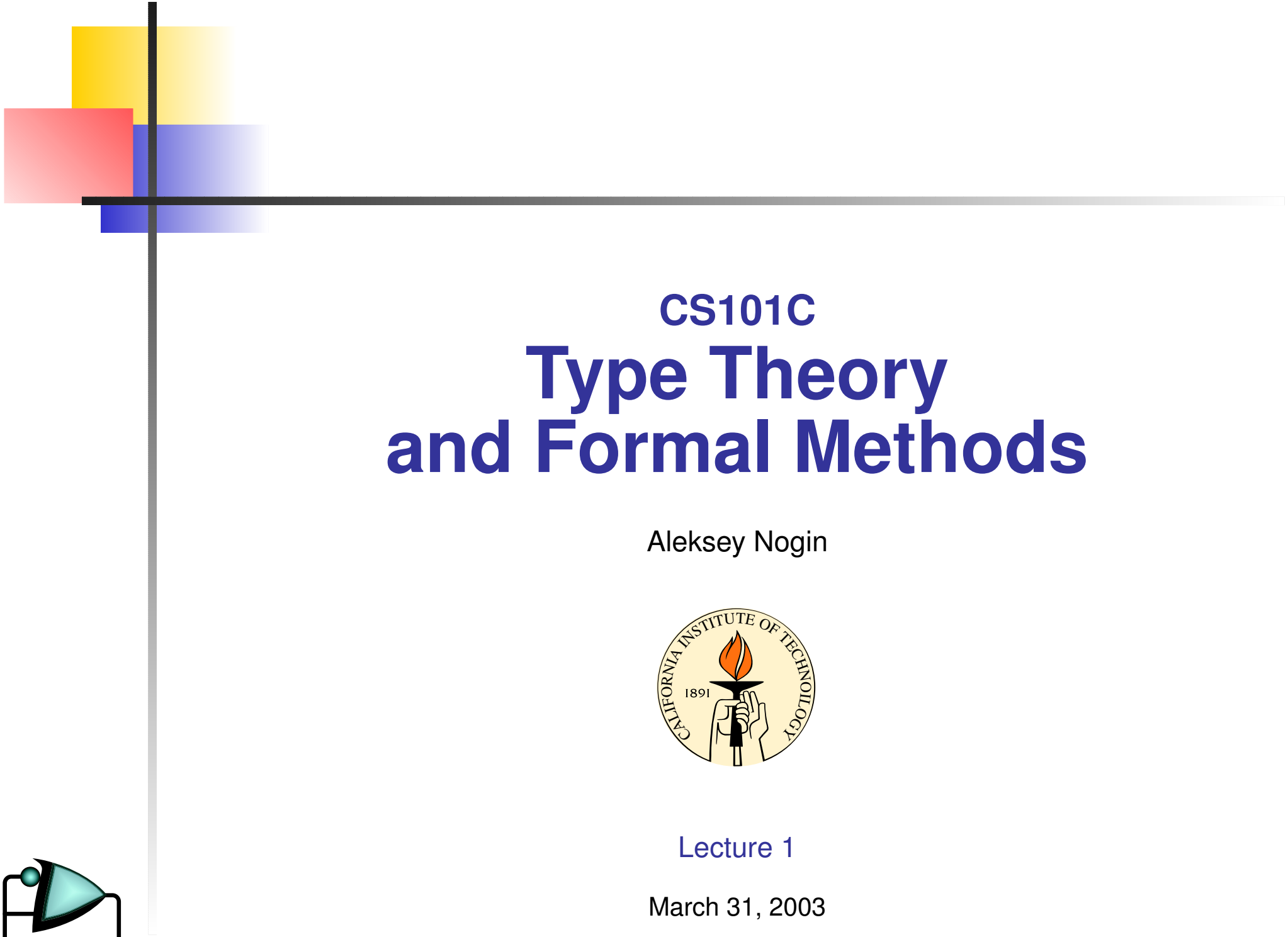


CS101C
Type Theory and Formal Methods

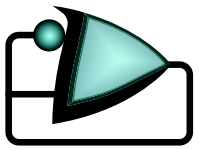
Aleksey Nogin

Lecture 1

March 31, 2003

Quick Information

Time:	MW 14:00 – 14:55
Place:	Jorgensen 74
Instructor:	Aleksey Nogin
TA:	Xin Yu
Office Hours:	TBA
Units:	9 (2+3+4), pass/fail or letter grade
Grading:	Homeworks (possibly final project)
Course Home Page:	http://nogin.org/cs101c/
Admin email:	cs101-admin@metaprl.org
Mailing list:	cs101-class@metaprl.org



