Royal Holloway
University of London

Quantum Bayesianism, tomography, and random numbers

Rüdiger Schack

Royal Holloway, University of London

Royal Holloway
University of London

What is a quantum state?

$|\psi\rangle$ expresses an agent's Bayesian degrees of belief about the consequences of his actions.

$|\psi\rangle$ is a function of the agent and the world.

Royal Holloway
University of London

Bayesian statistics

Hypotheses: H_0, H_1

Royal Holloway
University of London

Bayesian statistics

Hypotheses: H_0, H_1

Prior degrees of belief: $\Pr(H_0)$, $\Pr(H_1)$

Model: $\Pr(T|H_0)$, $\Pr(T|H_1)$

Royal Holloway
University of London

Bayesian statistics

Hypotheses: H_0, H_1

Prior degrees of belief: $\Pr(H_0)$, $\Pr(H_1)$

Model: $\Pr(T|H_0)$, $\Pr(T|H_1)$

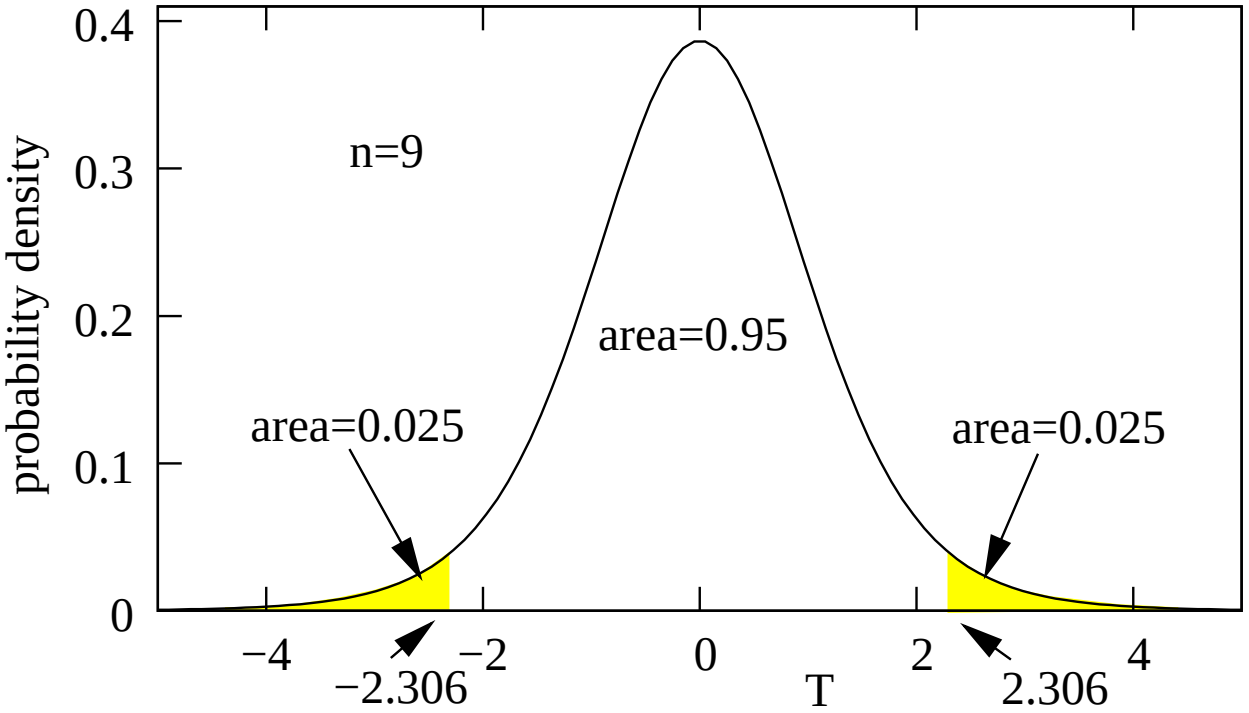
Data: $T_{\rm obs}$

Posterior: $\Pr(H_0|T_{\rm obs}) = \dfrac{\Pr(T_{\rm obs}|H_0)\Pr(H_0)}{\Pr(T_{\rm obs})}$.

