Knowledge and Information in Probabilistic Systems

Prakash Panangaden

PODC and CONCUR

PODC and CONCUR

- Two communities with shared interests but very different methods.

PODC and CONCUR

- Two communities with shared interests but very different methods.
- CONCUR: Emphasis on algebraic laws, equivalence, compositionality and modal logics.

PODC and CONCUR

- Two communities with shared interests but very different methods.
- CONCUR: Emphasis on algebraic laws, equivalence, compositionality and modal logics.
- PODC: Algorithms, combinatorial arguments, expressiveness, complexity and impossibility results.

PODC and CONCUR

- Two communities with shared interests but very different methods.
- CONCUR: Emphasis on algebraic laws, equivalence, compositionality and modal logics.
- PODC: Algorithms, combinatorial arguments, expressiveness, complexity and impossibility results.
- BOTH care about interaction between agents.

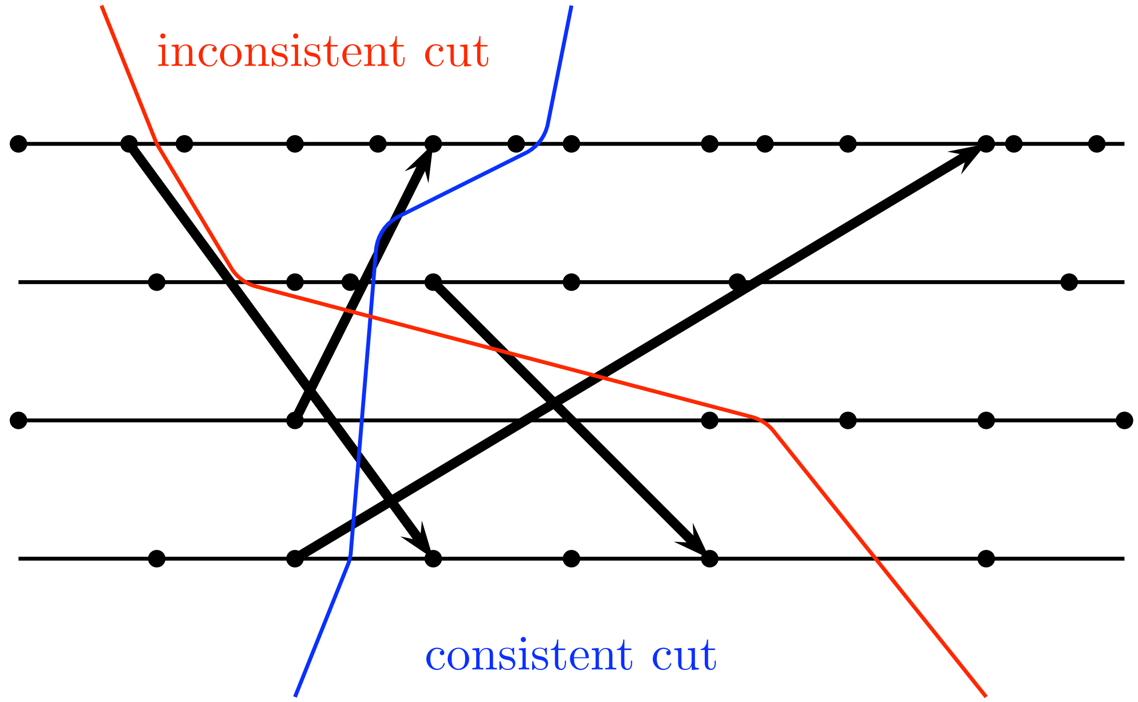
Knowledge

Knowledge

- Usually modelled with an equivalence relation on the set of states (possible worlds), which represents what the agents thinks is possible.

Knowledge

- Usually modelled with an equivalence relation on the set of states (possible worlds), which represents what the agents thinks is possible.
- If St is the set of states then the agent knows phi in state s if for all states t with s~t, phi is true in t.



A Lamport spacetime diagram

Agents: $\{1, \ldots, n\}$

Agents: $\{1, \ldots, n\}$

Propositions: $p, q, \ldots$

Agents: $\{1, \ldots, n\}$

Propositions: $p, q, \ldots$

Modal formulas: $K_i\phi$, where i is an agent

Agents: $\{1, \ldots, n\}$

Propositions: $p, q, \ldots$

Modal formulas: $K_i\phi$, where i is an agent

States: (a, c), a is a run, c is a consistent cut

Agents: $\{1, \ldots, n\}$

Propositions: $p, q, \ldots$

Modal formulas: $K_i \phi$, where i is an agent

States: (a, c), a is a run, c is a consistent cut

$(a, c) \sim_i (a', c')$ if the local states of i match

Agents: $\{1, \ldots, n\}$

Propositions: $p, q, \ldots$

Modal formulas: $K_i\phi$, where i is an agent

States: (a, c), a is a run, c is a consistent cut

$(a, c) \sim_i (a', c')$ if the local states of i match

$$(a, c) \models K_i\phi \text{ if}$$
$$\forall (a', c') \sim_i (a, c)\ (a', c') \models \phi$$

Axioms for Knowledge

1. All propositional tautologies
2. $(K_i\phi) \wedge (K_i(\phi \Rightarrow \psi)) \Rightarrow K_i\psi$
3. $K_i\phi \Rightarrow \phi$
4. $K_i\phi \Rightarrow K_iK_i\phi$
5. $\neg K_i\phi \Rightarrow K_i(\neg K_i\phi)$
6. *Modus Ponens*
7. From ϕ infer $K_i\phi$

Some Remarks

Some Remarks

- There are variant axiomatizations possible.