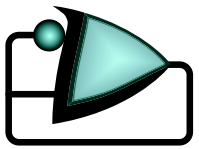
Formal Methods

Formal Methods is a science of mathematically describing and reasoning about computer-based systems (including hardware and software).

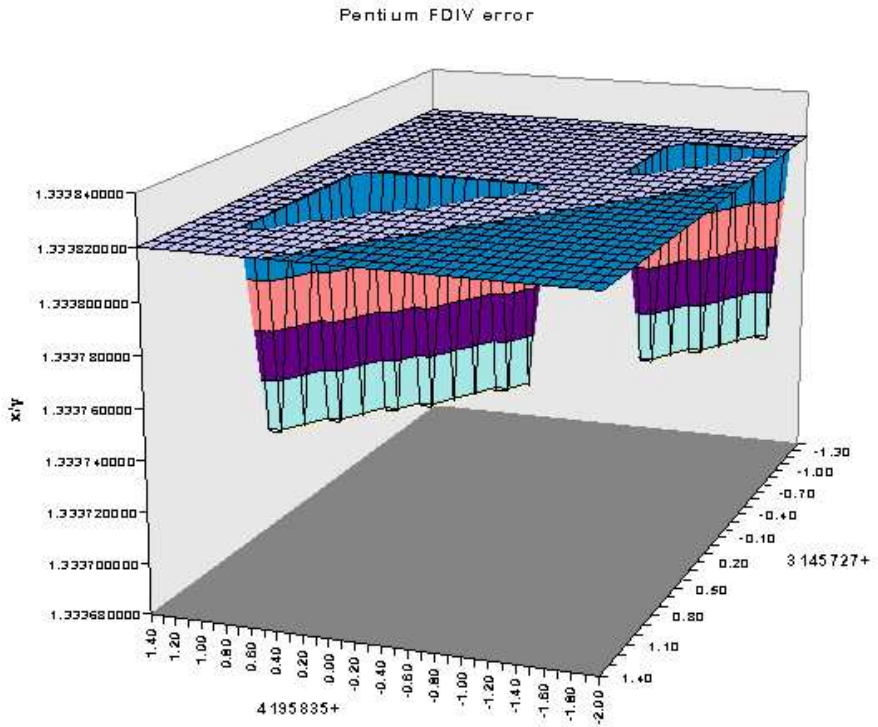
Formal Methods help in the reduction of errors introduced into a system, particularly at the earlier stages of design.

(From WWW Virtual Library — http://www.afm.sbu.ac.uk/)

This course will focus on Logic and Computer-Aided Reasoning sides of Formal Methods.



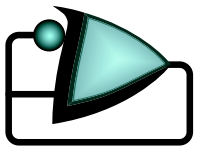
Pentium `FDIV` Bug



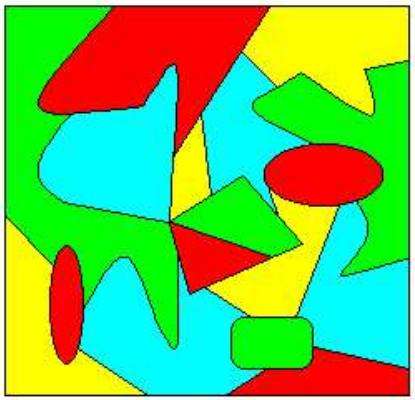
One of the most famous and most expensive bugs.

Pentium `FDIV` Bug (1994) cost Intel $475,000,000.

