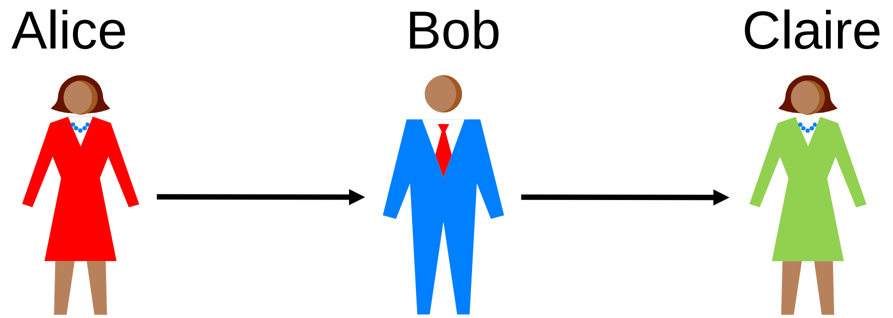
Subjective Logic and its applications to Security and Trust

NISNet Winter School
Finse, May 2011

Audun Jøsang, University of Oslo
http://folk.uio.no/josang/

How to model trust relationships?



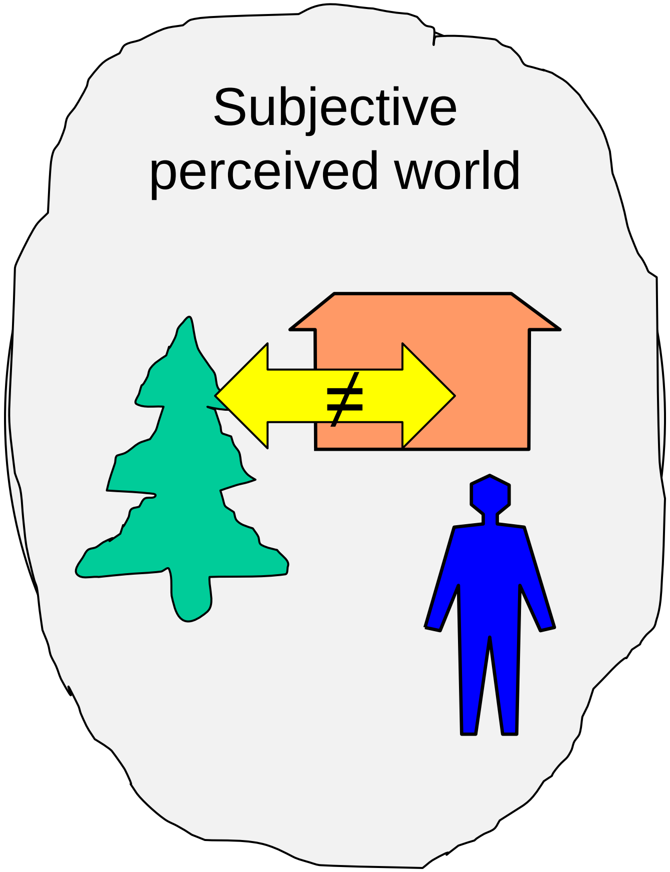
- Probabilities: $p(A{:}C) = p(A{:}B) \cdot p(B{:}C)$
- Min: $T(A{:}C) = \mathrm{Min}[\ T(A{:}B), T(B{:}C)\ ]$
- Max: $T(A{:}C) = \mathrm{Max}[\ T(A{:}B), T(B{:}C)\ ]$
- Average: $T(A{:}C) = (\ T(A{:}B) + T(B{:}C)\ )/2$

- What is needed is a formalism that can express and compute with uncertainty, i.e. *“I don’t know”*
- The answer is: Subjective Logic

Tutorial overview

- Semantic and formal representations of subjective opinions,
- The most important operators of subjective logic,
- Applications of subjective logic in the areas of:
  - Information fusion;
  - Trust reasoning
  - Intelligence analysis

Objective World v. Subjective World
(assumed) (perceived)



Characteristics and Formalisms

<u>Assumed world</u>

- Characteristics:
  - Crisp, frequentist, quantum
- Formalisms:
  - Binary logic
  - Frequentist probabilites
  - Quantum logic

<u>Perceived world</u>

- Characteristics:
  - Vague, fuzzy, uncertain
- Formalisms:
  - Subjective probabilities
  - Multi-valued logics
  - Fuzzy logic
  - Probabilistic logics
  - Subjective logic

Probabilistic and Subjective Logics

- Binary Logic
  - Expresses structures of propositions and argument models
- Probability Calculus
  - Expresses degrees of truth of propositions

- Probabilistic Logic
  - Proposition structures
  - Degrees of truth (probability values)

- Uncertainty
  - Expresses uncertainty about probability values

- Subjective logic
  - Proposition structures
  - Degrees of truth
  - Explicit uncertainty

Probabilistic Logic Examples

Binary Logic	**Probabilistic logic**
AND: $x \wedge y$	$p(x \wedge y) = p(x)p(y)$
OR: $x \vee y$	$p(x \vee y) = p(x) + p(y) - p(x)p(y)$
MP: $\{ x \rightarrow y,\ x \} \ \Rightarrow \ y$	$p(y) = p(x)p(y \mid x) + p(\bar{x})p(y \mid \bar{x})$
MT: $\{ x \rightarrow y, \bar{y} \} \ \Rightarrow \ \bar{x}$	$p(x \mid y) = \frac{a(x)p(y \mid x)}{a(x)p(y \mid x) + a(\bar{x})p(y \mid \bar{x})}$ $p(x \mid \bar{y}) = \frac{a(x)p(\bar{y} \mid x)}{a(x)p(\bar{y} \mid x) + a(\bar{x})p(\bar{y} \mid \bar{x})}$ $p(x) = p(y)p(x \mid y) + p(\bar{y})p(x \mid \bar{y})$

a: base rate

Probability and Uncertainty

Frequentist:

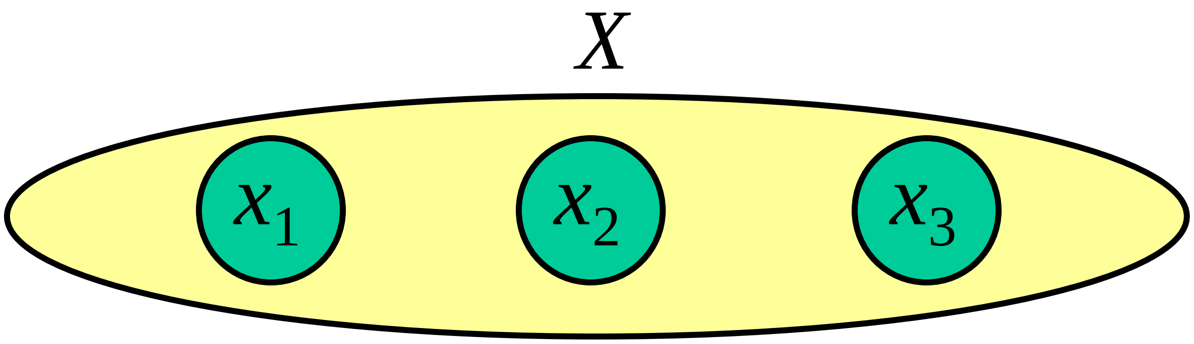
- *Relative frequency of "6" when throwing this dice is 1/6*
- Certain when based on much evidence
- Uncertain when based on little evidence

Subjective:

- *Probability of end of the world within 100Y is 0.5*
- Certain when structure of system is known
- Uncertain when structure of system is unknown

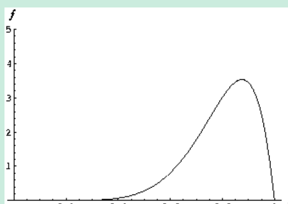
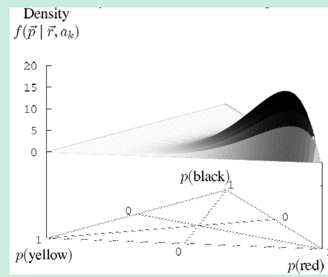
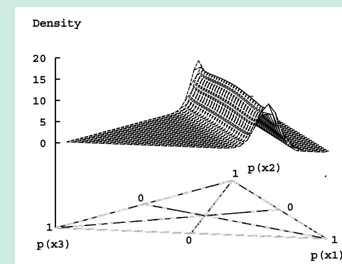
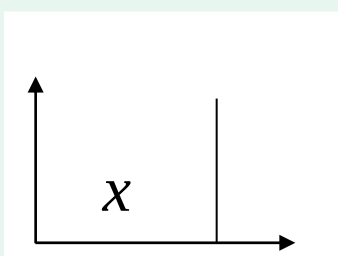
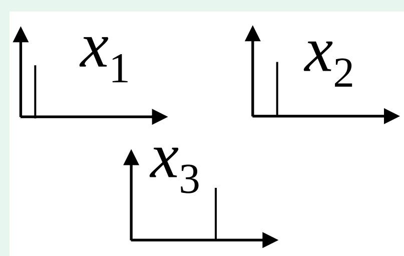
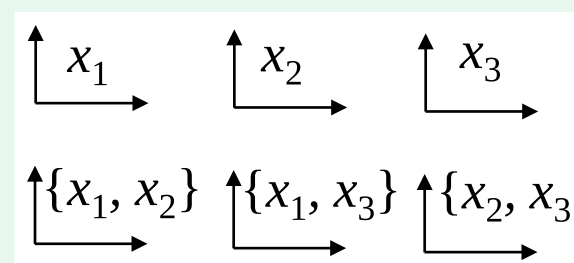
A Frame and its Reduce Powerset

- A frame X is a state space of distinct possibilities



- The powerset $\mathcal{P}(X) = 2^X$, the set of subsets of X
- The reduced powerset $\mathcal{R}(X) = \mathcal{P}(X) \setminus \{X, \emptyset\}$
- $\mathcal{R}(X) = \{\ x_1, x_2, x_3, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}\ \}$
- Cardinality $|X|$ (= 3 in this example)
- Cardinality $|\mathcal{R}(X)| = 2^{|X|} - 2$ (= 6 in this example)

Opinion Classes

	Binomial Opinion **Binary frame X** **Focal element x**	**Multinomial Opinion** **n-ary frame X** **Focal elements $x \in X$**	**Hyper Opinion** **n-ary frame X** **Focal elements $x \in \mathcal{R}(X)$**
Uncertain $u>0$ Corre- sponds to:	UB Opinion. Beta PDF  FIG 1: Beta function after 7 positive and 1 negative results	UM Opinion. Dirichlet PDF over X 	UH Opinion. Dirichlet PDF over $\mathcal{R}(X)$ 
Dogmatic $u=0$ Corre- sponds to:	DB Opinion. Probability of x 	DM Opinion. Proba. distr. over X 	DH Opinion. Proba. distr. over $\mathcal{R}(X)$ 

