Mon album photo

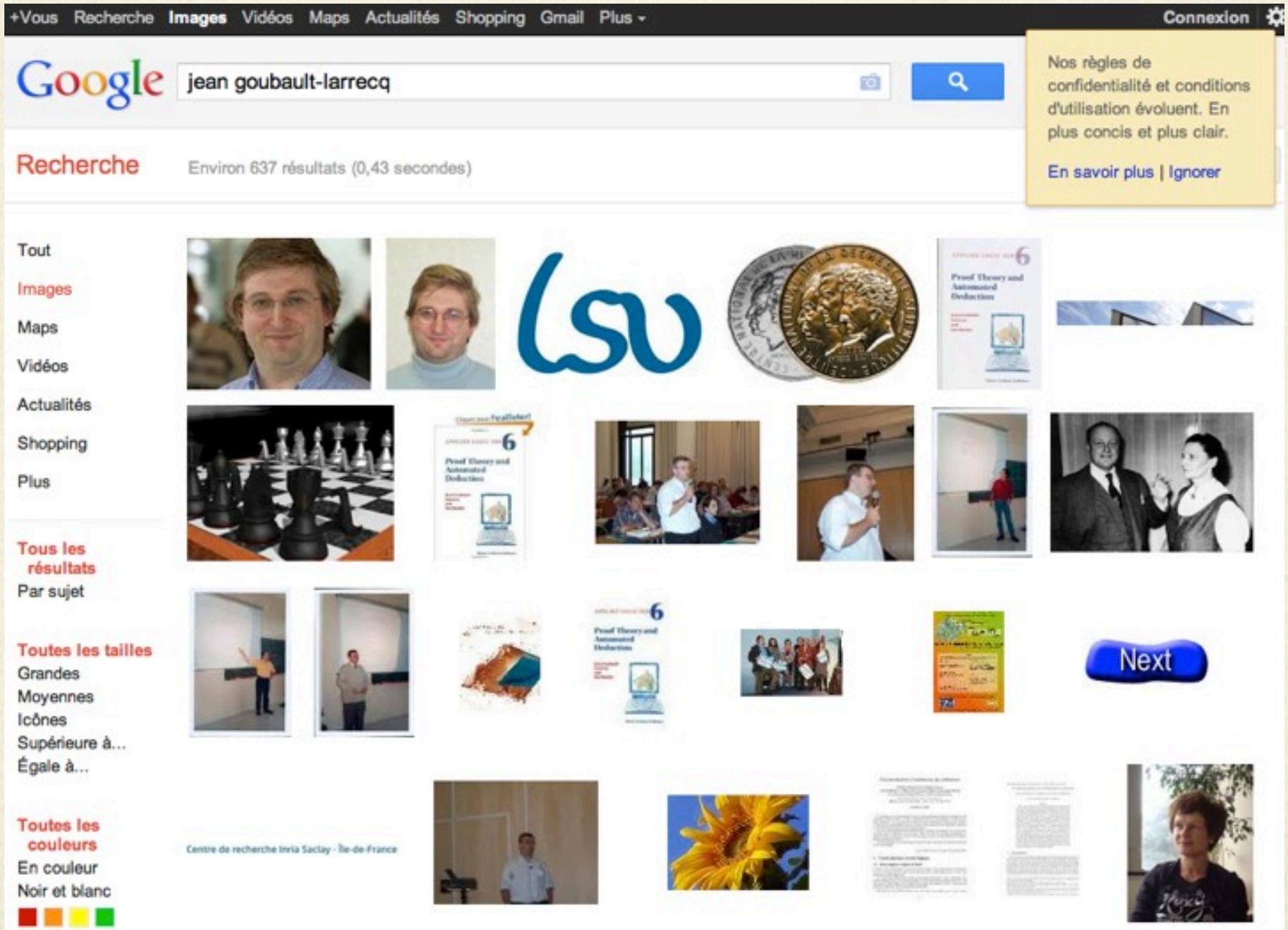
Jean Goubault-Larrecq

Disclaimer

- I'm going to talk about me, me, and me again...

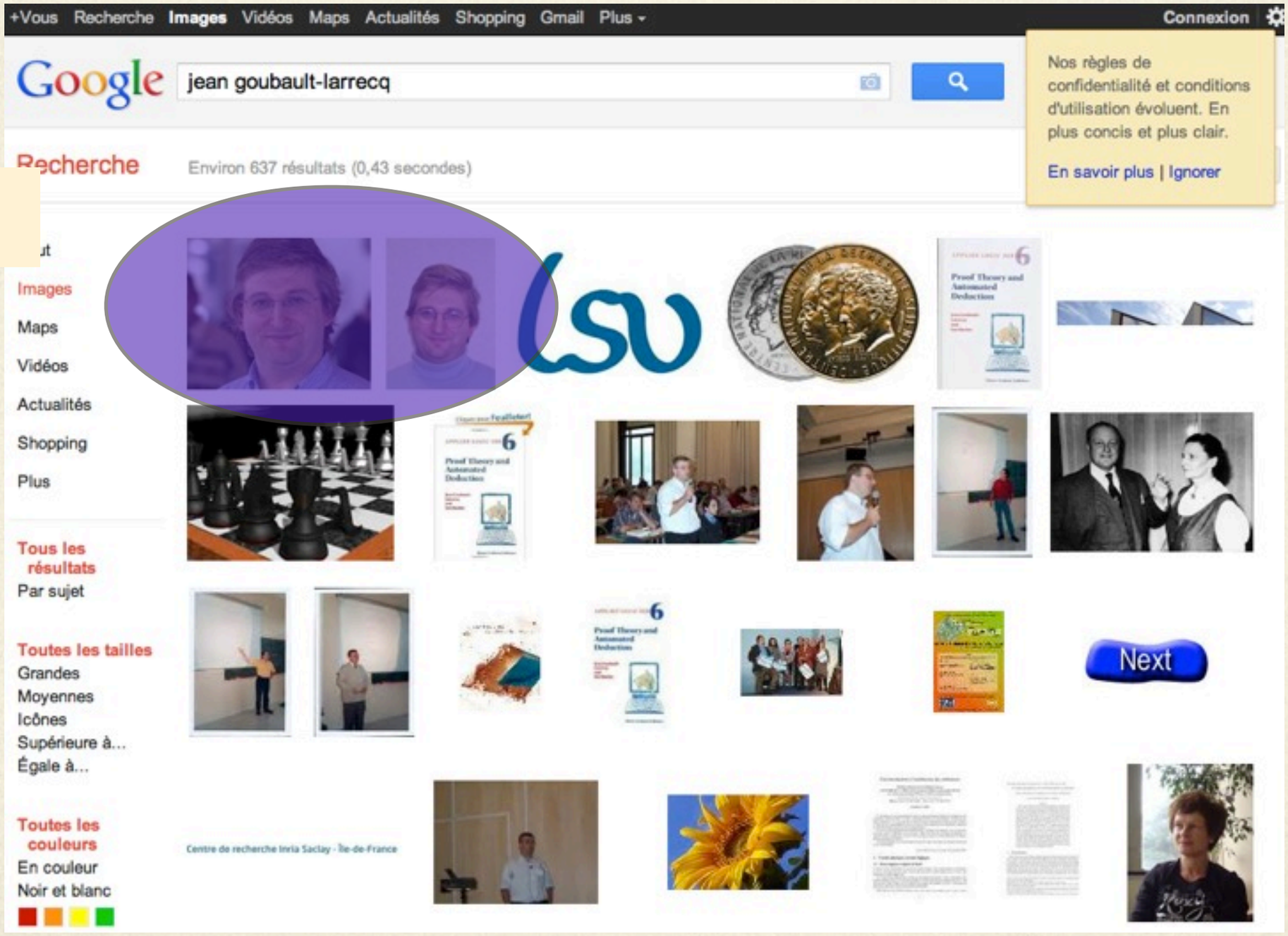
« Si tu ne parles pas de toi, qui va en parler?»
Laurent F.

What Google Images says

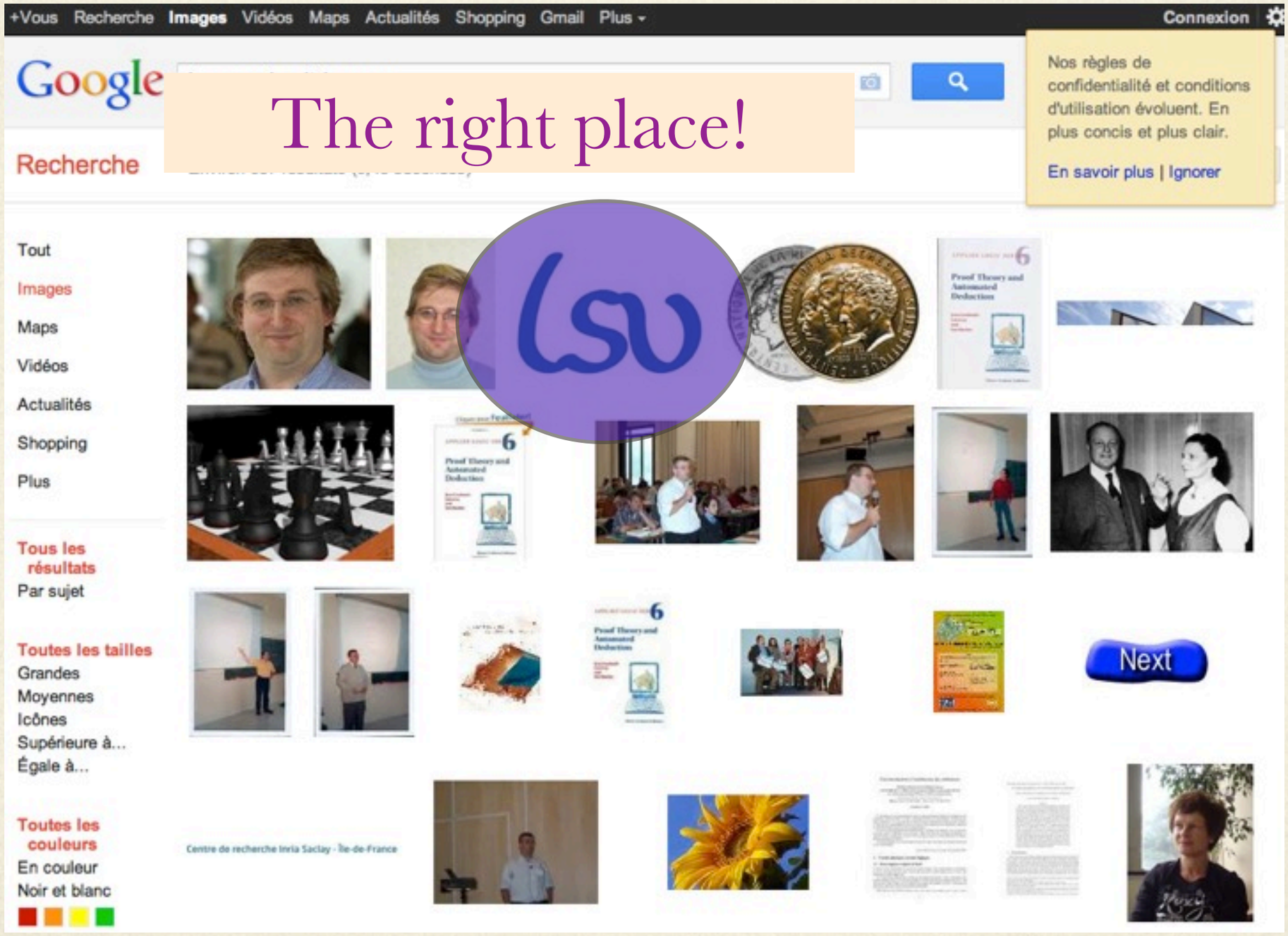


What Google Images says

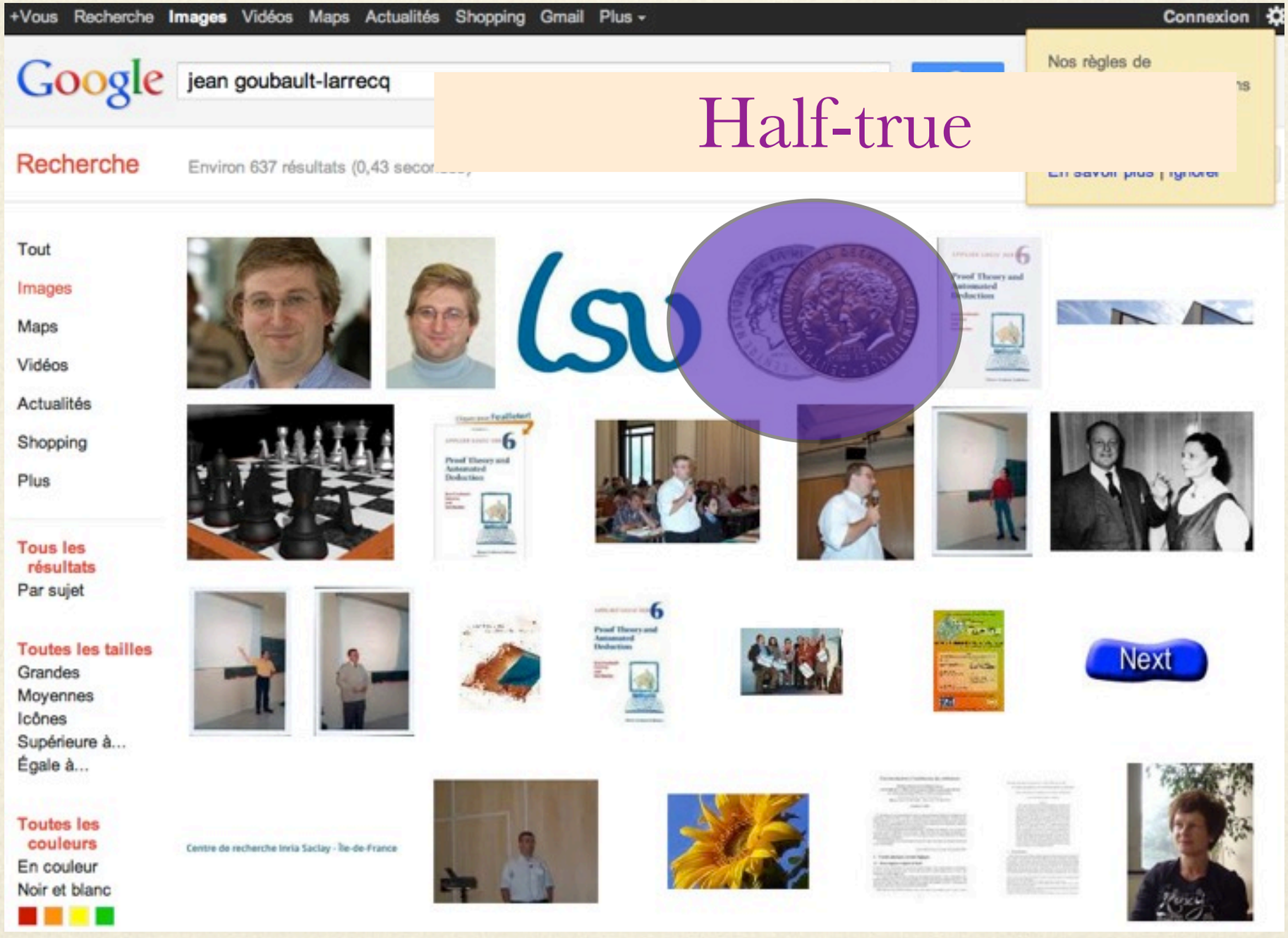
OK...



