto cs} ;
     a3b:  if (turn = Not(self)) {goto a3a} else {goto cs} ;
     cs:   skip;  \* critical section
     a4:   flag[self] := FALSE;
     } \* end while
    } \* end process
  }
********)

AXIOM Arithmetic == 0 # 1

\* BEGIN TRANSLATION
VARIABLES flag, turn, pc

vars == << flag, turn, pc >>

ProcSet == ({0,1})

Init == (* Global variables *)
        /\ flag = [i \in {0, 1} |-> FALSE]
        /\ turn = 0
        /\ pc = [self \in ProcSet |-> CASE self \in {0,1} -> "a0"]

a0(self) == /\ pc[self] = "a0"
            /\ pc' = [pc EXCEPT ![self] = "a1"]
            /\ UNCHANGED << flag, turn >>
```

```
        /\ pc = [self \in ProcSet |-> CASE self \in {0,1} -> "a0"]

a0(self) == /\ pc[self] = "a0"
            /\ pc' = [pc EXCEPT ![self] = "a1"]
            /\ UNCHANGED << flag, turn >>

a1(self) == /\ pc[self] = "a1"
            /\ flag' = [flag EXCEPT ![self] = TRUE]
            /\ pc' = [pc EXCEPT ![self] = "a2"]
            /\ UNCHANGED turn

a2(self) == /\ pc[self] = "a2"
            /\ turn' = Not(self)
            /\ pc' = [pc EXCEPT ![self] = "a3a"]
            /\ UNCHANGED flag

a3a(self) == /\ pc[self] = "a3a"
             /\ IF flag[Not(self)]
                   THEN /\ pc' = [pc EXCEPT ![self] = "a3b"]
                   ELSE /\ pc' = [pc EXCEPT ![self] = "cs"]
             /\ UNCHANGED << flag, turn >>

a3b(self) == /\ pc[self] = "a3b"
             /\ IF turn = Not(self)
                   THEN /\ pc' = [pc EXCEPT ![self] = "a3a"]
                   ELSE /\ pc' = [pc EXCEPT ![self] = "cs"]
             /\ UNCHANGED << flag, turn >>

cs(self) == /\ pc[self] = "cs"
            /\ TRUE
            /\ pc' = [pc EXCEPT ![self] = "a4"]
            /\ UNCHANGED << flag, turn >>

a4(self) == /\ pc[self] = "a4"
            /\ flag' = [flag EXCEPT ![self] = FALSE]
            /\ pc' = [pc EXCEPT ![self] = "a0"]
```

Track B

Computational Sciences

Scientific Information Interaction

CENTRE DE RECHERCHE COMMUN

INRIA
MICROSOFT RESEARCH

Dynamic Dictionary of math. functions

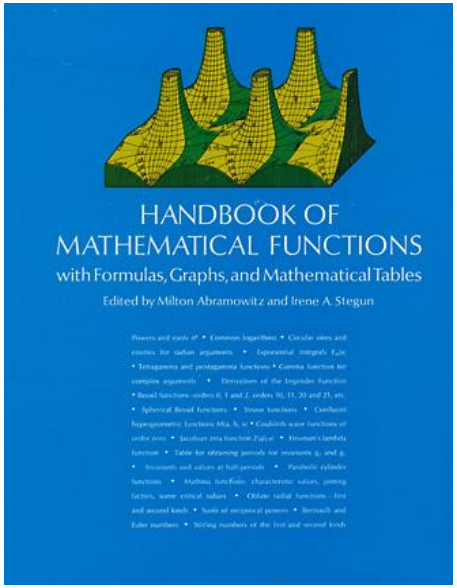
Bruno Salvy, INRIA Rocq.,
Alin Bostan, INRIA Rocq.,
Frédéric Chyzak, INRIA Rocq.

Alexandre Benoit, MSR-INRIA (intern)
Marc Mezzarobba, MSR-INRIA (intern)

Computer Algebra and Web for functions used by engineers

- easy interface
- dynamic tables of their properties
- generation of **programs** to compute them.

Maple 11



9. Bessel Functions of Integer Order

Mathematical Properties

Notation

The tables in this chapter are for Bessel functions of integer order; the text treats general orders. The conventions used are:

$z=x+iy$; x, y real.

n is a positive integer or zero.

ν, μ are unrestricted except where otherwise indicated; ν is supposed real in the sections devoted to Kelvin functions **9.9**, **9.10**, and **9.11**.

The notation used for the Bessel functions is that of Watson [9.15] and the British Association and Royal Society Mathematical Tables. The function $Y_\nu(z)$ is often denoted $N_\nu(z)$ by physicists and European workers.

Other notations are those of:

Aldis, Airey:

$$G_n(z) \text{ for } -\tfrac{1}{2}\pi Y_n(z), K_n(z) \text{ for } (-)^n K_n(z).$$

Clifford:

$$C_n(x) \text{ for } x^{-\frac{1}{2}n} J_n(2\sqrt{x}).$$

Gray, Mathews and MacRobert [9.9]:

$$Y_n(z) \text{ for } \tfrac{1}{2}\pi Y_n(z)+(\ln 2-\gamma)J_n(z),$$

$$\overline{Y}_\nu(z) \text{ for } \pi e^{\nu\pi i}\sec(\nu\pi)Y_\nu(z),$$

$$G_\nu(z) \text{ for } \tfrac{1}{2}\pi i H_\nu^{(1)}(z).$$

Jahnke, Emde and Lösch [9.32]:

$$\Lambda_\nu(z) \text{ for } \Gamma(\nu+1)(\tfrac{1}{2}z)^{-\nu}J_\nu(z).$$

Jeffreys:

$$Hs_\nu(z) \text{ for } H_\nu^{(1)}(z),\ Hi_\nu(z) \text{ for } H_\nu^{(2)}(z),$$

$$Kh_\nu(z) \text{ for } (2/\pi)K_\nu(z).$$

Heine:

$$K_n(z) \text{ for } -\tfrac{1}{2}\pi Y_n(z).$$

Neumann:

$$Y^n(z) \text{ for } \tfrac{1}{2}\pi Y_n(z)+(\ln 2-\gamma)J_n(z).$$

Whittaker and Watson [9.18]:

$$K_\nu(z) \text{ for } \cos(\nu\pi)K_\nu(z).$$

Bessel Functions J and Y

9.1. Definitions and Elementary Properties

Differential Equation

9.1.1 $$z^2\frac{d^2w}{dz^2}+z\frac{dw}{dz}+(z^2-\nu^2)w=0$$

Solutions are the Bessel functions of the first kind $J_{\pm\nu}(z)$, of the second kind $Y_\nu(z)$ (also called Weber's function) and of the third kind $H_\nu^{(1)}(z)$, $H_\nu^{(2)}(z)$ (also called the Hankel functions). Each is a regular (holomorphic) function of z throughout the z-plane cut along the negative real axis, and for fixed $z(\neq 0)$ each is an entire (integral) function of ν. When $\nu=\pm n$, $J_\nu(z)$ has no branch point and is an entire (integral) function of z.

