

Bayes Theorem If A, B are events, then

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A^c)P(A^c)}$$

Let:

A =Defendant is innocent

A^c =Defendant is guilty

B =Defendant's blood matches the crime scene profile

and let $p = P(A^c)$ (which we don't know, but might have a preconception about). We know that $P(B|A) = 1/1000000$, $P(B|A^c) = 1$, so plug into Bayes Theorem, get:

$$\begin{aligned} P(A|B) &= \frac{(1/1000000)(1 - p)}{(1/1000000)(1 - p) + p} \\ &= \frac{1 - p}{1 + 999999p} \end{aligned}$$

this varies depending on what is the 'prior' probability p of guilt:

18 Gödel's Theorem

18.1 Context

Question: Can computers do mathematics?

Can all mathematical theorems be done in a 'decidable' or 'computable' manner?

Question: What would/should *computable* mean?

Kurt Gödel (Vienna, 1931) *recursive sets and functions*

Alan Turing (Cambridge, 1936) *Turing Machines, computable numbers;*

(1950) Free will/determinism (*Turing test*)

Alonzo Church (Princeton, 1936) λ -calculus

Theorem: A function is recursive (in the sense of Gödel) if and only if it can be computed by a Turing machine if and only if it can be represented in the λ -calculus.

Church's Thesis: All rigorous notions of 'computability' are the same.

Question: Can every true statement P in (say) Peano Arithmetic be proved some formal system of logical deduction?

Answer: Yes; just make sure this statement P is one of the axioms!

Better Question: Is there a formal system of logical deduction such that all consequences are computable, and such that every true statement P in Peano Arithmetic be proved in this system?

(Why is this a different question?)

Attempted answer: Yes, just add all true statements of PA to our axiom system.

Problem: This might render the set of axioms not computable.

Instead: how might we prove a *negative* answer?

3 apparent paradoxes:

The Liar: “I am not true.” (Not representable in any consistent formal system)

Richard: “I am not provable.” (If representable in a formal system, then true but not provable in that system - WHY?)

Richard-plus: “I am not provable in S .” (True, and provable by us, but not provable in S .)

Gödel’s idea: Find a way to create a sentence G which somehow says of itself, “I am not provable in PA.”

Theorem 18.1. (*Gödel, informal*) Any sufficiently powerful formal system contains sentences which are true but not provable in that system. “Formal system” means 1st order language + a set of axioms. “Sufficiently powerful” means that every recursive function is representable in the system.

Let \mathcal{L} be the language of Peano Arithmetic (PA), let $\mathfrak{N} = (\mathbb{N}, 0, S, +, \times)$ be the standard model for \mathcal{L} .

Theorem 18.2. (*Gödel, formal*)

Let Δ be a set of sentences in \mathcal{L} such that:

- a) Δ is computable (i.e., “ $\phi \in \Delta$ ” is decidable for any ϕ)
- b) Every sentence in Δ is true in \mathfrak{N}
- c) Δ includes the axioms of PA

Then Δ is not complete for PA; that is, there is a sentence G of \mathcal{L} such that G is true in \mathfrak{N} but such that there is no deduction of G from Δ .

The proof idea is extremely clever, and incorporates some ideas we’ve discussed this semester, so I will sketch it.

Step1: Show that we can represent formulas and deductions as natural numbers

Assign numbers to the alphabet of \mathcal{L} :

$$\begin{array}{cccccccccccccccc} 0 & s & + & \times &) & (& \wedge & \vee & \implies & \sim & = & \forall & \exists & x & y & z & \dots \\ 2 & 3 & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 & 47 & 53 & \dots \end{array}$$

Extend to formulas; for example:

$$\exists x(x \times x = s(s(0)))$$

is assigned the “Gödel number”:

$$2^{41}3^{13}5^{43}7^711^{43}13^{11}17^{31}19^323^{13}29^331^{13}37^241^{11}43^{11}47^{11}$$

If ϕ is a WFF, write $\ulcorner \phi \urcorner$ for the Gödel number of ϕ .

If $\phi_1, \phi_2, \dots, \phi_n$ is a sequence of WFFs, for example a deduction of ϕ_n , write $\ulcorner \phi_1, \phi_2, \dots, \phi_n \urcorner$ for $2^{\ulcorner \phi_1 \urcorner}3^{\ulcorner \phi_2 \urcorner}5^{\ulcorner \phi_3 \urcorner} \dots \text{prime}_n^{\ulcorner \phi_n \urcorner}$

Thus: every WFF, or sequence of WFFs, can be represented by a natural number. The Fundamental Theorem of Algebra ensures that this representation is one-to-one, in fact it is not hard to see that given a number N , there is a procedure to figure out what WFF or sequence of WFFs (if any) gave rise to it.

Step 2: Find a formula $Pf(x, y)$ in the language such that:

if n is the Gödel number of a formula $\phi(y)$, and there is deduction of the formula $\phi(\bar{k})$ from Δ , then there is a deduction of

$$Pf[\bar{n}, \bar{k}]$$

from Δ , otherwise there is a deduction of

$$\sim Pf[\bar{n}, \bar{k}]$$

(Here \bar{n} is shorthand for $s(s(s(\cdots s(0))\cdots))$)

Put $g := \ulcorner \sim Pf(y, y) \urcorner$

and $G := \sim Pf(\bar{g}, \bar{g})$

Step 3: Show that G is true and unprovable (no deduction of G from Δ).