formalizing Arrow's theorem in Mizar

Freek Wiedijk

Radboud University Nijmegen

Computational Social Choice Seminar

Institute for Logic, Language & Computation

University of Amsterdam

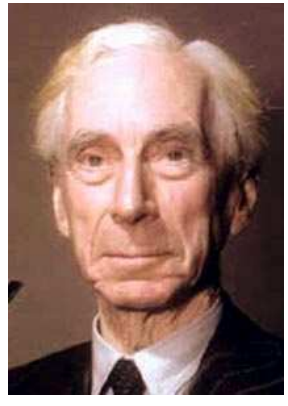
2009 03 06, 16 : 00

formalization

formalization without the computer

- Gottfried Leibniz, 1646–1716
  Calculus Ratiocinator

- Alfred North Whitehead & Bertrand Russell
  Principia Mathematica
  1910–1913



formalization with the computer

N.G. de Bruijn

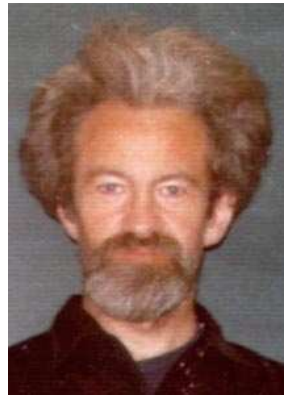
Automath

1968–1978

proof checker

proof assistant

interactive theorem prover



without the computer: formalization possible in theory

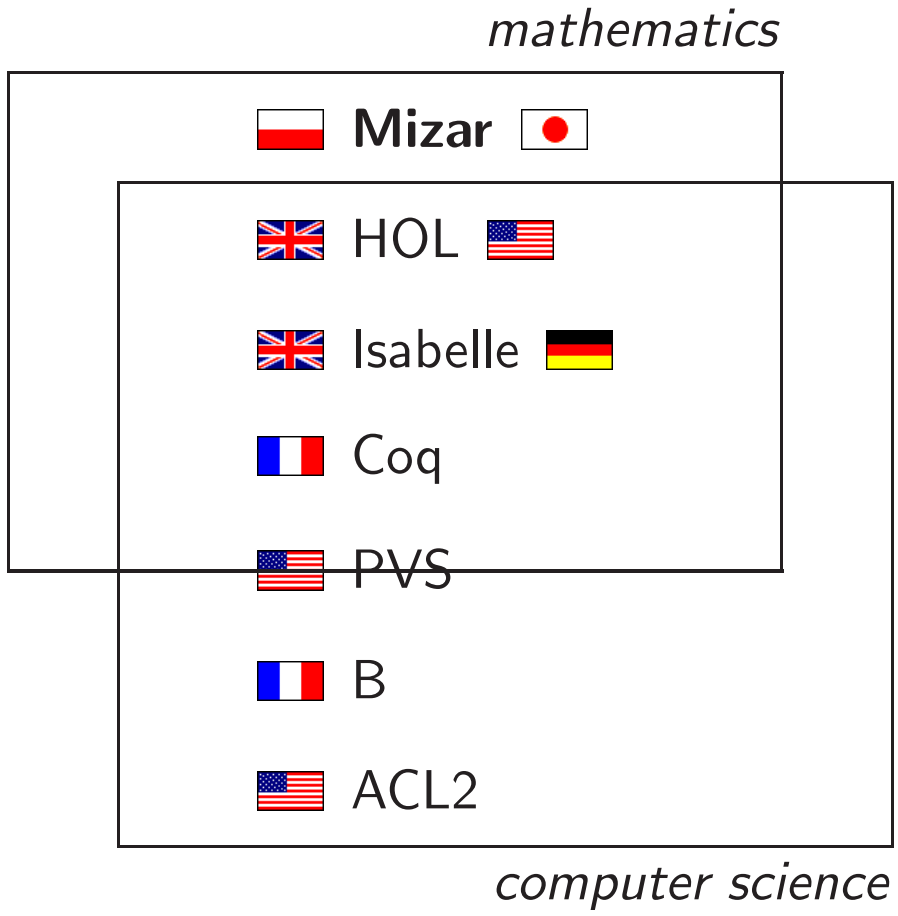
with the computer: formalization possible in practice