Important features of the various solutions are as follows: $J_\nu(z)(\mathscr{R}\nu\geq 0)$ is bounded as $z\to 0$ in any bounded range of arg z. $J_\nu(z)$ and $J_{-\nu}(z)$ are linearly independent except when ν is an integer. $J_\nu(z)$ and $Y_\nu(z)$ are linearly independent for all values of ν.

$H_\nu^{(1)}(z)$ tends to zero as $|z|\to\infty$ in the sector $0<\arg z<\pi$; $H_\nu^{(2)}(z)$ tends to zero as $|z|\to\infty$ in the sector $-\pi<\arg z<0$. For all values of ν, $H_\nu^{(1)}(z)$ and $H_\nu^{(2)}(z)$ are linearly independent.

Relations Between Solutions

9.1.2 $$Y_\nu(z)=\frac{J_\nu(z)\cos(\nu\pi)-J_{-\nu}(z)}{\sin(\nu\pi)}$$

The right of this equation is replaced by its limiting value if ν is an integer or zero.

9.1.3

$$H_\nu^{(1)}(z)=J_\nu(z)+iY_\nu(z)$$
$$=i\csc(\nu\pi)\{e^{-\nu\pi i}J_\nu(z)-J_{-\nu}(z)\}$$

9.1.4

$$H_\nu^{(2)}(z)=J_\nu(z)-iY_\nu(z)$$
$$=i\csc(\nu\pi)\{J_{-\nu}(z)-e^{\nu\pi i}J_\nu(z)\}$$

9.1.5 $$J_{-n}(z)=(-)^n J_n(z) \qquad Y_{-n}(z)=(-)^n Y_n(z)$$

9.1.6 $$H_{-\nu}^{(1)}(z)=e^{\nu\pi i}H_\nu^{(1)}(z) \qquad H_{-\nu}^{(2)}(z)=e^{-\nu\pi i}H_\nu^{(2)}(z)$$

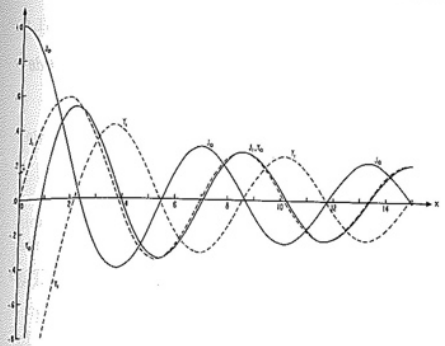


FIGURE 9.1. $J_0(x)$, $Y_0(x)$, $J_1(x)$, $Y_1(x)$.

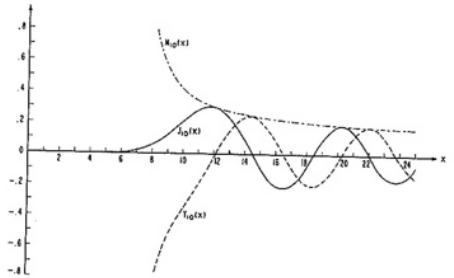


FIGURE 9.2. $J_{10}(x)$, $Y_{10}(x)$, *and* $M_{10}(x)=\sqrt{J_{10}^2(x)+Y_{10}^2(x)}$.

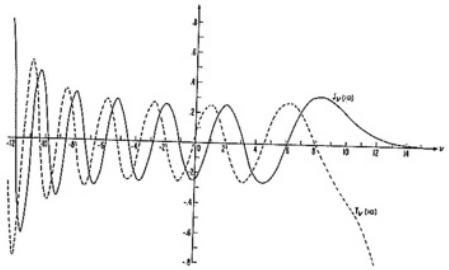


FIGURE 9.3. $J_\nu(10)$ *and* $Y_\nu(10)$.

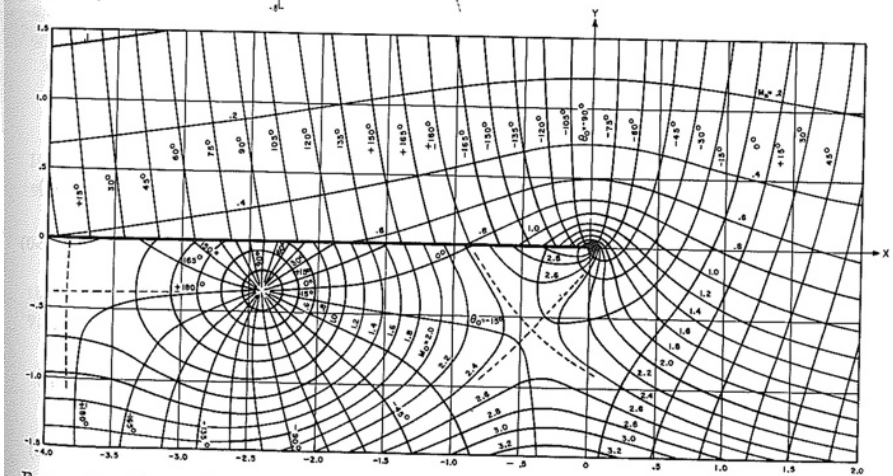


FIGURE 9.4. *Contour lines of the modulus and phase of the Hankel Function* $H_0^{(1)}(x+iy)=M_0e^{i\theta_0}$. From E. Jahnke, F. Emde, and F. Lösch, Tables of higher functions, McGraw-Hill Book Co., Inc., New York, N.Y., 1960 (with permission).