Binomial subjective opinions

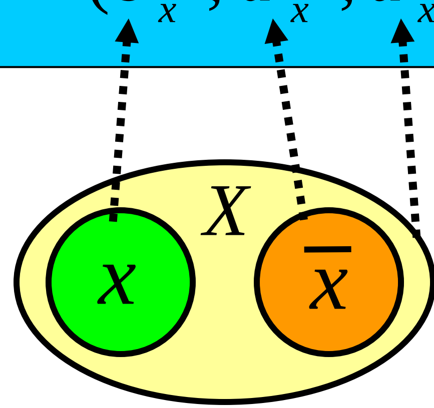
- Belief masses on binary frames
  - $b_x^A = b(x)$ is observer A's belief in x
  - $d_x^A = b(\bar{x})$ is observer A's disbelief in x
  - $u_x^A = b(X)$ is observer A's uncertainty about x
  - a_x^A is the base rate of x

Binomial opinion

$$\omega_x^A = (b_x^A, d_x^A, u_x^A, a_x^A)$$

base rate of x

Binary frame



$$b_x^A + d_x^A + u_x^A = 1$$

Opinion triangle

- Ordered quadruple:

  $\omega_x = (b_x, d_x, u_x, a_x)$

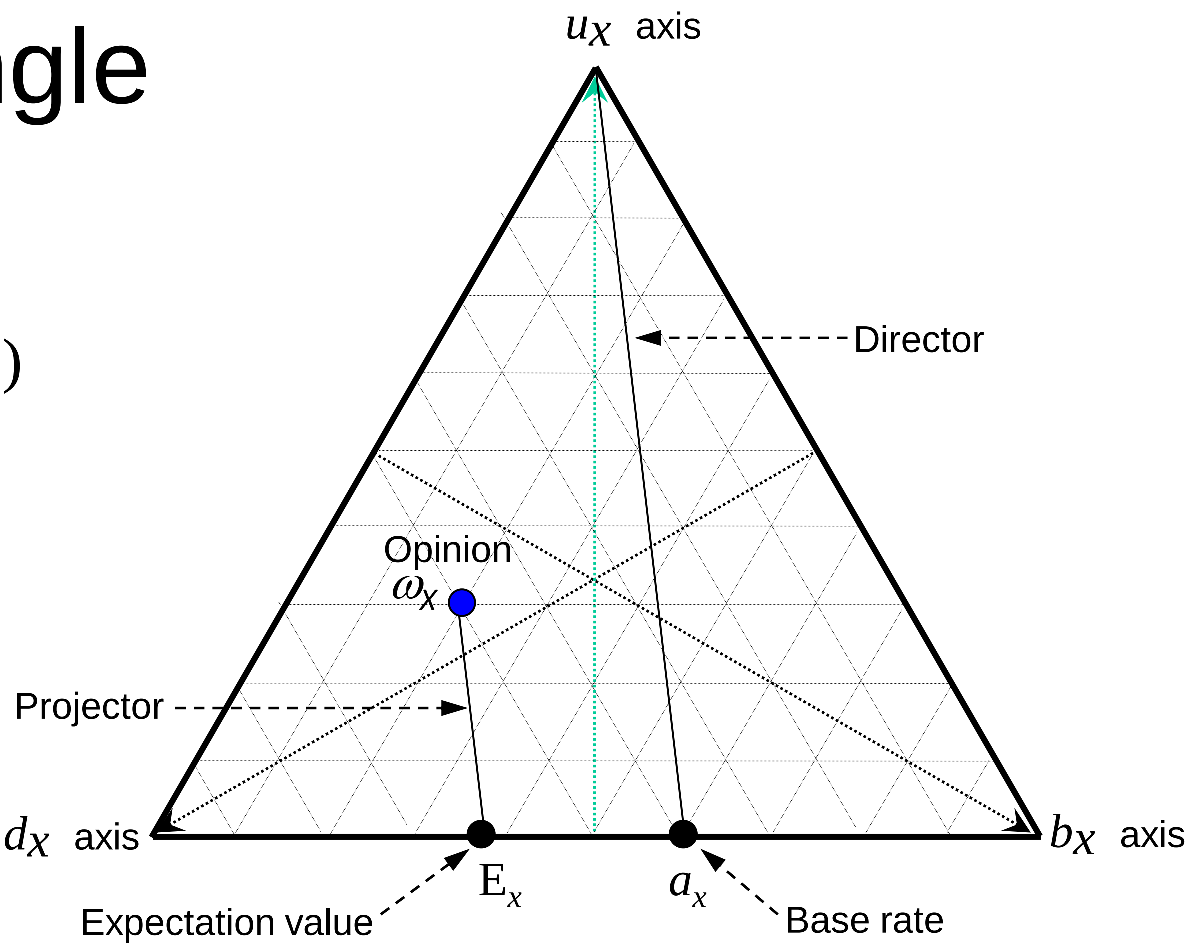
  – b_x : belief

  – d_x : disbelief

  – u_x : uncertainty

  – a_x : base rate

- $b_x + d_x + u_x = 1$



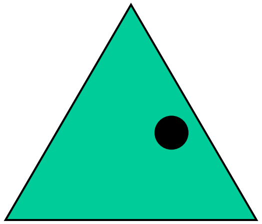
- Probability expectation value: $E(\omega_x) = b_x + a_x u_x$

Example $\omega_x = (0.2, 0.5, 0.3, 0.6)$, $E(\omega_x) = 0.38$

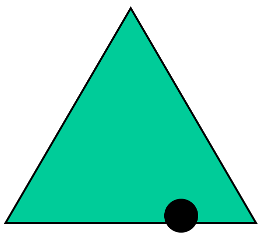
What are base rates?

- In probability and statistics, **base rate** refers to category probability unconditioned on evidence, often referred to as prior probabilities.
- For example, if it were the case that 1% of the public are "medical professionals" and 99% of the public are *not* "medical professionals“, then the base rates in this case are 1% and 99%, respectively.
- E.g. when picking a random person, the prior probability of being a medical professional is 1%

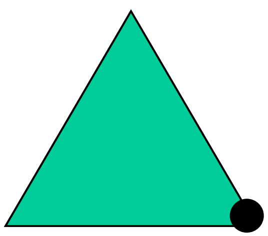
Opinion types



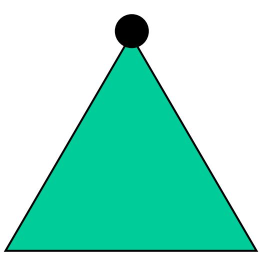
General uncertain opinion: $u_x \neq 0$.



Dogmatic opinion: $u_x = 0$.
Equivalent to probabilities.



Absolute opinion: $b_x = 1$.
Equivalent to TRUE.



Vacuous opinion: $u_x = 1$.
Equivalent to UNDEFINED.

Binomial opinions as Beta PDF

$$\mathrm{Beta}(p \mid \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha - 1}(1 - p)^{\beta - 1}$$

$$\alpha = r + Wa$$

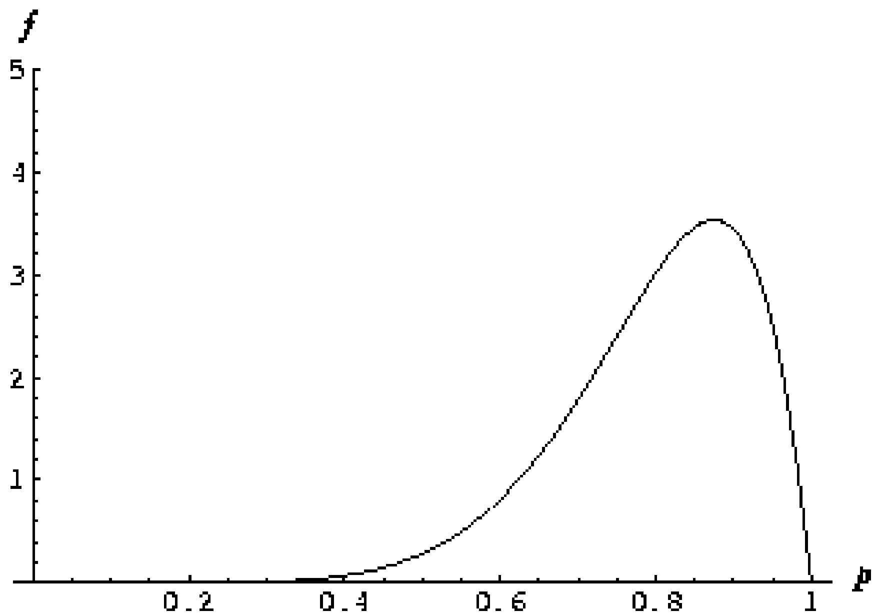
$$\beta = s + W(1\text{-}a)$$

r: # observations of x

s: # observations of $\bar{x}$

a: base rate of x

$W = 2$: non-informative prior weight



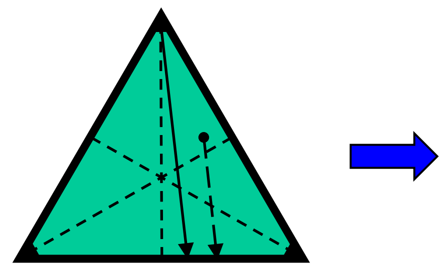
Example: $r = 7$, $s = 1$, $a = 0.5$ (default), $\mathrm{E}(p) = 0.8$

Binomial Opinion ↔ Beta PDF

- (r,s,a) represents Beta PDF parameters.
- (b,d,u,a) represents binomial opinion.