Bert Jutting

Checking Landau's 'Grundlagen' in the Automath system

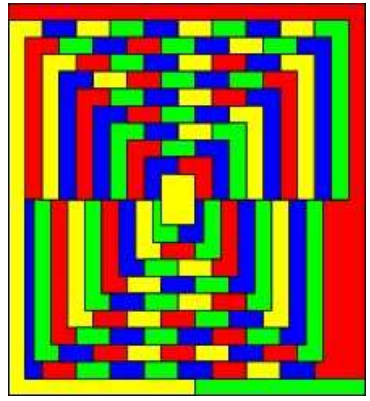
1977

main current proof assistants



landmark formalizations in mathematics

- Georges Gonthier
  INRIA & Microsoft Corporation
  four color theorem, 2004
  Coq



- John Harrison
  Cambridge University & Intel Corporation
  prime number theorem, 2008
  HOL

landmark formalizations in computer science

- Anthony Fox
  Cambridge University
  ARM processor, 1998
  HOL

- Xavier Leroy
  INRIA
  C compiler, 2006
  Coq

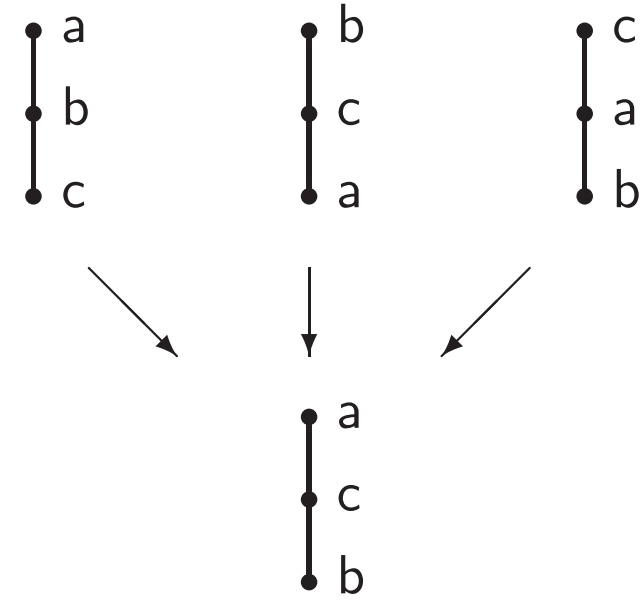
Arrow's theorem

social choice

N individuals

preferences: ranking A objects

combining individual preferences into a **social** preference



$N = 3$

$A = \{\mathsf{a}, \mathsf{b}, \mathsf{c}\}$

statement of the theorem

- **respect unanimity**
  if everyone prefers a to b, the group prefers a to b

- **independent of irrelevant alternatives**
  moving an alternative c
  does not affect the social preference between a and b

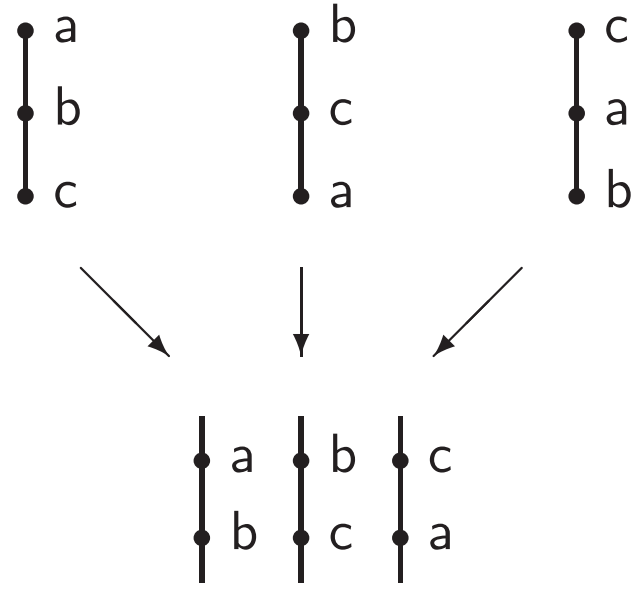
- there are at least three alternatives

this is only possible in a **dictatorship**

rule: social preference $=$ preference of a fixed individual

naive rule does not work

why not use majority voting?