Limiting Forms for Small Arguments

When ν is fixed and $z \to 0$

9.1.7

$$J_\nu(z) \sim (\tfrac{1}{2}z)^\nu/\Gamma(\nu+1) \qquad (\nu \neq -1, -2, -3, \ldots)$$

9.1.8

$$Y_0(z) \sim -iH_0^{(1)}(z) \sim iH_0^{(2)}(z) \sim (2/\pi)\ln z$$

9.1.9

$$Y_\nu(z) \sim -iH_\nu^{(1)}(z) \sim iH_\nu^{(2)}(z) \sim -(1/\pi)\Gamma(\nu)(\tfrac{1}{2}z)^{-\nu} \qquad (\Re\nu > 0)$$

Ascending Series

9.1.10

$$J_\nu(z) = (\tfrac{1}{2}z)^\nu \sum_{k=0}^{\infty} \frac{(-\frac{1}{4}z^2)^k}{k!\,\Gamma(\nu+k+1)}$$

9.1.11

$$Y_n(z) = -\frac{(\frac{1}{2}z)^{-n}}{\pi}\sum_{k=0}^{n-1}\frac{(n-k-1)!}{k!}(\tfrac{1}{4}z^2)^k + \frac{2}{\pi}\ln(\tfrac{1}{2}z)J_n(z) - \frac{(\frac{1}{2}z)^n}{\pi}\sum_{k=0}^{\infty}\{\psi(k+1)+\psi(n+k+1)\}\frac{(-\frac{1}{4}z^2)^k}{k!\,(n+k)!}$$

where $\psi(n)$ is given by **6.3.2.**

9.1.12

$$J_0(z) = 1 - \frac{\frac{1}{4}z^2}{(1!)^2} + \frac{(\frac{1}{4}z^2)^2}{(2!)^2} - \frac{(\frac{1}{4}z^2)^3}{(3!)^2} + \ldots$$

9.1.13

$$Y_0(z) = \frac{2}{\pi}\{\ln(\tfrac{1}{2}z)+\gamma\}J_0(z) + \frac{2}{\pi}\{\frac{\frac{1}{4}z^2}{(1!)^2} - (1+\tfrac{1}{2})\frac{(\frac{1}{4}z^2)^2}{(2!)^2} + (1+\tfrac{1}{2}+\tfrac{1}{3})\frac{(\frac{1}{4}z^2)^3}{(3!)^2} - \ldots\}$$

9.1.14

$$J_\nu(z)J_\mu(z) = (\tfrac{1}{2}z)^{\nu+\mu}\sum_{k=0}^{\infty}\frac{(-)^k\Gamma(\nu+\mu+2k+1)(\frac{1}{4}z^2)^k}{\Gamma(\nu+k+1)\Gamma(\mu+k+1)\Gamma(\nu+\mu+k+1)\,k!}$$

Wronskians

9.1.15

$$W\{J_\nu(z), J_{-\nu}(z)\} = J_{\nu+1}(z)J_{-\nu}(z) + J_\nu(z)J_{-(\nu+1)}(z) = -2\sin(\nu\pi)/(\pi z)$$

9.1.16

$$W\{J_\nu(z), Y_\nu(z)\} = J_{\nu+1}(z)Y_\nu(z) - J_\nu(z)Y_{\nu+1}(z) = 2/(\pi z)$$

9.1.17

$$W\{H_\nu^{(1)}(z), H_\nu^{(2)}(z)\} = H_{\nu+1}^{(1)}(z)H_\nu^{(2)}(z) - H_\nu^{(1)}(z)H_{\nu+1}^{(2)}(z) = -4i/(\pi z)$$

Integral Representations

9.1.18

$$J_0(z) = \frac{1}{\pi}\int_0^\pi \cos(z\sin\theta)\,d\theta = \frac{1}{\pi}\int_0^\pi \cos(z\cos\theta)\,d\theta$$

9.1.19

$$Y_0(z) = \frac{4}{\pi^2}\int_0^{\frac{1}{2}\pi}\cos(z\cos\theta)\{\gamma + \ln(2z\sin^2\theta)\}\,d\theta$$

9.1.20

$$J_\nu(z) = \frac{(\frac{1}{2}z)^\nu}{\pi^{\frac{1}{2}}\Gamma(\nu+\frac{1}{2})}\int_0^\pi \cos(z\cos\theta)\sin^{2\nu}\theta\,d\theta = \frac{2(\frac{1}{2}z)^\nu}{\pi^{\frac{1}{2}}\Gamma(\nu+\frac{1}{2})}\int_0^1 (1-t^2)^{\nu-\frac{1}{2}}\cos(zt)\,dt \quad (\Re\nu > -\tfrac{1}{2})$$

9.1.21

$$J_n(z) = \frac{1}{\pi}\int_0^\pi \cos(z\sin\theta - n\theta)\,d\theta = \frac{i^{-n}}{\pi}\int_0^\pi e^{iz\cos\theta}\cos(n\theta)\,d\theta$$

9.1.22

$$J_\nu(z) = \frac{1}{\pi}\int_0^\pi \cos(z\sin\theta - \nu\theta)\,d\theta - \frac{\sin(\nu\pi)}{\pi}\int_0^\infty e^{-z\sinh t - \nu t}\,dt \quad (|\arg z| < \tfrac{1}{2}\pi)$$

$$Y_\nu(z) = \frac{1}{\pi}\int_0^\pi \sin(z\sin\theta - \nu\theta)\,d\theta - \frac{1}{\pi}\int_0^\infty \{e^{\nu t} + e^{-\nu t}\cos(\nu\pi)\}e^{-z\sinh t}\,dt \quad (|\arg z| < \tfrac{1}{2}\pi)$$

9.1.23

$$J_0(x) = \frac{2}{\pi}\int_0^\infty \sin(x\cosh t)\,dt \quad (x>0)$$

$$Y_0(x) = -\frac{2}{\pi}\int_0^\infty \cos(x\cosh t)\,dt \quad (x>0)$$

9.1.24