It highlighted the need for formal verification.



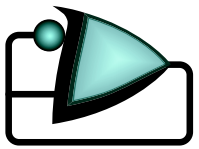
Four Color Theorem



The first proof of the Four Color Theorem (Appel and Haken, 1976) involved two programs and about 1200 hours (50 days) of CPU time.

Many mathematicians were at first very skeptical about the proof.

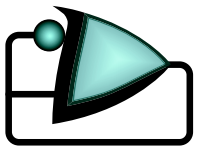
It turned out that one of the programs had a small bug (but a conservative one).



Formal Methods

Formal Methods are widely used in:

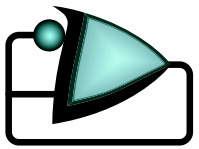
- Hardware verification: Intel, Motorola, AMD, HP, *etc*. Verifying floating point units is especially popular.
- Software verification: Microsoft, NASA, *etc*.
- Formal mathematics
- Education
- Other areas



Potential of Formal Methods

While the impact of formal methods is often limited, they have a great potential — far beyond what is possible today.

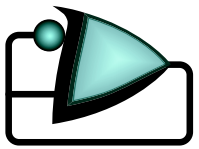
- Hardware: ability to handle whole chips, not just individual units.
- Software: ability to handle large programs with complex structure.
- Formal tools: accessible to ordinary engineers, not just those with a PhD.



Focusing on Understanding

- Currently most of the applications of formal methods focus on correctness (and sometimes on debugging).
- However a bigger value of formal methods is in being able to better understand the artifacts (uncover hidden assumptions, *etc*) we are working with and in using this knowledge during design and development.

- Example: Ensemble verification project at Cornell.



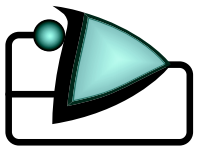
Proofs

What is a proof?

Proof is a sequence of *statements*, where each one is either an *axiom* or follows from previous statements in the proof using a *rule of inference*.

Example

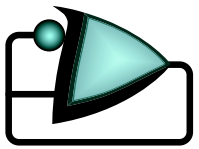
1. Socrates is a human (AXIOM).
2. All humans are mortal (AXIOM).
3. Socrates is mortal (FOLLOWS FROM (1) AND (2)).



Language of Propositional Logic

$\top$	"True"
$\bot$	"False"
$A, B, C \ldots$	variables
$A \vee B$	"A or B"
$A \wedge B$	"A and B"
$A \Rightarrow B$	"A implies B"
$\neg A$	"not A"

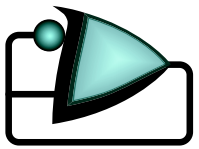
In classical logic, each variable (and each formula) always stands for either True or False.



Sequents

A sequent "$A_1;\ A_2;\ \ldots;\ A_n \vdash C$ stands for "If all the hypotheses $A_1,\ A_2,\ \ldots,\ A_n$ are true, then the conclusion C must be true as well."

We will use Greek letters $\Gamma,\ \Delta,\ \ldots$ to denote arbitrary sequences of hypotheses (e.g. $\Gamma \vdash C$).

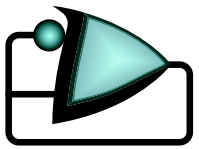


Inference Rules for Classical Logic – I

$$\frac{}{\Gamma;\ A;\ \Delta \vdash A}\ (\mathit{Axiom})$$

$$\frac{\Gamma;\ A;\ A;\ \Delta \vdash C}{\Gamma;\ A;\ \Delta \vdash C}\ (\mathit{Copy}) \qquad \frac{\Gamma;\ \Delta \vdash C}{\Gamma;\ A;\ \Delta \vdash C}\ (\mathit{Weakening})$$

$$\frac{}{\Gamma \vdash \top}\ (\mathit{True\text{-}intro}) \qquad \frac{}{\Gamma;\ \bot;\ \Delta \vdash C}\ (\mathit{False\text{-}elim})$$



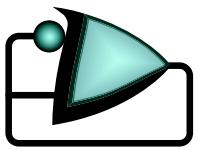
Inference Rules for Classical Logic – II