not transitive!

proofs of Arrow's theorem

John Geanakoplos

Three brief proofs of Arrow's impossibility theorem

2001

paper: 4.5 pages

statement: 0.4 pages

first proof: 1.2 pages

second proof: 1 page

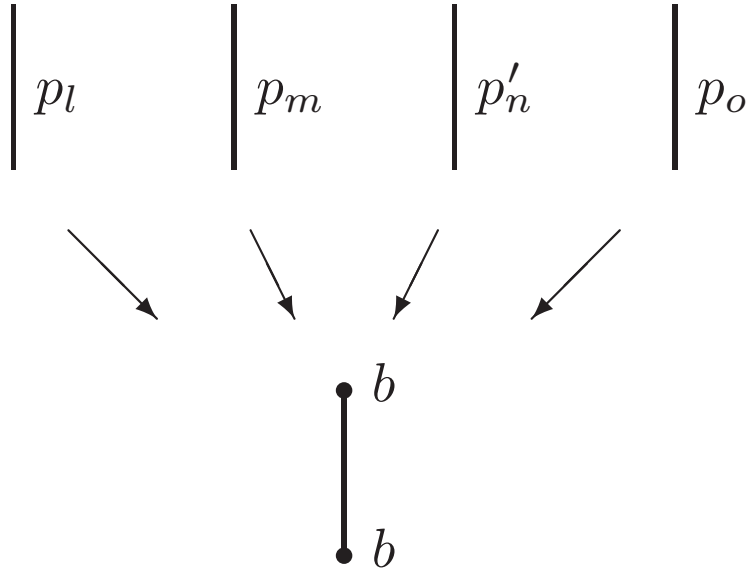
third proof: 0.8 pages

proofs get successively more abstract

first proof: pivotal voters

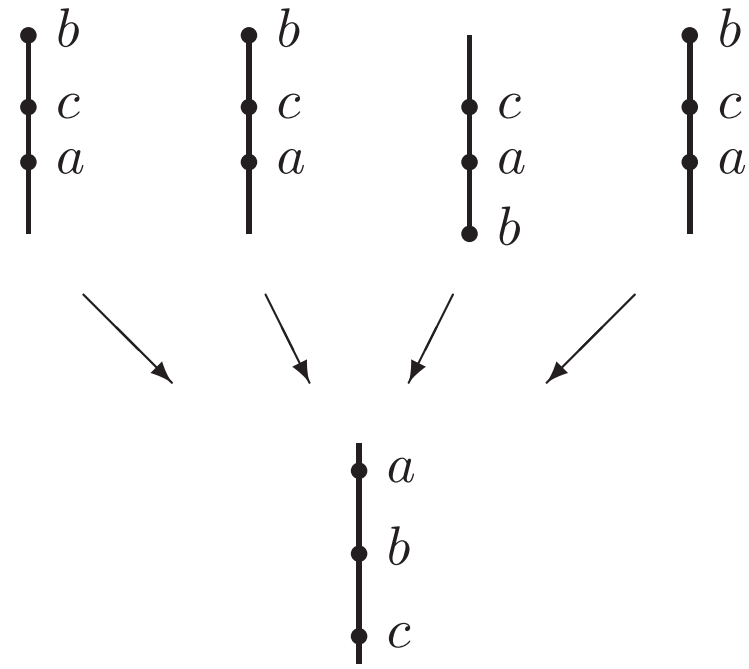
individual n is **pivotal** for alternative b $\overset{\text{def}}{\Longleftrightarrow}$

there is a situation where n can move b from the very bottom of the social preference to the very top by changing just his preference



first proof, first step: conservation of extremity

if **every** individual has an alternative b at the very top or very bottom
(not necessarily all at the same end)
then in the social preference b also is at the very top or very bottom

