MSR-INRIA Joint Centre

Jean-Jacques Lévy

June 3, 2009

Plan

1. Context

2. Track A
   - Math. Components (G.Gonthier)
   - Security (C. Fournet)
   - TLA+ (D. Doligez)

3. Track B
   - DDMF (Bruno Salvy)
   - ReActivity (J.-D. Fekete, Wendy Mackay)
   - Adaptative search (Youssef Hamadi, Marc Schoenauer)
   - Image & video mining (Jean Ponce)

CENTRE DE RECHERCHE COMMUN

INRIA
MICROSOFT RESEARCH

Demos - Short Talks

Track A (20mn each)

- Laurent Théry (INRIA Sophia)
- Pierre–Malo Deniélou (Imperial College)
  Cédric Fournet (MSRC)
  Eugen Zalinescu (Joint Centre)
- Kaustuv Chaudury (Joint Centre)

Track B (20mn each)

- Frédéric Chyzak (INRIA Rocq)
- Wendy Mackay (INRIA Saclay)
- Nikolaus Hansen (Joint Centre)
- Jean Ponce (ENS, INRIA Rocq)

Context

Management

INRIA

MSR Cambridge

Eric Boustouller
Stephen Emmott
Gérard Giraudon
Gérard Huet
Marc Jalabert
Jean Vuillemin
Ken Wood

Joint Centre

Michel Cosnard

Andrew Herbert

M. Thirion

J.-J. Lévy

P.-L.Xech

Michel Bidoit
Bruno Sportisse

Andrew Blake
Stephen Emmott
Malik Ghallab
Claude Puech

Bernard Ourghanlian
Thomas Serval

CENTRE DE RECHERCHE COMMUN
INRIA MICROSOFT RESEARCH

Organization

a rather complex system

- **7 research projects (in two tracks)**
- **12 resident researchers**
- **non permanent researchers funded by the Joint Centre**
- **permanent researchers paid by INRIA or MSR**
- **operational support by INRIA Saclay**
- **1 system manager** (Guillaume Rousse, INRIA Saclay)
- **1 administrative assistant** (Martine Thirion, Joint Centre)
- **1 deputy director** (Pierre-Louis Xech, MS France)
- **active support from MS France**
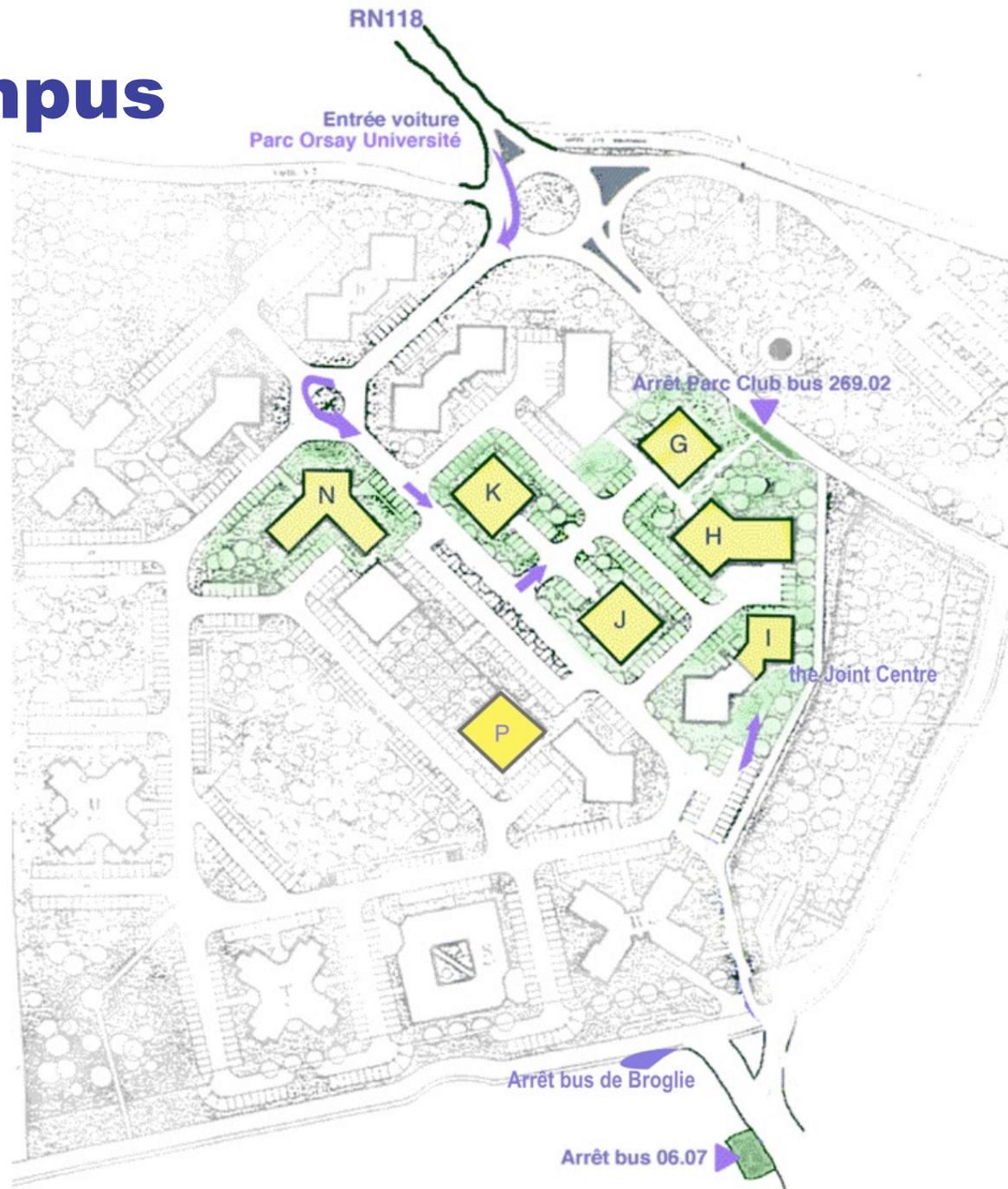
Localization