What Google Images says



What Google Images says

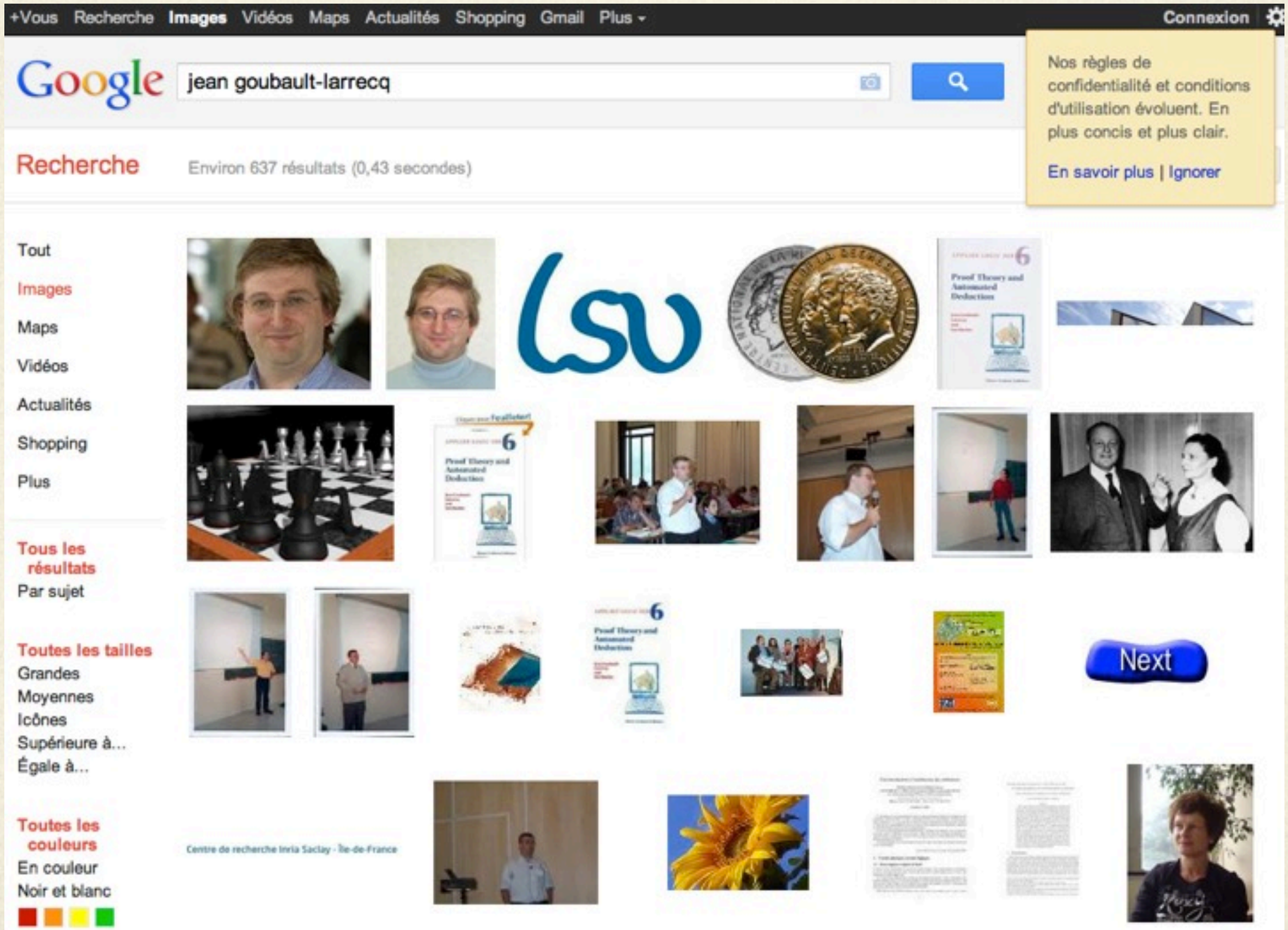


Half-true

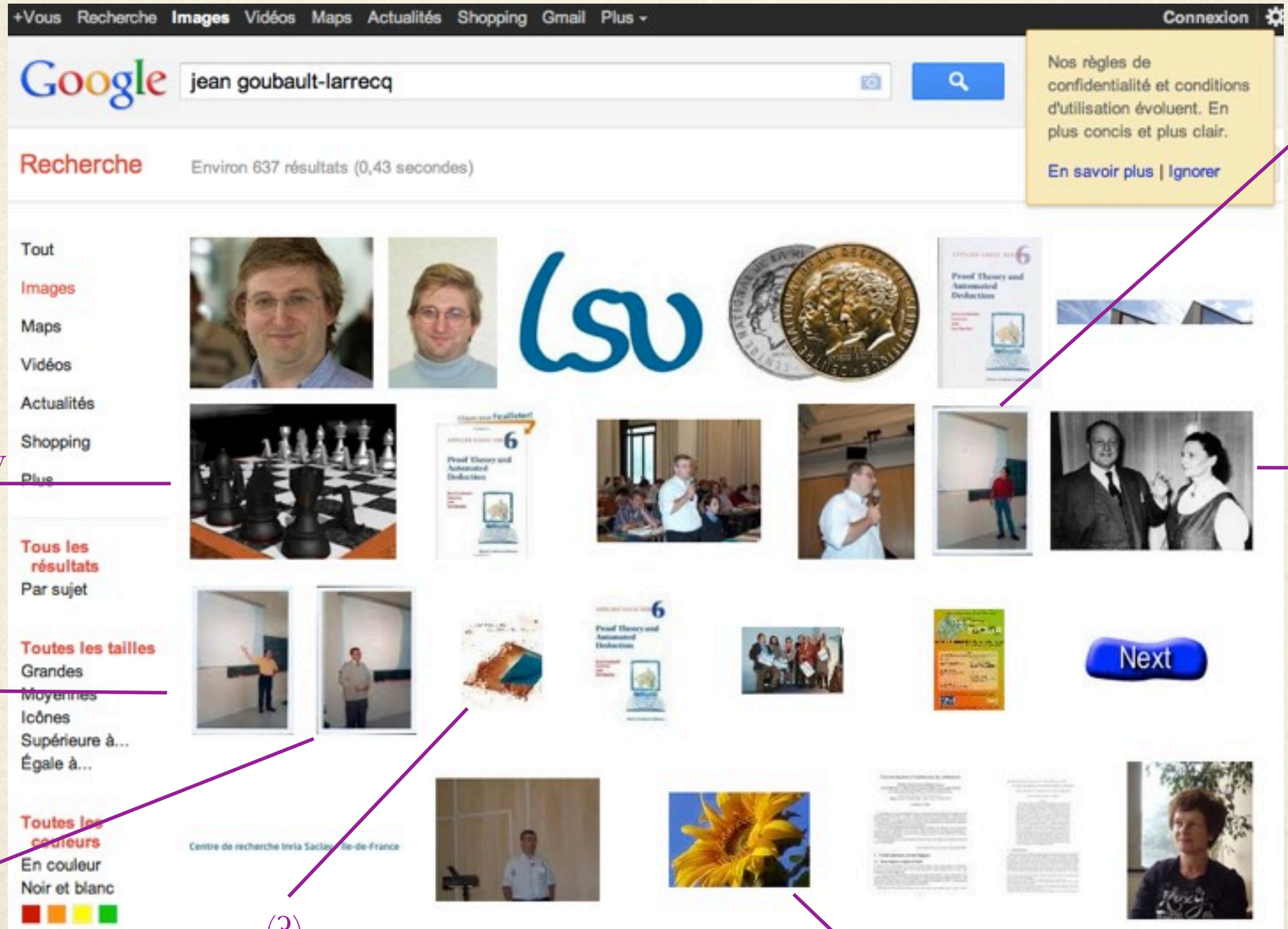
What Google Images says

My first book,
15th anniversary as well

What Google Images says



What Google Images says



No, I'm lousy at chess...

(?)

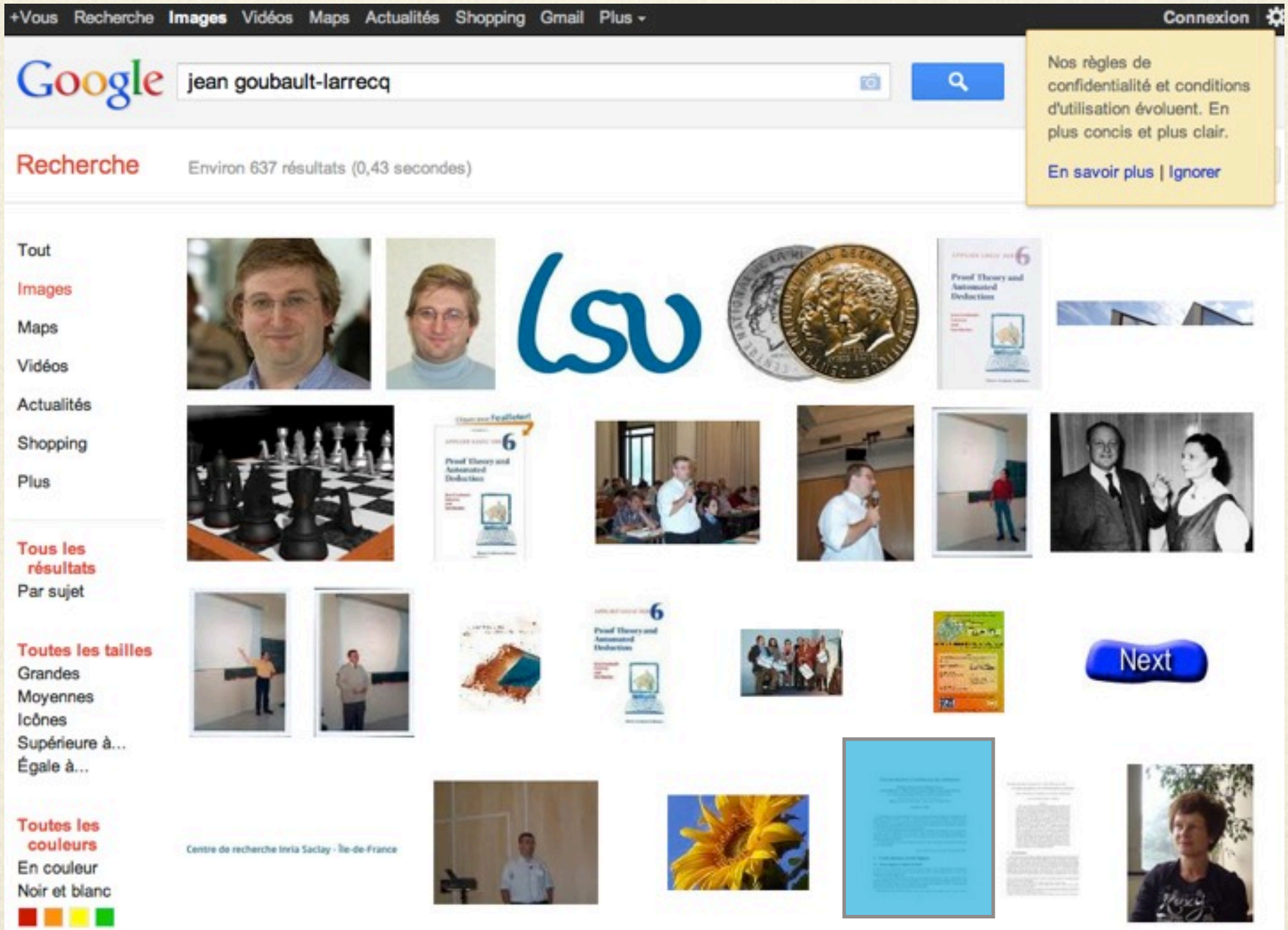
(?)

(?)

(?)

(?)

What Google Images says



What Google Images says

Une introduction à l'architecture des ordinateu

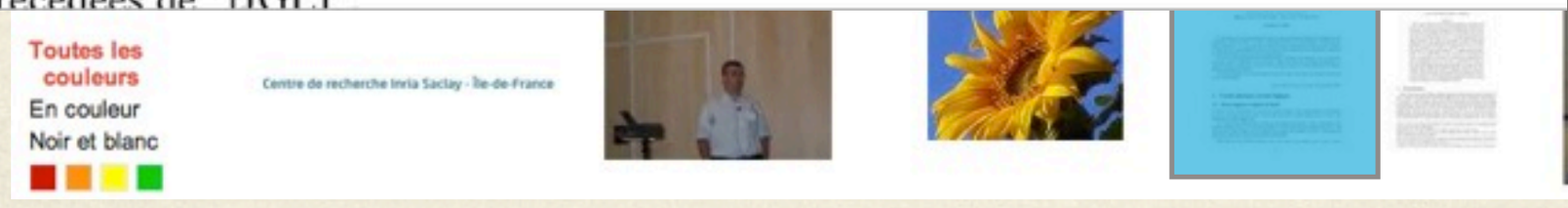
Béatrice Bérard, Jean Goubault-Larrecq
LSV/UMR 8643, CNRS, ENS Cachan & INRIA Futurs projet SECSI
61 avenue du président-Wilson, F-94235 Cachan Cedex
goubault@lsv.ens-cachan.fr
Phone: +33-1 47 40 75 68 Fax: +33-1 47 40 75 21

October 6, 2005

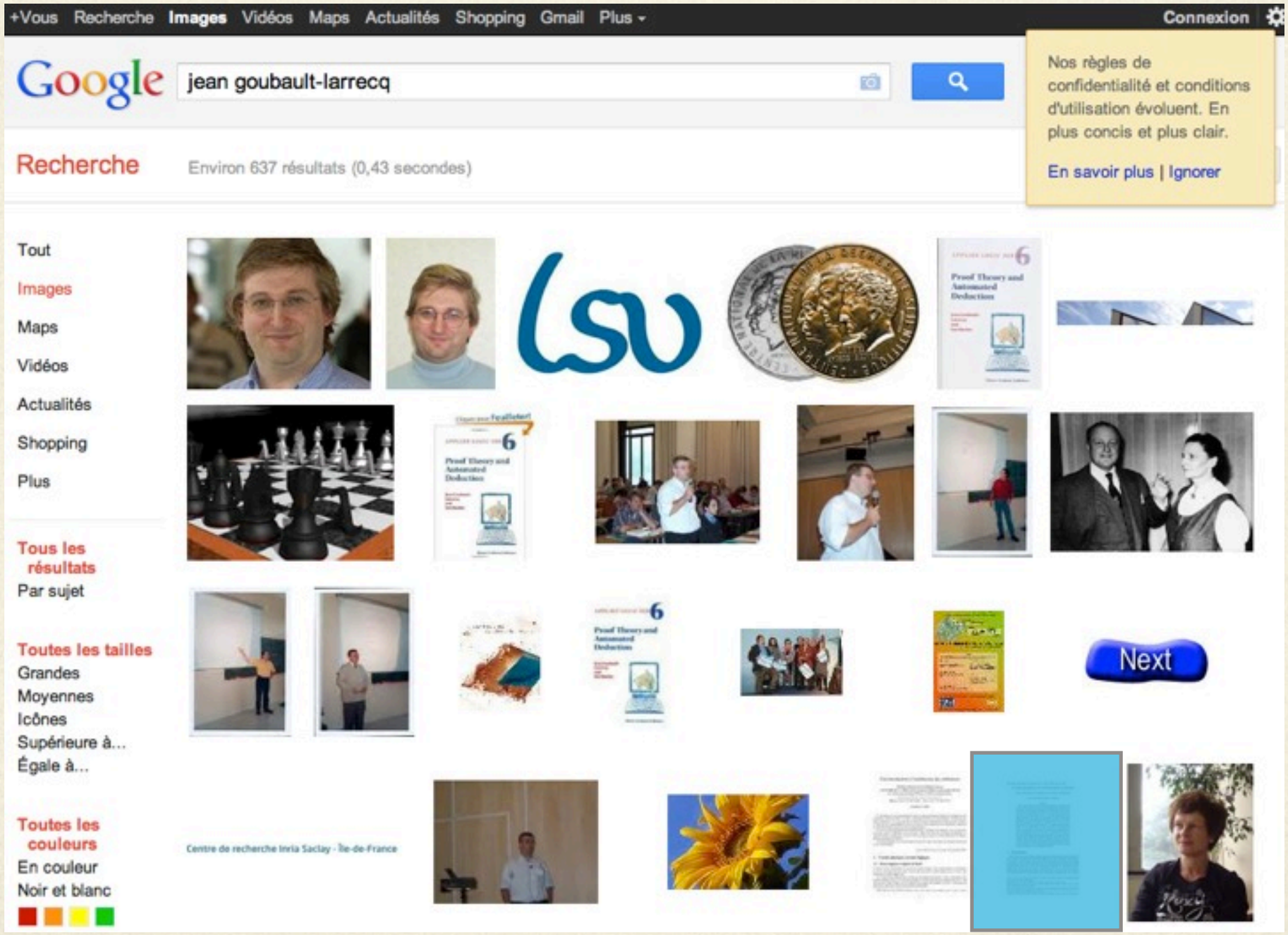
Ce document est la retranscription de notes de cours par Béatrice Bérard sur l'architecture des ordinateurs, datant de 1993. Ces notes s'inspiraient du livre d'A. Tannenbaum, "architecture des micro-ordinateurs". Ce cours présente les choses de façon suffisamment simple pour qu'on puisse se faire une idée raisonnablement claire de la façon dont fonctionnent les ordinateurs, depuis les circuits électroniques jusqu'à la micro-programmation.