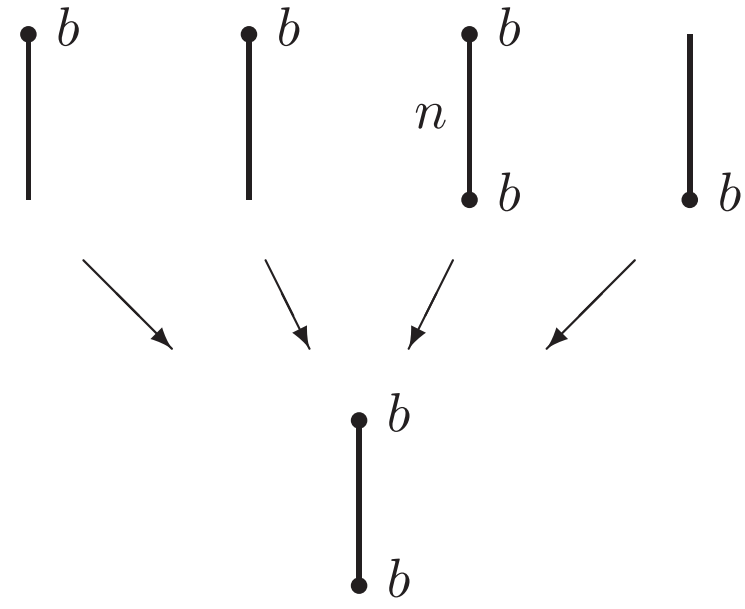


first proof, second step: finding a pivotal voter for an object

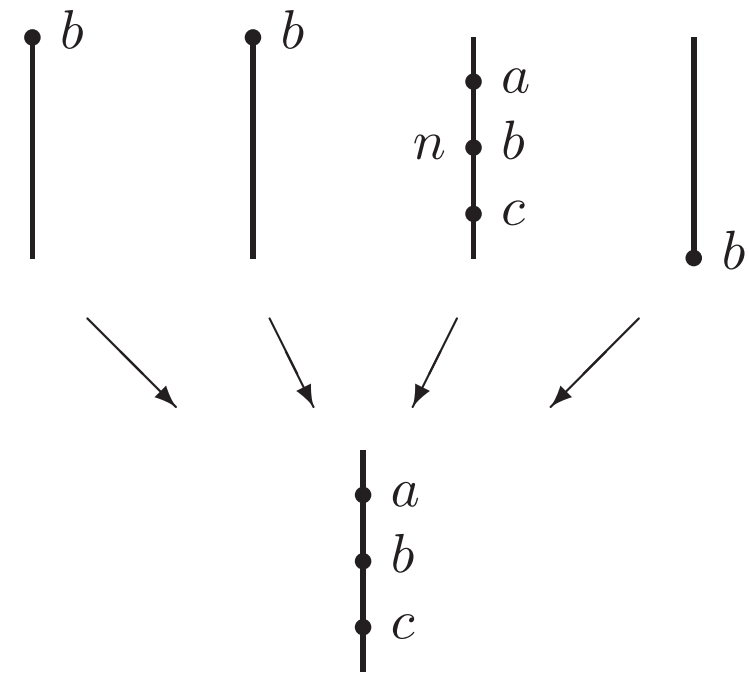
(i) put b at the very bottom everywhere

(ii) move b to the very top one individual at the time

at some point in the social preference b will 'flip' from bottom to top



first proof, third step: pivotal voters are dictators for all other objects



first proof, fourth step: relating pivotal voters for different objects

$b_1 \neq b_2$

n_1 is a pivotal voter for b_1

n_2 is a pivotal voter for b_2

n_1 is a dictator for $b_2 \implies$ only n_1 can move b_2 around

n_2 can move b_2 from top to bottom

$\therefore$

$n_1 = n_2$

same individual: dictator for **all** alternatives

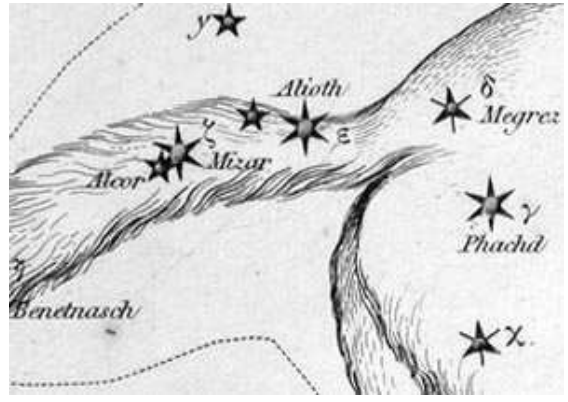
□

Mizar

mathematics versus computer science

Mizar proof assistant:

primarily designed for **mathematics**



most main current proof assistants:

primarily designed for **computer science**

only secondarily designed for mathematics

Uniwersytet w Białymstoku

Andrzej Trybulec

Mizar

1974–today

Białystok, Poland

main development

Nagano, Japan