Some Remarks

- There are variant axiomatizations possible.
- The axioms given correspond to assuming that the possibility relation is an equivalence relation.

Some Remarks

- There are variant axiomatizations possible.
- The axioms given correspond to assuming that the possibility relation is an equivalence relation.
- The axioms given are for a static situation.

Some Remarks

- There are variant axiomatizations possible.
- The axioms given correspond to assuming that the possibility relation is an equivalence relation.
- The axioms given are for a static situation.
- Many combinations are possible: time, probability, dynamic update.

Co-algebras

- Intimately tied to transition systems and to modal logics.
- An algebra: op: A x A ---> A
- A co-algebra: co-op: A ---> A x A
- Split instead of combine.

Labelled Transition Systems as Coalgebras

Labelled Transition Systems as Coalgebras

Consider a map $t : S \to \mathcal{P}(S)$.

Labelled Transition Systems as Coalgebras

Consider a map $t : S \to \mathcal{P}(S)$.

This defines a transition system over S.

Labelled Transition Systems as Coalgebras

Consider a map $t : S \to \mathcal{P}(S)$.

This defines a transition system over S.

With labels: $t : S \times \mathcal{L} \to \mathcal{P}(S)$.

Labelled Transition Systems as Coalgebras

Consider a map $t : S \to \mathcal{P}(S)$.

This defines a transition system over S.

With labels: $t : S \times \mathcal{L} \to \mathcal{P}(S)$.

Which is the same as: $t \subseteq S \times \mathcal{L} \times S$.

Labelled Transition Systems as Coalgebras

Consider a map $t : S \to \mathcal{P}(S)$.

This defines a transition system over S.

With labels: $t : S \times \mathcal{L} \to \mathcal{P}(S)$.

Which is the same as: $t \subseteq S \times \mathcal{L} \times S$.

The usual notion of labelled transition system.

Bisimulation

An equivalence relation that is intimately related to transition systems.

$s \sim t$ means:

$\forall a \in \mathcal{L},\ s \xrightarrow{a} s'$ implies

$\exists t'$ such that $t \xrightarrow{a} t'$ with $s' \sim t'$

and vice versa.

May not be the most useful equivalence relation (far too fine) but it is mathematically natural and is intimately tied to the transition system.

Logic and Bisimulation

Logic and Bisimulation

Intimate tie-up between bisimulation and modal logic: van Bentham, Hennessy & Milner.

Logic and Bisimulation

Intimate tie-up between bisimulation and modal logic: van Bentham, Hennessy & Milner.

$$\phi ::== T | \neg\phi | \phi \wedge \phi | \langle a \rangle \phi$$

Logic and Bisimulation

Intimate tie-up between bisimulation and modal logic: van Bentham, Hennessy & Milner.

$$\phi ::== T|\neg\phi|\phi \wedge \phi|\langle a\rangle\phi$$

Two states are bisimilar *if and only if* they satisfy the same formulas of the modal logic.

Logic and Bisimulation

Intimate tie-up between bisimulation and modal logic: van Bentham, Hennessy & Milner.

$$\phi ::== T|\neg\phi|\phi \wedge \phi|\langle a\rangle\phi$$

Two states are bisimilar *if and only if* they satisfy the same formulas of the modal logic.

The modal formulas are the maximal set of first-order formulas invariant under bisimulation.

The trinity

- There is a close relation between
- transition systems and bisimulation
- modal logic and
- coalgebras.

Combining Modalities

- Combine coalgebras in a suitable way.
- Purely mathematical; one still needs a conceptual understanding.
- May have formidable technical difficulties: e.g. combining probability and nondeterminism.

How does Epistemic Logic Fit In?

How does Epistemic Logic Fit In?

- Epistemic logic is a modal logic.

How does Epistemic Logic Fit In?

- Epistemic logic is a modal logic.
- It concerns the behaviour of interacting agents.

How does Epistemic Logic Fit In?

- Epistemic logic is a modal logic.
- It concerns the behaviour of interacting agents.
- How does it relate, if at all?

Epistemic Ideas in Concurrency

Epistemic Ideas in Concurrency

- Security: information flow, anonymity.

Epistemic Ideas in Concurrency

- Security: information flow, anonymity.
- Suppose we model a protocol intended to maintain anonymity using a process algebra.