$$J_\nu(x) = \frac{2(\frac{1}{2}x)^{-\nu}}{\pi^{\frac{1}{2}}\Gamma(\frac{1}{2}-\nu)}\int_1^\infty \frac{\sin(xt)\,dt}{(t^2-1)^{\nu+\frac{1}{2}}} \quad (|\Re\nu| < \tfrac{1}{2}, x>0)$$

$$Y_\nu(x) = -\frac{2(\frac{1}{2}x)^{-\nu}}{\pi^{\frac{1}{2}}\Gamma(\frac{1}{2}-\nu)}\int_1^\infty \frac{\cos(xt)\,dt}{(t^2-1)^{\nu+\frac{1}{2}}} \quad (|\Re\nu| < \tfrac{1}{2}, x>0)$$

9.1.25

$$H_\nu^{(1)}(z) = \frac{1}{\pi i}\int_{-\infty}^{\infty+\pi i} e^{z\sinh t - \nu t}\,dt \quad (|\arg z| < \tfrac{1}{2}\pi)$$

$$H_\nu^{(2)}(z) = -\frac{1}{\pi i}\int_{-\infty}^{\infty-\pi i} e^{z\sinh t - \nu t}\,dt \quad (|\arg z| < \tfrac{1}{2}\pi)$$

9.1.26

$$J_\nu(x) = \frac{1}{2\pi i}\int_{-i\infty}^{i\infty}\frac{\Gamma(-t)(\frac{1}{2}x)^{\nu+2t}}{\Gamma(\nu+t+1)}\,dt \quad (\Re\nu > 0, x>0)$$

In the last integral the path of integration must lie to the left of the points $t = 0, 1, 2, \ldots$.

Recurrence Relations

9.1.27

$$\mathscr{C}_{\nu-1}(z) + \mathscr{C}_{\nu+1}(z) = \frac{2\nu}{z}\mathscr{C}_\nu(z)$$

$$\mathscr{C}_{\nu-1}(z) - \mathscr{C}_{\nu+1}(z) = 2\mathscr{C}_\nu'(z)$$

$$\mathscr{C}_\nu'(z) = \mathscr{C}_{\nu-1}(z) - \frac{\nu}{z}\mathscr{C}_\nu(z)$$

$$\mathscr{C}_\nu'(z) = -\mathscr{C}_{\nu+1}(z) + \frac{\nu}{z}\mathscr{C}_\nu(z)$$

$\mathscr{C}$ denotes $J, Y, H^{(1)}, H^{(2)}$ or any linear combination of these functions, the coefficients in which are independent of z and ν.

9.1.28

$$J_0'(z) = -J_1(z) \qquad Y_0'(z) = -Y_1(z)$$

If $f_\nu(z) = z^p\mathscr{C}_\nu(\lambda z^q)$ where p, q, λ are independent of ν, then

9.1.29

$$f_{\nu-1}(z) + f_{\nu+1}(z) = (2\nu/\lambda)z^{-q}f_\nu(z)$$

$$(p+\nu q)f_{\nu-1}(z) + (p-\nu q)f_{\nu+1}(z) = (2\nu/\lambda)z^{1-q}f_\nu'(z)$$

$$zf_\nu'(z) = \lambda q z^q f_{\nu-1}(z) + (p-\nu q)f_\nu(z)$$

$$zf_\nu'(z) = -\lambda q z^q f_{\nu+1}(z) + (p+\nu q)f_\nu(z)$$

Formulas for Derivatives

9.1.30

$$\left(\frac{1}{z}\frac{d}{dz}\right)^k\{z^\nu\mathscr{C}_\nu(z)\} = z^{\nu-k}\mathscr{C}_{\nu-k}(z)$$

$$\left(\frac{1}{z}\frac{d}{dz}\right)^k\{z^{-\nu}\mathscr{C}_\nu(z)\} = (-)^k z^{-\nu-k}\mathscr{C}_{\nu+k}(z) \qquad (k=0,1,2,\ldots)$$

9.1.31

$$\mathscr{C}_\nu^{(k)}(z) = \frac{1}{2^k}\{\mathscr{C}_{\nu-k}(z) - \binom{k}{1}\mathscr{C}_{\nu-k+2}(z) + \binom{k}{2}\mathscr{C}_{\nu-k+4}(z) - \ldots + (-)^k\mathscr{C}_{\nu+k}(z)\} \qquad (k=0,1,2,\ldots)$$

Recurrence Relations for Cross-Products

If

9.1.32

$$p_\nu = J_\nu(a)Y_\nu(b) - J_\nu(b)Y_\nu(a)$$
$$q_\nu = J_\nu(a)Y_\nu'(b) - J_\nu'(b)Y_\nu(a)$$
$$r_\nu = J_\nu'(a)Y_\nu(b) - J_\nu(b)Y_\nu'(a)$$
$$s_\nu = J_\nu'(a)Y_\nu'(b) - J_\nu'(b)Y_\nu'(a)$$

then

9.1.33

$$p_{\nu+1} - p_{\nu-1} = -\frac{2\nu}{a}q_\nu - \frac{2\nu}{b}r_\nu$$

$$q_{\nu+1} + r_\nu = \frac{\nu}{a}p_\nu - \frac{\nu+1}{b}p_{\nu+1}$$

$$r_{\nu+1} + q_\nu = \frac{\nu}{b}p_\nu - \frac{\nu+1}{a}p_{\nu+1}$$

$$s_\nu = \frac{1}{2}p_{\nu+1} + \frac{1}{2}p_{\nu-1} - \frac{\nu^2}{ab}p_\nu$$

and

9.1.34

$$p_\nu s_\nu - q_\nu r_\nu = \frac{4}{\pi^2 ab}$$

Analytic Continuation

In **9.1.35** to **9.1.38**, m is an integer.