second biggest user group

$\approx$ 220 Mizar users

'authors'

MML

Mizar Mathematical Library

1043 ‘articles’ = files

$\approx$ 48 thousand ‘theorems’ = lemmas

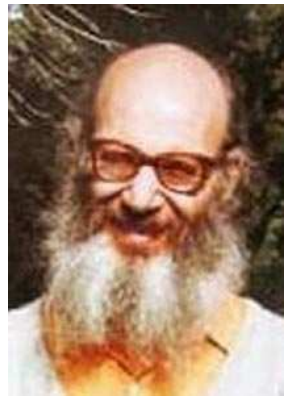
$\approx$ 2.3 million lines

$\approx$ 75 Megabytes of coded mathematics

set theory

Mizar =
first order predicate logic + 'schemes' +
axiomatic set theory

+ 'soft' type system

Tarski-Grothendieck set theory

ZFC +
arbitrarily large models of ZFC

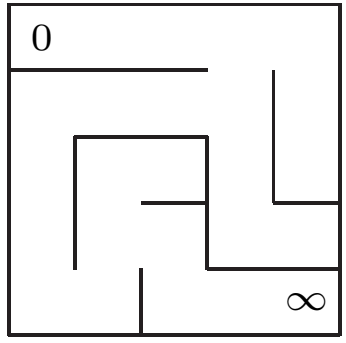
= Grothendieck universes
= strongly inaccessible cardinals

the axioms

TARSKI:def 3	$X \subseteq Y \Leftrightarrow (\forall x.\, x \in X \Rightarrow x \in Y)$
TARSKI:def 5	$\langle x, y \rangle = \{\{x, y\}, \{x\}\}$
TARSKI:def 6	$X \sim Y \Leftrightarrow \exists Z.\, (\forall x.\, x \in X \Rightarrow \exists y.\, y \in Y \wedge \langle x, y \rangle \in Z) \wedge$
	$(\forall y.\, y \in Y \Rightarrow \exists x.\, x \in X \wedge \langle x, y \rangle \in Z) \wedge$
	$(\forall x \forall y \forall z \forall u.\, \langle x, y \rangle \in Z \wedge \langle z, u \rangle \in Z \Rightarrow (x = z \Leftrightarrow y = u))$