- Op → Beta:

$$\begin{cases} r = Wb \,/\, u \\ s = Wd \,/\, u \\ b + d + u = 1 \end{cases}$$



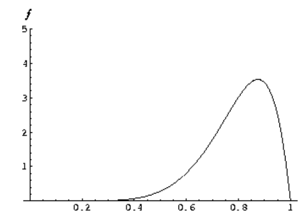


FIG 1: Beta function after 7 positive and 1 negative results

- Beta → Op:

$$\begin{cases} b = \dfrac{r}{r+s+W} \\ d = \dfrac{s}{r+s+W} \\ u = \dfrac{W}{r+s+W} \end{cases}$$

$W = 2$

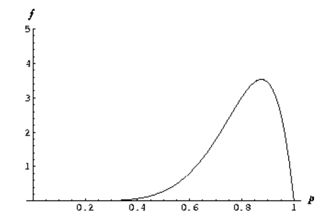
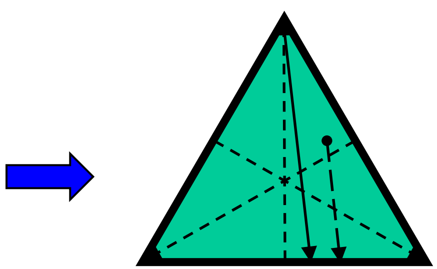
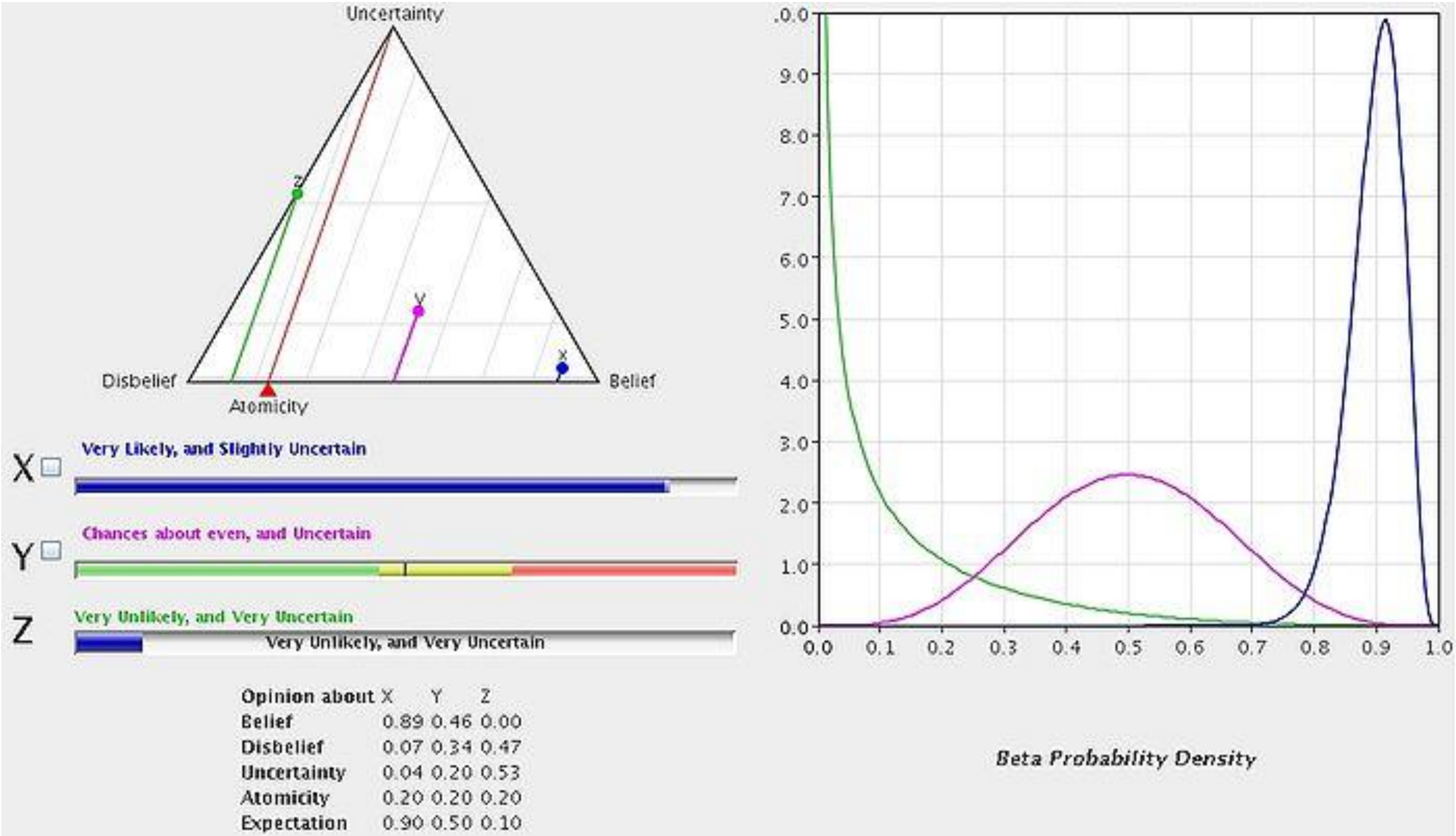


FIG 1: Beta function after 7 positive and 1 negative results



Online demo



http://folk.uio.no/josang/sl/

Fuzzy verbal categories

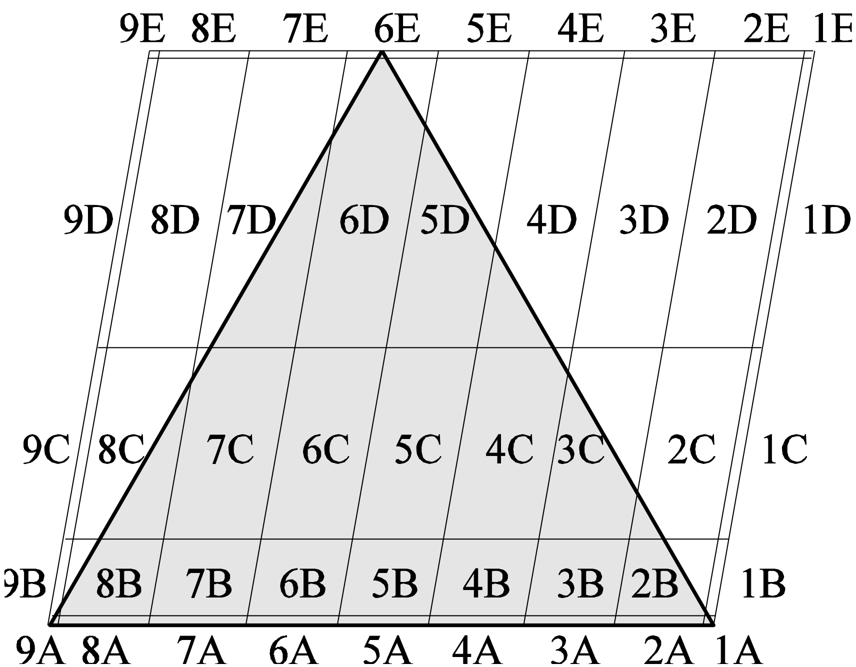
Likelihood Categories:		Absolutely not	Very unlikely	Unlikely	Somewhat unlikely	Chances about even	Somewhat likely	Likely	Very likely	Absolutely
Certainty Categories:		**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
Completely uncertain	**E**	9E	8E	7E	6E	5E	4E	3E	2E	1E
Very uncertain	**D**	9D	8D	7D	6D	5D	4D	3D	2D	1D
Uncertain	**C**	9C	8C	7C	6C	5C	4C	3C	2C	1C
Slightly uncertain	**B**	9B	8B	7B	6B	5B	4B	3B	2B	1B
Completely certain	**A**	9A	8A	7A	6A	5A	4A	3A	2A	1A

Soliciting opinions from people

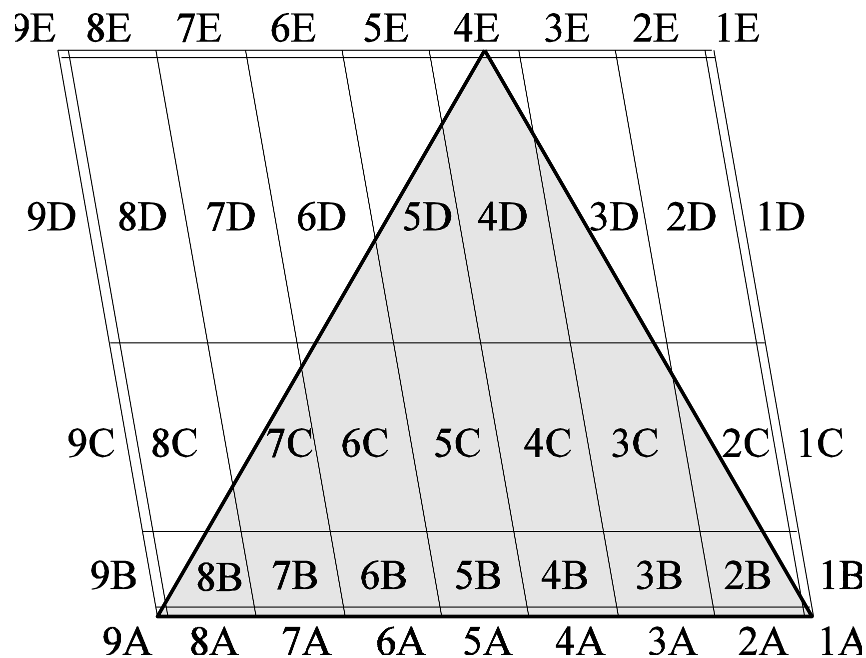
- People find it difficult to express opinions as numerical values
- Fuzzy verbal categories are intuitively easier
- Opinions have 2-dimensional fuzzy categories
  - Likelihood dimension
  - Certainty dimension
- Suitable categories depend on application
  - Example shows 9 likelihoods and 5 certainties
  - 1A corresponds to TRUE
  - 9A corresponds to FALSE
  - High uncertainty most natural around medium likelihood