Epistemic Ideas in Concurrency

- Security: information flow, anonymity.
- Suppose we model a protocol intended to maintain anonymity using a process algebra.
- Nondeterminism is resolved by a “scheduler”; in the end we quantify over all schedulers.

Epistemic Ideas in Concurrency

- Security: information flow, anonymity.
- Suppose we model a protocol intended to maintain anonymity using a process algebra.
- Nondeterminism is resolved by a “scheduler”; in the end we quantify over all schedulers.
- But this includes schedulers that could leak information.

Example: Voting

Example: Voting

- Two candidates: a,b. Two voters: v,w.

Example: Voting

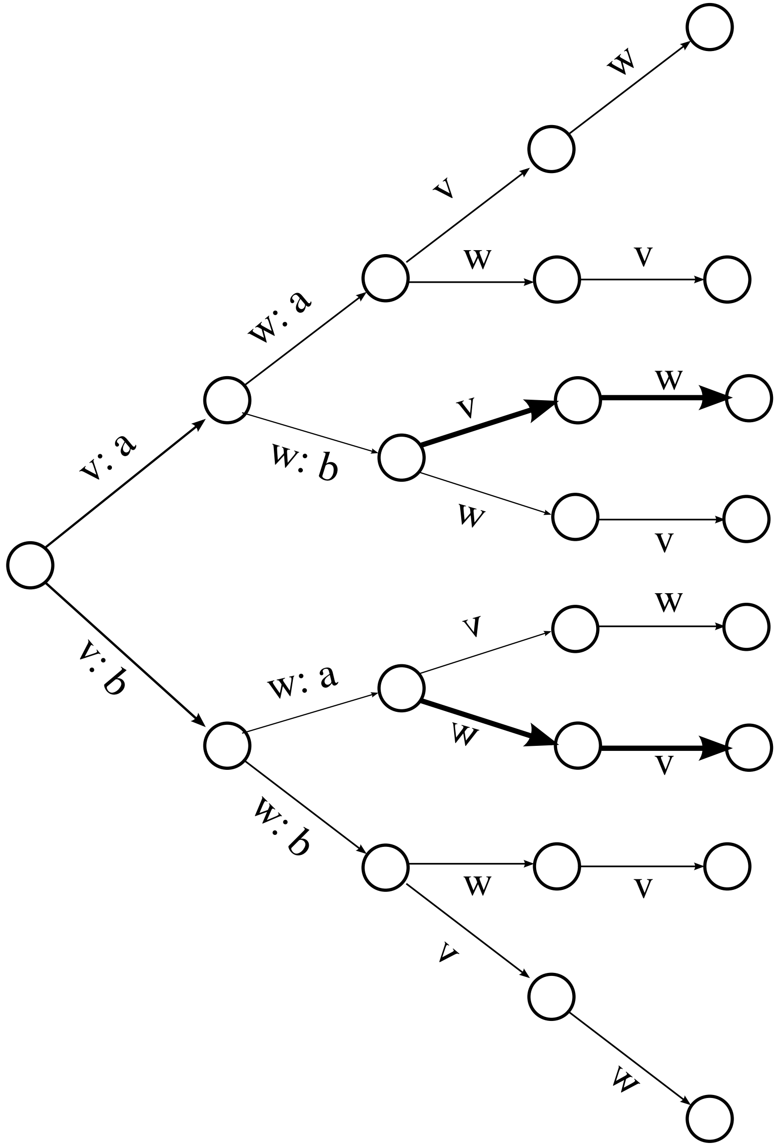
- Two candidates: a,b. Two voters: v,w.
- The system must reveal the list of people who actually voted (in any order) and the total votes for the candidate.

Example: Voting

- Two candidates: a,b. Two voters: v,w.
- The system must reveal the list of people who actually voted (in any order) and the total votes for the candidate.
- It must **not** reveal who voted for whom; unless the vote is unanimous.

Example: Voting

- Two candidates: a,b. Two voters: v,w.
- The system must reveal the list of people who actually voted (in any order) and the total votes for the candidate.
- It must **not** reveal who voted for whom; unless the vote is unanimous.
- A scheduler can leak the votes!



A scheduler that leaks voting preferences.

What do schedulers know?

What do schedulers know?

- The scheduler that resolves the nondeterminism in the order in which voters names are output should not “know” who voted for whom.

What do schedulers know?

- The scheduler that resolves the nondeterminism in the order in which voters names are output should not “know” who voted for whom.
- Chatzikokolakis and Palamidessi [CONCUR 07] described schedulers with an explicit syntax and operational semantics and used syntactic restrictions to control what scheduler knew.

What do schedulers know?

- The scheduler that resolves the nondeterminism in the order in which voters names are output should not “know” who voted for whom.
- Chatzikokolakis and Palamidessi [CONCUR 07] described schedulers with an explicit syntax and operational semantics and used syntactic restrictions to control what scheduler knew.
- They had **two** schedulers to resolve different choices.

What do schedulers know?