Royal Holloway
University of London

Frequentist statistics

Model: $\Pr(T|H_0)$



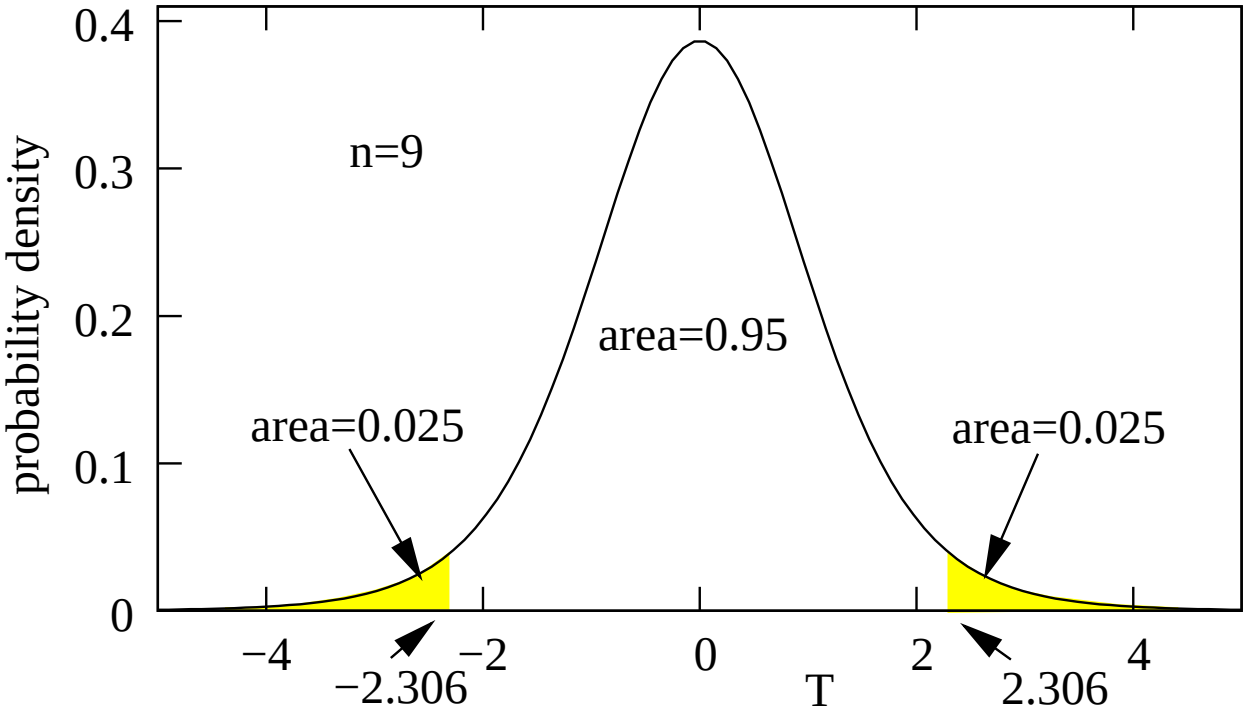
Find $P = \Pr(|T| > |T_{\rm obs}|)$.

Reject H_0 if $P < 5\%$

Royal Holloway
University of London

Frequentist statistics

Model: $\Pr(T|H_0)$



Find $P = \Pr(|T| > |T_{\rm obs}|)$.
Reject H_0 if $P < 5\%$

"a hypothesis that may be true may be rejected because it has not predicted observable results that have not occurred" (H. Jeffreys, 1961)

Royal Holloway
University of London

The quantum-mechanical core

(a) Prior belief: The agent writes down his prior quantum state.

Royal Holloway
University of London

The quantum-mechanical core

(a) Prior belief: The agent writes down his prior quantum state.

(b) Action: The agent acts on the world to elicit a measurement outcome.

Royal Holloway
University of London

The quantum-mechanical core

(a) Prior belief: The agent writes down his prior quantum state.

(b) Action: The agent acts on the world to elicit a measurement outcome.

(c) Quantum mechanics: The agent uses the quantum rules to update his quantum state.

Royal Holloway
University of London

The quantum-mechanical core

(a) Prior belief: The agent writes down his prior quantum state.

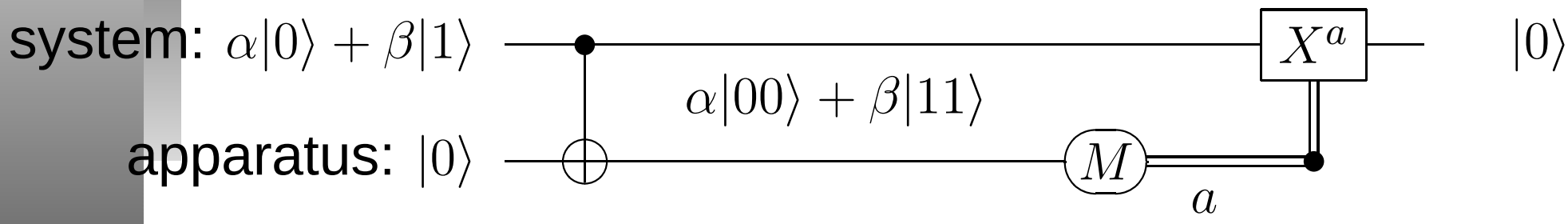
(b) Action: The agent acts on the world to elicit a measurement outcome.