TARSKI:def 1	$x \in \{y\} \Leftrightarrow x = y$
TARSKI:def 2	$x \in \{y, z\} \Leftrightarrow x = y \vee x = z$
TARSKI:def 4	$x \in \bigcup X \Leftrightarrow \exists Y.\, x \in Y \wedge Y \in X$
TARSKI:2	$(\forall x.\, x \in X \Leftrightarrow x \in Y) \Rightarrow X = Y$
TARSKI:7	$x \in X \Rightarrow \exists Y.\, Y \in X \wedge \neg \exists x.\, x \in X \wedge x \in Y$
TARSKI:sch 1	$(\forall x\, \forall y\, \forall z.\, P[x, y] \wedge P[x, z] \Rightarrow y = z) \Rightarrow$
	$(\exists X.\, \forall x.\, x \in X \Leftrightarrow \exists y.\, y \in A \wedge P[y, x])$
TARSKI:9	$\exists M.\, N \in M \wedge (\forall X \forall Y.\, X \in M \wedge Y \subseteq X \Rightarrow Y \in M) \wedge$
	$(\forall X.\, X \in M \Rightarrow \exists Z.\, Z \in M \wedge \forall Y.\, Y \subseteq X \Rightarrow Y \in Z) \wedge$
	$(\forall X.\, X \subseteq M \Rightarrow X \sim M \vee X \in M)$

procedural versus declarative proofs



- **procedural**

  E E S E N E S S S W W W S E E E

  HOL, Isabelle, Coq, PVS, B

- **declarative**

  (0,0) (1,0) (2,0) (3,0) (3,1) (2,1) (1,1) (0,1) (0,2) (0,3) (0,4) (1,4) (1,3) (2,3) (2,4) (3,4) (4,4)

  Mizar, Isabelle, ACL2

versje

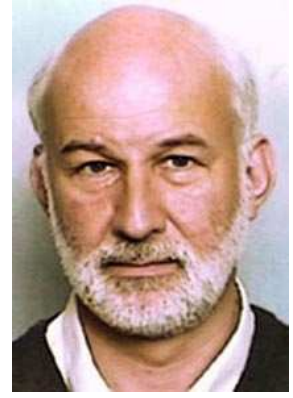
Een bolleboos riep laatst met zwier
gewapend met een vel A-vijf:
Er is geen allergrootst getal,
dat is wat ik bewijzen ga.
Stel, dat ik u nu zou bedriegen
en hier een potje stond te jokken,
dan ik zou zonder overdrijven
het grootste kunnen op gaan noemen.
Maar ben ik klaar, roept u gemeen:
'Vermeerder dat getal met twee!'
En zien we zeker en gewis
dat dit toch niet het grootste was.
En gaan we zo nog door een poos,
dan merkt u: dit is onbegrensd.
En daarmee heb ik q.e.d.
Ik ben hier diep gelukkig door.
'Zo gaan', zei hij voor hij bezwijmde,
'bewijzen uit het ongedichte'.

```
theorem
  not ex n st for m holds n >= m
proof

  assume not thesis;
  then consider n such that
A1: for m holds n >= m;

  set n' = n + 2;

  n' > n by XREAL_1:31;

  then not for m holds n >= m;

  hence contradiction by A1;

end;
```

formalizing Arrow's theorem in Mizar

a suggestion

Krzysztof Apt, 2006:



formalization of Arrow's theorem

$\Downarrow$

attention for formalization from the economics community

formalizations of social choice theory

- Tobias Nipkow
  Technische Universität München, Germany
  Arrow, 2002 & **Gibbard-Satterthwaite**
  Isabelle

- Peter Gammie
  University of New South Wales, Sydney, Australia
  Arrow, 2006 & **Gibbard-Satterthwaite**, 2007
  Isabelle

- *this talk*
  Arrow, 2007
  Mizar

the formal Mizar statement

```
reserve A,N for finite non empty set;
reserve a,b for Element of A;
reserve i,n for Element of N;
reserve o for Element of LinPreorders A;
reserve p,p' for Element of Funcs(N,LinPreorders A);
reserve f for Function of Funcs(N,LinPreorders A),LinPreorders A;

theorem Th14:
  (for p,a,b st for i holds a <_p.i, b holds a <_f.p, b) &
  (for p,p',a,b st
      for i holds (a <_p.i, b iff a <_p'.i, b) &
                  (b <_p.i, a iff b <_p'.i, a)
    holds a <_f.p, b iff a <_f.p', b) &
  card A >= 3 implies
  ex n st for p,a,b st a <_p.n, b holds a <_f.p, b
```

demo

errors in the original?