Fuzzy category to opinion mapping

- Depends on base rate
- Mapped to centre of corresponding field



base rate $a = 1/3$



base rate $a = 2/3$

Mapping categories to opinions

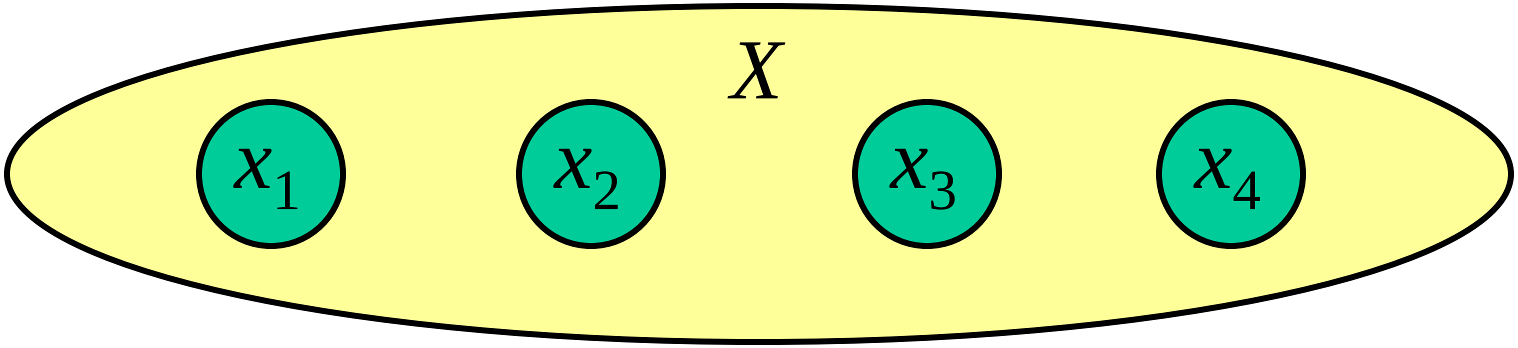
- Overlay category matrix with opinion triangle
- Matrix skewed as a function of base rate
- Not all categories map to opinions
  - For a low base rate, it is impossible to describe an event as highly likely and uncertain, but possible to describe it as highly unlikely and uncertain.
  - E.g. with regard to tuberculosis which has a low base rate, it would be wrong to say that a patient is likely to be infected, with high uncertainty. Similarly it would be possible to say that the patient is probably not infected, with high uncertainty

From binary to multi dimensional frames

- Binary frames can specify a single proposition and its complement.
- Common to have situations with multiple mutually exclusive states
- Opinions can be defined over multi-dimensional frames → multinomial opinions
- Subjective logic operators can be defined for multinomial opinions

n-ary frame of discernment

- Generalisation of binary state space
- Set of exclusive and exhaustive singletons.
- Example Frame: $X=\{x_1, x_2, x_3, x_4\}$, $|X|=4$.



- $|\mathcal{R}(X)| = 2^{|X|} - 2 = 14$.

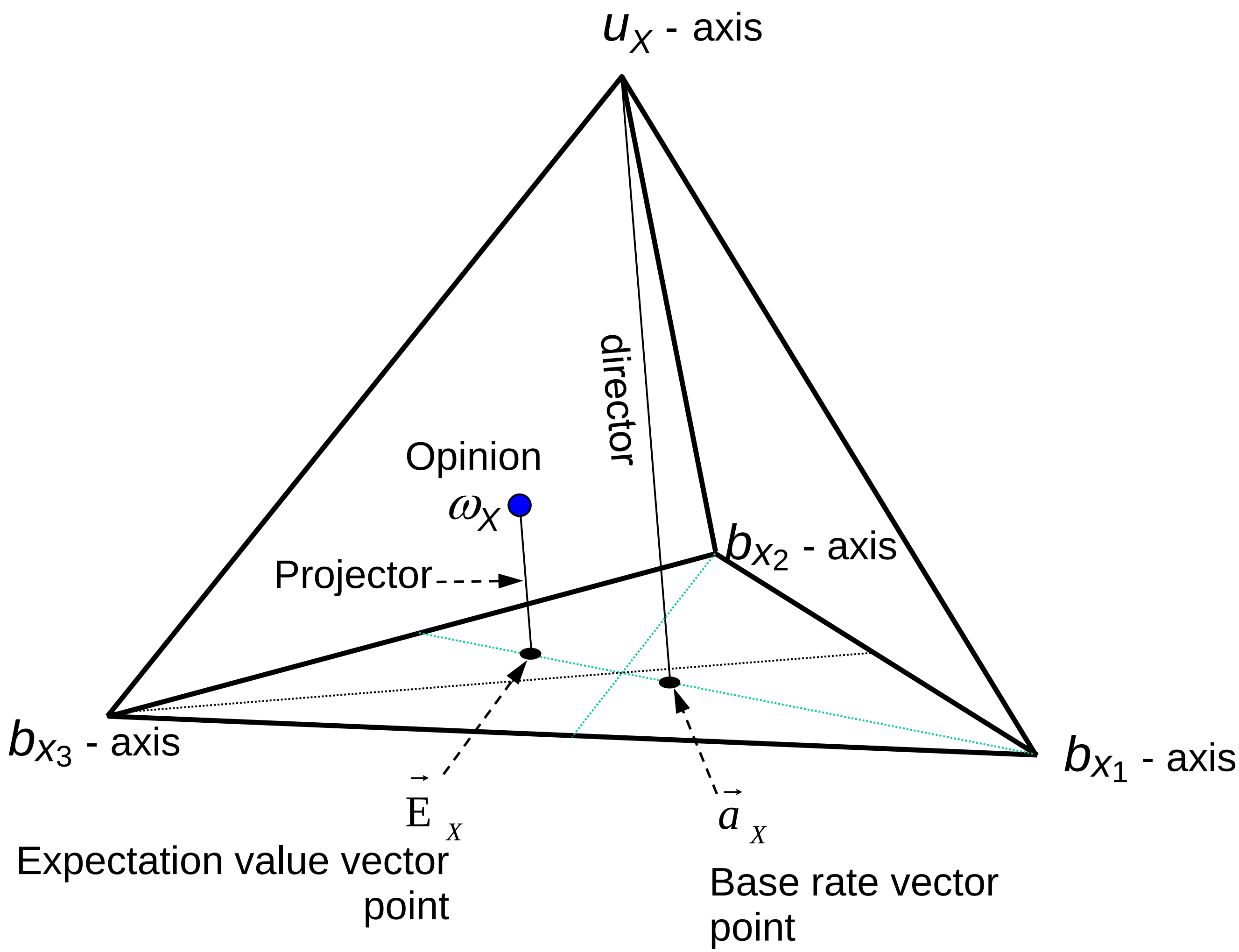
Multinomial Opinions

- Frame: $X=\{x_1 \ldots x_k\}$
- Uncertainty mass: u
- Belief vector: $\vec{b} : \{ b(x_i) \mid i = 1 \ldots k \}$, $u + \Sigma b(x_i) = 1$
- Base rates: $\vec{a} : \{ a(x_i) \mid i = 1 \ldots k \}$, $\Sigma a(x_i) = 1$

- Multinomial opinion: $\omega = (\vec{b}, u, \vec{a})$

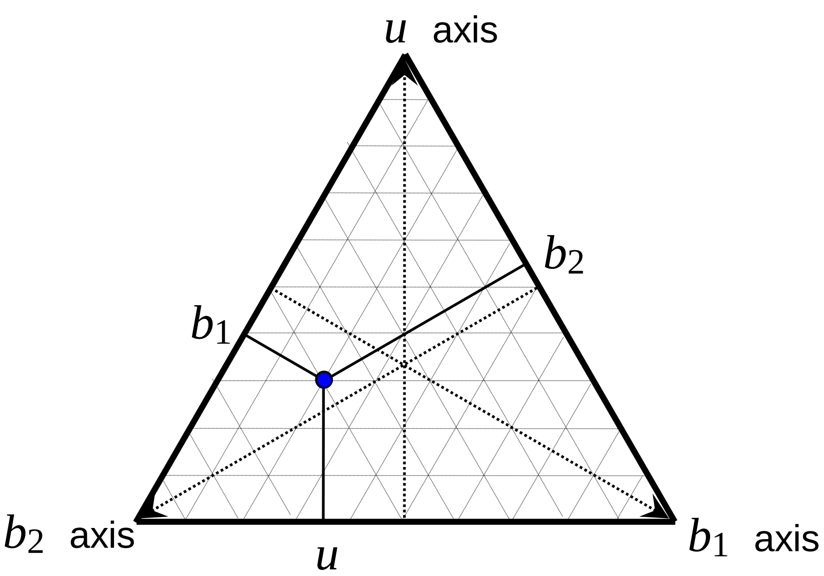
- Expectation: $\vec{\mathrm{E}}(x_i) = b(x_i) + a(x_i)u$

Opinion tetrahedron (ternary frame)



Multinomial opinion as point in a simplex

- The triangle and tetrahedron are the 2D and 3D instances of the simplex geometrical shape
- Multinomial opinions can in general be represented as a point inside a simplex.
- The equation $\Sigma b_i + u = 1$ represents a barycentric coordinate system.



Trinomial opinion as Dirichlet PDF

$$\mathrm{Dir}(\vec{p} \mid \vec{\alpha}) = \frac{\Gamma\left(\sum_{i=1}^{k} \alpha(x_i)\right)}{\prod_{i=1}^{k} \Gamma\left(\alpha(x_i)\right)} \prod_{i=1}^{k} p(x_i)^{\alpha(x_i)-1}$$