- The scheduler that resolves the nondeterminism in the order in which voters names are output should not “know” who voted for whom.
- Chatzikokolakis and Palamidessi [CONCUR 07] described schedulers with an explicit syntax and operational semantics and used syntactic restrictions to control what scheduler knew.
- They had **two** schedulers to resolve different choices.

Games and Knowledge

- Games are an ideal setting to explore epistemic concepts.
- Economists have been particularly active in developing these ideas.

Many types of games

Many types of games

- Games for verification: Luca de Alfaro, Henzinger, Chatterjee, Abramsky, Ong, Murawski,...

Many types of games

- Games for verification: Luca de Alfaro, Henzinger, Chatterjee, Abramsky, Ong, Murawski,...
- Games in economics: see, e.g. Adam Brandenburger's review on epistemic games.

Many types of games

- Games for verification: Luca de Alfaro, Henzinger, Chatterjee, Abramsky, Ong, Murawski,...
- Games in economics: see, e.g. Adam Brandenburger's review on epistemic games.
- Game semantics: Abramsky, Jagadeesan, Malacaria, Hyland, Ong, Nickau, Laird, McCusker...

Many types of games

- Games for verification: Luca de Alfaro, Henzinger, Chatterjee, Abramsky, Ong, Murawski,...
- Games in economics: see, e.g. Adam Brandenburger's review on epistemic games.
- Game semantics: Abramsky, Jagadeesan, Malacaria, Hyland, Ong, Nickau, Laird, McCusker...
- Games in logic: model theory, EF, Lorenzen,...

Games between schedulers.

Games between schedulers.

- In order to make the epistemic aspects more explicit we can think of schedulers as playing games.

Games between schedulers.

- In order to make the epistemic aspects more explicit we can think of schedulers as playing games.
- The concurrent process is the "board" and the moves end up choosing the action.

Games between schedulers.

- In order to make the epistemic aspects more explicit we can think of schedulers as playing games.
- The concurrent process is the "board" and the moves end up choosing the action.
- We control what the schedulers "know" by putting restrictions on the allowed strategies.

Restricting Strategies

Restricting Strategies

- What can an agent "see" in formulating its strategy? This controls what it "knows."

Restricting Strategies

- What can an agent "see" in formulating its strategy? This controls what it "knows."
- One possible restriction: an agent knows what choices are available to it **and what choices were available to it in the past.**

Restricting Strategies

- What can an agent "see" in formulating its strategy? This controls what it "knows."
- One possible restriction: an agent knows what choices are available to it **and what choices were available to it in the past.**
- This corresponds exactly to the CP syntactic restrictions [C,Knight, P 08].

Restricting Strategies

- What can an agent "see" in formulating its strategy? This controls what it "knows."
- One possible restriction: an agent knows what choices are available to it **and what choices were available to it in the past.**
- This corresponds exactly to the CP syntactic restrictions [C,Knight, P 08].
- Easy to impose epistemic restrictions on strategies.

Games and Concurrency

Games and Concurrency

- New direction in concurrency: Process algebras as defining interacting agents.

Games and Concurrency

- New direction in concurrency: Process algebras as defining interacting agents.
- Games are already used in many ways in concurrency, semantics, logic and economics.

Games and Concurrency

- New direction in concurrency: Process algebras as defining interacting agents.
- Games are already used in many ways in concurrency, semantics, logic and economics.
- But we still do not have a systematic way of describing and reasoning about interacting agents algebraically.

Some specific goals

Some specific goals

- Develop a process algebra for agents playing games.

Some specific goals

- Develop a process algebra for agents playing games.
- Use epistemic logic to control what agents know.

Some specific goals

- Develop a process algebra for agents playing games.
- Use epistemic logic to control what agents know.
- Tie this logic to strategies in a way analogous to the relation between bisimulation and modal logic.

Some specific goals

- Develop a process algebra for agents playing games.
- Use epistemic logic to control what agents know.
- Tie this logic to strategies in a way analogous to the relation between bisimulation and modal logic.
- Use this to reason about information flow.

Probability

Probability

- What happens when we add probability to the mix?

Probability

- What happens when we add probability to the mix?
- There is a beautiful relation between probability, bisimulation and logic.

Probability

- What happens when we add probability to the mix?
- There is a beautiful relation between probability, bisimulation and logic.
- We shall review this quickly.

Fully Probabilistic Transition Systems

- A transition system with probabilities and actions (labels) associated with the transitions.

- $$(S, \mathcal{L}, \forall a \in \mathcal{L}\ T_a : S \times S \to [0,1])$$

- The model is *reactive*: All probabilistic data is *internal* - no probabilities associated with environment behaviour.

Fully Probabilistic Transition Systems

- A transition system with probabilities and actions (labels) associated with the transitions.
-

$$(S, \mathcal{L}, \forall a \in \mathcal{L}\ T_a : S \times S \to [0, 1])$$

- The model is *reactive*: All probabilistic data is *internal* - no probabilities associated with environment behaviour.

