

# Evidential Reasoning

Riccardo Pucella

Ph.D. Seminar

November 2, 2006

# A Puzzle?

---

Suppose Alice has two coins

- F  $\longrightarrow$  Fair (Pr heads =  $1/2$ )
- DH  $\longrightarrow$  Double-headed (Pr heads = 1)

She chooses one of the coins and tosses it

- It lands heads

What is the probability that the coin is double-headed?

# Another Puzzle?

---

Suppose Alice has two coins

- F  $\longrightarrow$  Fair (Pr heads =  $1/2$ )
- DH  $\longrightarrow$  Double-headed (Pr heads = 1)

She chooses one of the coins and tosses it 100 times

- It lands heads every time

What is the probability that the coin is double-headed?

# Quantifying An Intuition

---

These puzzles are similar but “feel” different

- In the second puzzle, it seems “more plausible” that the coin is double-headed

Can we quantify this plausibility?

- Plausibility of DH should be higher in the second puzzle than in the first

# Evidence

---

The outcome of an **experiment** (Heads, Tails) provides evidence for an **hypothesis** (Fair, Double-Headed)

Many approaches to encoding evidence are based on comparing **likelihood functions**

$\mu_h(\text{ob})$  = probability of observing ob if h holds

- $\mu_{\text{DH}}(\text{Heads}) = 1$
- $\mu_{\text{F}}(\text{Heads}) = 1/2$

# Shafer's Approach

---

**Evidence space**  $E = (H, O, \mu)$ :

- $H$ : hypotheses  $\{h_1, \dots, h_n\}$
- $O$ : observations
- $\mu$ :  $H$ -indexed likelihood functions

Weight of evidence of observation  $ob$  for hypothesis  $h$

$$w_E(ob, h) = \frac{\mu_h(ob)}{\mu_{h_1}(ob) + \dots + \mu_{h_n}(ob)}$$

# Revisiting The Puzzles

---

$$E = ( \{ \text{Fair, DH} \}, \{ \text{Heads, Tails} \}, \mu )$$

$\mu$	Fair	DH
Heads	1/2	1
Tails	1/2	0

$w_E$	Fair	DH
Heads	1/3	2/3
Tails	1	0

# Revisiting The Puzzles

---

$$E' = ( \{ \text{Fair, DH} \}, \{100\text{Heads}, <100\text{Heads}\}, \mu')$$

$\mu'$	Fair	DH
100 Heads	$2^{-100}$	1
< 100 Heads	$1-2^{-100}$	0

$w_{E'}$	Fair	DH
100 Heads	$\sim 0$	$\sim 1$
< 100 Heads	1	0

# Justifying Evidence

---

Consider the first puzzle.

Suppose we have a probability on Alice's choice

- Then probability of coin being DH after seeing Heads can be computed by Bayes' Theorem:

$$\Pr(DH \mid Heads) = \frac{\Pr(Heads \mid DH)\Pr(DH)}{\Pr(Heads)}$$

Evidence captures the information used in this update...

# Dempster's Rule Of Combination

---

Given two functions  $f_1, f_2: X \rightarrow [0, 1]$ :

$$(f_1 \oplus f_2)(x) = \frac{f_1(x)f_2(x)}{\sum_{y \in X} f_1(y)f_2(y)}$$

If  $f_1, f_2$  are probability distributions,  $f_1 \oplus f_2$  defines a probability distribution

# Updating Via Evidence

---

Can use weight of evidence function  $\lambda x.w_E(\text{ob}, x)$  to update prior  $\mu_0$  to a posterior  $\mu_{\text{ob}}$ :

$$\mu_{\text{ob}} = \mu_0 \oplus (\lambda x.w_E(\text{ob}, x))$$

**Theorem:** If  $\text{Pr}(h) = \mu_0(h)$ , then  $\mu_{\text{ob}}(h) = \text{Pr}(h \mid \text{ob})$

# Combining Evidence

---

Can also use Dempster's Rule of Combination to combine (independent) pieces of evidence:

$$w_E(\langle ob_1, ob_2 \rangle, -) = w_E(ob_1, -) \oplus w_E(ob_2, -)$$

So,  $w_E(100\text{Heads}, -) = w_E(\text{Heads}, -) \oplus \dots \oplus w_E(\text{Heads}, -)$

# Why Should Anyone Care?

---

Evidence  $w(\text{ob},h)$  has an intuitive meaning whether we have a prior or not

In CS, **we are loathe to posit priors**

- Contrast: economics, epidemiology, ...
  - Priors are often ascertained experimentally
  - CS not very experimental

Average-case complexity theory?