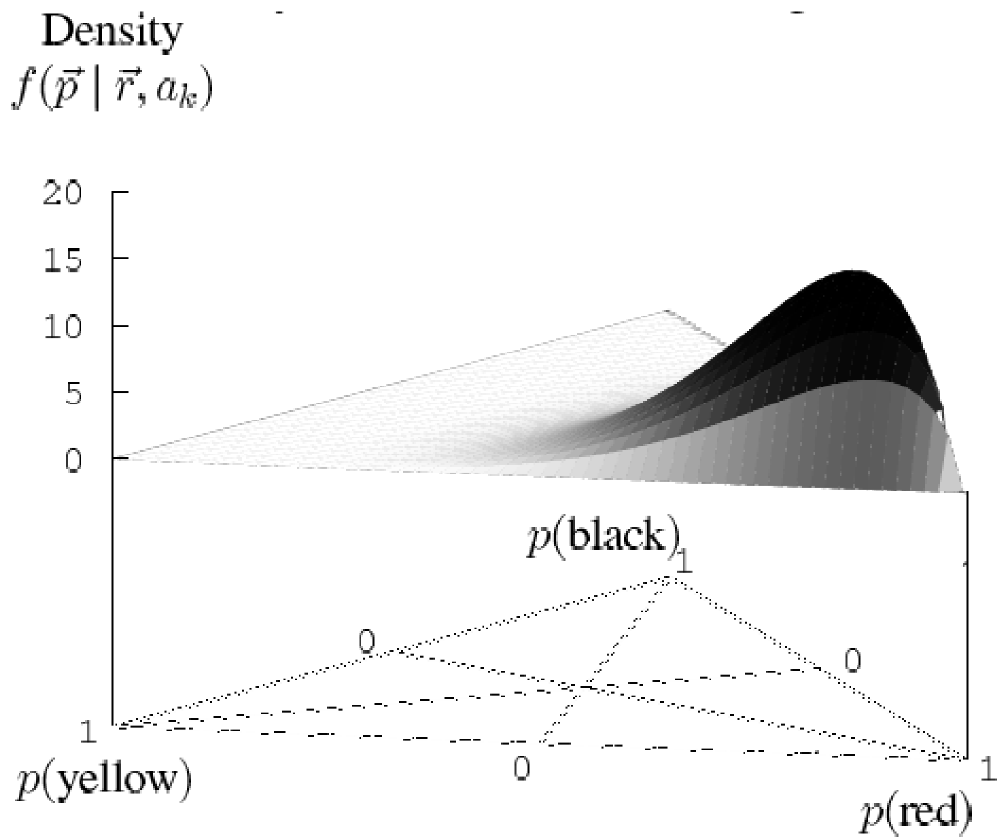
$$\Sigma\, p(x_i) = 1$$

$$\alpha(x_i) = r(x_i) + Wa(x_i)$$

$r(x_i)$: # observations of x_i

$a(x_i)$: base rate of x_i

$W = 2$: non-informative prior weight



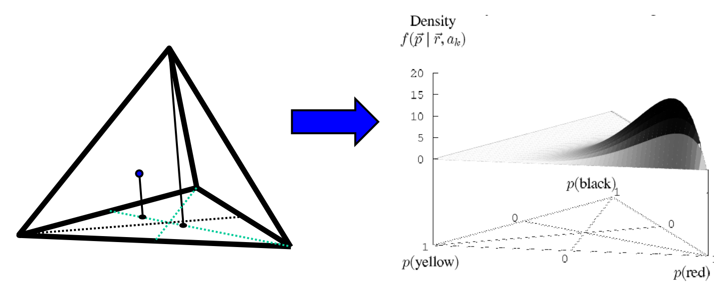
Example:

- 6 red balls
- 1 yellow ball
- 1 black ball

Multinomial Opinion ↔ Dirichlet PDF

- $(\vec{r}, \vec{a})$ represents Dirichlet PDF parameters.
- $(\vec{b}, u, \vec{a})$ represents multinomial opinion.
- Op → Dir:

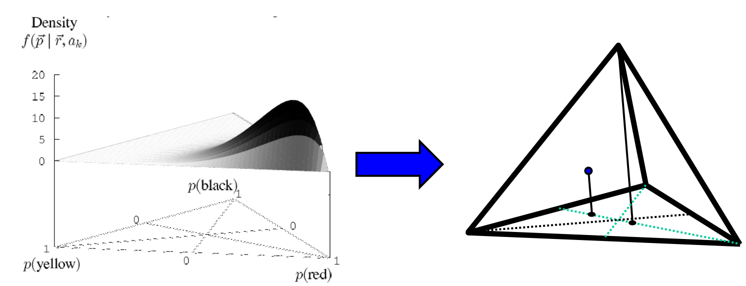
$$\begin{cases} r(x_i) = \dfrac{W b(x_i)}{u} \\ u + \sum b(x_i) = 1 \end{cases}$$



- Dir → Op:

$$\begin{cases} b(x_i) = \dfrac{r(x_i)}{W + \sum r(x_i)} \\ u = \dfrac{W}{W + \sum r(x_i)} \end{cases}$$

$W = 2$



Non-informative prior weight: W

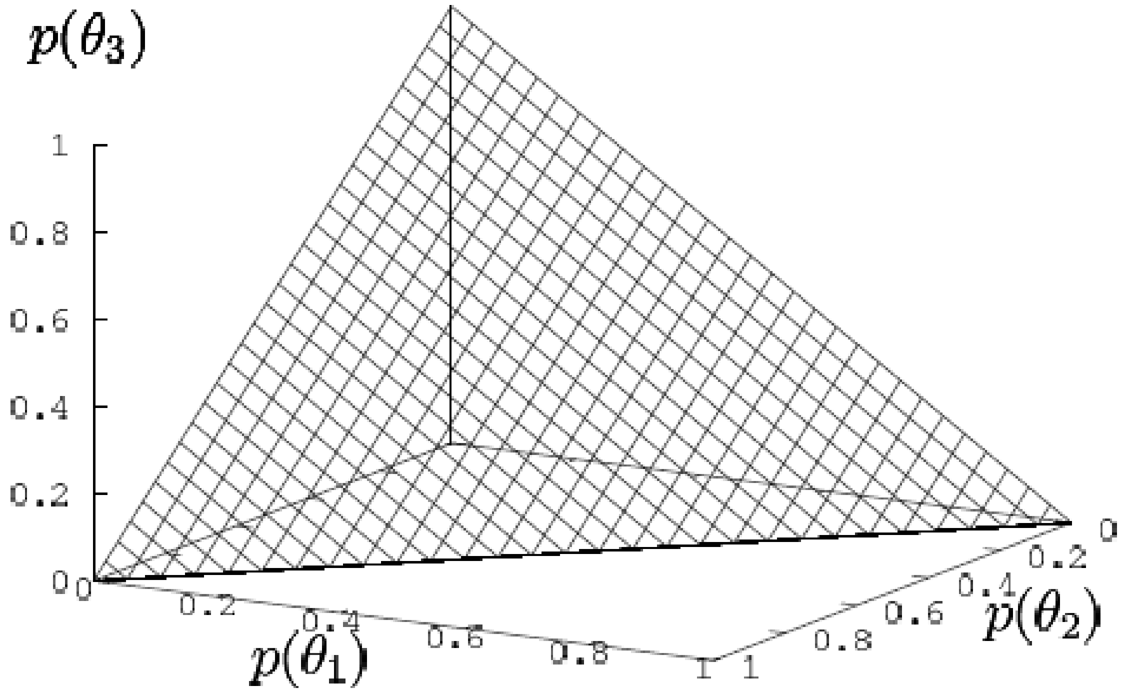
- Value normally set to $W = 2$.
- When W is equal to the frame cardinality, then the prior Dirichlet PDF is a uniform.
- Beta PDF is a binomial Dirichlet PDF
- Normally required that the prior Beta is uniform, which dictates $W = 2$
- Specifying uniform prior Dirichlet PDF for large frames would make the Dirichlet PDF insensitive to new observations.

Example: ternary state space

Example:

Urn with balls of 3 different colours

- t1 = θ1 = Red
- t2 = θ2 = Yellow
- t3 = θ3 = Black



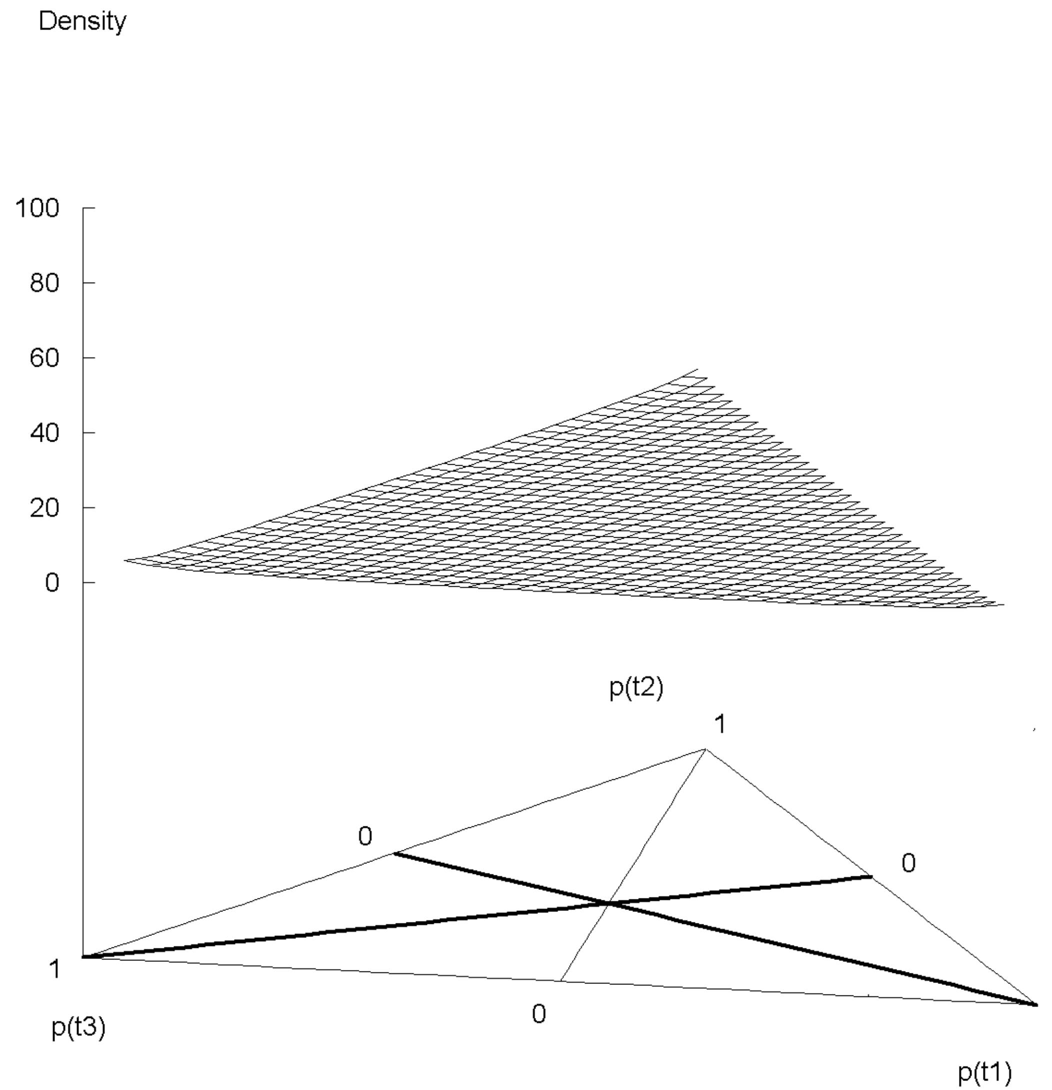
- Additivity requires: $p(t_1) + p(t_2) + p(t_3) = 1$

Prior ternary Dirichlet PDF, $W = 2$

Example:

Urn with balls of 3 different colours. Ternary *a priori* probability density.