Extended to systems with *arbitrary measurable* state spaces in LICS'97 by Blute, Desharnais, Edalat and P. We called them *Labelled Markov Processes*, very similar to *Markov Decision Processes* without the rewards.

Larsen-Skou Bisimulation

- Let $\mathcal{S} = (S, \mathcal{L}, T_a)$ be a probabilistic transition system.
- An equivalence relation R on S is a **bisimulation** if whenever sRs', with $s, s' \in S$, we have that for all $a \in \mathcal{L}$ and every R-equivalence class, A, $T_a(s, A) = T_a(s', A)$.
- The notation $T_a(s, A)$ means "the probability of starting from s and jumping to a state in the set A."
- Two states are bisimilar if there is some bisimulation relation R relating them.

Larsen-Skou Bisimulation

- Let $\mathcal{S} = (S, \mathcal{L}, T_a)$ be a probabilistic transition system.
- An equivalence relation R on S is a **bisimulation** if whenever sRs', with $s, s' \in S$, we have that for all $a \in \mathcal{L}$ and every R-equivalence class, A, $T_a(s, A) = T_a(s', A)$.
- The notation $T_a(s, A)$ means "the probability of starting from s and jumping to a state in the set A."
- Two states are bisimilar if there is some bisimulation relation R relating them.

Some painful technical problems had to be overcome to extend this to LMPs.

Logical Characterization of Bisimulation

Logical Characterization of Bisimulation

$$\phi ::== \mathsf{T} | \phi_1 \wedge \phi_2 | \langle a \rangle_q \phi$$

Logical Characterization of Bisimulation

$$\phi ::== \mathsf{T} | \phi_1 \wedge \phi_2 | \langle a \rangle_q \phi$$

$$s \models \langle a \rangle_q \phi \text{ iff } \exists A \in \Sigma (\forall s' \in A, s' \models \phi) \wedge (\tau_a(s, A) > q).$$

Logical Characterization of Bisimulation

$$\phi ::== \mathsf{T} | \phi_1 \wedge \phi_2 | \langle a \rangle_q \phi$$

$$s \models \langle a \rangle_q \phi \text{ iff } \exists A \in \Sigma (\forall s' \in A, s' \models \phi) \wedge (\tau_a(s, A) > q).$$

Two systems are bisimilar iff they obey the same formulas of this logic
[Desharnais, Edalat, P 1998,2002]

Logical Characterization of Bisimulation

$$\phi ::== \mathsf{T} | \phi_1 \wedge \phi_2 | \langle a \rangle_q \phi$$

$$s \models \langle a \rangle_q \phi \text{ iff } \exists A \in \Sigma (\forall s' \in A, s' \models \phi) \wedge (\tau_a(s, A) > q).$$

Two systems are bisimilar iff they obey the same formulas of this logic
[Desharnais, Edalat, P 1998,2002]

Notice that there is no negation not even any negative propositions!
Simpler than the non-probabilistic case.

Probabilistic logic and probabilistic bisimulation fit together beautifully.

Probabilistic logic and probabilistic bisimulation fit together beautifully.

Kozen explored probabilistic dynamic logic and discovered a remarkable Stone-type duality.

Probabilistic logic and probabilistic bisimulation fit together beautifully.

Kozen explored probabilistic dynamic logic and discovered a remarkable Stone-type duality.

Probability theory itself is a kind of logic!

Kozen's Analogy

Kozen's Analogy

Logic	Probability
State : s	Distribution : μ
Formula : ϕ	Random Variable : X
Satisfaction : $s \models \phi$	Integration : $\int X d\mu$

Kozen's Analogy

Logic	Probability
State : s	Distribution : μ
Formula : ϕ	Random Variable : X
Satisfaction : $s \models \phi$	Integration : $\int X d\mu$

Probability theory as a kind of "logic."

Probability and Knowledge

Probability and Knowledge

- The main goal : reasoning under uncertainty. Classic texts available by Pearl and by Halpern.

Probability and Knowledge

- The main goal : reasoning under uncertainty. Classic texts available by Pearl and by Halpern.
- What is the right logic?

Probability and Knowledge

- The main goal : reasoning under uncertainty. Classic texts available by Pearl and by Halpern.
- What is the right logic?
- For “pure” probability conditioning serves as an analogue of logical implication.

Probability and Knowledge

- The main goal : reasoning under uncertainty. Classic texts available by Pearl and by Halpern.
- What is the right logic?
- For "pure" probability conditioning serves as an analogue of logical implication.
- What happens when we combine probability and knowledge or belief?

Probabilistic Epistemic Logic

- One can combine modalities for probability and knowledge.
- Interpret them using epistemic probability frames.
- Can be generalized to non measure-theoretic formalisms for modelling uncertainty.
- See “Reasoning About Uncertainty” by J. Halpern

Information vs Knowledge

- Information theory measures information in bits. No attempt to say which bits are important.
- Information theory gives "inference rules" for reasoning about how information is updated.
- Is information theory a kind of logic?

What is information?

What is information?

- A measure of uncertainty.

What is information?