(c) Quantum mechanics: The agent uses the quantum rules to update his quantum state.

Quantum mechanics does not provide a rule for choosing the prior quantum state.

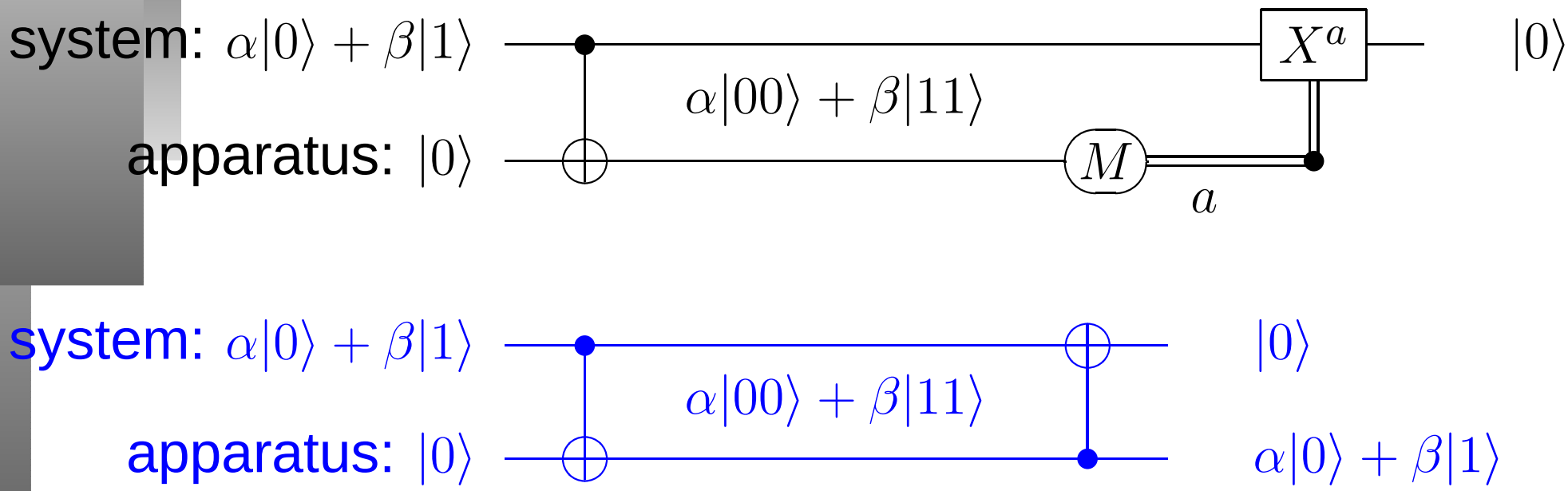
Royal Holloway
University of London

State preparation



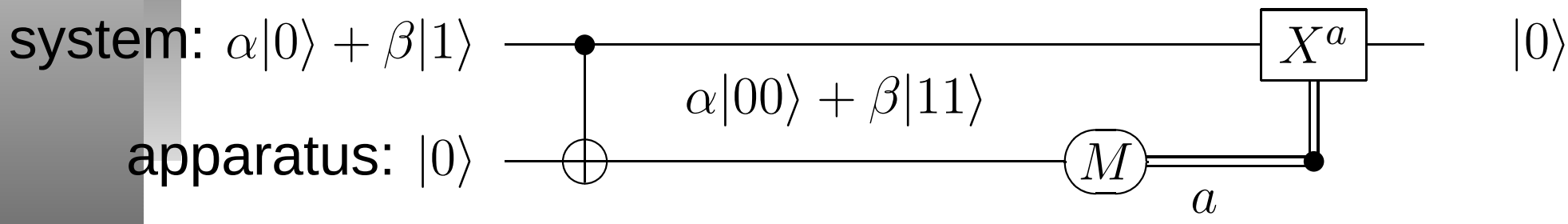
Royal Holloway
University of London

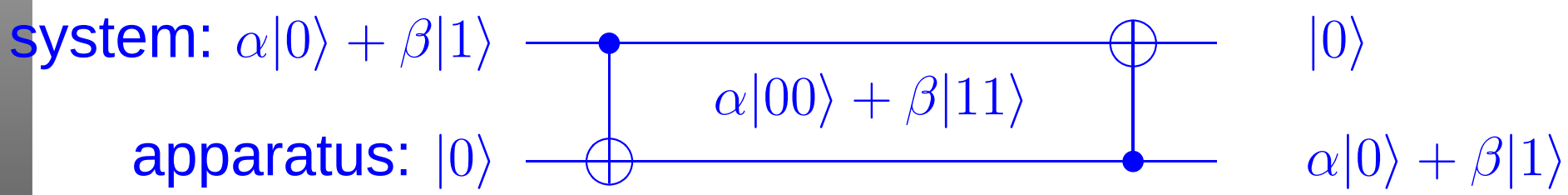
State preparation

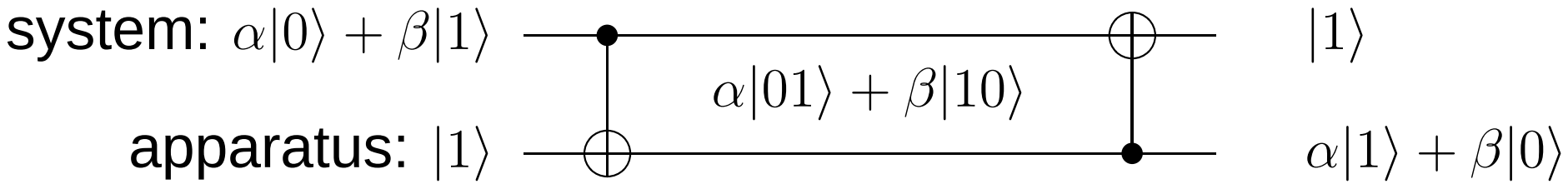


Royal Holloway
University of London

State preparation

