Beyond Propositions

Instead of propositional variables that are true or false, e.g. ValveIsClosed, move to predicates and arguments that allow more precision, e.g. IsClosed(valve1)

- Also include simple expressions that evaluate to true or false … e.g. involving naturals, integers, etc
  (temp > 50) /\ (temp < 100) , water_level > 311.5
- Predicates, e.g. IsReadOnly(file1), IsRed(coat)

(Predicate(x): the truth of the statement is predicated on the value of x)

Predicates

- Basic predicate of arity 1 (taking a single argument) is sometimes called a *property*
- E.g. HasProperty(object)
  - IsRed(block)
  - IsOpen(valve1)
  - IsActive(process23)
  - IsIdle(cpu1)

Predicates

- A predicate of arity 2 or more is often called a *relation*
  - Siblings(Helen, Jim, Blair)
- A binary relation has two arguments:
  - ParentOf(John, Sam)
- A predicate may be treated as just a function whose range is boolean

Predicate Calculus/First Order Logic

- Predicates allow us to say:
  - IsGreen(x) /\ HasLegs(x) --> IsFrog(x)
- Predicate calculus also has quantifiers

$$\forall x(IsMan(x) \rightarrow IsMortal(x))$$

$$\forall p\ (Running(p) \rightarrow \exists\ p2(Suspended\ (p2))$$

$$\exists comp(IsIdle(comp))$$

Predicate Calculus/First Order Logic Syntax

- Syntax of propositions
- Syntax of expressions that are allowed:
  - e.g. x+y, x<y, x*y,
- Exercise: write down the BNF for a suitable subset of natural number expressions
- Quantified statements $\forall x P(x)$

  $\exists x Q(x)$

Semantics

- Is this formula in First Order Logic true or false?

$$\forall x \; \exists y \;\; (y + 1) = x$$

- Ans:?

- Is this formula true or false?

$$\forall x \; \forall y \; ((x < y) \rightarrow \exists z \;\; (x < z \wedge z < y))$$

- Ans:?

Interpretation

- A formula is true with respect to a *model*
- A model provides:
  - **a universe**

    i.e. a set of objects for variables to range over e.g. naturals, booleans, reals
  - **an interpretation**

    this maps constants, functions and predicate symbols in the logic to objects, functions and predicates in the universe of the model

$$\forall x \; \exists y \;\; (y + 1) = x$$

This is "true" under an interpretation where the universe is the naturals and +,= and 1 have the usual meanings

Semantics: the picture

$$\forall x \; \exists \; y \;\; (y + 1) = x$$

Rules of Inference

- The propositional rules of inference
- Extra rules for additional syntax:
- e.g.

$$\frac{\forall x \; P(x)}{\exists y \; P(y)} \qquad \frac{Q(t)}{\exists j \; Q(j)}$$

Notation: Set of hypotheses above the line, conclusion below.

Informally, whenever I can establish that the formulae above the line hold (are true) then I can conclude that the formula below the line is true

Predicate Calculus/First Order Logic

- The propositional calculus was decidable … we could use the Rules of Inference to simplify to Conjunctive Normal Form and check if a formula was a tautology.

Proof seems quite powerful …

"Then Logic would take you by the throat, and force you to do it!" What the Tortoise said to Achilles, Lewis Carroll

- What about the Predicate Calculus? Is it decidable?

Truth procedure?

David Hilbert(1862-1943) one of the most prominent mathematicians around the early 1900s, proposed a grand program to devise a single formal procedure that would derive all mathematical truth:

``*Once a logical formalism is established one can expect that a systematic, sotosay computational, treatment of logic formulas is possible, which would somewhat correspond to the theory of equations in algebra."*

But ...

- Godel's Incompleteness Theorem (1931)

  in any formal system powerful enough to form statements about what it can prove, there will always be true statements that the system can express but can't prove.