9.1.35

$$J_\nu(ze^{m\pi i}) = e^{m\nu\pi i}J_\nu(z)$$

9.1.36

$$Y_\nu(ze^{m\pi i}) = e^{-m\nu\pi i}Y_\nu(z) + 2i\sin(m\nu\pi)\cot(\nu\pi)J_\nu(z)$$

9.1.37

$$\sin(\nu\pi)H_\nu^{(1)}(ze^{m\pi i}) = -\sin\{(m-1)\nu\pi\}H_\nu^{(1)}(z) - e^{-\nu\pi i}\sin(m\nu\pi)H_\nu^{(2)}(z)$$

9.1.38

$$\sin(\nu\pi)H_\nu^{(2)}(ze^{m\pi i}) = \sin\{(m+1)\nu\pi\}H_\nu^{(2)}(z) + e^{\nu\pi i}\sin(m\nu\pi)H_\nu^{(1)}(z)$$

9.1.39

$$H_\nu^{(1)}(ze^{\pi i}) = -e^{-\nu\pi i}H_\nu^{(2)}(z)$$
$$H_\nu^{(2)}(ze^{-\pi i}) = -e^{\nu\pi i}H_\nu^{(1)}(z)$$

9.1.40

$$J_\nu(\bar{z}) = \overline{J_\nu(z)} \qquad Y_\nu(\bar{z}) = \overline{Y_\nu(z)}$$

$$H_\nu^{(1)}(\bar{z}) = \overline{H_\nu^{(2)}(z)} \qquad H_\nu^{(2)}(\bar{z}) = \overline{H_\nu^{(1)}(z)} \qquad (\nu \text{ real})$$

Generating Function and Associated Series

9.1.41

$$e^{\frac{1}{2}z(t-1/t)} = \sum_{k=-\infty}^{\infty} t^k J_k(z) \qquad (t \neq 0)$$

9.1.42

$$\cos(z\sin\theta) = J_0(z) + 2\sum_{k=1}^{\infty} J_{2k}(z)\cos(2k\theta)$$

9.1.43

$$\sin(z\sin\theta) = 2\sum_{k=0}^{\infty} J_{2k+1}(z)\sin\{(2k+1)\theta\}$$

9.1.44

$$\cos(z\cos\theta) = J_0(z) + 2\sum_{k=1}^{\infty}(-)^k J_{2k}(z)\cos(2k\theta)$$

9.1.45

$$\sin(z\cos\theta) = 2\sum_{k=0}^{\infty}(-)^k J_{2k+1}(z)\cos\{(2k+1)\theta\}$$

9.1.46

$$1 = J_0(z) + 2J_2(z) + 2J_4(z) + 2J_6(z) + \ldots$$

9.1.47

$$\cos z = J_0(z) - 2J_2(z) + 2J_4(z) - 2J_6(z) + \ldots$$

9.1.48

$$\sin z = 2J_1(z) - 2J_3(z) + 2J_5(z) - \ldots$$

9.1.72

$$\lim_{\nu\to\infty}\{\nu^{\mu}Q_{\nu}^{-\mu}\left(\cos\frac{x}{\nu}\right)\}=-\tfrac{1}{2}\pi Y_{\mu}(x) \qquad (x>0)$$

For $P_{\nu}^{-\mu}$ and $Q_{\nu}^{-\mu}$, see chapter **8.**

Continued Fractions

9.1.73

$$\frac{J_{\nu}(z)}{J_{\nu-1}(z)}=\cfrac{1}{2\nu z^{-1}-\cfrac{1}{2(\nu+1)z^{-1}-\cfrac{1}{2(\nu+2)z^{-1}-\cdots}}}$$

$$=\cfrac{\frac{1}{2}z/\nu}{1-\cfrac{\frac{1}{4}z^2/\{\nu(\nu+1)\}}{1-\cfrac{\frac{1}{4}z^2/\{(\nu+1)(\nu+2)\}}{1-\cdots}}}$$

Multiplication Theorem

9.1.74

$$\mathscr{C}_{\nu}(\lambda z)=\lambda^{\pm\nu}\sum_{k=0}^{\infty}\frac{(\mp)^k(\lambda^2-1)^k(\frac{1}{2}z)^k}{k!}\mathscr{C}_{\nu\pm k}(z) \qquad (|\lambda^2-1|<1)$$

If $\mathscr{C}=J$ and the upper signs are taken, the restriction on λ is unnecessary.

This theorem will furnish expansions of $\mathscr{C}_{\nu}(re^{i\theta})$ in terms of $\mathscr{C}_{\nu\pm k}(r)$.