- A measure of uncertainty.
- Can we really analyze it quantitatively?

What is information?

- A measure of uncertainty.
- Can we really analyze it quantitatively?
- What do the numerical values mean?

What is information?

- A measure of uncertainty.
- Can we really analyze it quantitatively?
- What do the numerical values mean?
- Is it tied to "knowledge"?

What is information?

- A measure of uncertainty.
- Can we really analyze it quantitatively?
- What do the numerical values mean?
- Is it tied to "knowledge"?
- Is it subjective?

What do we want?

What do we want?

We want a definition that satisfies the following conditions:

What do we want?

We want a definition that satisfies the following conditions:

For a point distribution the uncertainty is 0

For a uniform distribution the uncertainty is maximized.

What do we want?

We want a definition that satisfies the following conditions:

For a point distribution the uncertainty is 0

For a uniform distribution the uncertainty is maximized.

When we combine systems the uncertainty is **additive**

What do we want?

We want a definition that satisfies the following conditions:

For a point distribution the uncertainty is 0

For a uniform distribution the uncertainty is maximized.

When we combine systems the uncertainty is **additive**

As we vary the probabilities the uncertainty changes

What do we want?

We want a definition that satisfies the following conditions:

For a point distribution the uncertainty is 0
For a uniform distribution the uncertainty is maximized.

When we combine systems the uncertainty is **additive**

As we vary the probabilities the uncertainty changes

continuously

Entropy

Entropy

$$H(p_1, \ldots, p_n) = -\sum_i p_i \log_2 p_i$$

Entropy

$$H(p_1, \ldots, p_n) = -\sum_i p_i \log_2 p_i$$

- $H(0, 0, \ldots, 1, 0, \ldots, 0) = 0$
- $H(\frac{1}{n}, \ldots, \frac{1}{n}) = \log_2 n.$
- Clearly continuous.

Are there other candidates?

Are there other candidates?

Entropy is the unique continuous function that is:

Are there other candidates?

Entropy is the unique continuous function that is:

- maximized by the uniform distribution
- minimized by the point distribution
- additive when you combine systems
- and ....

What does it tell us?

If you have a distribution $p(s)$ on a set S,
you can define a code such that it takes $H(p)$
bits on the average to encode the members of the set.

How far apart are distributions ?

We want a “distance” between distributions.

How far apart are distributions ?

We want a "distance" between distributions.

$$KL(p \mapsto q) = n \sum_{s \in S} p(s)[\log_2 p(s) - \log_2 q(s).$$

How far apart are distributions ?

We want a "distance" between distributions.

$$KL(p \mapsto q) = n \sum_{s \in S} p(s)[\log_2 p(s) - \log_2 q(s).$$

Recall that it takes $H(p)$ bits to describe a set distributed according to p. What if we used q instead?

How far apart are distributions ?

We want a "distance" between distributions.

$$KL(p \mapsto q) = n \sum_{s \in S} p(s)[\log_2 p(s) - \log_2 q(s).$$

Recall that it takes $H(p)$ bits to describe a set distributed according to p. What if we used q instead?

It would require $H(p) + KL(p \mapsto q)$ bits.

Relative Entropy

The Kullback-Leibler distance is often called *relative entropy.*

Relative Entropy

The Kullback-Leibler distance is often called *relative entropy.*

Suppose $S = \{a, b\}$ and $p(a) = \frac{1}{2} = p(b)$ while $q(a) = \frac{1}{4}$ and $q(b) = \frac{3}{4}$.

Relative Entropy

The Kullback-Leibler distance is often called *relative entropy.*

Suppose $S = \{a, b\}$ and $p(a) = \frac{1}{2} = p(b)$ while $q(a) = \frac{1}{4}$ and $q(b) = \frac{3}{4}$.

$KL(p \mapsto q) = 0.2075$ and $KL(q \mapsto p) = 0.1887$.

Mutual Information

Mutual Information

- A measure of how much one "knows" about one distribution given another distribution.

Mutual Information

- A measure of how much one "knows" about one distribution given another distribution.
- More precisely, given a correlated pair of random variables, given the outcome of one of them what do you "know" about the other one.

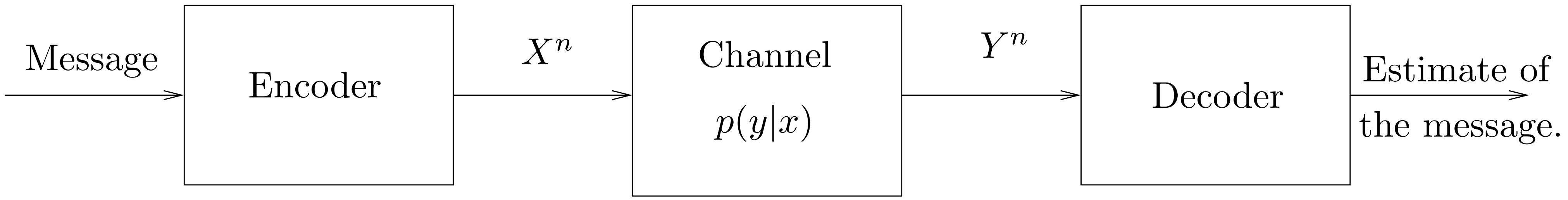
Mutual Information

- A measure of how much one "knows" about one distribution given another distribution.
- More precisely, given a correlated pair of random variables, given the outcome of one of them what do you "know" about the other one.
- Written $I(X;Y) = I(Y;X)$.