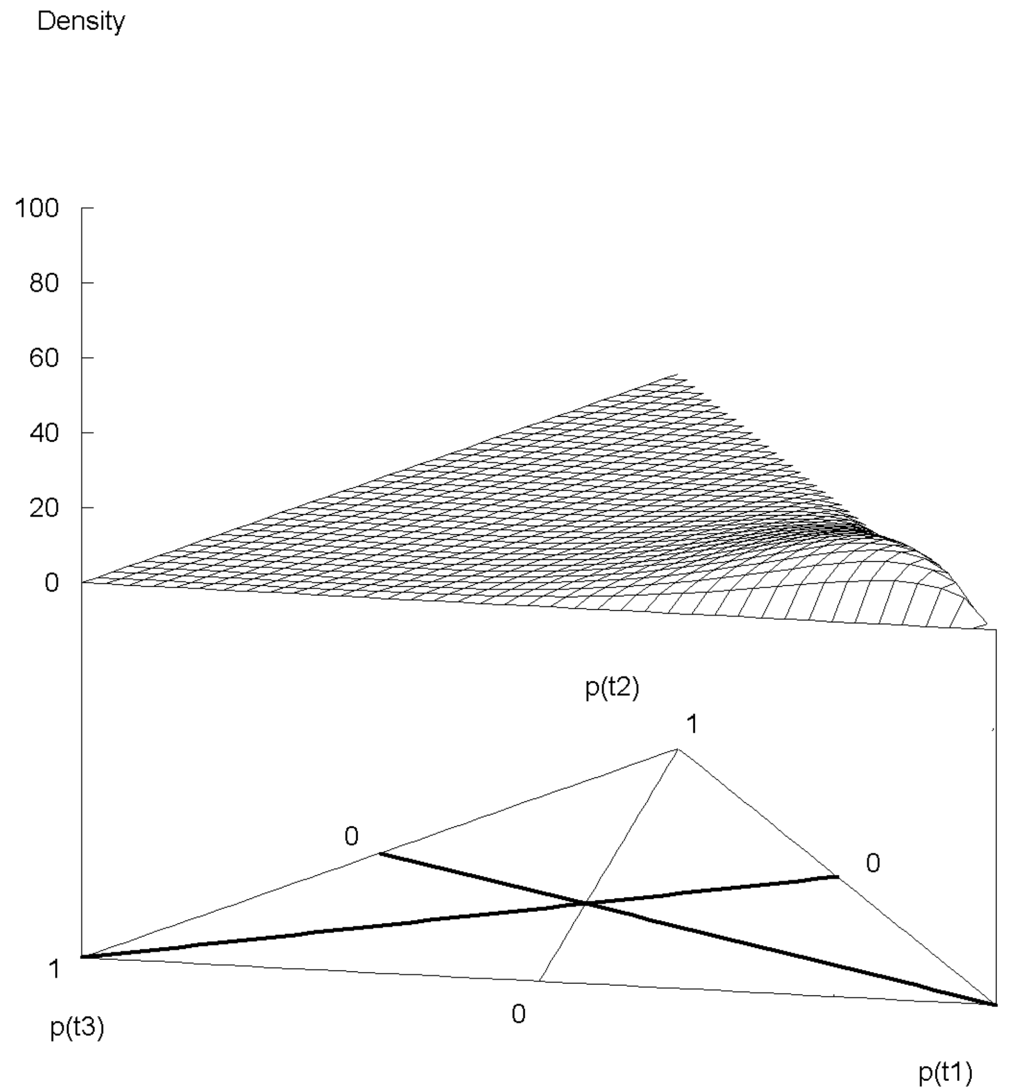
- t1: Red
- t2: Yellow
- t3: Black



Example posterior ternary Dirichlet PDF with $W = 2$

A posteriori probability density after picking:

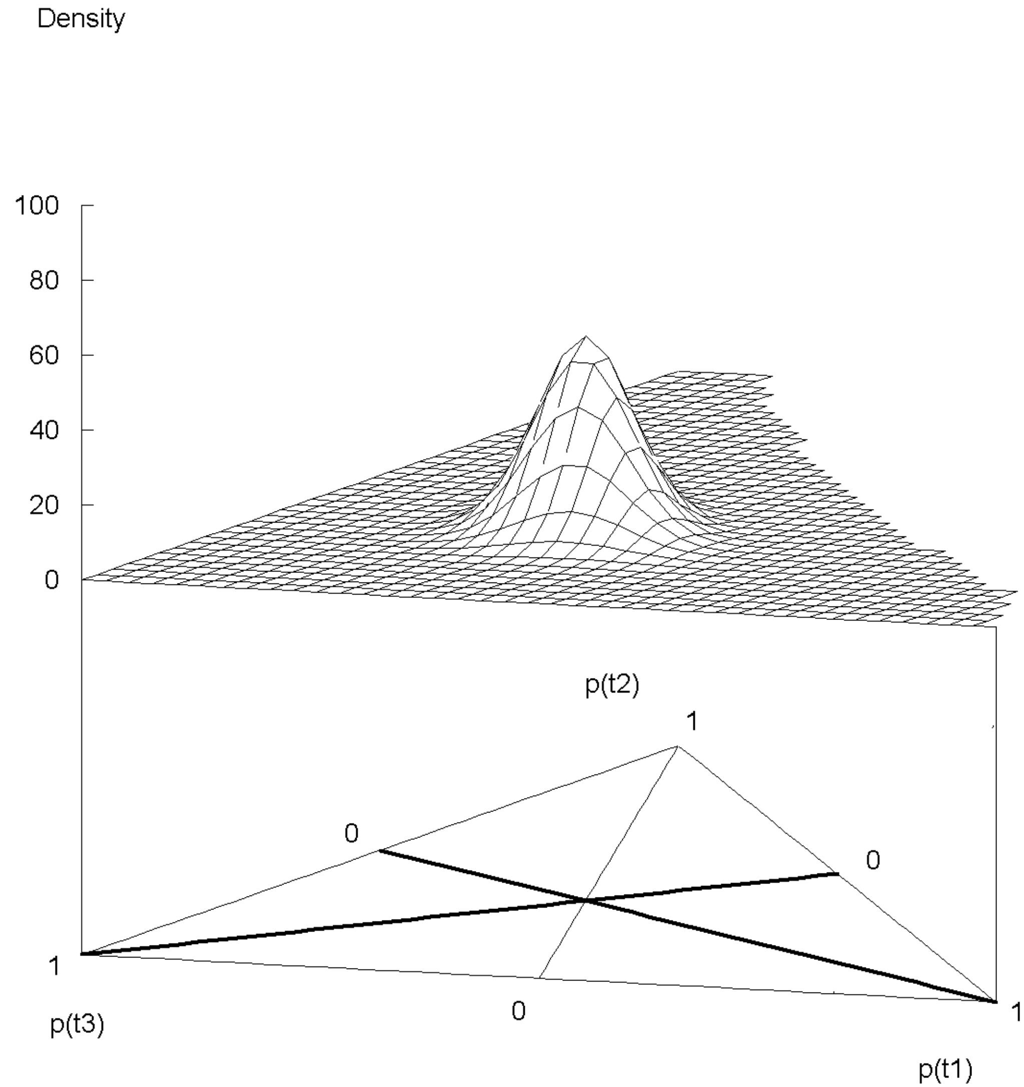
- 6 red balls (t1)
- 1 yellow ball (t2)
- 1 black ball (t3)



Example posterior ternary Dirichlet PDF with $W = 2$

A posteriori probability density after picking:

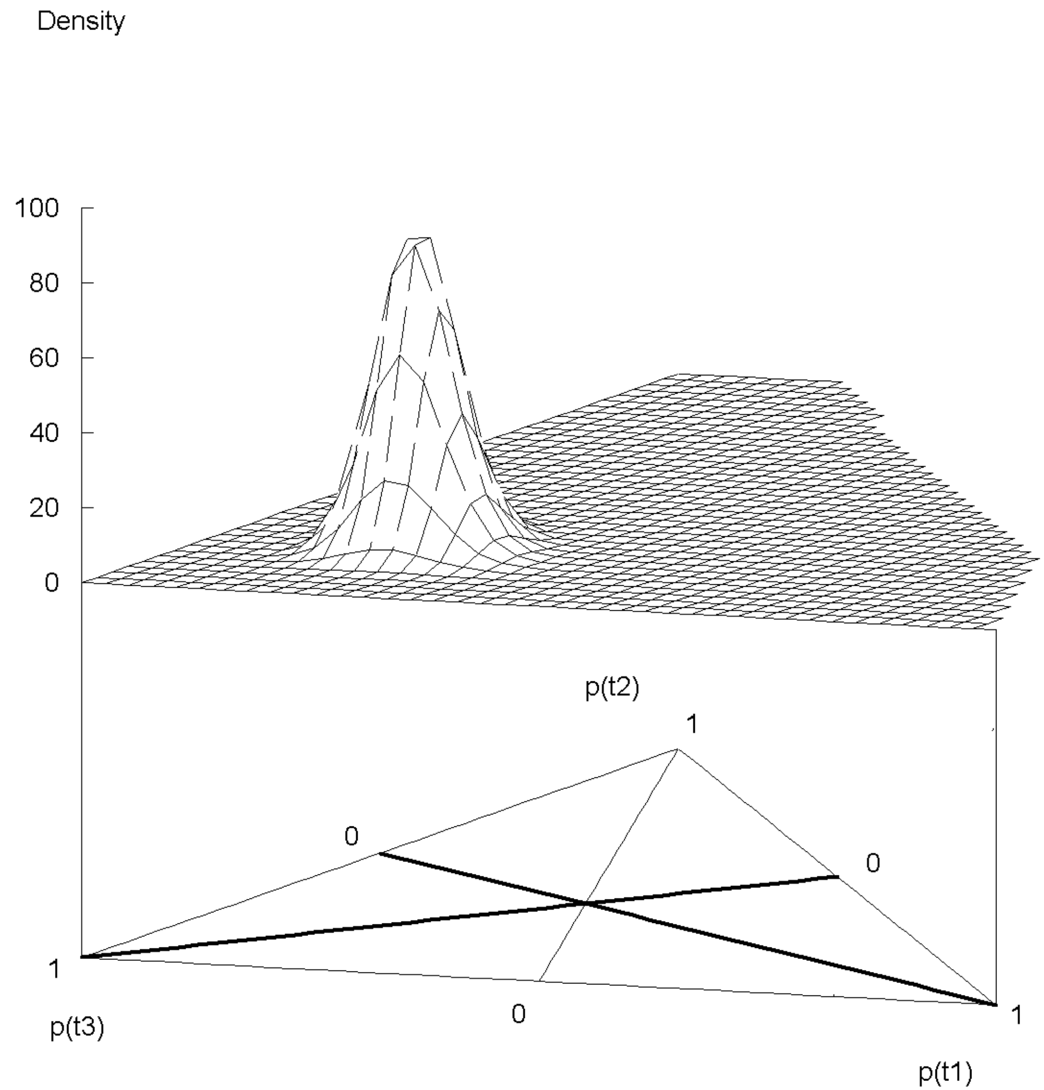
- 20 red balls (t1)
- 20 yellow balls (t2)
- 20 black balls (t3)