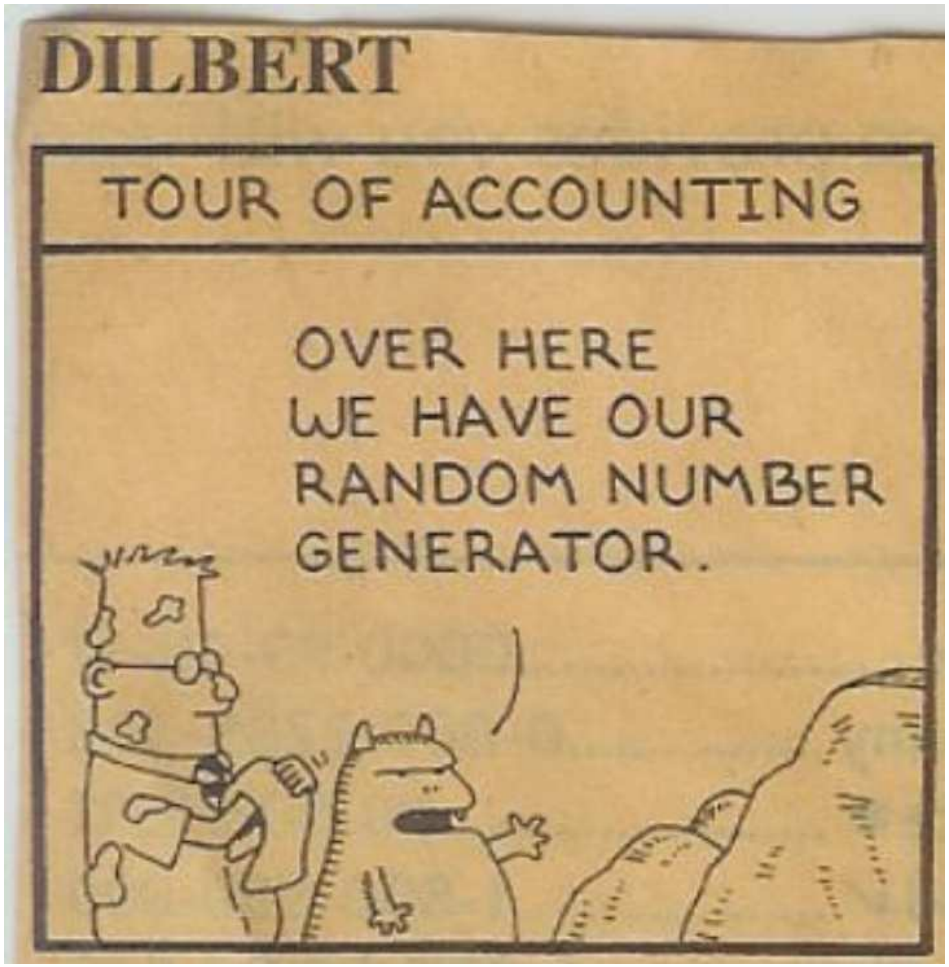






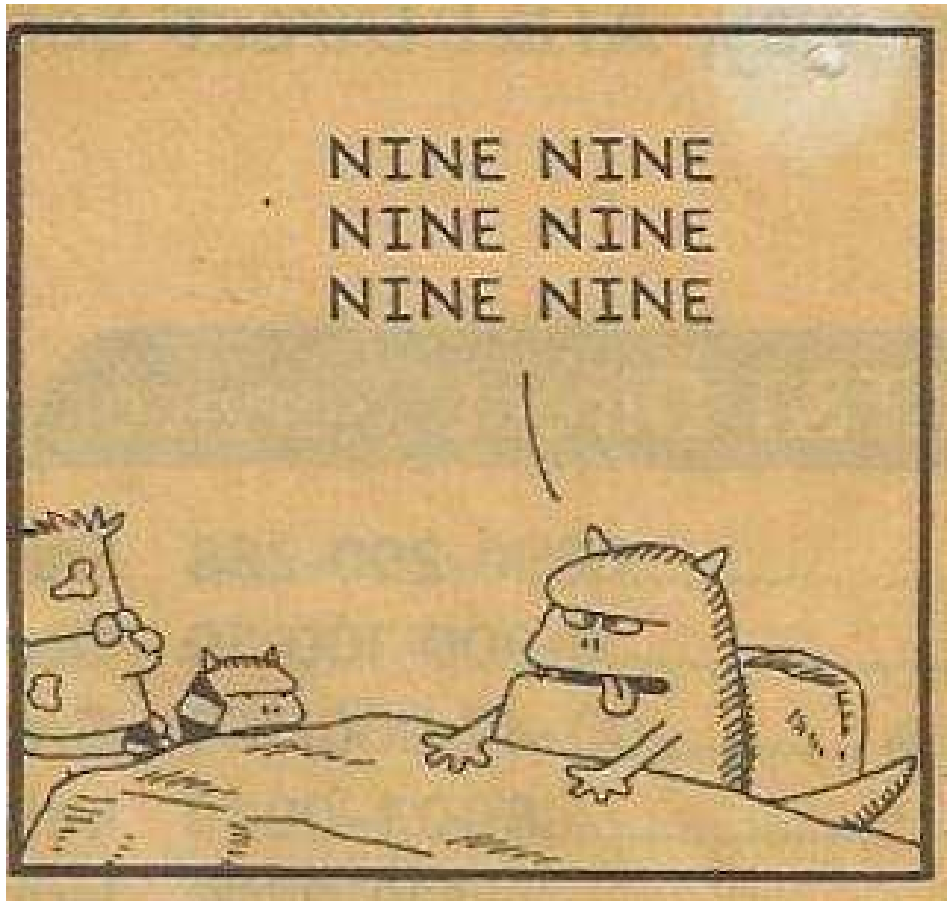
Royal Holloway
University of London

www.dilbert.com



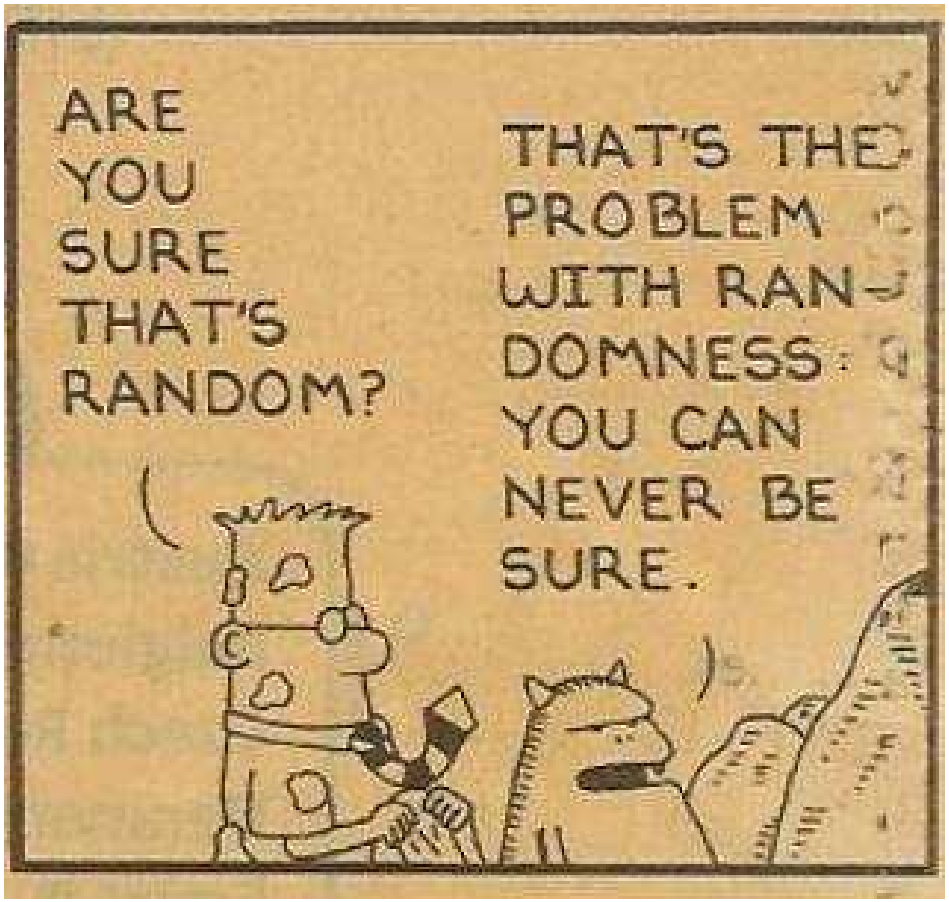
Royal Holloway
University of London

www.dilbert.com



Royal Holloway
University of London

www.dilbert.com



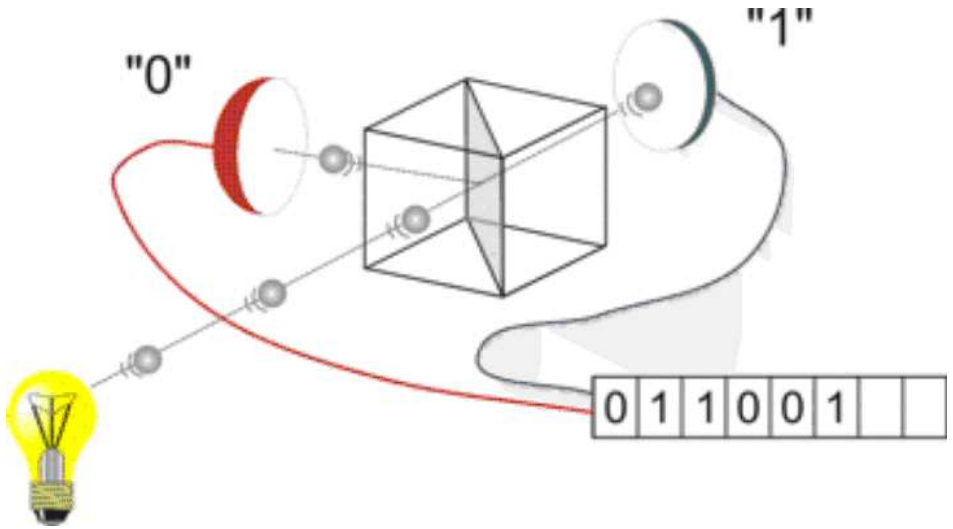
Royal Holloway
University of London

Quantum random numbers (©www.randomnumbers.info)

0 1 1 0 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 0 1 1 0 1 1
0 1 0 0 1 1 1 1 1 0 1 1 0 1 0 1 0 1 1 1 0 1 1 1 1