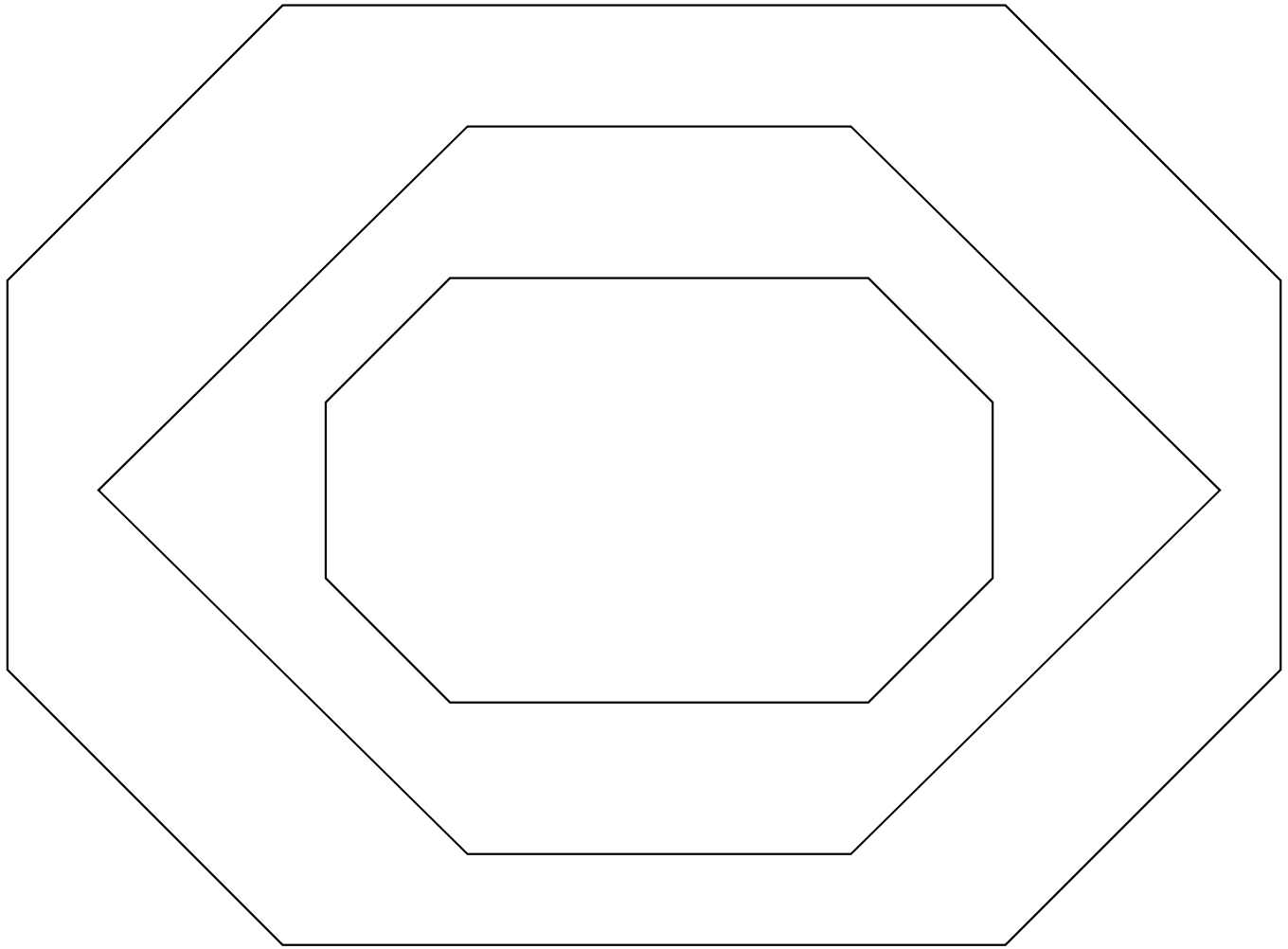
"all consistent axiomatic formulations of number theory include undecidable propositions"

- c.f. "This statement is false"

(cf. Church and Turing … computability)

Proof: a picture

(after Hofstadter Godel, Excher,Bach:An Eternal Golden Braid)



Formal Systems

- The Propositional Calculus (Boolean logic) was easy … the laws could be derived from the semantics of the syntax described via Truth Tables

- The Predicate Calculus(1^{st} order logic) has many similar rules, plus rules for quantifiers and … although Godel's Incompleteness Theorem tells us that there are some statements we cannot prove (or disprove) ... the logic and rules don't look too strange

Formal Systems

- Many systems are not so straightforward; they may not have precise semantics (such as that given by truth tables) and may not have rules derived from the semantics.
- These formal systems are axiomatized … the basic axioms and rules are introduced without proof.
- For these axiomatized systems one tries to keep the number of axioms and rules to a minimum.