Addition Theorems

Neumann's

9.1.75 $$\mathscr{C}_{\nu}(u\pm v)=\sum_{k=-\infty}^{\infty}\mathscr{C}_{\nu\mp k}(u)J_k(v) \qquad (|v|<|u|)$$

The restriction $|v|<|u|$ is unnecessary when $\mathscr{C}=J$ and ν is an integer or zero. Special cases are

9.1.76 $$1=J_0^2(z)+2\sum_{k=1}^{\infty}J_k^2(z)$$

9.1.77

$$0=\sum_{k=0}^{2n}(-)^kJ_k(z)J_{2n-k}(z)+2\sum_{k=1}^{\infty}J_k(z)J_{2n+k}(z) \quad (n\geq 1)$$

9.1.78

$$J_n(2z)=\sum_{k=0}^{n}J_k(z)J_{n-k}(z)+2\sum_{k=1}^{\infty}(-)^kJ_k(z)J_{n+k}(z)$$

Graf's

9.1.79

$$\mathscr{C}_{\nu}(w)\begin{matrix}\cos\\ \sin\end{matrix}\nu\chi=\sum_{k=-\infty}^{\infty}\mathscr{C}_{\nu+k}(u)J_k(v)\begin{matrix}\cos\\ \sin\end{matrix}k\alpha \qquad (|ve^{\pm i\alpha}|<|u|)$$

Gegenbauer's

9.1.80

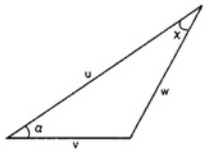
$$\frac{\mathscr{C}_{\nu}(w)}{w^{\nu}}=2^{\nu}\Gamma(\nu)\sum_{k=0}^{\infty}(\nu+k)\frac{\mathscr{C}_{\nu+k}(u)}{u^{\nu}}\frac{J_{\nu+k}(v)}{v^{\nu}}C_k^{(\nu)}(\cos\alpha)$$
$$(\nu\neq 0,-1,\ldots,|ve^{\pm i\alpha}|<|u|)$$

In **9.1.79** and **9.1.80,**

$w=\sqrt{(u^2+v^2-2uv\cos\alpha)}$,

$$u-v\cos\alpha=w\cos\chi,\quad v\sin\alpha=w\sin\chi$$

the branches being chosen so that $w\to u$ and $\chi\to 0$ as $v\to 0$. $C_k^{(\nu)}(\cos\alpha)$ is Gegenbauer's polynomial (see chapter **22**).



Gegenbauer's addition theorem.

If u, v are real and positive and $0\leq\alpha\leq\pi$, then w, χ are real and non-negative, and the geometrical relationship of the variables is shown in the diagram.

The restrictions $|ve^{\pm i\alpha}|<|u|$ are unnecessary in **9.1.79** when $\mathscr{C}=J$ and ν is an integer or zero, and in **9.1.80** when $\mathscr{C}=J$.

Degenerate Form ($u=\infty$):

9.1.81

$$e^{iz\cos\alpha}=\Gamma(\nu)(\tfrac{1}{2}v)^{-\nu}\sum_{k=0}^{\infty}(\nu+k)i^kJ_{\nu+k}(v)C_k^{(\nu)}(\cos\alpha)$$
$$(\nu\neq 0,-1,\ldots)$$

Neumann's Expansion of an Arbitrary Function in a Series of Bessel Functions

9.1.82 $$f(z)=a_0J_0(z)+2\sum_{k=1}^{\infty}a_kJ_k(z) \qquad (|z|<c)$$

where c is the distance of the nearest singularity of $f(z)$ from $z=0$,

9.1.83 $$a_k=\frac{1}{2\pi i}\int_{|z|=c'}f(t)O_k(t)dt \qquad (0<c'<c)$$

and $O_k(t)$ is Neumann's polynomial. The latter is defined by the generating function

9.1.84

$$\frac{1}{t-z}=J_0(z)O_0(t)+2\sum_{k=1}^{\infty}J_k(z)O_k(t) \qquad (|z|<|t|)$$

$O_n(t)$ is a polynomial of degree $n+1$ in $1/t$; $O_0(t)=1/t$,

9.1.85

$$O_n(t)=\frac{1}{4}\sum_{k=0}^{\leq\frac{1}{2}n}\frac{n(n-k-1)!}{k!}\left(\frac{2}{t}\right)^{n-2k+1} \qquad (n=1,2,\ldots)$$

The more general form of expansion

9.1.86 $$f(z)=a_0J_{\nu}(z)+2\sum_{k=1}^{\infty}a_kJ_{\nu+k}(z)$$

	$f(s)$			$F(t)$
29.3.126	$e^{as}E_1(as)$	$(a>0)$	5	$\frac{1}{t+a}$
29.3.127	$\frac{1}{a}-se^{as}E_1(as)$	$(a>0)$	5	$\frac{1}{(t+a)^2}$
29.3.128	$a^{1-n}e^{as}E_n(as)$	$(a>0;n=0,1,2,\ldots)$	5	$\frac{1}{(t+a)^n}$
29.3.129	$\left[\frac{\pi}{2}-\mathrm{Si}(s)\right]\cos s+\mathrm{Ci}(s)\sin s$		5	$\frac{1}{t^2+1}$

29.4. Table of Laplace-Stieltjes Transforms [4]

	$\phi(s)$		$\Phi(t)$
29.4.1	$\int_0^{\infty}e^{-st}d\Phi(t)$		$\Phi(t)$
29.4.2	e^{-ks}	$(k>0)$	$u(t-k)$
29.4.3	$\frac{1}{1-e^{-ks}}$	$(k>0)$	$\sum_{n=0}^{\infty}u(t-nk)$
29.4.4	$\frac{1}{1+e^{-ks}}$	$(k>0)$	$\sum_{n=0}^{\infty}(-1)^nu(t-nk)$
29.4.5	$\frac{1}{\sinh ks}$	$(k>0)$	$2\sum_{n=0}^{\infty}u[t-(2n+1)k]$
29.4.6	$\frac{1}{\cosh ks}$	$(k>0)$	$2\sum_{n=0}^{\infty}(-1)^nu[t-(2n+1)k]$
29.4.7	$\tanh ks$	$(k>0)$	$u(t)+2\sum_{n=1}^{\infty}(-1)^nu(t-2nk)$
29.4.8	$\frac{1}{\sinh(ks+a)}$	$(k>0)$	$2\sum_{n=0}^{\infty}e^{-(2n+1)a}u[t-(2n+1)k]$
29.4.9	$\frac{e^{-hs}}{\sinh(ks+a)}$	$(k>0,h>0)$	$2\sum_{n=0}^{\infty}e^{-(2n+1)a}u[t-h-(2n+1)k]$
29.4.10	$\frac{\sinh(hs+b)}{\sinh(ks+a)}$	$(0<h<k)$	$\sum_{n=0}^{\infty}e^{-(2n+1)a}\{e^bu[t+h-(2n+1)k]-e^{-b}u[t-h-(2n+1)k]\}$
29.4.11	$\sum_{n=0}^{\infty}a_ne^{-k_ns}$	$(0<k_0<k_1<\ldots)$	$\sum_{n=0}^{\infty}a_nu(t-k_n)$

For the definition of the Laplace-Stieltjes transform see [29.7]. In practice, Laplace-Stieltjes transforms are often written as ordinary Laplace transforms involving Dirac's delta function $\delta(t)$. This "function" may formally be considered as the derivative of the unit step function, $du(t)=\delta(t)dt$, so that $\int_{-\infty}^{x}du(t)=\int_{-\infty}^{x}\delta(t)dt=\begin{cases}0 & (x<0)\\ 1 & (x>0).\end{cases}$ The correspondence **29.4.2**, for instance, then assumes the form $e^{-ks}=\int_0^{\infty}e^{-st}\delta(t-k)dt$.