Mutual Information

- A measure of how much one “knows” about one distribution given another distribution.
- More precisely, given a correlated pair of random variables, given the outcome of one of them what do you “know” about the other one.
- Written I(X;Y) = I(Y;X).
- Clearly an epistemic concept.

Channels



A typical channel.

How well can we estimate the intended message if the channel is noisy?

Channel Capacity

We want some way of measuring how well we can estimate the message based on what we receive.

Channel Capacity

We want some way of measuring how well we can estimate the message based on what we receive.

How about $I(X;Y)$?

Channel Capacity

We want some way of measuring how well we can estimate the message based on what we receive.

How about $I(X;Y)$?

But this depends on the input distribution!

Channel Capacity

We want some way of measuring how well we can estimate the message based on what we receive.

How about $I(X;Y)$?

But this depends on the input distribution!

$$C = \max_{p(x)} I(X;Y).$$

Anonymity

Anonymity

- Define a protocol that keeps the identity of an agent secret.

Anonymity

- Define a protocol that keeps the identity of an agent secret.
- Well known examples: dining cryptographers, crowds, etc.

Anonymity

- Define a protocol that keeps the identity of an agent secret.
- Well known examples: dining cryptographers, crowds, etc.
- Randomization is a key resource used in these protocols

Anonymity

- Define a protocol that keeps the identity of an agent secret.
- Well known examples: dining cryptographers, crowds, etc.
- Randomization is a key resource used in these protocols
- Need probabilistic notions of anonymity: Halpern and O'Neill; Bhargava and Palamidessi, Chatzikokolakis and Palamidessi

Anonymity and Capacity

Anonymity and Capacity

- Anonymity protocols try to keep the identity of an agent secret.

Anonymity and Capacity

- Anonymity protocols try to keep the identity of an agent secret.
- One can view such a protocol as a communication channel.

Anonymity and Capacity

- Anonymity protocols try to keep the identity of an agent secret.
- One can view such a protocol as a communication channel.
- The lack of anonymity is measured by the channel capacity.

Anonymity and Capacity

- Anonymity protocols try to keep the identity of an agent secret.
- One can view such a protocol as a communication channel.
- The lack of anonymity is measured by the channel capacity.
- Perfect anonymity corresponds to zero capacity.

Information Theory and Epistemic Logic

Information Theory and Epistemic Logic

- Krasucki, Parikh and Ndjatou: How much common knowledge is there?

Information Theory and Epistemic Logic

- Krasucki, Parikh and Ndjatou: How much common knowledge is there?
- What if there are two agents with slightly different partitions of the possible worlds?

Information Theory and Epistemic Logic

- Krasucki, Parikh and Ndjatou: How much common knowledge is there?
- What if there are two agents with slightly different partitions of the possible worlds?
- Epistemic logic may tell us that nothing is common knowledge!

Information Theory and Epistemic Logic

- Krasucki, Parikh and Ndjatou: How much common knowledge is there?
- What if there are two agents with slightly different partitions of the possible worlds?
- Epistemic logic may tell us that nothing is common knowledge!
- Intuitively, there should be high probability of one agent guessing what the other knows.

- Key point noted by Krasucki et al.: How much information is acquired when probabilities change as a result of new data?

- Key point noted by Krasucki et al.: How much information is acquired when probabilities change as a result of new data?

- They define **information gain** and develop its properties and its relations with mutual information and common knowledge.

- Key point noted by Krasucki et al.: How much information is acquired when probabilities change as a result of new data?
- They define **information gain** and develop its properties and its relations with mutual information and common knowledge.
- Information gain turns out to be exactly the same as relative entropy!

Approximate Reasoning

Approximate Reasoning

- Orthodox logic is too sensitive to perturbations in quantitative data.

Approximate Reasoning

- Orthodox logic is too sensitive to perturbations in quantitative data.
- One needs metrics and metric reasoning principles: Jou and Smolka, DGJP, van Breugel and Worrell, ...

Approximate Reasoning

- Orthodox logic is too sensitive to perturbations in quantitative data.
- One needs metrics and metric reasoning principles: Jou and Smolka, DGJP, van Breugel and Worrell, ...
- What are appropriate "approximate" concepts of knowledge? Surely something information theoretic.

Approximate Reasoning

- Orthodox logic is too sensitive to perturbations in quantitative data.
- One needs metrics and metric reasoning principles: Jou and Smolka, DGJP, van Breugel and Worrell, ...
- What are appropriate "approximate" concepts of knowledge? Surely something information theoretic.
- But, beware of applying information theory naively: there are many counter-examples.