Les processeurs aujourd'hui sont infiniment plus compliqués, les mémoires vives ne fonctionnent plus à base de flip-flops, soyez prévenus. Mais ceci reste une excellente introduction. Je mettrai quelques commentaires en notes en bas de page au sujet de certains points que je souhaute préciser, précédées de "[GL]".

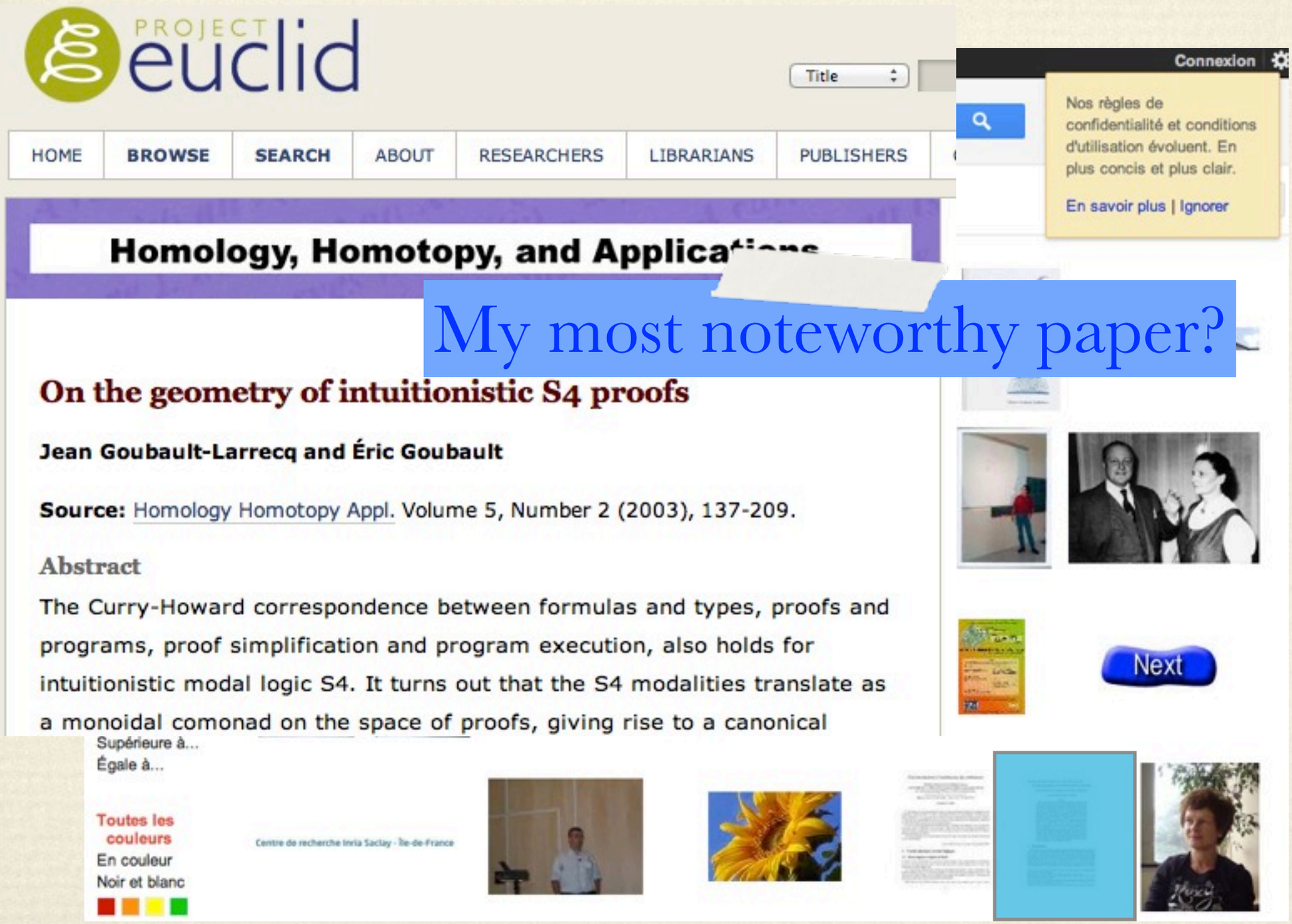
A few lecture notes



What Google Images says

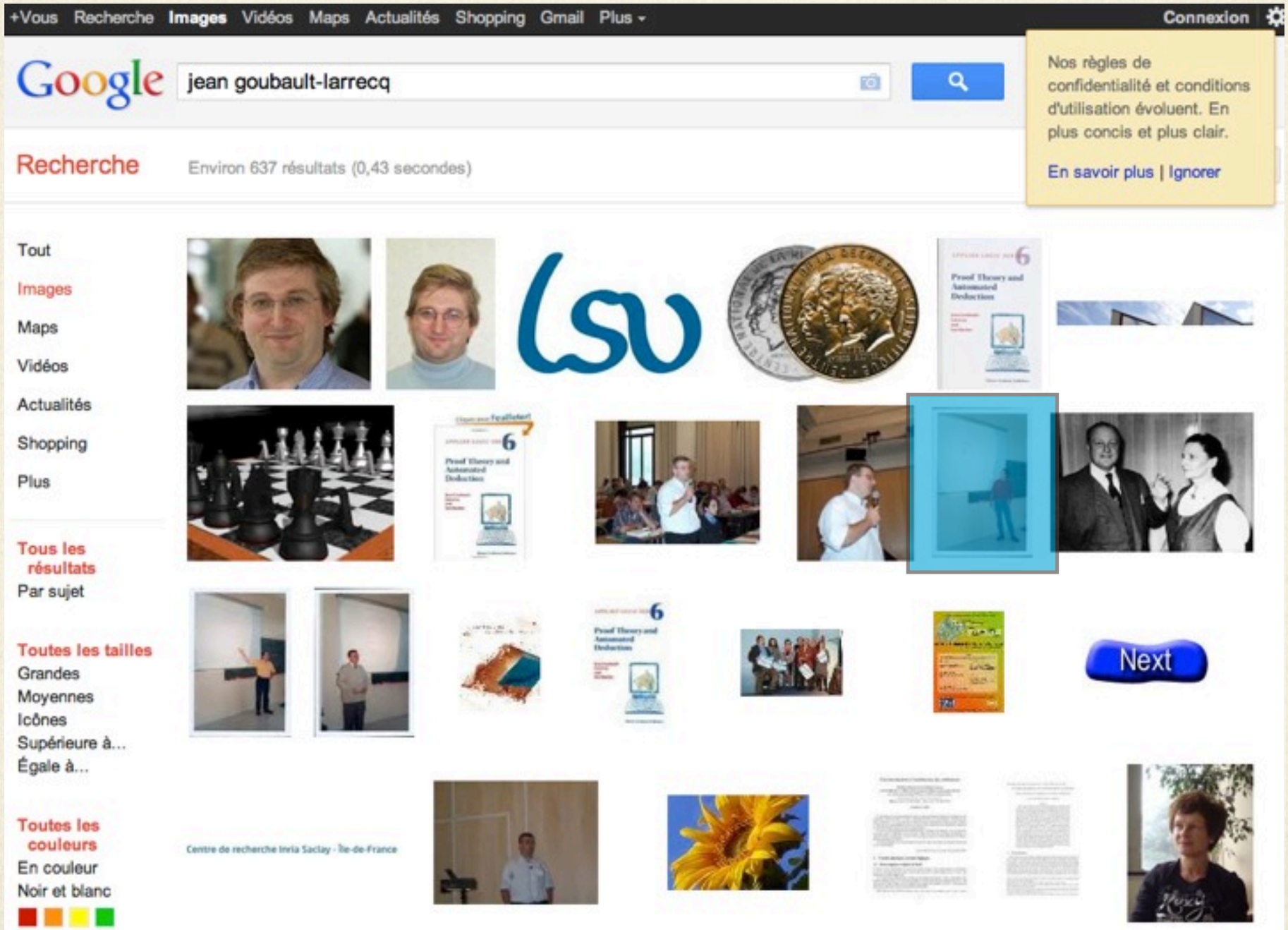


What Google Images says



My most noteworthy paper?

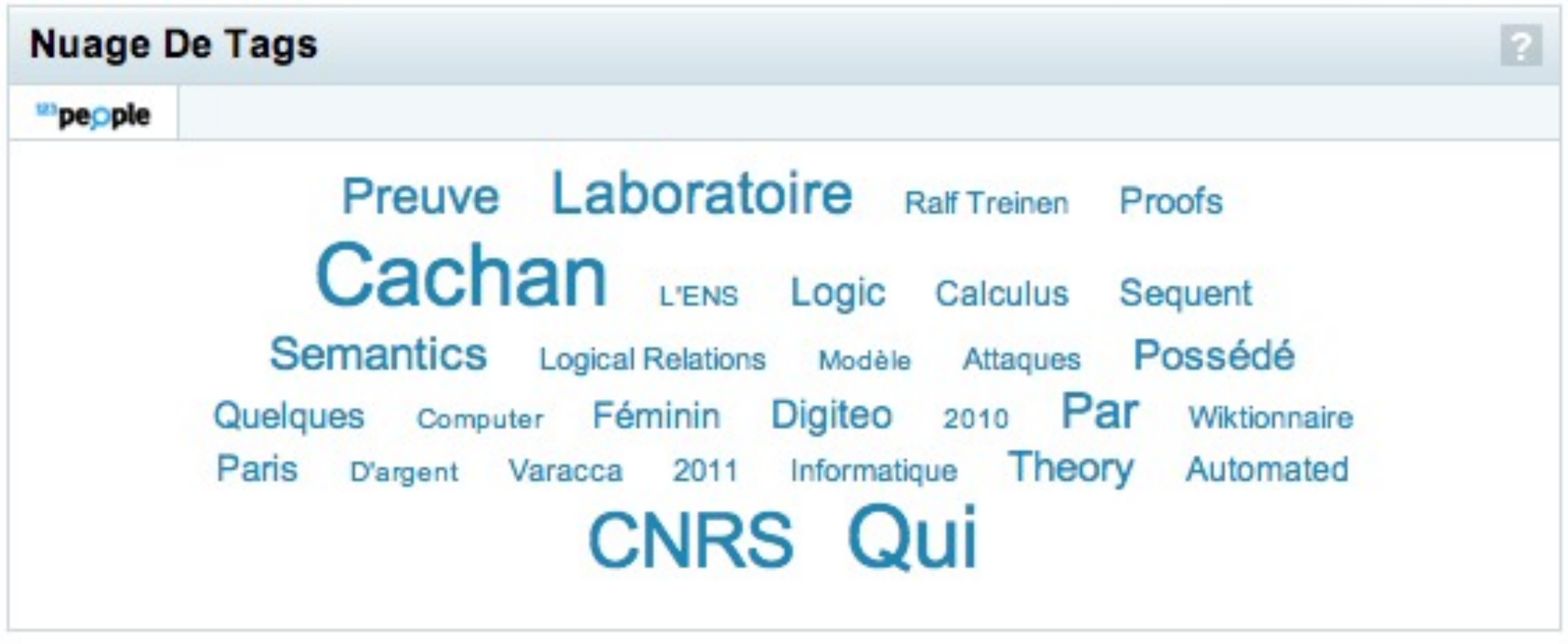
What Google Images says



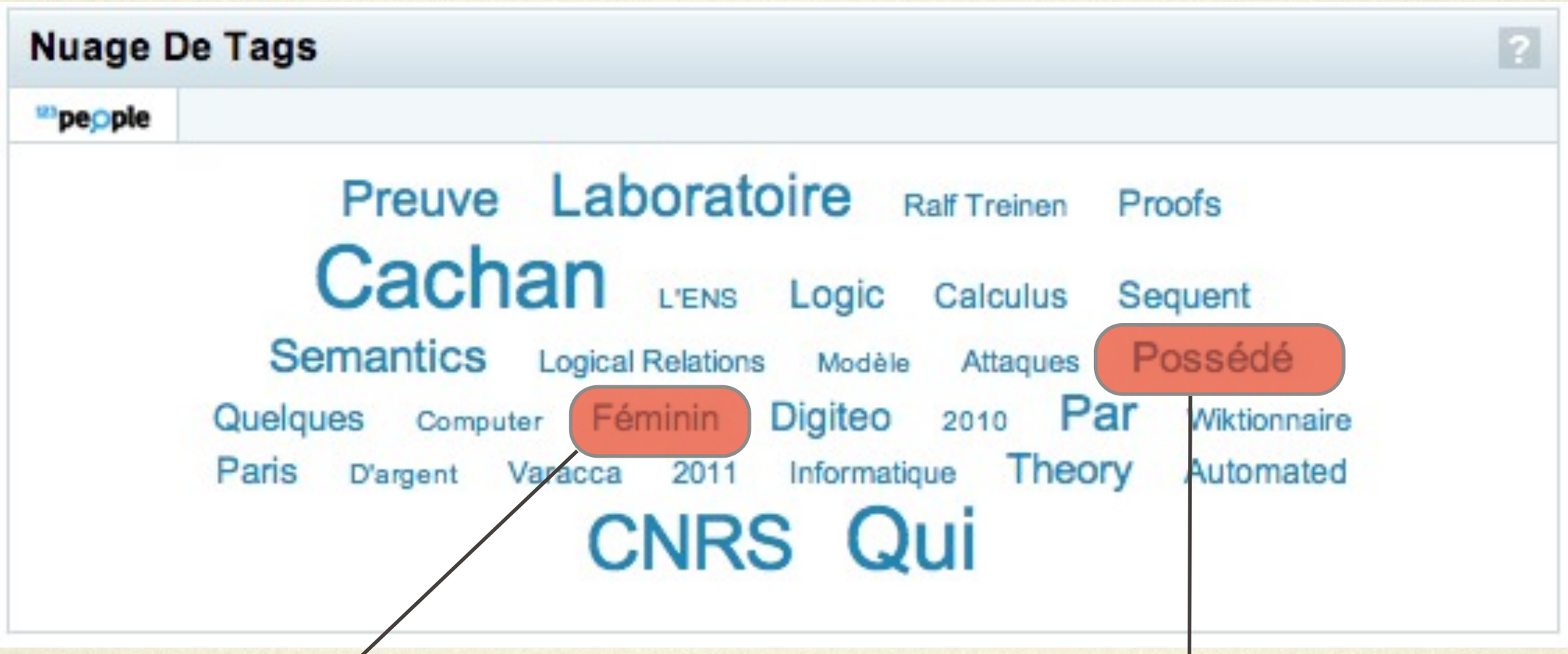
What Google Images says

Funny, I did not know I had a 123 People account

123 People


Nuage De Tags
?
123people
Preuve
Laboratoire
Ralf Treinen
Proofs
Cachan
L'ENS
Logic
Calculus
Sequent
Semantics
Logical Relations
Modèle
Attaques
Possédé
Quelques
Computer
Féminin
Digiteo
2010
Par
Wiktionnaire
Paris
D'argent
Varacca
2011
Informatique
Theory
Automated
CNRS
Qui

123 People



?