[4] Adapted by permission from P. M. Morse and H. Feshbach, Methods of theoretical physics, vols. 1, 2, McGraw-Hill Book Co., Inc., New York, N.Y., 1953.

9. Bessel Functions of Integer Order

Mathematical Properties

is chapter are for Bessel func-
rder; the text treats general
entions used are:

al.
teger or zero.
icted except where otherwise
osed real in the sections devoted
s **9.9, 9.10,** and **9.11.**
ed for the Bessel functions is
15] and the British Association
y Mathematical Tables. The
ten denoted $N_\nu(z)$ by physicists
kers.
are those of:

Bessel Functions J and Y

9.1. Definitions and Elementary Properties

Differential Equation

9.1.1 $$z^2\frac{d^2w}{dz^2}+z\frac{dw}{dz}+(z^2-\nu^2)w=0$$

Solutions are the Bessel functions of the first kind $J_{\pm\nu}(z)$, of the second kind $Y_\nu(z)$ (also called Weber's function) and of the third kind $H_\nu^{(1)}(z)$, $H_\nu^{(2)}(z)$ (also called the Hankel functions). Each is a regular (holomorphic) function of z throughout the z-plane cut along the negative real axis, and for fixed $z(\neq 0)$ each is an entire (integral) function of ν. When $\nu=\pm n$, $J_\nu(z)$ has no branch point and is an entire (integral) function of z.

ReActivity

Wendy Mackay, INRIA Saclay,
J.-D. Fekete, INRIA Saclay,

– **logs** of experiments for biologists, historians, other scientists

Adaptive combinatorial Search

Youssef Hamadi, MSRC
Marc Schoenauer, INRIA-Saclay

– improve **the usability** of *Combinatorial Search* algorithms.
– automate the fine tuning of solver parameters.
– parallel solver: “disolver”

Cloud computing action

Gabriel Antoniu (INRIA Rennes)
Bertrand Thirion (INRIA Saclay)

- **correlation** between Neurospin MRI images and genomic data
  - thousands of most precise images
  - thousands of genomic variables
- with **middleware** of G. Antoniu
  - BlobSeer (*a la Map-Reduce*) for grid machines
- on top of **Azure**

Cloud computing action

NeuroSpin

Neuroimaging center at Saclay

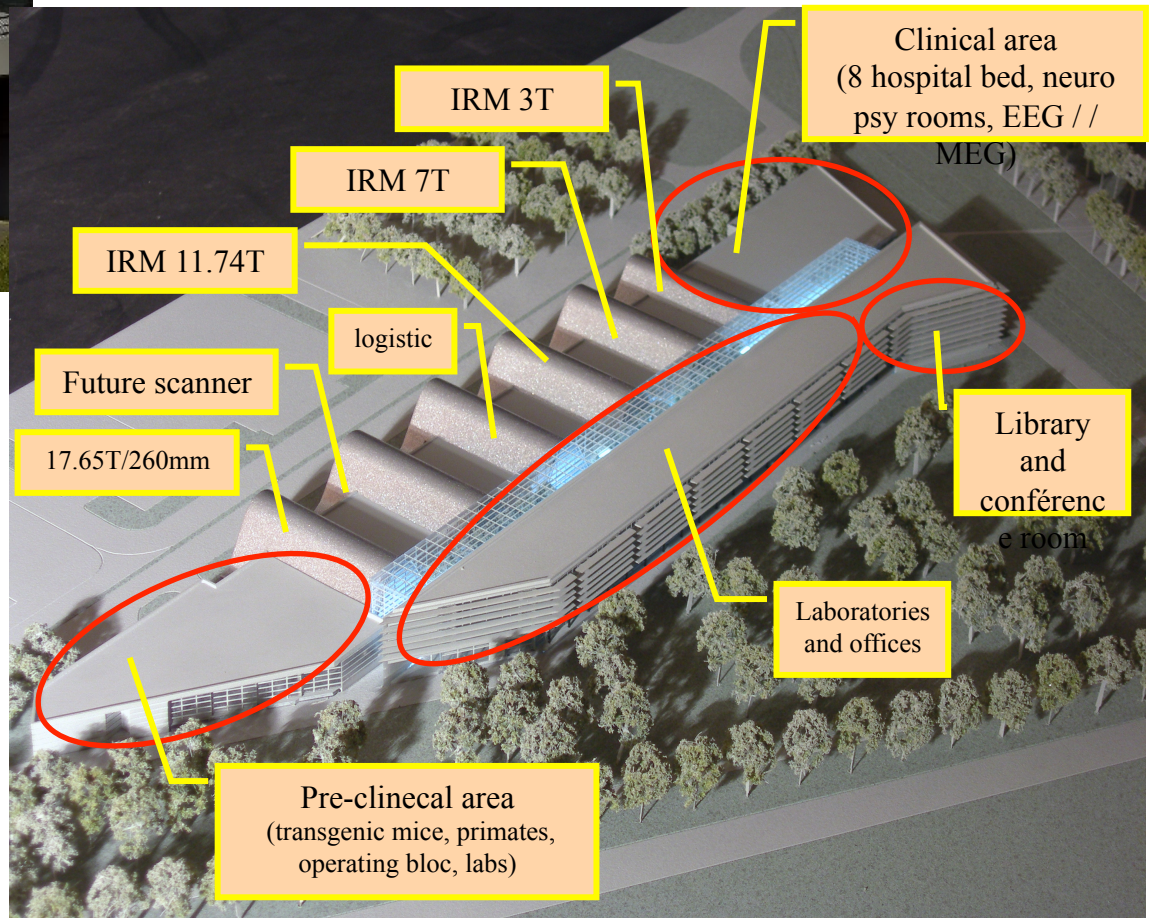


Image and Video mining

Jean Ponce, ENS
Andrew Blake, MSRC
Etienne Mémin, INRIA Rennes
Cordelia Schmid, INRIA Grenoble
Ivan Laptev, INRIA Rocq.