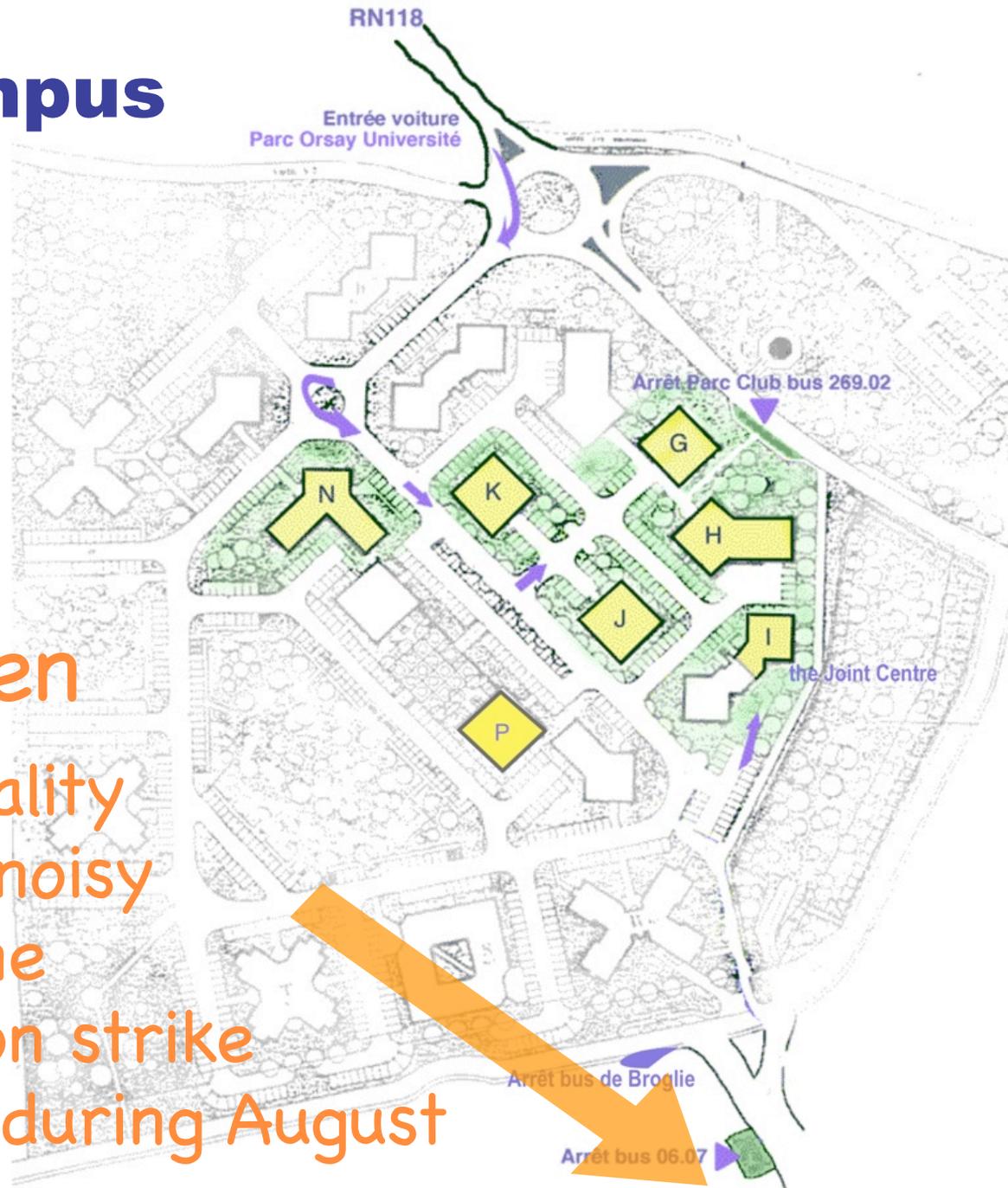## the plateau de Saclay

Localization
the plateau de Saclay

= long term investment

Campus

RN118

Entrée voiture
Parc Orsay Université

Arrêt Parc Club bus 269.02

N

K

G

H

J

I

the Joint Centre

P

Arrêt bus de Broglie

Arrêt bus 06.07

INRIA
MICROSOFT RESEARCH

Campus

Canteen

- low quality
- hyper noisy
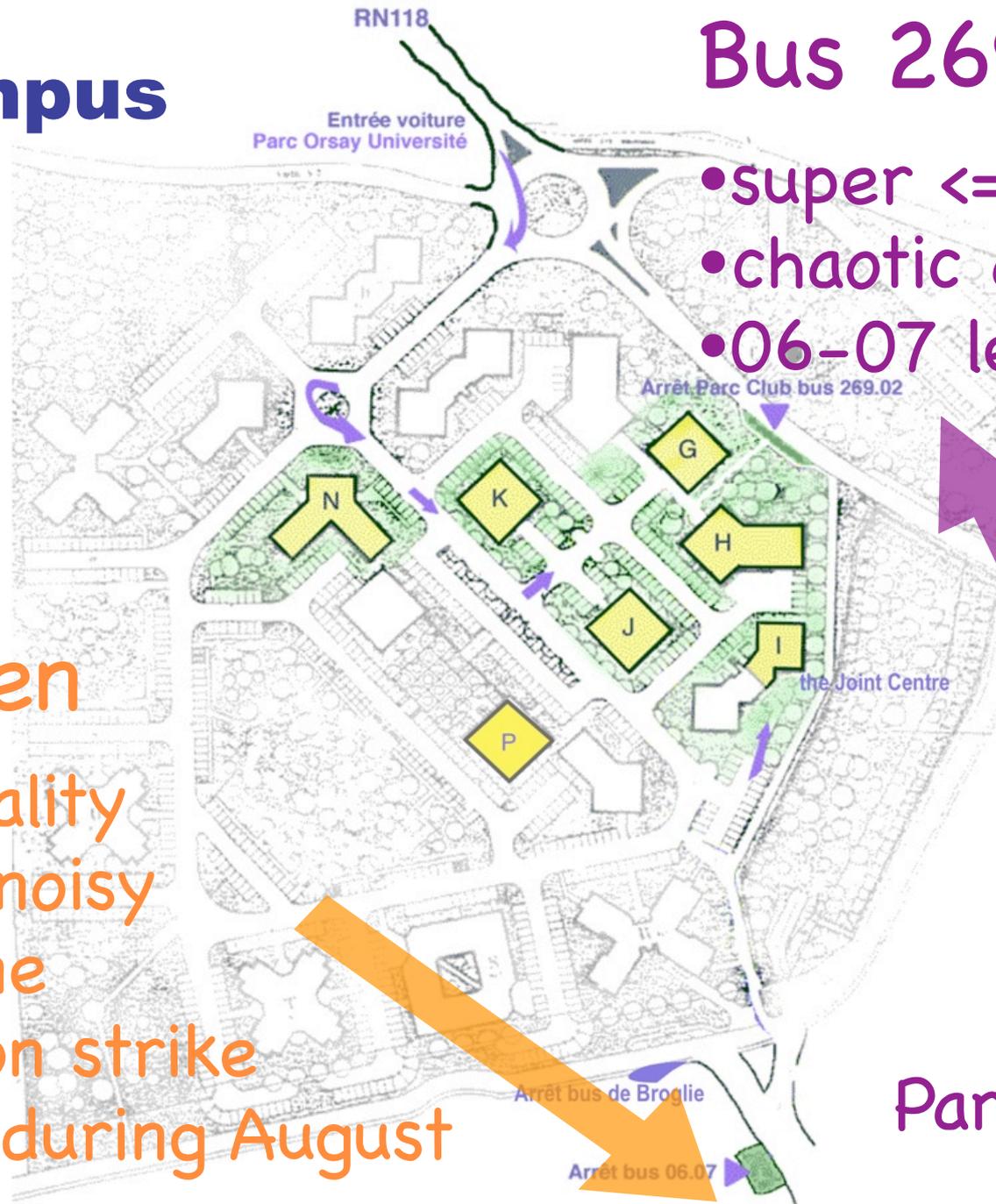- long line
- often on strike
- closed during August

Campus

Bus 269-02
- super <= 10am
- chaotic after
- 06-07 less many

6mn

Canteen
- low quality
- hyper noisy
- long line
- often on strike
- closed during August

RER B
Paris = 30mn

INRIA
MICROSOFT RESEARCH