I would like something to explain this to me...

The real me

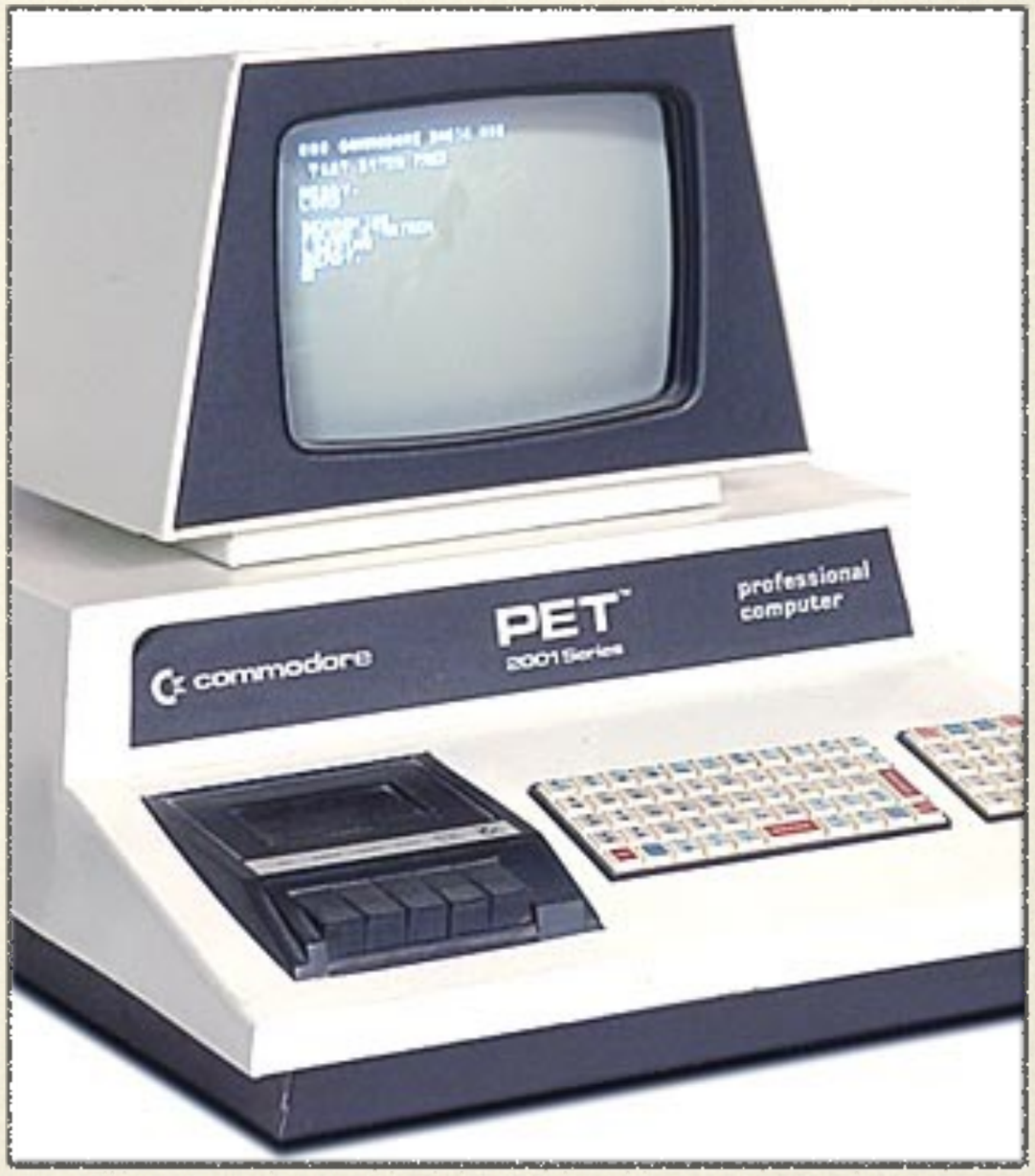
- At age 11, my math teacher made me discover computers,
  and **programming**

The real me

- At 13, I was interested in:
- **chemistry**
- mechanical engineering
- ancient greek
- ~~not computer science~~

The real me

- At age 15, I rediscovered **computers**,
  thanks to my parents



The real me

At age 20 (at X), I was undecided: mathematics,physics, **computer science**?

Some of my computers in 1985

The real me

At age 20 (at X), I was undecided: mathematics,physics, **computer science**?

Minus: every computer scientist (or geek) I knew was more or less nuts

Some of my computers in 1985

The real me

At age 20 (at X), I was undecided: mathematics,physics, **computer science**?

Minus: every computer scientist (or geek) I knew was more or less nuts

Plus: anyway, I was spending 100% of my leisure time programming

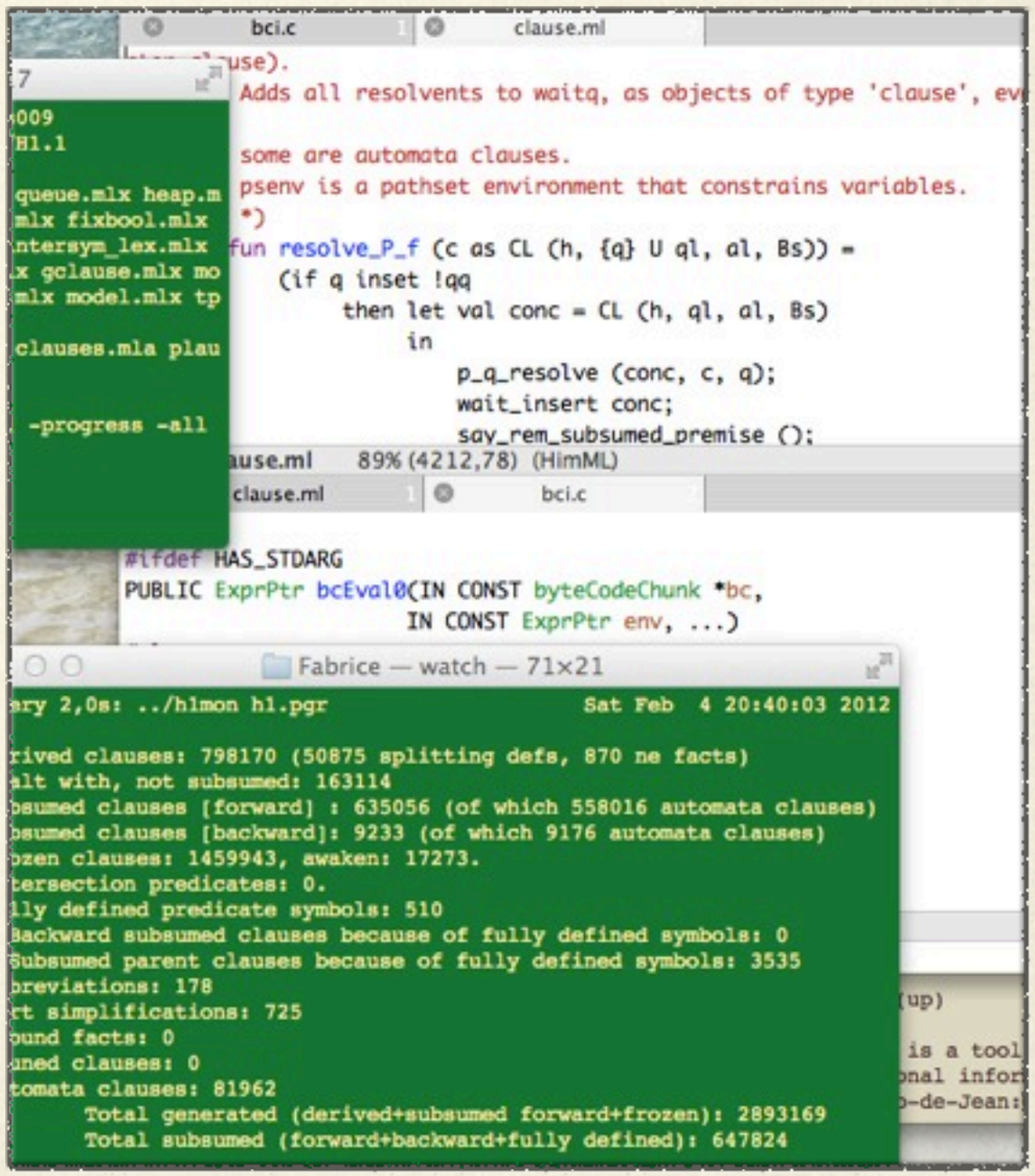
(being paid for what I would do anyway: a dream?)

Some of my computers in 1985

The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)

- I still am sort of a **geek**



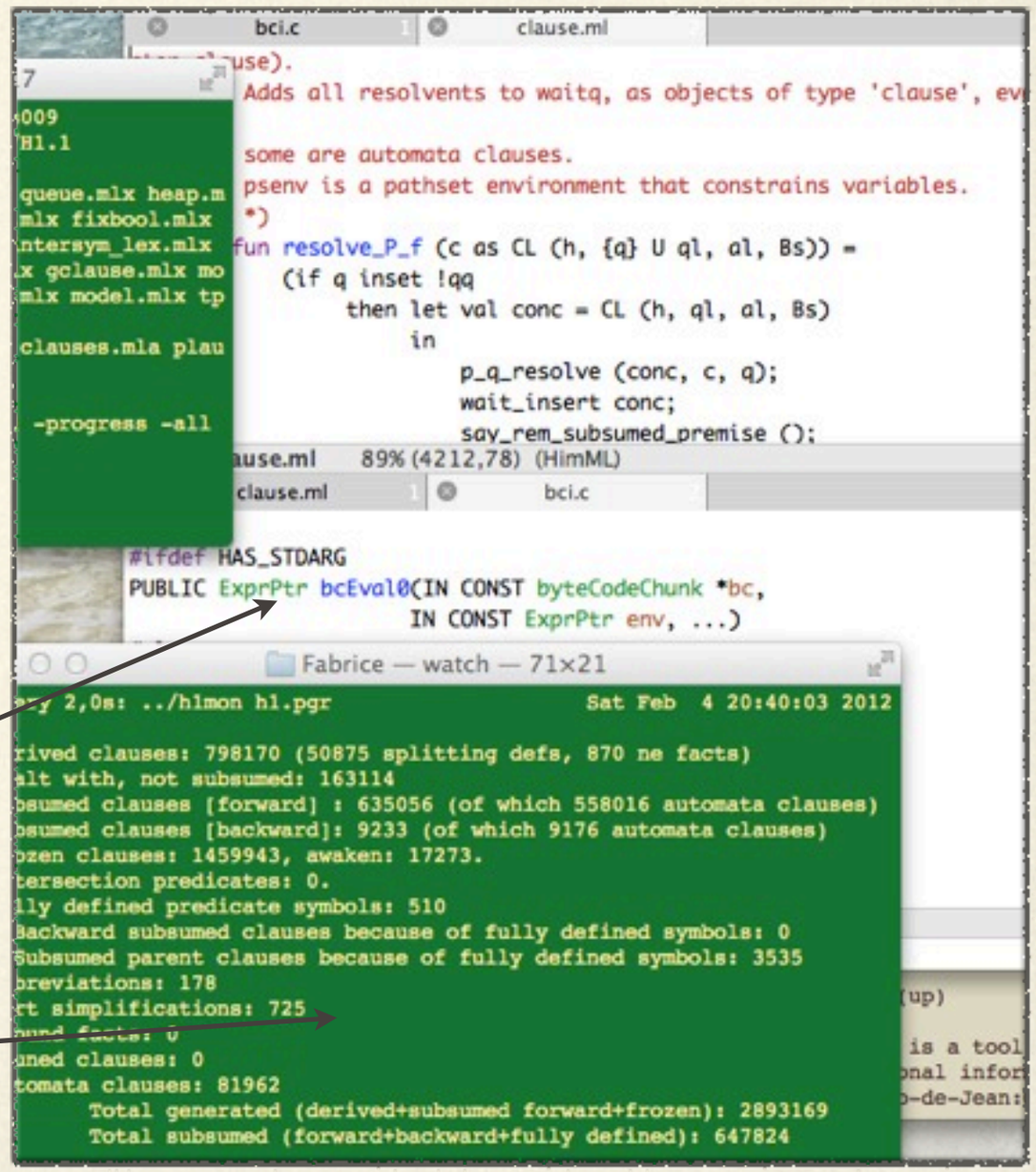
The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)