Josef Sivic, INRIA Rocq.
Rick Zelinsky, MSRR

Computer vision and Machine learning for:

- *archaeology and cultural heritage preservation*: **3D object** modeling and recognition from historical paintings and photographs
- environmental *sciences*: **change detection** in dynamic satellite imagery
- *sociology*: **human activity** modeling and recognition in video archives

Image and Video mining

– *archaeology and cultural heritage preservation*: **3D object** modeling and recognition from historical paintings and photographs

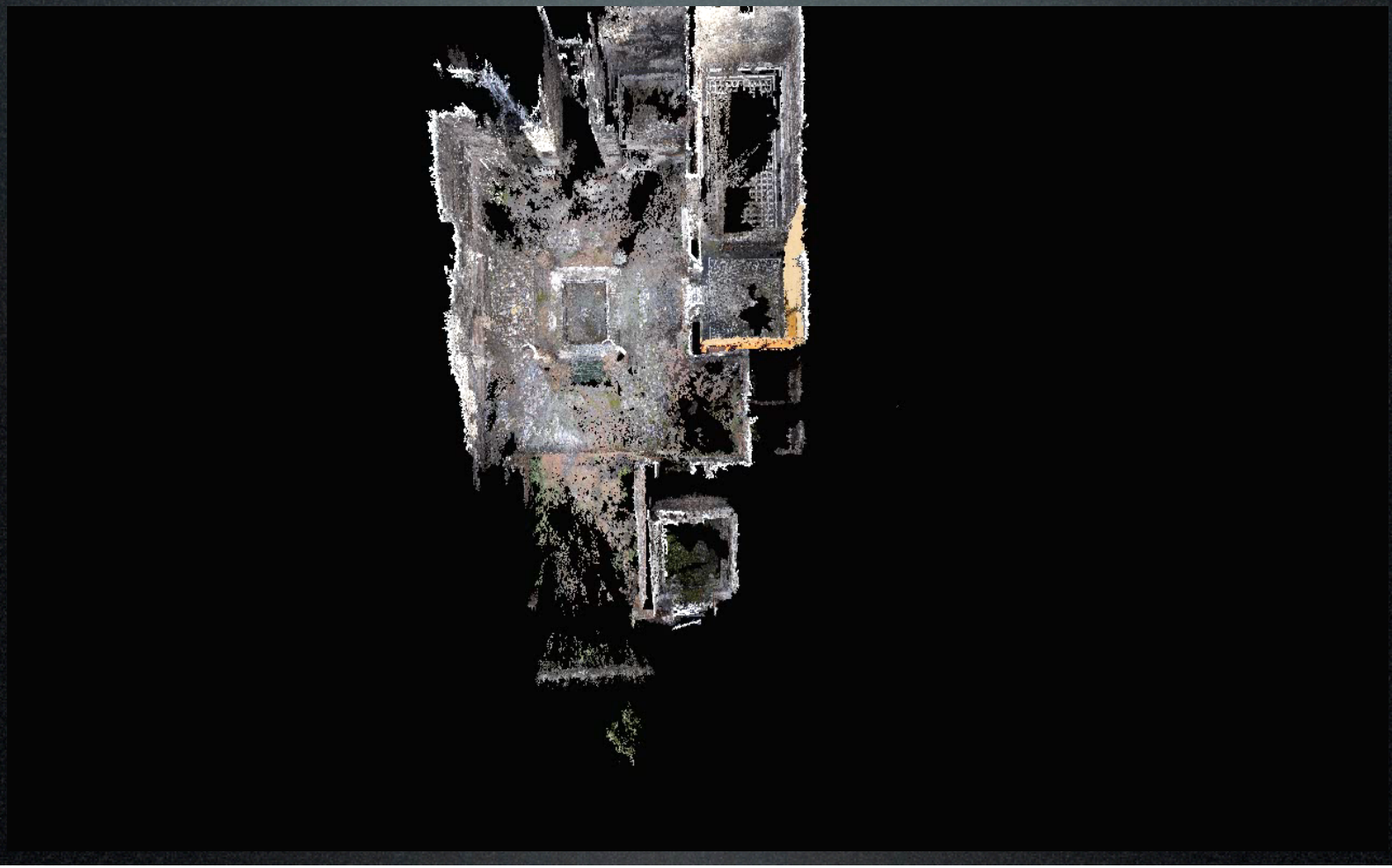


Image and Video mining

– *sociology*: **human activity** modeling and recognition in video archives

Conclusion

Logics in track A

Math. components	Coq	higher-order + reflection
Security	PV/CV	applied pi-calculus + stochastic
Spec. / Verif.	TLA+	1st order + ZF + temporal

Sciences in track B

DDMF	computer algebra	hard sciences
Adapt. search	constraints, machine learning	hard sciences, biology
Reactivity	chi + visualisation	soft sciences, biology
I.V. mining	computer vision	humanities, environment


CENTRE DE RECHERCHE
COMMUN
INRIA
MICROSOFT RESEARCH