People

PhD Students

- Francois GARILLOT
- Sidi OULD BIHA
- Iona PASCA
- Roland ZUMKELLER
- Pierre-Malo DENIELOU
- Nataliya GUTS
- Jérémy PLANUL
- Santiago ZANELLA
- Alexandre BENOIT
- Marc MEZZAROBA
- Nathalie HENRY (+)
- Nicolas MASSON
- Arnaud SPIVAK
- Aurélien TABARD

- Alexandro ARBALAEZ
- Alvaro FIALHO
- Adrien GAIDON

Post Docs

- Stéphane LE ROUX
- Guillaume MELQUIOND (*)
- Assia MAHBOUBI (*)
- Ricardo CORIN (*)
- Gurvan LE GUERNIC
- Eugen ZALINESCU
- Tamara REZK (*)
- Kaustuv CHAUDURI (*?)
- Stefan GERHOLD
- Fanny CHEVALIER
- Niklas ELMQVIST
- Catherine LEDONTAL
- Tomer MOSCOVICH
- Theophanis TSANDILAS
- Nikolaus HANSEN (*?)
- Neva CHERNIAVSKY

_____
(*) Now on permanent INRIA position, (+) on permanent MSR position

Track A

Software Security
Trustworthy Computing

CENTRE DE RECHERCHE
COMMUN

INRIA
MICROSOFT RESEARCH

Mathematical components

Georges Gonthier, MSRC
Assia Mahboubi, INRIA Saclay/LIX
Andrea Asperti, Bologna
Y. Bertot, L. Rideau, L. Théry, Sidi Ould Biha,
Iona Pasca, INRIA Sophia

François Garillot, MSR-INRIA (PhD)
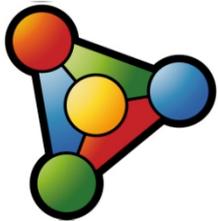Guillaume Melquiond, MSR-INRIA (postdoc)
Stéphane le Roux, MSR-INRIA (postdoc)
Benjamin Werner, INRIA Saclay/LIX,
Roland Zumkeller, LIX (PhD)

Computational proofs

- computer assistance for long formal proofs.