- I still am sort of a **geek**

HimML, my own version of the ML language

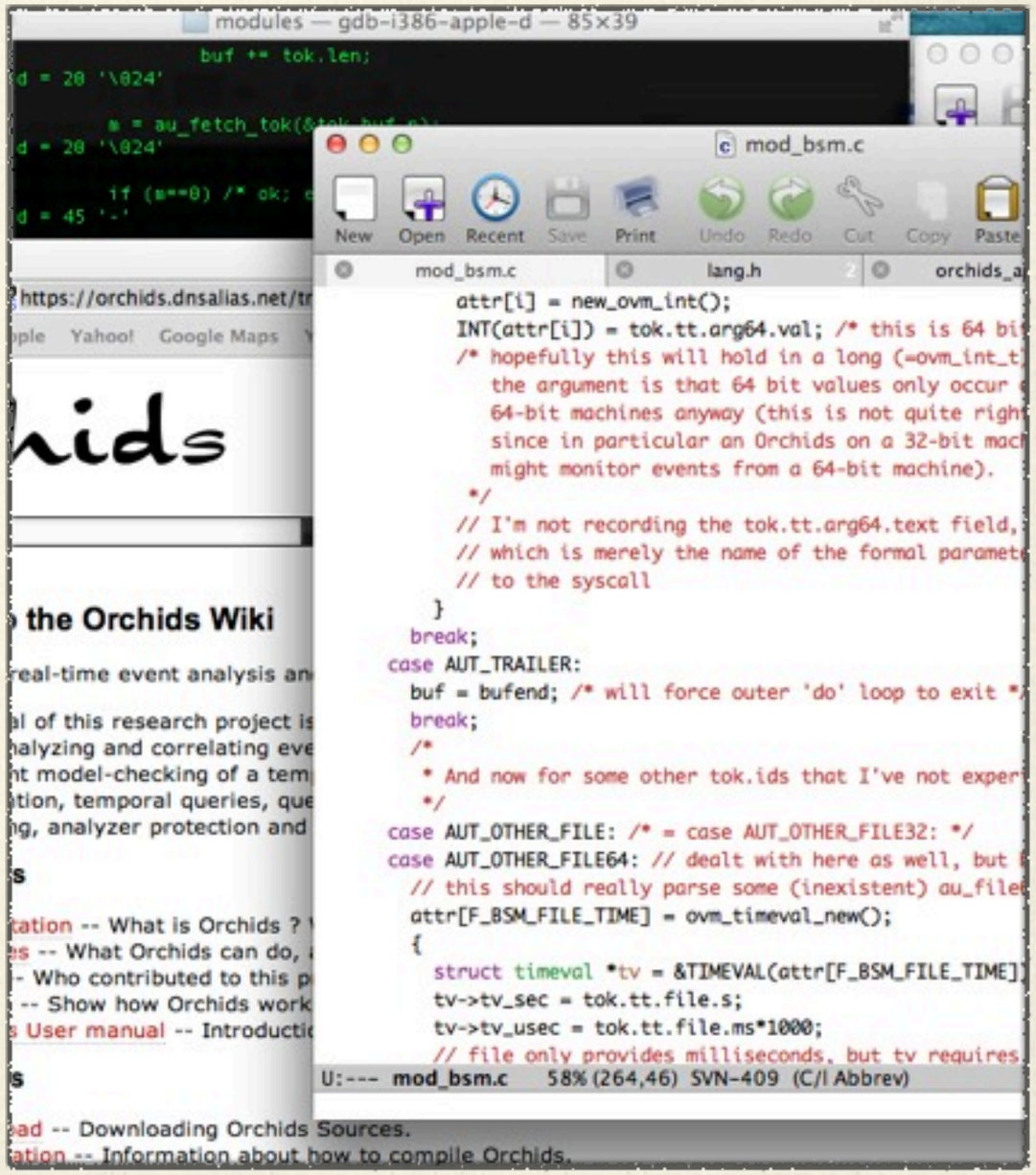
`h1`, an efficient prover / tree automata library



The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)

- I still am sort of a **geek**



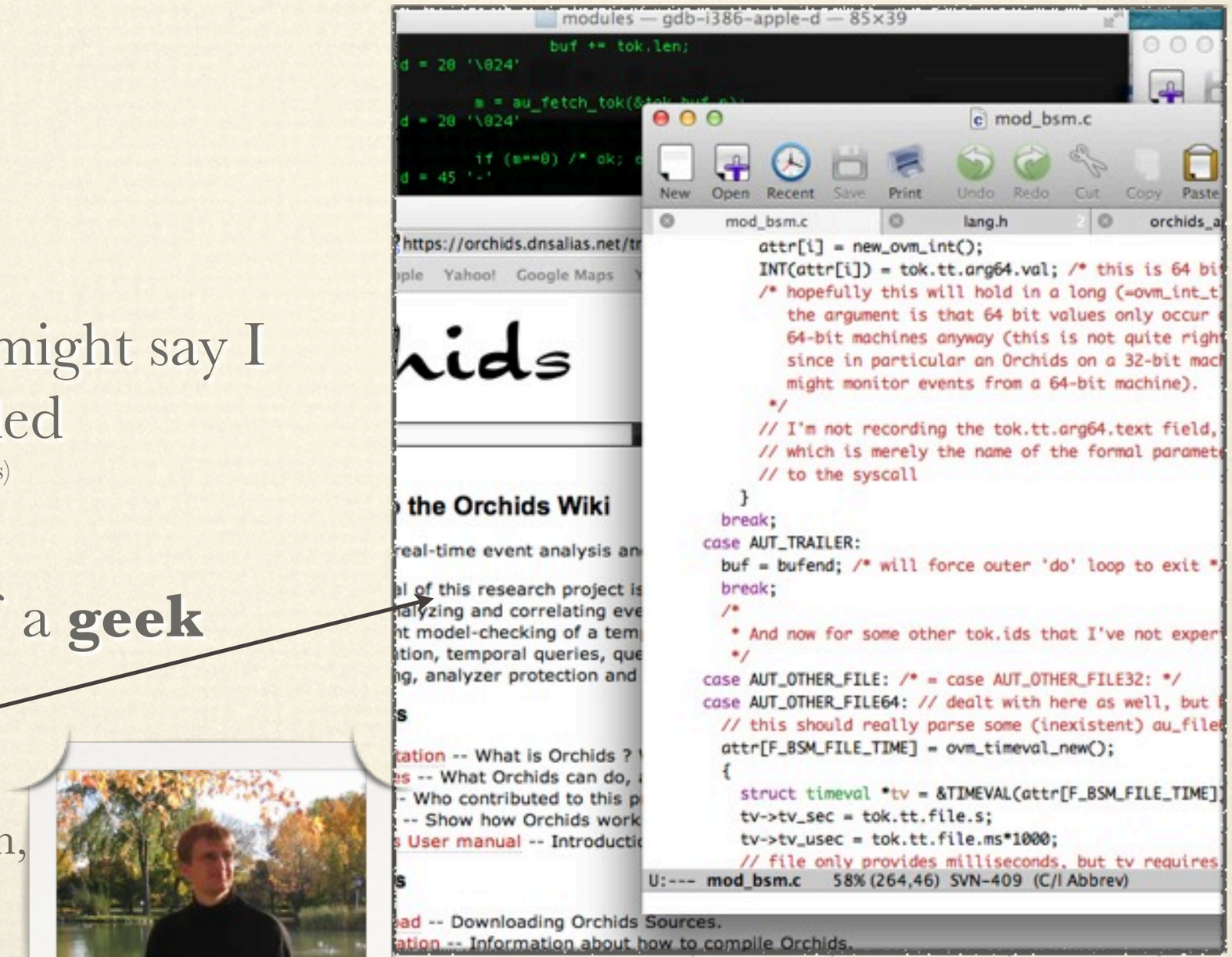
The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)

- I still am sort of a **geek**

orchids

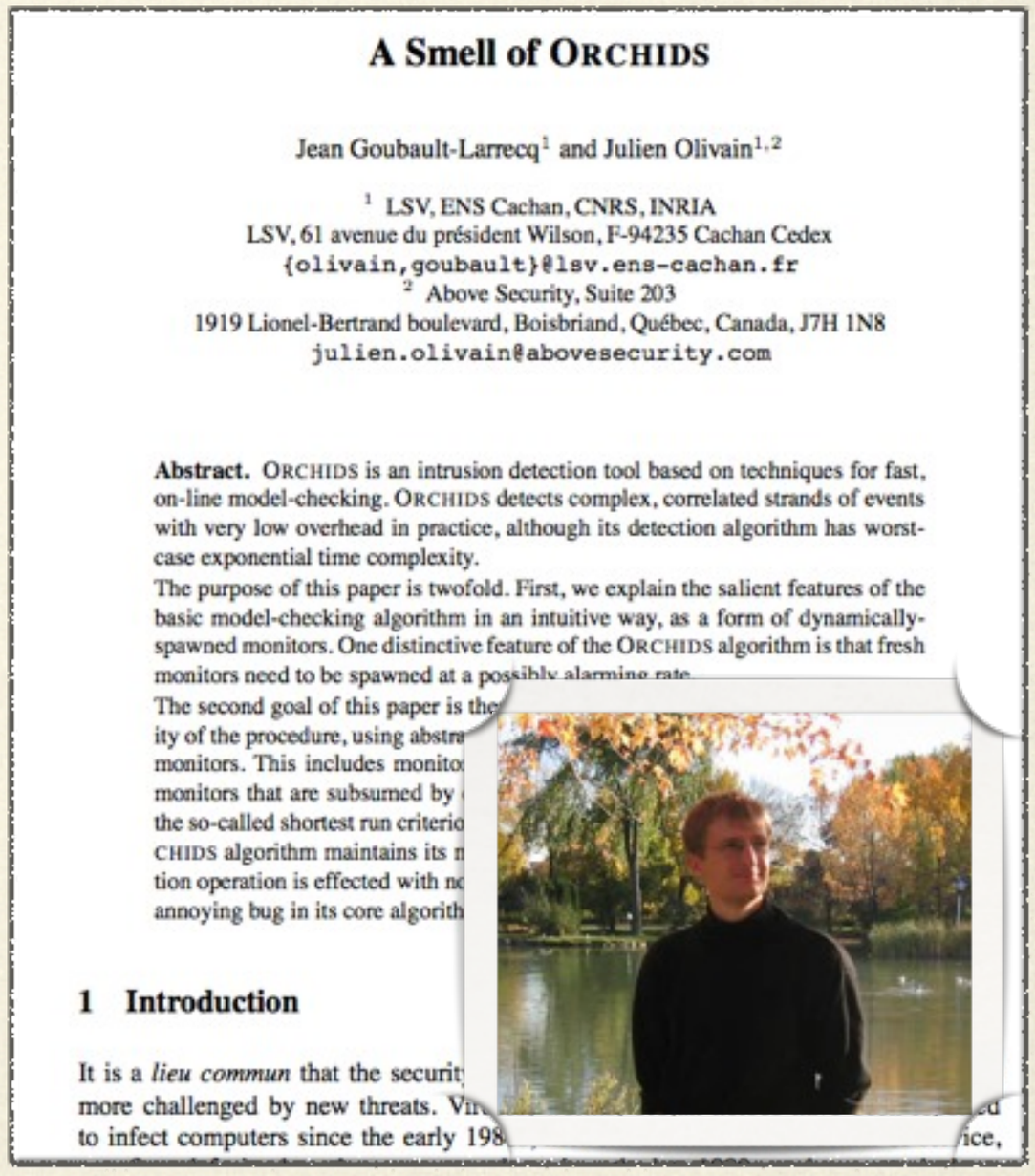
our intrusion detection system, with **Julien Olivain**



The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in **security**

(here, intrusion detection—related to previous code snippet)



A Smell of ORCHIDS

Jean Goubault-Larrecq[1] and Julien Olivain[1,2]

[1] LSV, ENS Cachan, CNRS, INRIA
LSV, 61 avenue du président Wilson, F-94235 Cachan Cedex
{olivain,goubault}@lsv.ens-cachan.fr
[2] Above Security, Suite 203
1919 Lionel-Bertrand boulevard, Boisbriand, Québec, Canada, J7H 1N8
julien.olivain@abovesecurity.com

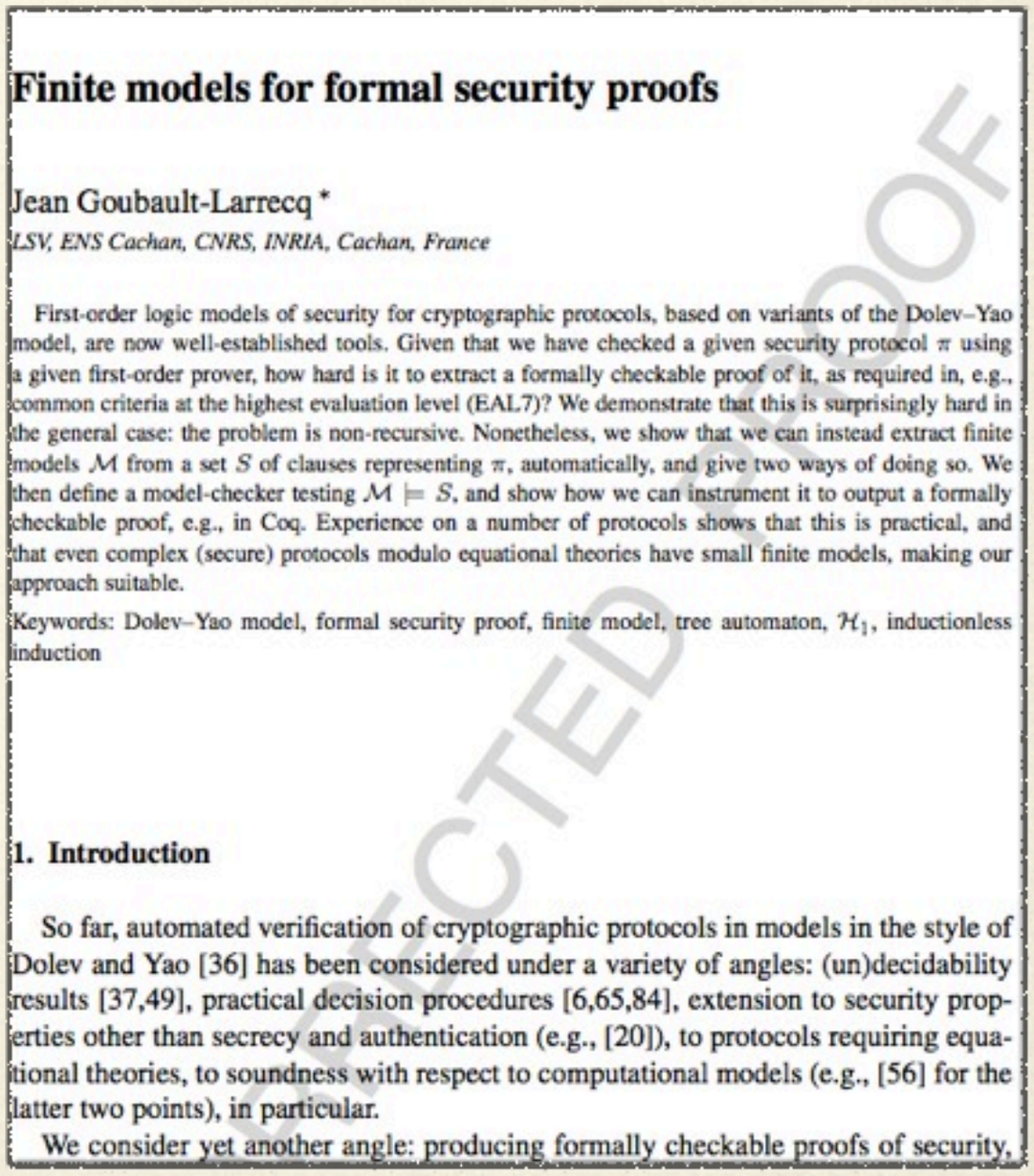
Abstract. ORCHIDS is an intrusion detection tool based on techniques for fast, on-line model-checking. ORCHIDS detects complex, correlated strands of events with very low overhead in practice, although its detection algorithm has worst-case exponential time complexity.
The purpose of this paper is twofold. First, we explain the salient features of the basic model-checking algorithm in an intuitive way, as a form of dynamically-spawned monitors. One distinctive feature of the ORCHIDS algorithm is that fresh monitors need to be spawned at a possibly alarming rate.
The second goal of this paper is the
ity of the procedure, using abstra
monitors. This includes monito
monitors that are subsumed by
the so-called shortest run criterio
CHIDS algorithm maintains its n
tion operation is effected with n
annoying bug in its core algorith

1 Introduction

It is a *lieu commun* that the securit
more challenged by new threats. Vi
to infect computers since the early 198

The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in security using **automated deduction**



Finite models for formal security proofs

Jean Goubault-Larrecq *
LSV, ENS Cachan, CNRS, INRIA, Cachan, France

First-order logic models of security for cryptographic protocols, based on variants of the Dolev–Yao model, are now well-established tools. Given that we have checked a given security protocol π using a given first-order prover, how hard is it to extract a formally checkable proof of it, as required in, e.g., common criteria at the highest evaluation level (EAL7)? We demonstrate that this is surprisingly hard in the general case: the problem is non-recursive. Nonetheless, we show that we can instead extract finite models $\mathcal{M}$ from a set S of clauses representing π, automatically, and give two ways of doing so. We then define a model-checker testing $\mathcal{M} \models S$, and show how we can instrument it to output a formally checkable proof, e.g., in Coq. Experience on a number of protocols shows that this is practical, and that even complex (secure) protocols modulo equational theories have small finite models, making our approach suitable.