0 1 1 1 1 1 0 1 1 0 0 1 0 0 0 1 1 0 1 0 1 1 1 0 1
0 0 1 0 1 1 1 1 0 1 1 0 0 0 0 0 1 0 1 0 0 1 0 1 0
1 1 1 0 1 0 1 1 1 0 0 0 1 1 0 0 0 0 1 1 0 1 0 0
1 0 0 1 1 1 0 1 1 1 0 1 0 0 0 1 0 1 1 0 1 0 0 1 1
0 0 0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1
0 0 0 0 0 1 0 0 1 1 1 1 0 1 0 1 1 0 1 1 0 0 0 0 1
1 0 0 1 1 1 1 1 0 1 1 0 0 0 0 0 1 0 0 1 0 1 0 1 0
0 1 0 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0

Royal Holloway
University of London

Quantum random numbers



©www.idquantique.com

Royal Holloway
University of London

Quantum random numbers

$|\psi\rangle = \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n}$ (“Prior”)

Measurement $\rightarrow x \in \{0,1\}^n$ (“Action”)

$\Pr(x) = 2^{-n}$

Royal Holloway
University of London

Bayesian quantum tomography

$$\rho^{(N+M)} = \int d\rho \; p(\rho) \; \rho^{\otimes(N+M)}$$

measure N subsystems

get outcome $\vec{\alpha}$

$$\rho^{(M)} = \int d\rho \; p(\rho|\vec{\alpha}) \; \rho^{\otimes M}$$

$p(\rho|\vec{\alpha})$ given by a quantum Bayes rule.