Example posterior ternary Dirichlet PDF with $W = 2$

A posteriori probability density after picking:

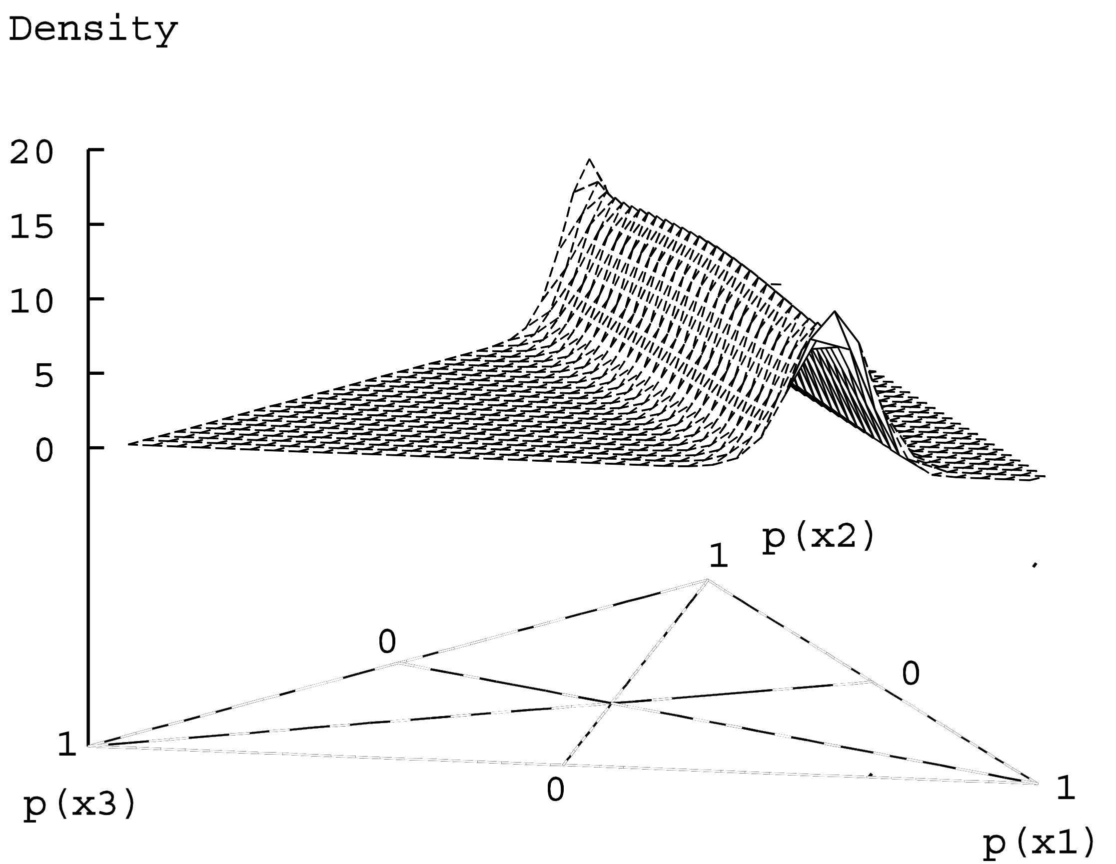
- 20 red balls (t1)
- 20 yellow balls (t2)
- 50 black balls (t3)



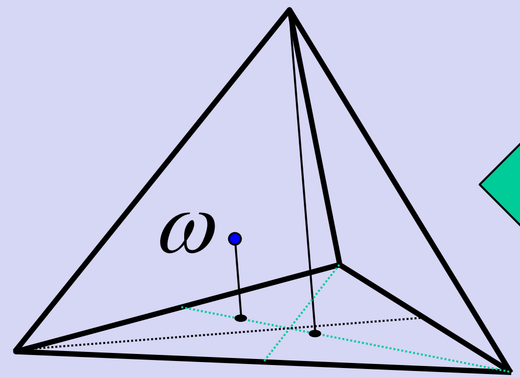
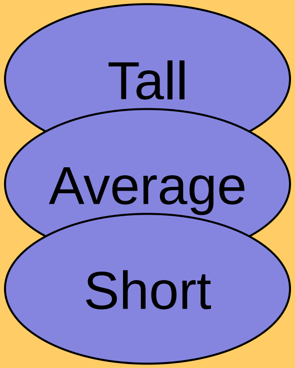
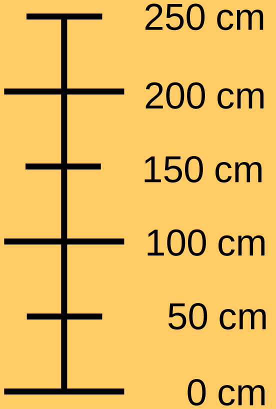
Hyper Opinions

- Frame: $X = \{x_1 \ldots x_k\}$
- Reduced powerset: $\mathcal{R}(X) = \mathcal{P}(X) \setminus \{X, \emptyset\}$
- Uncertainty mass: u
- Belief vector: $\vec{b} : \{ b(x_i) \mid i = 1 \ldots (2^k - 2) \}$, $x_i \in \mathcal{R}(X)$
- Base rates: $\vec{a} : \{ a(x_i) \mid i = 1 \ldots k \}$, $\Sigma a(x_i) = 1$
- Hyper opinion: $\omega = (\vec{b}, u, \vec{a})$
- Expectation: $\vec{\mathrm{E}}(x_i) = a(x_j / x_i) b(x_i) + a(x_i) u$

Hyper Dirichlet PDF



Opinions v. Fuzzy membership functions

<table>
<tr><th></th><th>Fuzzy concept</th><th>Crisp concept</th></tr>
<tr><td>Subjective opinions</td><td>
</td><td>Friendly aircraft
Enemy aircraft
Something else</td></tr>
<tr><td>Fuzzy membership functions</td><td>
</td><td>
</td></tr>
</table>

Opinions v. Fuzzy membership functions

Opinions

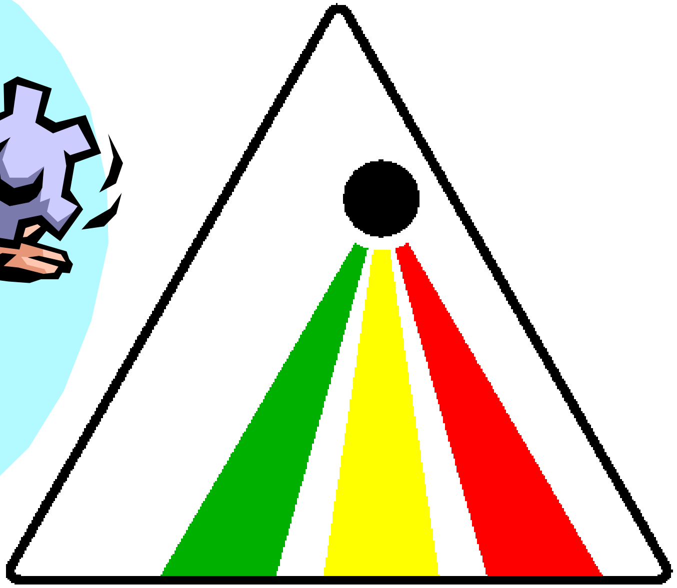
- Crisp frame
- States mutually exclusive
- Opinion measures express uncertainty and are therefore fuzzy

Fuzzy memb. Func.

- Fuzzy categories
- Categories are partly overlapping
- Measures are crisp, e.g. height of a person can be measured in centimetres and millimetres

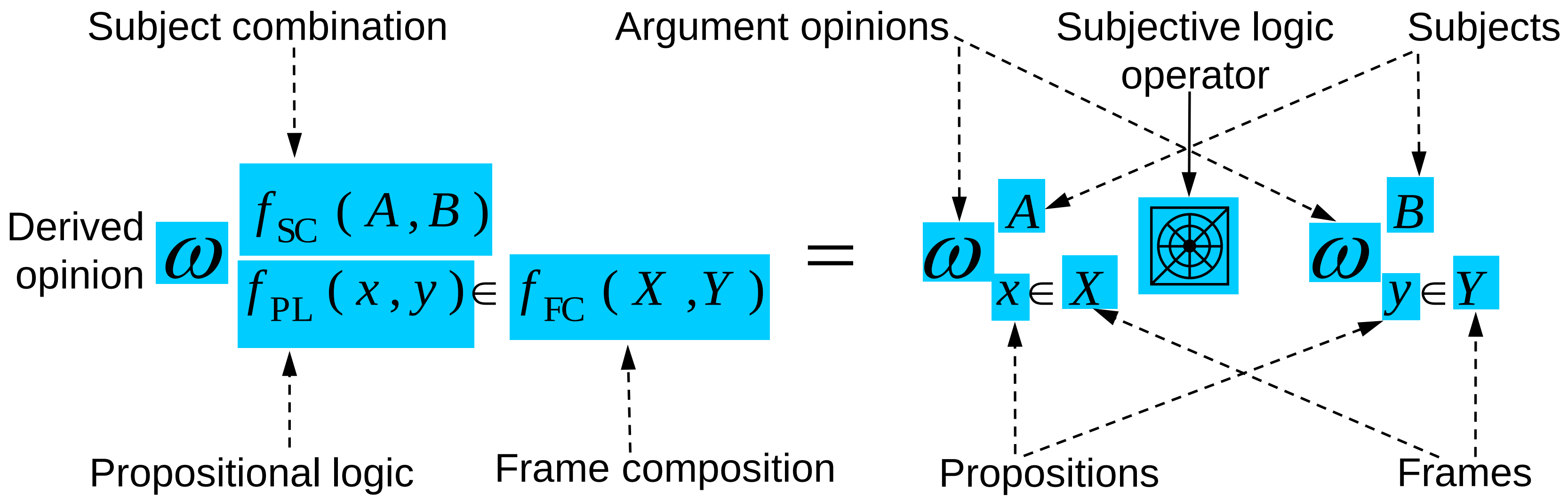
Possible to combine opinions representation and fuzzy membership functions

Subjective Logic Operators



Operator notation

- Possible attributes of opinions:
  - Who: the belief owner (superscript)
  - What: the proposition (subscript)
  - Where: the frame (normally omitted)