Keywords: Dolev–Yao model, formal security proof, finite model, tree automaton, $\mathcal{H}_1$, inductionless induction

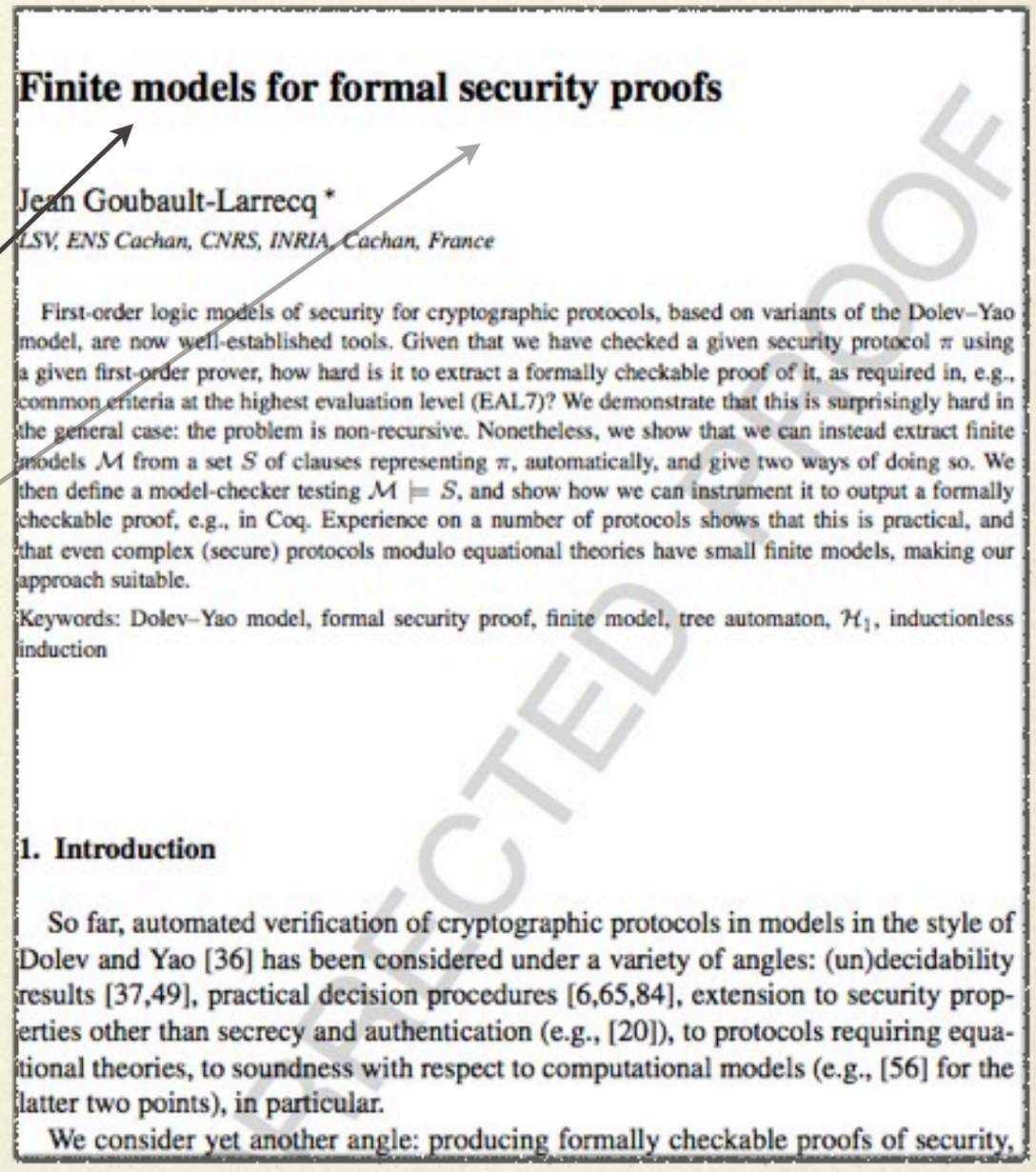
1. Introduction

So far, automated verification of cryptographic protocols in models in the style of Dolev and Yao [36] has been considered under a variety of angles: (un)decidability results [37,49], practical decision procedures [6,65,84], extension to security properties other than secrecy and authentication (e.g., [20]), to protocols requiring equational theories, to soundness with respect to computational models (e.g., [56] for the latter two points), in particular.

We consider yet another angle: producing formally checkable proofs of security,

The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in security using **automated deduction**



Finite models for formal security proofs

Jean Goubault-Larrecq *
LSV, ENS Cachan, CNRS, INRIA, Cachan, France

First-order logic models of security for cryptographic protocols, based on variants of the Dolev–Yao model, are now well-established tools. Given that we have checked a given security protocol π using a given first-order prover, how hard is it to extract a formally checkable proof of it, as required in, e.g., common criteria at the highest evaluation level (EAL7)? We demonstrate that this is surprisingly hard in the general case: the problem is non-recursive. Nonetheless, we show that we can instead extract finite models $\mathcal{M}$ from a set S of clauses representing π, automatically, and give two ways of doing so. We then define a model-checker testing $\mathcal{M} \models S$, and show how we can instrument it to output a formally checkable proof, e.g., in Coq. Experience on a number of protocols shows that this is practical, and that even complex (secure) protocols modulo equational theories have small finite models, making our approach suitable.

Keywords: Dolev–Yao model, formal security proof, finite model, tree automaton, $\mathcal{H}_1$, inductionless induction

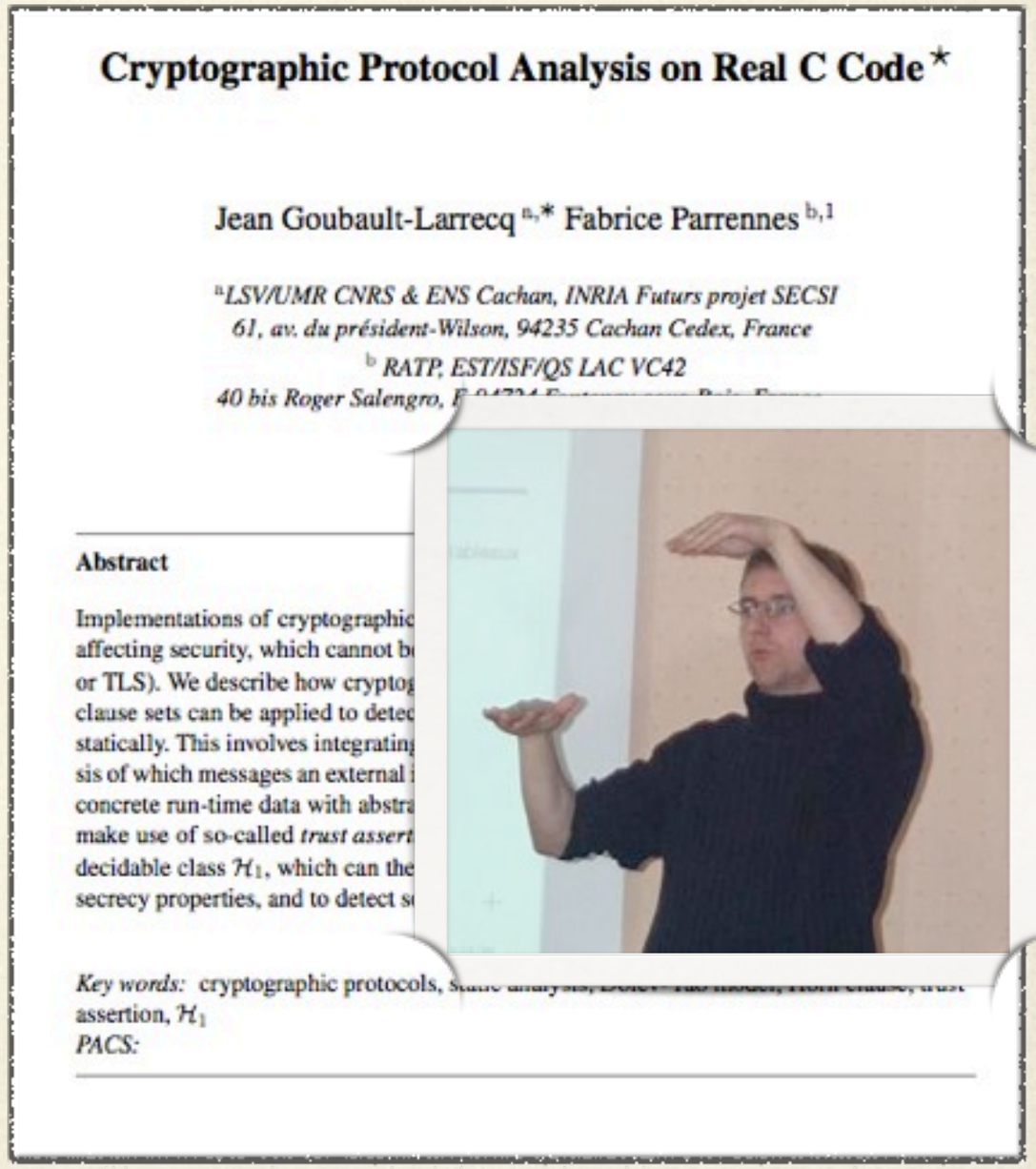
1. Introduction

So far, automated verification of cryptographic protocols in models in the style of Dolev and Yao [36] has been considered under a variety of angles: (un)decidability results [37,49], practical decision procedures [6,65,84], extension to security properties other than secrecy and authentication (e.g., [20]), to protocols requiring equational theories, to soundness with respect to computational models (e.g., [56] for the latter two points), in particular.

We consider yet another angle: producing formally checkable proofs of security,

The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in security, using automated deduction and **static analysis**



Cryptographic Protocol Analysis on Real C Code ⋆

Jean Goubault-Larrecq [a,*] Fabrice Parrennes [b,1]

[a] *LSV/UMR CNRS & ENS Cachan, INRIA Futurs projet SECSI*
61, av. du président-Wilson, 94235 Cachan Cedex, France
[b] *RATP, EST/ISF/QS LAC VC42*
40 bis Roger Salengro,

Abstract

Implementations of cryptographic
affecting security, which cannot b
or TLS). We describe how cryptog
clause sets can be applied to detec
statically. This involves integratin
sis of which messages an external
concrete run-time data with abstra
make use of so-called *trust assert*
decidable class $\mathcal{H}_1$, which can the
secrecy properties, and to detect s

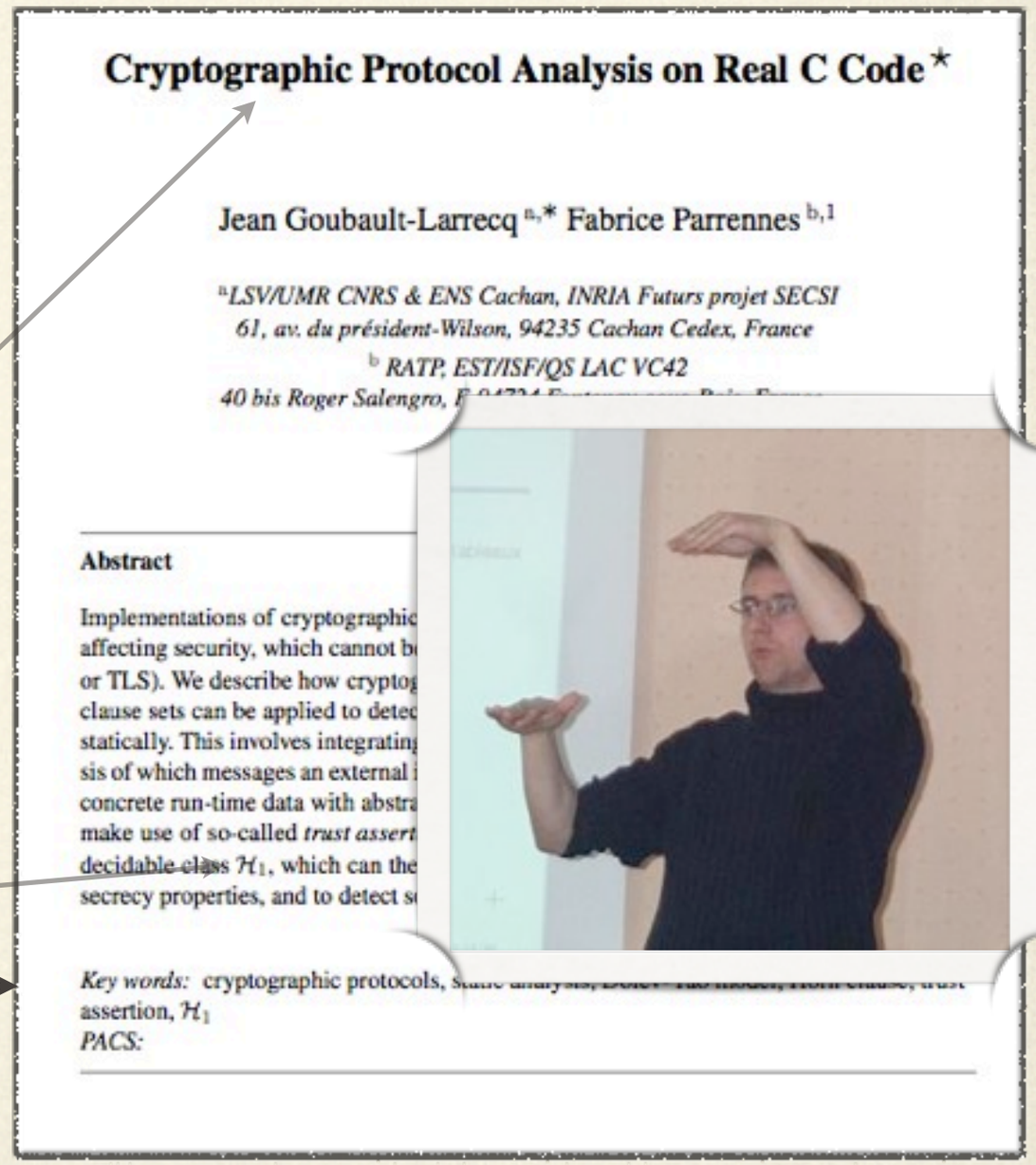
Key words: cryptographic protocols,
assertion, $\mathcal{H}_1$
PACS:

The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)