Terminology

- Theorem: a sentence that that has been shown to be true by logical argument i.e. derived by formal *proof*
- Axiom (or postulate): a sentence that is asserted to by true without proof.
- A rule of inference has premises and a conclusion. Whenever the premises hold, one may deduce the conclusion.
- As well as postulating certain sentences to be true; one often postulates new rules as being valid
  - these rules are axiomatized

Axiomatization

- Syntax: expressed in BNF or similar
- Semantics: may be stated in natural language
- Axioms (axiom schemas) and Rules: introduced without proof

(An axiom schema contains schema variables, such as P=P *has variable* P *and holds for any* P)

Logic Example

- A simplified subset of the BAN Logic is given as an example of axiomatization.
- The BAN Logic was introduced in 1989 in the paper “A Logic of Authentication” by Michael Burrows, Martin Abadi, Roger Needham
- “This method supplies logical propositions and inference rules which under certain conditions allow conclusions to be drawn about the security of a range of protocols”
- “ground breaking approach in the field of security protocol development”

Axiomatized Logic Example

- Syntax:
- The only propositional connective is conjunction.
- P |= X: P believes X, or P would be entitled to believe X.
- P <| X: P sees X. Someone has sent message containing X to P
- P |¬ X: P once said X. P at some time sent message including X.
- P |=> X: P has jurisdiction over X. Principal P is an authority on X.
- P <-^{k}-> Q: P and Q may use a shared key to communicate
- {X}k: Formula X is encrypted under the key K

Axiomatized Logic Example

- Axioms (or axiom schemas usually):
  (like rules with no premises)

e.g.

- A |= S |=> A <-^{k}-> B

- A believes the server S has jurisdiction over shared keys for A and B

Axiomatized Logic Example

- Rules such as:
  - $\dfrac{P \mid= Q \leftarrow^{k}\rightarrow P, \quad P \lhd \{X\}k}{P \mid= Q \mid\neg X}$
- If P believes key K is shared with Q and sees a message X encrypted with K then P believes that Q once said X
  - $\dfrac{P \mid= Q \Rightarrow X, \quad P \mid= Q \mid= X}{P \mid= X}$
- If P believes that Q has jurisdiction over X and P believes Q on the truth of X then P believes X

Applying Rules of Inference

- The application of inference rules needs to be controlled
- Even for the propositional calculus can have long proofs if ad-hoc application of rules
  - Standard methods for Conjunctive/Disjunctive Normal Form
- Try to have a small number of primitive inference rules with a rationale
  - e.g. introduction and elimination rules that grow and shrink (respectively) a formula by adding or cutting an operator

An equality rule of inference may be used as a rewrite rule

Rewrite Rules

Transforming a formula by a set of rewrite rules prompts several questions

- How does one choose the order of rules?
- Will different order of application yield the same result?
- Will the process terminate or will the formula grow forever or oscillate, shrinking and growing?
- …

- A set of rewrite rules is *confluent* if different order of application yields the same result (*conguent* if terminating and confleunt)
- In general checking if a set of rewrites is confluent is undecidable … but much study on particular cases, systems, techniques etc.

Logic Example

- Axiomatized logic, try to have
  - small number of axioms
  - small number of rules
- Minimise what any theorems derived depend on
- Control the application of rules
- c.f. correctness by construction

Proof: another picture

Axiom1

Axiom2

Axiom3

Rule of Inference

Rule of Inference

theoremA

theoremB

theoremC