- reflection of computations into Coq-logic: ssreflect.

4-color

Appel-Haken

finite groups

Feit-Thompson

Kepler

Hales

Mathematical components

Recent results:

– new tactics using Reflexion and Coq pattern matching

– advanced theorems of Linear Algebra

– Composition of Theories

– Coq development (**ss-reflect** more integrated inside Coq distrib)

Objective:

– prove Feit-Thompson in 2011-12 ?!!

Secure Distributed Computations and their Proofs

Cédric Fournet, MSRC
Karthik Bhargavan, MSRC
Ricardo Corin, INRIA Rocq.
Pierre-Malo Deniélou, INRIA Rocq.
G. Barthe, 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 (intern)

Distributed computations + Security

– programming with secure communications

– certified compiler from high-level primitives to low-level crypto-protocols

– formal proofs of probabilistic protocols

# Secure Distributed Computations and their Proofs

Recent results:

- **secure sessions** v2 (proofs by typing)

- concurrent secure sessions v1

- correctness proofs of TLS implementations

- information flow + cryptography

- secure logs

- secure modeling of e-cash
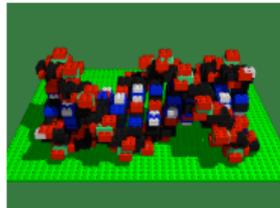
Tools for formal proofs

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

Natural proofs

- first-order set theory + temporal logic

- specification/verification of concurrent programs.

- tools for automatic theorem proving
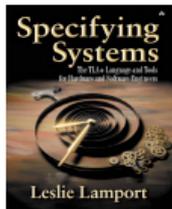
TLA+

tools for proofs

Zenon

CENTRE DE RECHERCHE COMMUN

INRIA MICROSOFT RESEARCH

Tools for formal proofs

Recent results:

- **Proof Manager** with incremental, non-linear proofs

- declarative meta-language

- proofs like done by Mathematicians

- proof of the atomic Bakery algorithm with PM

Logics in track A

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

Track B

Computational Sciences
Scientific Information Interaction
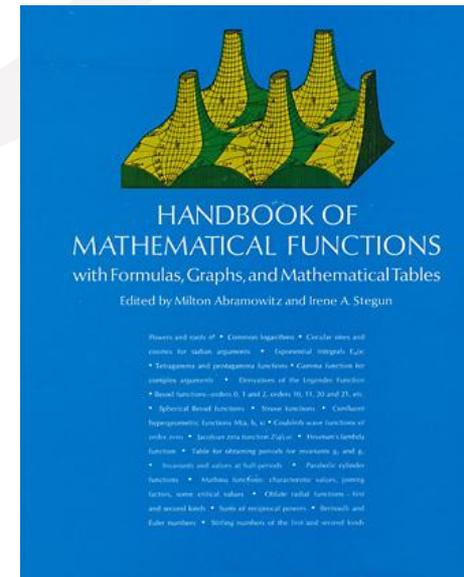
Dynamic dictionary of math functions

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

Henry Cohn, [Theory Group] MSRR
Alexandre Benoit, MSR-INRIA (intern)
Marc Mezzarobba, MSR-INRIA (intern)

Computer Algebra and Web for useful functions,

– dynamic tables of their properties.

– generation of programs to compute them.

Maple 11

HANDBOOK OF
MATHEMATICAL FUNCTIONS
with Formulas, Graphs, and Mathematical Tables
Edited by Milton Abramowitz and Irene A. Stegun

CENTRE DE RECHERCHE COMMUN

INRIA MICROSOFT RESEARCH

Dynamic dictionary of math functions

Recent results:

– arbitrary precision computations with certified bounds on numerical errors (used to determine lengths of Taylor expansions)

– approximations by Chebyshev series

– certificates (with proofs expressed in natural language)

– progress in GUI

– new **releases of DDMF** (last night)

ReActivity

Wendy Mackay, INRIA Saclay,
J.-D. Fekete, INRIA Saclay,
Mary Czerwinski, MSRR,
George Robertson, MSRR

Michel Beaudouin-Lafon, Paris 11,
Olivier Chapuis, CNRS,
Pierre Dragicevic, INRIA Saclay,
Emmanuel Pietriga, INRIA Saclay,
Aurélien Tabard, Paris 11 (PhD)

Logs of experiments for biologists, historians, other scientists

– mixed inputs from lab notebooks and computers,

– interactive visualization of scientific activity,

– support for managing scientific workflow.