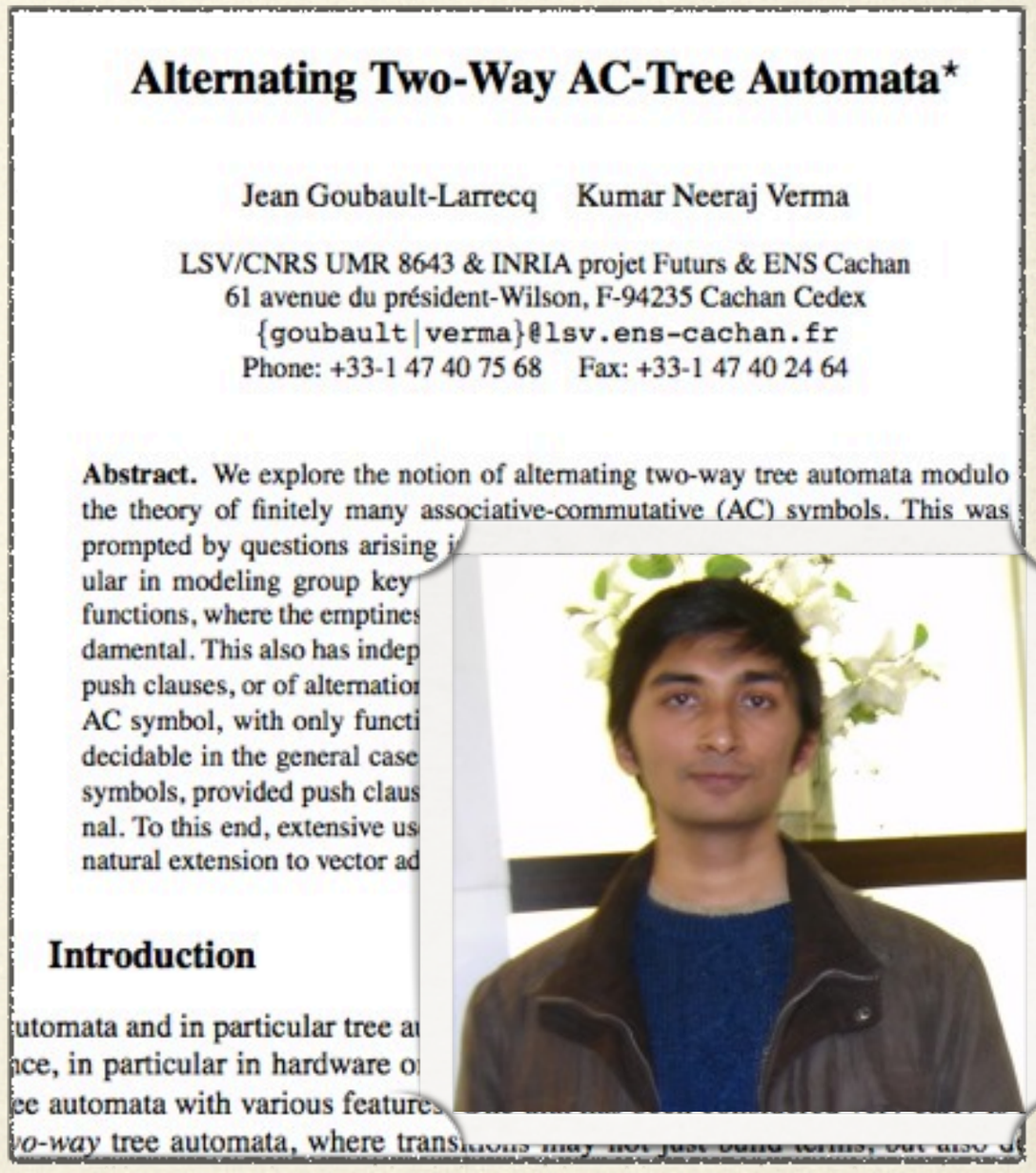
- I still am sort of a geek

- I'm a computer scientist working in security, using automated deduction and **static analysis**



The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in security and automated deduction, and **tree automata**



Alternating Two-Way AC-Tree Automata*

Jean Goubault-Larrecq Kumar Neeraj Verma

LSV/CNRS UMR 8643 & INRIA projet Futurs & ENS Cachan
61 avenue du président-Wilson, F-94235 Cachan Cedex
{goubault|verma}@lsv.ens-cachan.fr
Phone: +33-1 47 40 75 68 Fax: +33-1 47 40 24 64

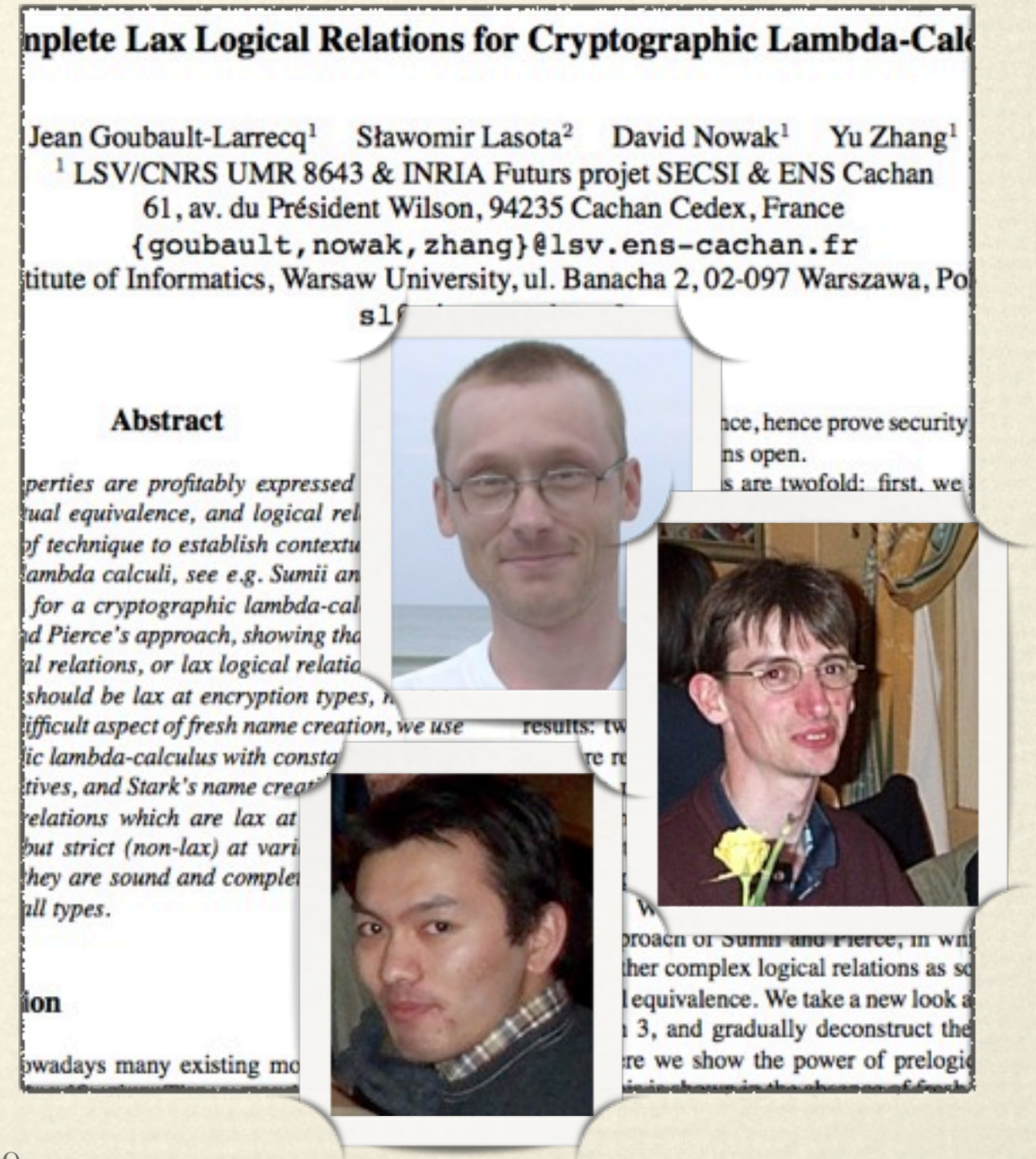
Abstract. We explore the notion of alternating two-way tree automata modulo the theory of finitely many associative-commutative (AC) symbols. This was prompted by questions arising i
ular in modeling group key
functions, where the emptines
damental. This also has indep
push clauses, or of alternatio
AC symbol, with only functi
decidable in the general case
symbols, provided push claus
nal. To this end, extensive us
natural extension to vector ad

Introduction

utomata and in particular tree a
nce, in particular in hardware o
ee automata with various feature
o-way tree automata, where trans

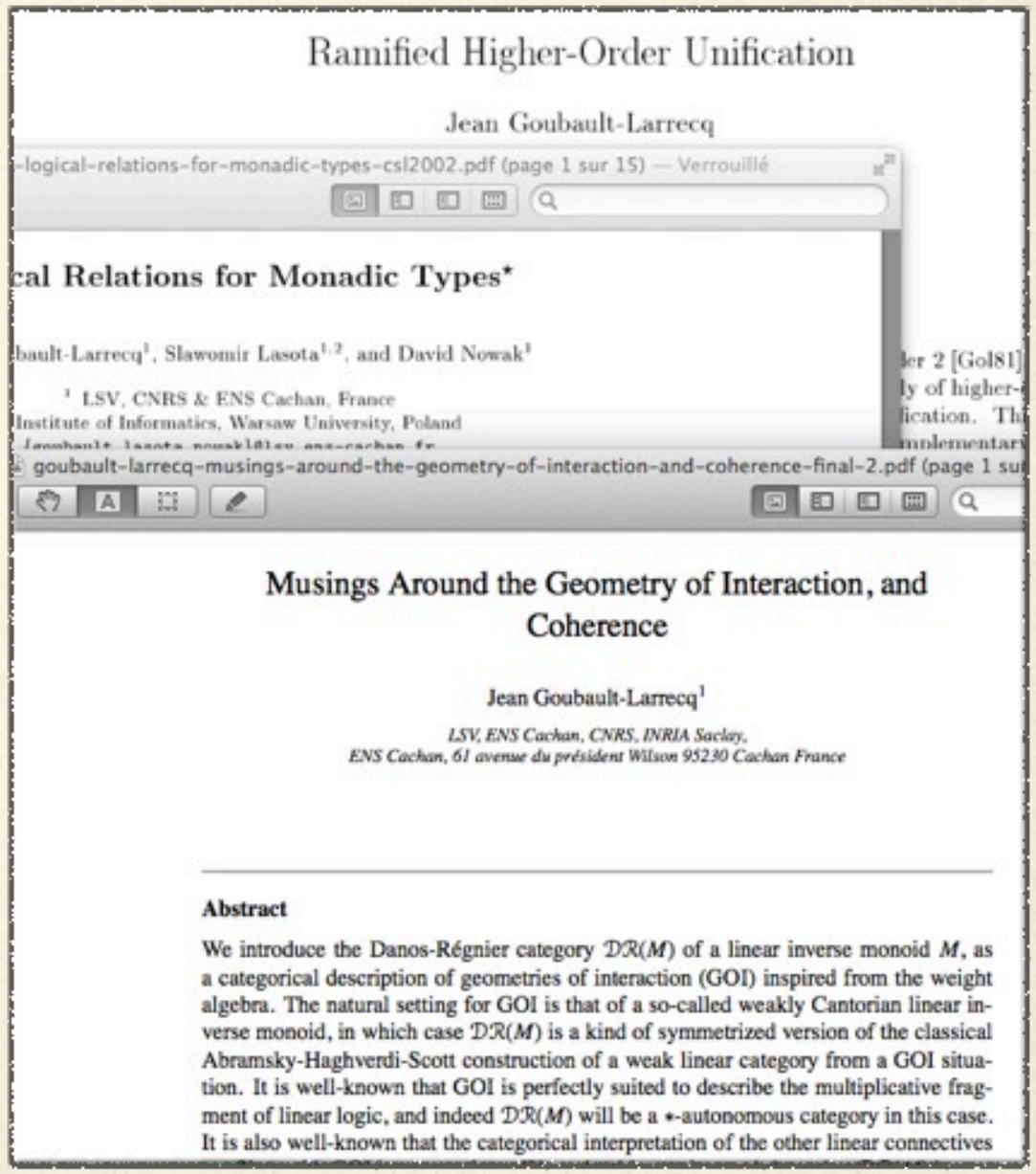
The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in **security**, automated deduction, tree automata, **logic**



The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in security, automated deduction, tree automata, **logic**



Ramified Higher-Order Unification

Jean Goubault-Larrecq

-logical-relations-for-monadic-types-csl2002.pdf (page 1 sur 15) — Verrouillé

cal Relations for Monadic Types*

bault-Larrecq[1], Slawomir Lasota[1,2], and David Nowak[1]

[1] LSV, CNRS & ENS Cachan, France
Institute of Informatics, Warsaw University, Poland

goubault-larrecq-musings-around-the-geometry-of-interaction-and-coherence-final-2.pdf (page 1 su

Musings Around the Geometry of Interaction, and Coherence

Jean Goubault-Larrecq[1]

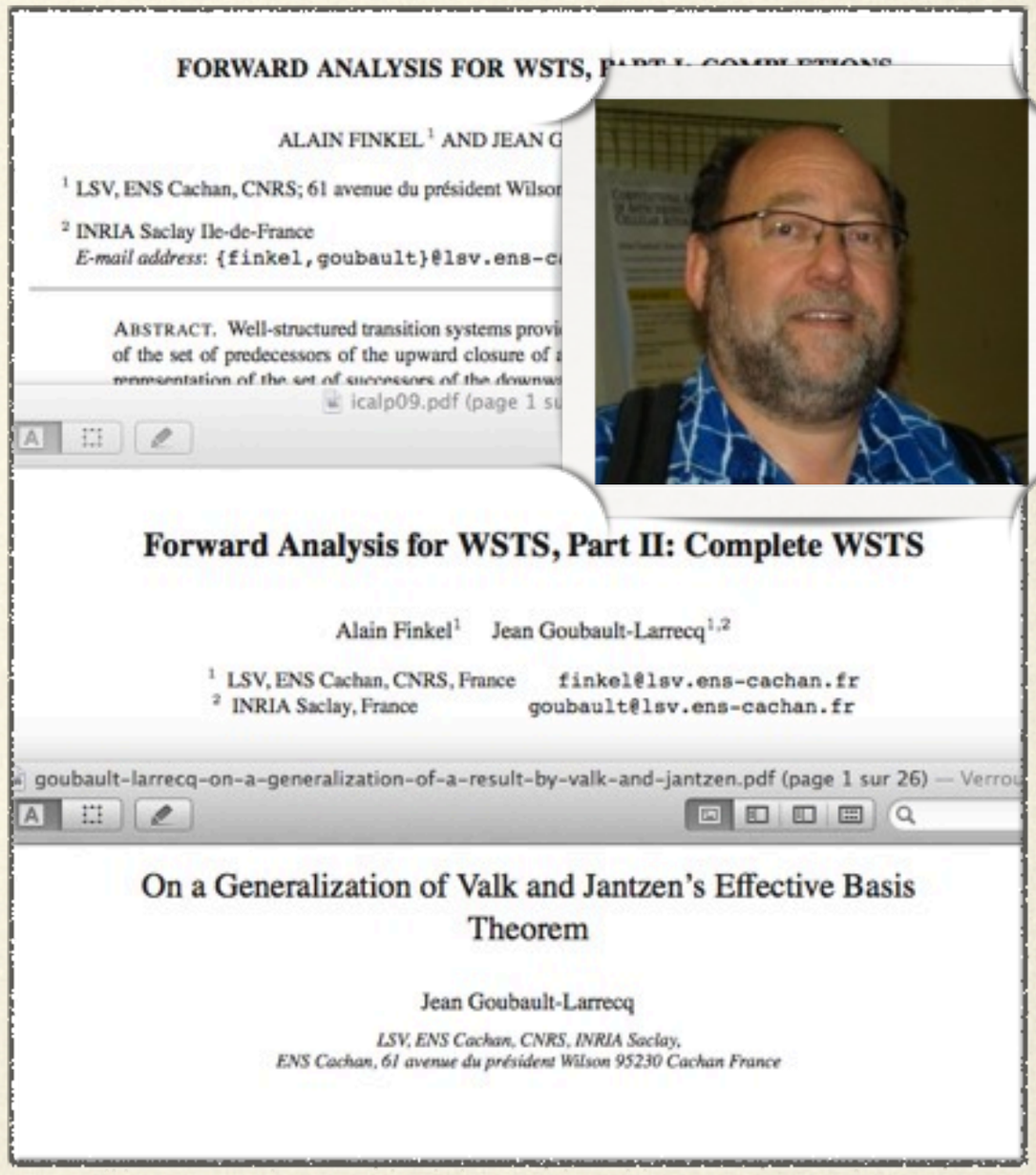
LSV, ENS Cachan, CNRS, INRIA Saclay,
ENS Cachan, 61 avenue du président Wilson 94230 Cachan France