Royal Holloway
University of London

Quantum Bayes rule: detail

$$p(\rho|\vec{\alpha}) = \frac{p(\rho)p(\vec{\alpha}|\rho)}{p_\alpha} \ ,$$

where $p(\vec{\alpha}|\rho) = \mathrm{tr}\big(\, \rho^{\otimes N}\, E_{\alpha_1} \otimes \cdots \otimes E_{\alpha_N}\big)$,

$\vec{\alpha} = (\alpha_1, \ldots, \alpha_N)$,

$\{E_k\}$ is a POVM,

and $p_\alpha = \int d\rho\; p(\rho)\, p(\vec{\alpha}|\rho)$.

Royal Holloway
University of London

Bayesian quantum tomography: practicalities

$p(\rho|\vec{\alpha})$ is a distribution on a D^2-dimensional space.

Don't compute (or store) it:

Instead, use MCMC (Metropolis-Hastings algorithm) to obtain quantities of interest directly from $\vec{\alpha}$ and $p(\rho)$ (the prior).

(See Robin Blume-Kohout, quant-ph, 2006)

Royal Holloway
University of London

Frequentist quantum tomography

Given POVM $\{E_k\}$ and outcome $\vec{\alpha} = (\alpha_1, \ldots, \alpha_N)$, find $\rho = \rho_{ML}$ such that

$p(\vec{\alpha}|\rho) = \mathrm{tr}\big(\, \rho^{\otimes N}\, E_{\alpha_1} \otimes \cdots \otimes E_{\alpha_N}\big)$ is maximal.

(This is the maximum-likelihood estimator.)

Royal Holloway
University of London

Three priors: 1

Exchangeable (de Finetti) prior:

$$\rho^{(N)} = \int d\rho \; p(\rho) \; \rho^{\otimes N}$$

HHHHHHHHHHHHHHHHHHHHHHHHHHHHHH

Royal Holloway
University of London

Three priors: 2

Rosenkrantz and Guildenstern prior:

$$\rho^{(N)} = 1^{\otimes N}$$

HHHHHHHHHHHHHHHHHHHHHHHHHHHHHH?

Royal Holloway
University of London

Three priors: 3

Counter-inductive prior:

$$\rho^{(N)} = c_0 \sum_{k=1}^{N} 2^{-k^2} \Big(|0\rangle\langle 0|^{\otimes k} \otimes |1\rangle\langle 1|^{\otimes (N-k)} + |1\rangle\langle 1|^{\otimes k} \otimes |0\rangle\langle 0|^{\otimes (N-k)} \Big)$$

HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHT

Royal Holloway
University of London

Three priors: 3

State of the remaining $N-m$ qubits after getting m times 0 in a $\{|0\rangle, |1\rangle\}$ measurement:

$$\rho^{(N-m)} = c_m 2^{-m^2} |1\rangle\langle 1|^{\otimes(N-m)} + \sum_{k=1}^{N-m} c_m 2^{-(m+k)^2} |0\rangle\langle 0|^{\otimes k} \otimes |1\rangle\langle 1|^{\otimes(N-m-k)}$$

where $c_m 2^{-m^2}$ approaches 1 as m increases.

Royal Holloway
University of London

True randomness?

n bits from quantum device: $\Pr(x) = 2^{-n}$

n bits from tossing a coin: $\Pr(x) = 2^{-n}$

What is the difference?

Royal Holloway
University of London

Two players

One trial,

one sample space, S,

two agents, A and B,

two beliefs $P_A : S \to [0,1]$ and $P_B : S \to [0,1]$.

Royal Holloway
University of London

Insider states

P_B is an insider state with respect to P_A if

(i) there exists an event E such that $P_B(E) = 1$ and $P_A(E) < 1$, and

Royal Holloway
University of London

Insider states

P_B is an insider state with respect to P_A if

(i) there exists an event E such that $P_B(E) = 1$ and $P_A(E) < 1$, and

(ii) there exists no event E such that $P_A(E) = 1$ and $P_B(E) < 1$.