# Application: Probabilistic Algorithms

---

Rabin's primality test for a number  $n$

- Polynomial-time computable predicate  $P(n,a)$  such that:
  - $n$  composite  $\Rightarrow P(n,a)=1$  for  $\geq n/2$  choices of  $a$
  - $n$  prime  $\Rightarrow P(n,a)=0$  for all  $a$

Pick a number  $a$  at random between 0 and  $n$

If  $P(n,a) = 1$  return "composite"; otherwise return "prime"

$w$	prime	composite
"prime"	$\geq 2/3$	$\leq 1/3$
"composite"	0	1

# Application: Intrusion Detection

---

A monitor observes sequences of actions from users

- Are these actions from an intruder (INT hypothesis) or a regular user (REG hypothesis)?
- Need a model of what users typically do (likelihoods)

**Threshold of evidence:** if evidence for INT higher than some  $\alpha$ , treat actions as an attack

General problem: making decisions without a prior

- Not quite classical decision theory: we do have partial probabilistic information

# Application: Security Properties

---

CROWDS: A protocol that guarantees anonymity of message senders

- Collect users into groups (crowds)
- When sending a message, randomly forward through the crowd

Formalization of anonymity property:

$$\forall a, a'. w(\text{msg}, \text{SentBy}(a)) = w(\text{msg}, \text{SentBy}(a'))$$

# A Third Puzzle?

---

Suppose Alice has two coins

- B            Biased towards heads (Pr heads =  $3/4$ )
- DH          Double-headed (Pr heads = 1)

Suppose Bob has a fair coin

1. Alice and Bob each hand a coin to Zoe
2. Zoe tosses one of the coins
3. Outcome is heads

What is the probability that Zoe chose Alice's coin?

# Refining Hypotheses?

---

Obvious approach:

- AD : coin is Alice's and is double-headed
- AB: coin is Alice's and is biased
- B: coin is Bob's

Can compute weights of evidence as before

- What's the evidence for "Zoe chose Alice's coin"?

If we have a prior probability on choice, cannot update using these weights

# One Proposal

---

Consider all possible evidence spaces consistent with the information

- Agent ascribing weight of evidence does not know which is the right one
- Compute weights of evidence with respect to each evidence space
- Get a range of possible weights of evidence

# Generalized Weight of Evidence

---

Generalized evidence space  $G = (H, O, \Delta)$

- H: hypotheses
- O: observations
- $\Delta$ : set of indexed likelihood functions
  - E.g.  $\{\mu_{DH}, \mu_B\}$

$$S(G) = \{ (H, O, \mu) \mid \mu \in \Delta \}$$

$$W_G = \{ w_E \mid E \in S(G) \}$$

Can reason with *upper* and *lower* weight of evidence

# Updating Priors

---

Can update prior  $\mu_0$  by natural generalization

$$\mathcal{P}_{ob} = \{\mu_0 \oplus w(ob, -) \mid w \in w_G\}$$

- This gives a set of all possible posteriors

**Theorem:** Bounds on posteriors agree with taking all possible results of Bayes' Theorem applied to the prior

# Combining Evidence

---

Consider the Alice/Bob/Zoe puzzle with repeated tosses

- Zoe always makes same choice

- Same coin repeated?

$$w_G = \{ w' \mid w'(\langle ob_1, ob_2 \rangle, -) = w(ob_1, -) \oplus w(ob_2, -), w \in w_G \}$$

- Different coin chosen at every toss?

$$w_G = \{ w' \mid w'(\langle ob_1, ob_2 \rangle, -) = w_1(ob_1, -) \oplus w_2(ob_2, -), w_1, w_2 \in w_G \}$$

# To Conclude

---

Evidence is central to many ways of thinking in CS

- Provides a handle on nondeterminism and probabilities

Easy to use for simple scenarios

Evidence depends on the “program” of the experiment

- More on this topic in Part II - Semantics Seminar



Application:

# Updating Sets of Probabilities

---

Some situations are best represented using sets of probability distributions

- Bag with 100 marbles, 30 yellow, 70 red or blue

Cannot learn.

Use evidence to capture how much evidence has been accumulated.

Can we give this an interpretation?