Abstract

We introduce the Danos-Régnier category $\mathcal{DR}(M)$ of a linear inverse monoid M, as a categorical description of geometries of interaction (GOI) inspired from the weight algebra. The natural setting for GOI is that of a so-called weakly Cantorian linear inverse monoid, in which case $\mathcal{DR}(M)$ is a kind of symmetrized version of the classical Abramsky-Haghverdi-Scott construction of a weak linear category from a GOI situation. It is well-known that GOI is perfectly suited to describe the multiplicative fragment of linear logic, and indeed $\mathcal{DR}(M)$ will be a $*$-autonomous category in this case. It is also well-known that the categorical interpretation of the other linear connectives

The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in security, automated deduction, tree automata, logic, **verification**

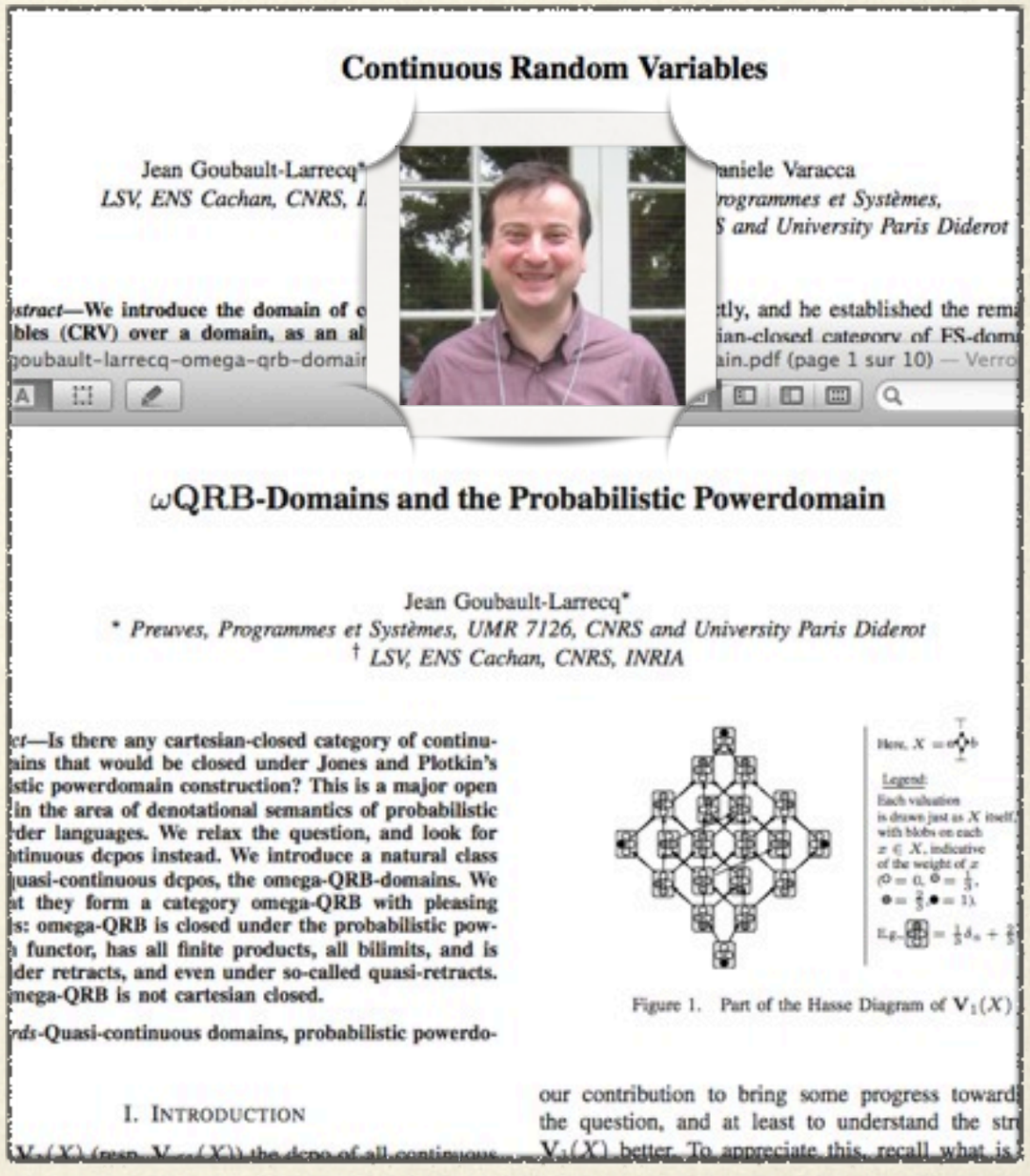


The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)

- I still am sort of a geek

- I'm a computer scientist working in security, automated deduction, tree automata, logic, verification, **semantics**



Continuous Random Variables

Jean Goubault-Larrecq*
LSV, ENS Cachan, CNRS, I

aniele Varacca
rogrammes et Systèmes,
S and University Paris Diderot

stract—We introduce the domain of c
bles (CRV) over a domain, as an al
goubault-larrecq-omega-qrb-domai

tly, and he established the rema
ian-closed category of FS-dom
ain.pdf (page 1 sur 10) — Verro

ωQRB-Domains and the Probabilistic Powerdomain

Jean Goubault-Larrecq*
* *Preuves, Programmes et Systèmes, UMR 7126, CNRS and University Paris Diderot*
† *LSV, ENS Cachan, CNRS, INRIA*

ct—Is there any cartesian-closed category of continu-
ains that would be closed under Jones and Plotkin's
stic powerdomain construction? This is a major open
in the area of denotational semantics of probabilistic
der languages. We relax the question, and look for
tinuous dcpos instead. We introduce a natural class
uasi-continuous dcpos, the omega-QRB-domains. We
t they form a category omega-QRB with pleasing
s: omega-QRB is closed under the probabilistic pow-
functor, has all finite products, all bilimits, and is
der retracts, and even under so-called quasi-retracts.
mega-QRB is not cartesian closed.

rds-Quasi-continuous domains, probabilistic powerdo-

Here, $X =$

Legend:
Each valuation is drawn just as X itself, with blobs on each $x \in X$, indicative of the weight of x ($\circ = 0$, $\bullet = \frac{1}{3}$, $\bullet = \frac{2}{3}$, $\bullet = 1$).

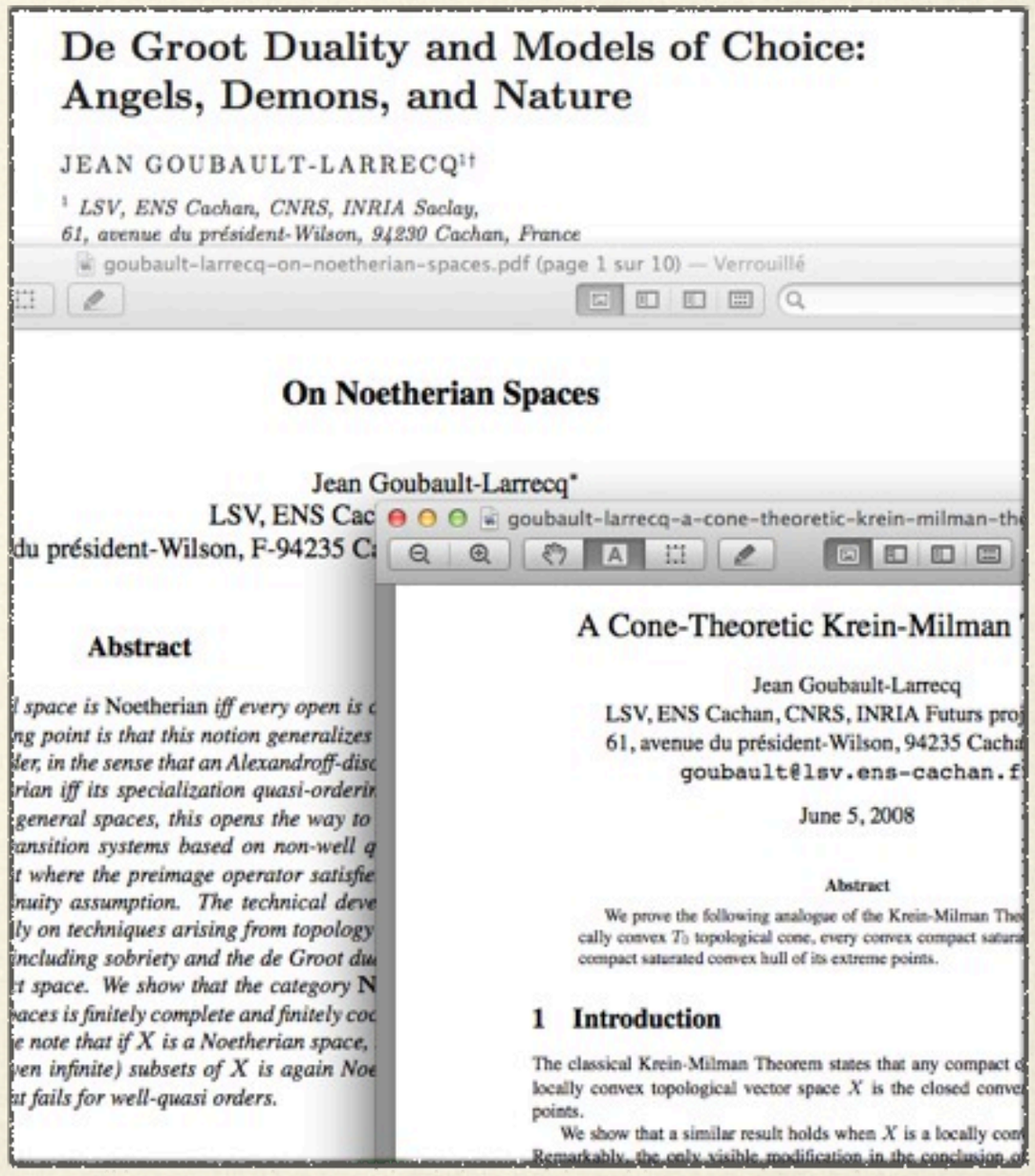
Figure 1. Part of the Hasse Diagram of $\mathbf{V}_1(X)$

I. Introduction

our contribution to bring some progress toward
the question, and at least to understand the str
$\mathbf{V}_1(X)$ better. To appreciate this, recall what is

The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)
- I still am sort of a geek
- I'm a computer scientist working in security, automated deduction, tree automata, logic, verification, semantics, **topology**

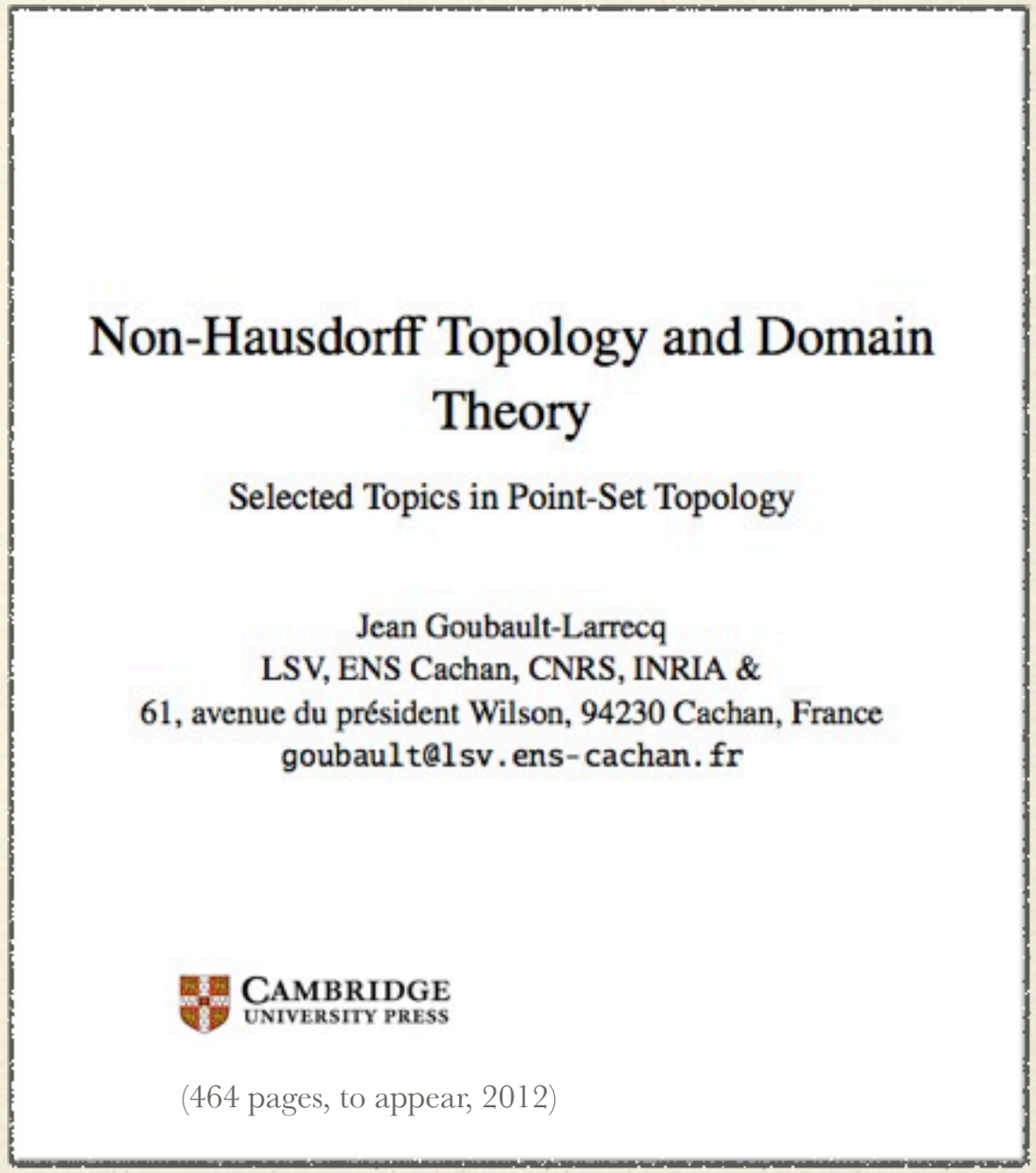


The real me

- At age 46, one might say I am still undecided
  (although I have given up on physics)

- I still am sort of a geek

- I'm a computer scientist working in security, automated deduction, tree automata, logic, verification, semantics, **topology**


Non-Hausdorff Topology and Domain Theory

Selected Topics in Point-Set Topology

Jean Goubault-Larrecq
LSV, ENS Cachan, CNRS, INRIA &
61, avenue du président Wilson, 94230 Cachan, France
goubault@lsv.ens-cachan.fr

CAMBRIDGE UNIVERSITY PRESS

(464 pages, to appear, 2012)

Thanks!

- to all who have supported me throughout the years

- starting with **Dominique Bolignano**, to whom I owe much

Thanks!

- to all of you who have supported me throughout the years, in particular:

Thanks!

- to all of you who have supported me throughout the years, in particular:
  - My students
  - My coauthors
  - And everybody at LSV.