Royal Holloway
University of London

Insider states

P_B is an insider state with respect to P_A if

(i) there exists an event E such that $P_B(E) = 1$ and $P_A(E) < 1$, and

(ii) there exists no event E such that $P_A(E) = 1$ and $P_B(E) < 1$.

There exists an insider state w.r.t. any nontrivial P_A.

Royal Holloway
University of London

Quantum mechanics

Given: A single system $\mathcal{S}$.

2 agents $\alpha = A, B$

Royal Holloway
University of London

Quantum mechanics

Given: A single system $\mathcal{S}$.

2 agents $\alpha = A, B$

2 state assignments ρ_A, ρ_B

"Agent α assigns the state ρ_α to $\mathcal{S}$."

Royal Holloway
University of London

Quantum mechanics

Given: A single system $\mathcal{S}$.

2 agents $\alpha = A, B$

2 state assignments ρ_A, ρ_B

"Agent α assigns the state ρ_α to $\mathcal{S}$."

POVM $\{E_k\}$

${p_\alpha}^k = \mathrm{tr}(E_k \rho_\alpha)$
probability assigned by agent α to the outcome k

Royal Holloway
University of London

Insider states

ρ_B is an insider state w.r.t. ρ_A

if

(i) There exists a POVM $\{E_k\}$ and an outcome k such that ${p_B}^k = 1$ and ${p_A}^k < 1$, and

(ii) There exists no POVM $\{E_k\}$ and outcome k such that ${p_A}^k = 1$ and ${p_B}^k < 1$.

Royal Holloway
University of London

Quantum random numbers

There exists no insider state w.r.t. a pure state $|\psi\rangle$.

Royal Holloway
University of London

Quantum random numbers

There exists no insider state w.r.t. a pure state $|\psi\rangle$.

Nobody has insider information about my quantum random numbers.

Royal Holloway
University of London

Royal Holloway
University of London

Rule (i)

(i) $P \geq 0$

Worth \$1 if E is true

ticket price $\$q < 0$

A is willing to sell the ticket for a negative amount of money. Sure loss!

Royal Holloway
University of London

Rule (ii)

(ii) $P(E) = 1$ if A believes that E is certain to occur.

Worth \$1 if E is true

ticket price $\$q < \$1$

A is willing to sell a ticket—which is definitely worth $\$1$ to her—for less than $\$1$. Sure loss!

Royal Holloway
University of London

Rule (iii)

(iii) $P(E \vee F) = P(E) + P(F)$ if A believes that E and F are mutually exclusive.

Let $H = E \vee F$, $E \wedge F = \emptyset$.

Worth \$1 if H is true	ticket price \$q
Worth \$1 if E is true	ticket price \$r
Worth \$1 if F is true	ticket price \$s

E.g., A would buy the blue ticket for $\$q$ and sell the green tickets for $\$r + \$s$. If $q > r + s$, sure loss!.

Royal Holloway
University of London

Rule (iv)

(iv) $P(E \wedge F) = P(E|F)P(F)$

Worth \$1 if $E \wedge F$
Worth $\$P(E|F)$ if $\neg F$

price $\$P(E|F)$

Royal Holloway
University of London

Rule (iv)

(iv) $P(E \wedge F) = P(E|F)P(F)$

Worth \$1 if $E \wedge F$ Worth $\$P(E\|F)$ if $\neg F$	price $\$P(E\|F)$
Worth \$1 if $E \wedge F$	price $\$P(E \wedge F)$

Royal Holloway
University of London

Rule (iv)

(iv) $P(E \wedge F) = P(E|F)P(F)$

Worth \$1 if $E \wedge F$ Worth $\$P(E\|F)$ if $\neg F$	price $\$P(E\|F)$
Worth \$1 if $E \wedge F$	price $\$P(E \wedge F)$
Worth $\$P(E\|F)$ if $\neg F$	price $\$P(E\|F)P(\neg F)$

Royal Holloway
University of London

Rule (iv)

(iv) $P(E \wedge F) = P(E|F)P(F)$

Worth \$1 if $E \wedge F$ Worth $\$P(E\|F)$ if $\neg F$	price $\$P(E\|F)$
Worth \$1 if $E \wedge F$	price $\$P(E \wedge F)$
Worth $\$P(E\|F)$ if $\neg F$	price $\$P(E\|F)P(\neg F)$

Consistency implies

$\$P(E|F) = \$P(E \wedge F) + P(E|F)P(\neg F)$

Rule (iv) follows using $P(\neg F) = 1 - P(F)$.