not really

one small detail

step one, conservation of extremity:

> *suppose to the contrary that for some a and c, both distinct from b, the social preference puts $a \geq b \geq c$*

proof only works if also $a \neq c$

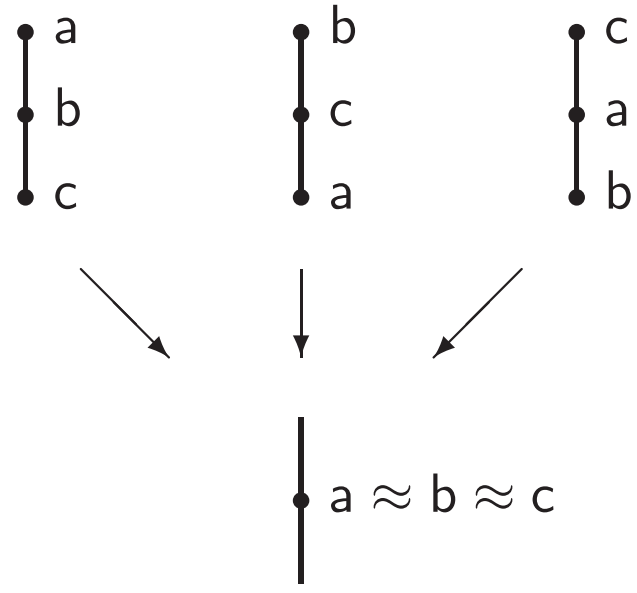
does not directly folllow from the 'to the contrary'

in the formalization this is handled as a trivial separate case

variants

orders versus preorders

maybe allowing alternatives to be ‘equivalent’ helps?



specifics of the statement

- **respect unanimity**

  should we respect $<$?

  should we respect $\lesssim$?

  the first is enough, the second does not work

- **independent of irrelevant alternatives**

  should $<$ be independent?

  should $\lesssim$ be independent?

  both are needed

- **dictator**

  dictator for $<$?

  dictator for $\lesssim$?

  the second does not follow

a variant of Geanakoplos' statement

- Geanakoplos' proof:

individual preferences	$\longrightarrow$	preorders
social preference	$\longrightarrow$	preorder

- seems stronger, but really is just different:

individual preferences	$\longrightarrow$	orders
social preference	$\longrightarrow$	preorder

  theorem statement becomes a bit simpler

follows easily from the first

formalization of this argument is surprisingly laborious

and how about Gibbard-Satterthwaite?

Philip J. Reny

Arrow's theorem and the Gibbard-Satterthwaite theorem: a unified approach

2000

both proofs next to each other in two columns

would be fun to do the same with two Mizar proofs
(or maybe have both proofs be instances of a single Mizar scheme)

the future

is formalization difficult?

not really

but labor intensive

given

- correct informal textbook source
- declarative proof assistant

formalization is straight-forward

just transcribe the textbook source

de Bruijn factor

- de Bruijn factor **in space**

$$\frac{\text{size of formalization}}{\text{size of informal textbook source}} \approx 4$$

- de Bruijn factor **in time**

$$\frac{\text{time to formalize}}{\text{size of informal textbook source}} \approx 1 \, \frac{\text{man} \cdot \text{week}}{\text{textbook page}}$$

getting it right

- first 'proof' of Arrow's theorem

  Kenneth Arrow
  A difficulty in the concept of social welfare
  Journal of Political Economy
  1950

- first *fully* correct proof of Arrow's theorem?

  Richard Routley (= Richard Sylvan)
  Repairing proofs of Arrow's general impossibility theorem
  Notre Dame Journal of Formal Logic
  1979

formalization of the real world

- mathematics: abstractions
- computer science: man-made abstractions
- economics: the real world!

formalization useful for economists?