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\textit{Or-intro-1}) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\textit{Or-intro-2})$$

$$\frac{\Gamma;\ A;\ \Delta \vdash C \quad \Gamma;\ B;\ \Delta \vdash C}{\Gamma;\ A \vee B;\ \Delta \vdash C}\ (\textit{Or-elim})$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\textit{And-intro}) \qquad \frac{\Gamma;\ A;\ B;\ \Delta \vdash C}{\Gamma;\ A \wedge B;\ \Delta \vdash C}\ (\textit{And-elim})$$

$$\frac{\Gamma;\ A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\textit{Imp-intro}) \qquad \frac{\Gamma;\ \Delta \vdash A \quad \Gamma;\ B;\ \Delta \vdash C}{\Gamma;\ A \Rightarrow B;\ \Delta \vdash C}\ (\textit{Imp-elim})$$

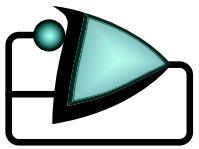


Inference Rules for Classical Logic – III

$$\frac{\Gamma;\ A \vdash \bot}{\Gamma \vdash \neg A}\ (\textit{Not-intro}) \qquad \frac{\Gamma;\ \Delta \vdash A}{\Gamma;\ \neg A;\ \Delta \vdash C}\ (\textit{Not-elim})$$

$$\frac{\Gamma;\ \neg A \vdash \bot}{\Gamma \vdash A}\ (\textit{Proof by contradiction})$$

$$\frac{\Gamma;\ \Delta;\ \Gamma';\ \Delta' \vdash C}{\Gamma;\ \Gamma';\ \Delta;\ \Delta' \vdash C}\ (\textit{Swap})$$



Inference Rules for Classical Logic – All

$$\frac{}{\Gamma;\ A;\ \Delta \vdash A}\ (\textit{Axiom}) \qquad \frac{\Gamma;\ A;\ A;\ \Delta \vdash C}{\Gamma;\ A;\ \Delta \vdash C}\ (\textit{Copy}) \qquad \frac{\Gamma;\ \Delta \vdash C}{\Gamma;\ A;\ \Delta \vdash C}\ (\textit{Weakening})$$

$$\frac{\Gamma;\ \Delta;\ \Gamma';\ \Delta' \vdash C}{\Gamma;\ \Gamma';\ \Delta;\ \Delta' \vdash C}\ (\textit{Swap}) \qquad \frac{}{\Gamma \vdash \top}\ (\textit{True-intro}) \qquad \frac{}{\Gamma;\ \bot;\ \Delta \vdash C}\ (\textit{False-elim})$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ (\textit{Or-intro-1}) \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ (\textit{Or-intro-2}) \qquad \frac{\Gamma;\ A;\ \Delta \vdash C \quad \Gamma;\ B;\ \Delta \vdash C}{\Gamma;\ A \vee B;\ \Delta \vdash C}\ (\textit{Or-elim})$$

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ (\textit{And-intro}) \qquad \frac{\Gamma;\ A;\ B;\ \Delta \vdash C}{\Gamma;\ A \wedge B;\ \Delta \vdash C}\ (\textit{And-elim})$$

$$\frac{\Gamma;\ A \vdash B}{\Gamma \vdash A \Rightarrow B}\ (\textit{Imp-intro}) \qquad \frac{\Gamma;\ \Delta \vdash A \quad \Gamma;\ B;\ \Delta \vdash C}{\Gamma;\ A \Rightarrow B;\ \Delta \vdash C}\ (\textit{Imp-elim})$$

$$\frac{\Gamma;\ A \vdash \bot}{\Gamma \vdash \neg A}\ (\textit{Not-intro}) \qquad \frac{\Gamma;\ \Delta \vdash A}{\Gamma;\ \neg A;\ \Delta \vdash C}\ (\textit{Not-elim}) \qquad \frac{\Gamma;\ \neg A \vdash \bot}{\Gamma \vdash A}\ (\textit{Proof by contradiction})$$