Some goals

Some goals

- Develop a theory of probabilistic interacting agents: agents playing stochastic games.

Some goals

- Develop a theory of probabilistic interacting agents: agents playing stochastic games.
- This will lead to a mixture of probability and nondeterminism.

Some goals

- Develop a theory of probabilistic interacting agents: agents playing stochastic games.
- This will lead to a mixture of probability and nondeterminism.
- Additivity is lost: one has capacities instead. What information-theoretic concepts apply?

Some goals

- Develop a theory of probabilistic interacting agents: agents playing stochastic games.
- This will lead to a mixture of probability and nondeterminism.
- Additivity is lost: one has capacities instead. What information-theoretic concepts apply?
- Relate the dynamics with an appropriate quantitative logic: perhaps a suitable multi-agent generalization of information theory.

Information Theory as a Logic

- Why does it matter?
- It would give us compositional ways of reasoning about information flow.
- Perhaps a duality theory lurking underneath the surface.

Quantum Information

Quantum Information

- Information is physical -- Landauer

Quantum Information

- Information is physical -- Landauer
- but Physics is logical -- Abramsky

Quantum Information

- Information is physical -- Landauer
- but Physics is logical -- Abramsky
- Entirely new phenomena are possible: entanglement and teleportation, knowing “less than nothing!” [Andreas Winter]

Quantum Information

- Information is physical -- Landauer
- but Physics is logical -- Abramsky
- Entirely new phenomena are possible: entanglement and teleportation, knowing "less than nothing!" [Andreas Winter]
- Can it do anything for standard distributed protocols?

Leader election

Leader election

- Using an appropriate shared quantum state (the W state) n agents can choose a leader in one step, with each agent using the same protocol and with every agent having the same probability of being elected.

Leader election

- Using an appropriate shared quantum state (the W state) n agents can choose a leader in one step, with each agent using the same protocol and with every agent having the same probability of being elected.
- With a GHZ state one can do distributed consensus.

Leader election

- Using an appropriate shared quantum state (the W state) n agents can choose a leader in one step, with each agent using the same protocol and with every agent having the same probability of being elected.
- With a GHZ state one can do distributed consensus.
- Both these protocols are trivial: can we use these resources to do more clever things?

Teleportation

Teleportation

- If Alice and Bob share an entangled pair, Alice can send two classical bits to Bob which allows Bob to reconstruct a quantum state that Alice had.

Teleportation

- If Alice and Bob share an entangled pair, Alice can send two classical bits to Bob which allows Bob to reconstruct a quantum state that Alice had.
- At the end of the protocol Alice will not have the quantum state anymore.

Quantum Knowledge

Quantum Knowledge

- If one adapts the standard epistemic machinery of Kripke structures [van der Meyden et al.] you get wierd effects: Alice no longer knows -- even in a time stamped sense -- what she once knew.

Quantum Knowledge

- If one adapts the standard epistemic machinery of Kripke structures [van der Meyden et al.] you get wierd effects: Alice no longer knows -- even in a time stamped sense -- what she once knew.
- Another approach [d'Hondt, P]: there is no such thing as quantum knowledge!

Quantum Knowledge

- If one adapts the standard epistemic machinery of Kripke structures [van der Meyden et al.] you get wierd effects: Alice no longer knows -- even in a time stamped sense -- what she once knew.
- Another approach [d'Hondt, P]: there is no such thing as quantum knowledge!
- Measurements create classical knowledge.

Goals

Goals

- What is the logic of quantum information? Strange things happen: negative mutual information.

Goals

- What is the logic of quantum information? Strange things happen: negative mutual information.
- Reason compositionally about quantum protocols: process algebras, equivalences, resource inequalities [Devetak et al.]

Goals

- What is the logic of quantum information? Strange things happen: negative mutual information.
- Reason compositionally about quantum protocols: process algebras, equivalences, resource inequalities [Devetak et al.]
- Develop interesting protocols for distributed computing tasks.

Conclusions

- Concurrency theory should incorporate the idea of games between agents and investigate richer modes of interaction than currently available: some key ideas due to Abramsky.
- Epistemic ideas should come to the fore.
- Information theory should be developed as a kind of quantitative epistemic logic.

Wild ideas

Wild ideas

- What is information theory in a “relativistic” setting?

Wild ideas

- What is information theory in a “relativistic” setting?
- Mutual information is very dependent on absolute time, what does it mean when we do not have absolute global states?

Wild ideas

- What is information theory in a "relativistic" setting?
- Mutual information is very dependent on absolute time, what does it mean when we do not have absolute global states?
- Believe it or not "relativistic quantum information theory" is alive and well!!

Thanks for listening!

Thanks to Samson Abramsky, Vincent Danos, Josee Desharnais, Vineet Gupta, Radha Jagadeesan, Sophia Knight, Dexter Kozen, Keye Martin, Catuscia Palamidessi, Caitlin Phillips, Doina Precup and many others.