CENTRE DE RECHERCHE COMMUN

INRIA
MICROSOFT RESEARCH
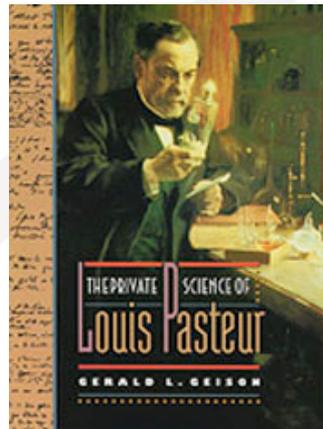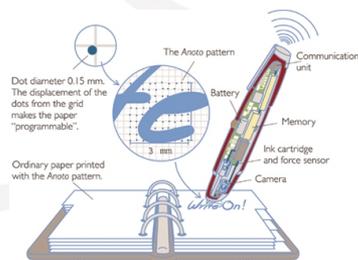
ReActivity

Recent results:

– workshop on Interacting with **Temporal Data** at CHI'09 (35 participants)

– streamlining the computation of aggregated metrics on Wikipedia "live" and small focused "Dashboard visualizations" tools

– WILD: Wall-sized **Interaction** with Large Datasets (32 screens, 8 Vicon, 1 interactive table expansions)

– Augmented Paper/Electronic Notebooks

Adaptive Combinatorial Search for E-science

Youssef Hamadi, MSRC
Marc Schoenauer, INRIA-Saclay
Anne Auger, INRIA-Saclay

Lucas Bordeaux, MSRC
Michèle Sebag, CNRS

Parallel constraint programming and optimization for very large scientific data

– improve the usability of *Combinatorial Search* algorithms.

– automate the fine tuning of solver parameters.

– parallel solver: "disolver"

MoGo

Adaptive Combinatorial Search for E-science

Recent results:

- **multi-armed bandit techniques** to select operators in evolutionary algorithms)

- adaptive search in **continuous search** spaces

- incremental learning for searching with **constraint programming**

Image and video mining for science and humanities

Jean Ponce, ENS
Andrew Blake, MSRC
Francis Bach, INRIA Rocquencourt
Hélène Dessales, ENS
Néva Cherniavsky, MSR-INRIA

Patrick Pérez, INRIA Rennes
Cordelia Schmid, INRIA Grenoble
Bryan Russell, MSR-INRIA
Ivan Laptev, INRIA
Andrien Gaidon, MSR-INRIA

Computer vision and Machine learning for:

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

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

– environmental *sciences*: change detection in dynamic satellite imagery
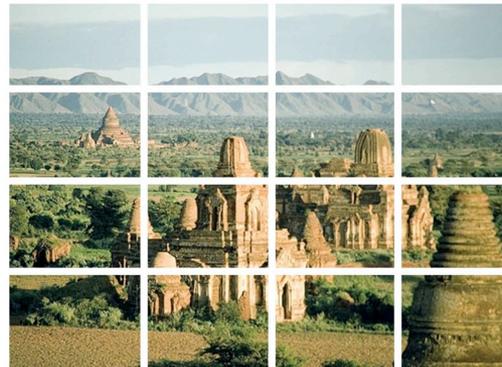
Sciences in track B

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

Objectives

- 30 resident researchers

- tight links with French academia (phD, post-doc)

- develop useful research for scientific community

- provide public tools (BSD-like license)

- become a new and attractive pole in CS research

- and source of spin off companies

- vision and medical applications ?

CENTRE DE RECHERCHE
COMMUN

INRIA
MICROSOFT RESEARCH