Operator generalisation

- Subjective logic is a generalisation of binary logic and probability calculus.
  - Probability calculus i.c.o. dogmatic opinions
  - Binary logic i.c.o. absolute opinions
- Includes uncertainty.
- Includes belief ownership
- Operator types:
  - Classic operators, e.g. multiplication (AND) and deduction (MODUS PONENS)
  - Special operators: e.g. trust transitivity and consensus

Operator principles

- When corresponding probability operator exists, the expectation value of the result is always equal to the result of the probability operator applied to the expectation values of the input arguments.
  - e.g. $\mathrm{E}(\omega_x \cdot \omega_y) = \mathrm{E}(\omega_x) \cdot \mathrm{E}(\omega_y)$ for multiplication
- Similarly for corresponding binary logic operators
  - e.g. Let $\mathrm{V}(\omega_x)$ denote TRUE/FALSE valuation of absolute opinions, then $\mathrm{V}(\omega_x \cdot \omega_y) = \mathrm{V}(\omega_x) \wedge \mathrm{V}(\omega_y)$

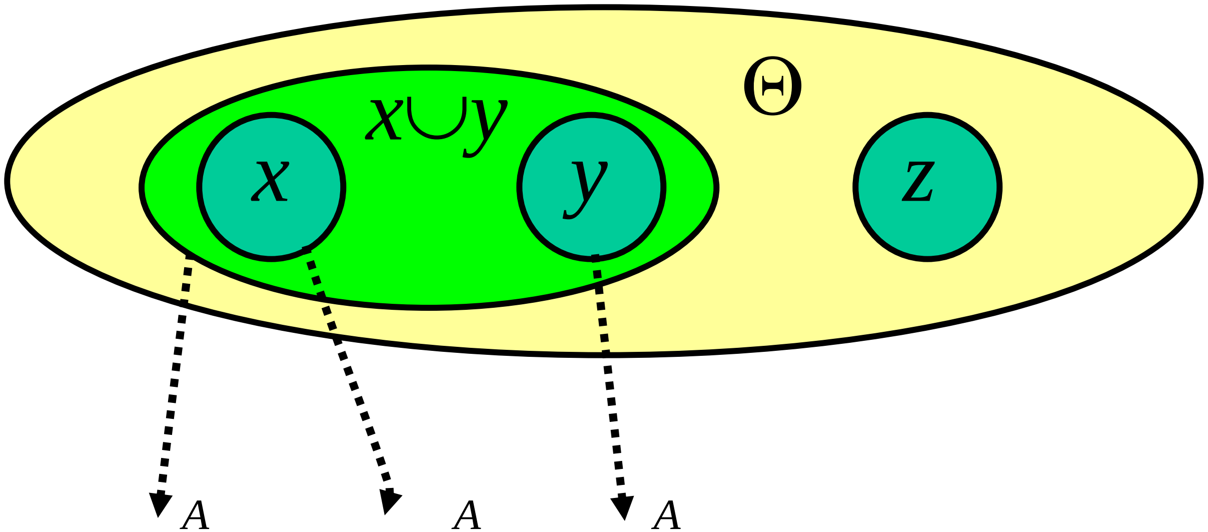
Subjective logic operators 1

Opinion operator name	**Opinion operator symbol**	**Logic operator symbol**	**Logic operator name**
Addition	+	$\cup$	UNION
Subtraction	-	\	DIFFERENCE
Complement	¬	$\overline{x}$	NOT
Expectation	E(x)	n.a.	n.a.
Multiplication	·	$\wedge$	AND
Division	/	$\overline{\wedge}$	UN-AND
Comultiplication	$\sqcup$	$\vee$	OR
Codivision	$\overline{\sqcup}$	$\overline{\vee}$	UN-OR

Subjective logic operators 2

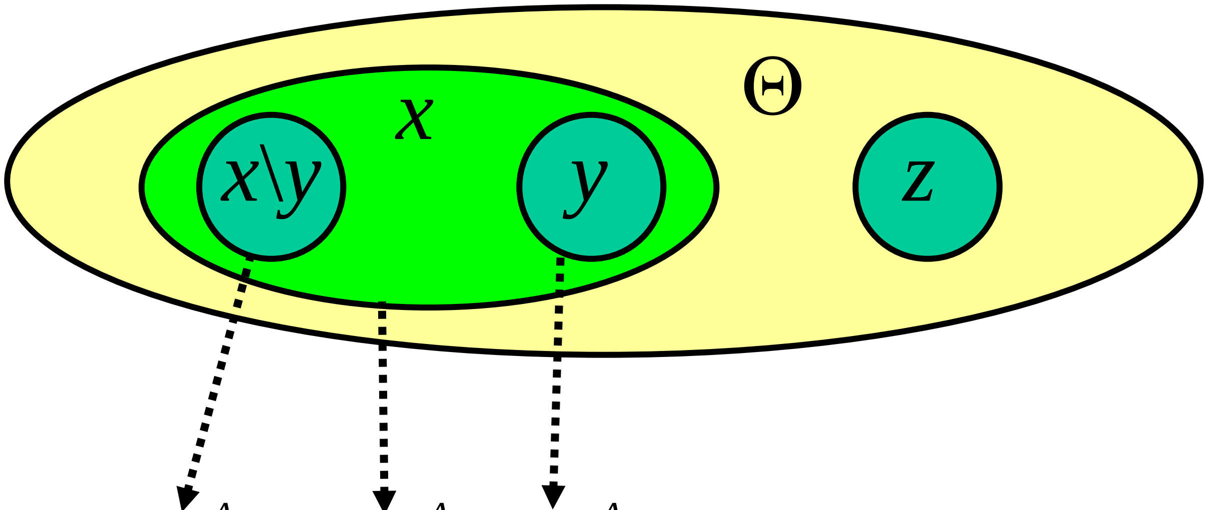
Opinion operator name	**Opinion operator symbol**	**Logic operator symbol**	**Logic operator name**
Transitive discounting	$\otimes$	:	TRANSITIVITY
Cumulative fusion	$\oplus$	$\Diamond$	n.a.
Constraint combination	$\odot$	&	n.a.
Conditional deduction	$\circledcirc$	$\|\|$	DEDUCTION (Modus Ponens)
Conditional abduction	$\overline{\circledcirc}$	$\overline{\|\|}$	ABDUCTION (Modus Tollens)

Addition



- Notation $\omega^{A}_{x \cup y} = \omega^{A}_{x} + \omega^{A}_{y}$
- Probability version: $P(x \cup y) = P(x) + P(y)$
- Commutative and associative.
- No corresponding binary logic operator

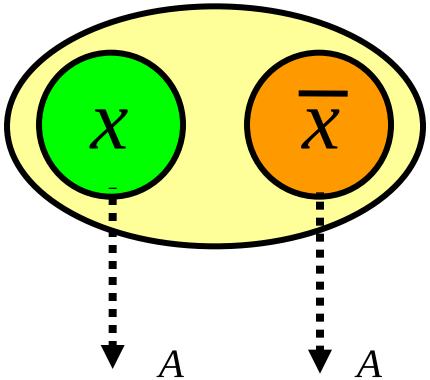
Subtraction



- Notation $\omega^{A}_{x\setminus y} = \omega^{A}_{x} - \omega^{A}_{y}$
- Probability version: $P(x\setminus y)=P(x) - P(y)$
- No corresponding binary logic operator

Complement

- Notation:
- Involutive:
- Corresponds to NOT.

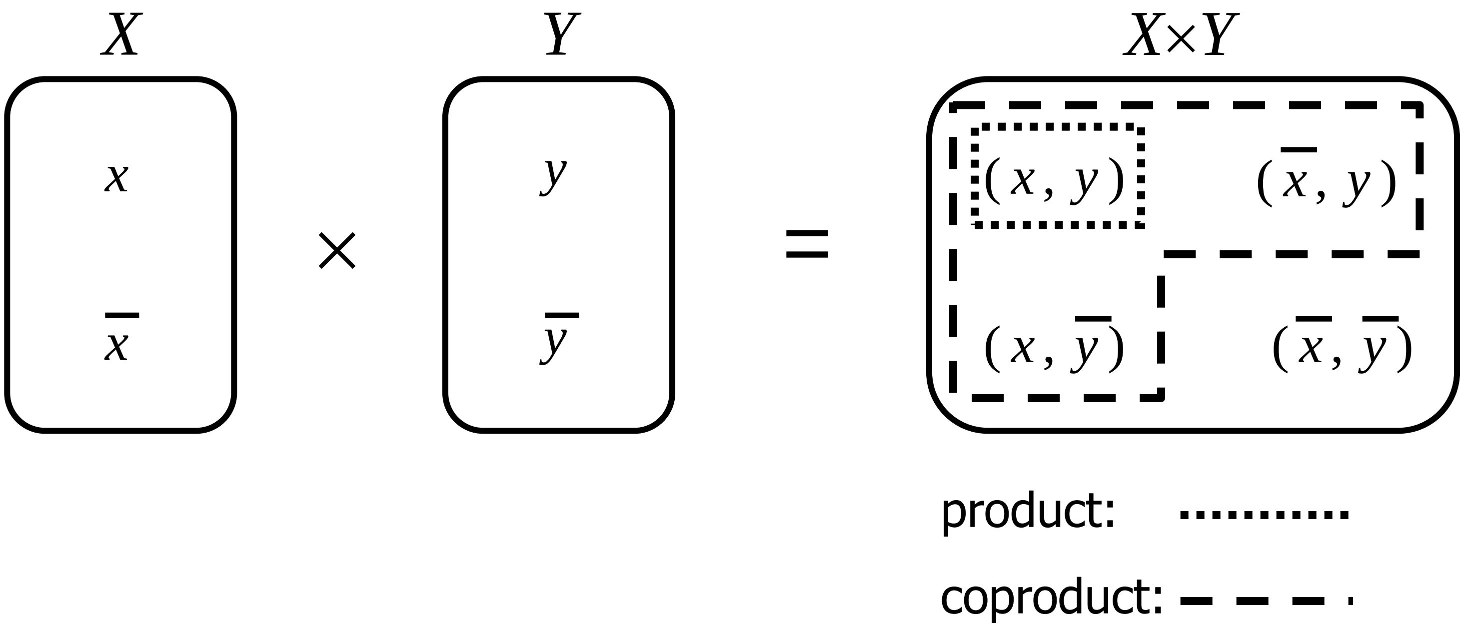


$$\neg\,\omega_x^A = \omega_{\bar{x}}^A$$

$$\neg(\neg\,\omega_x^A) = \omega_x^A$$

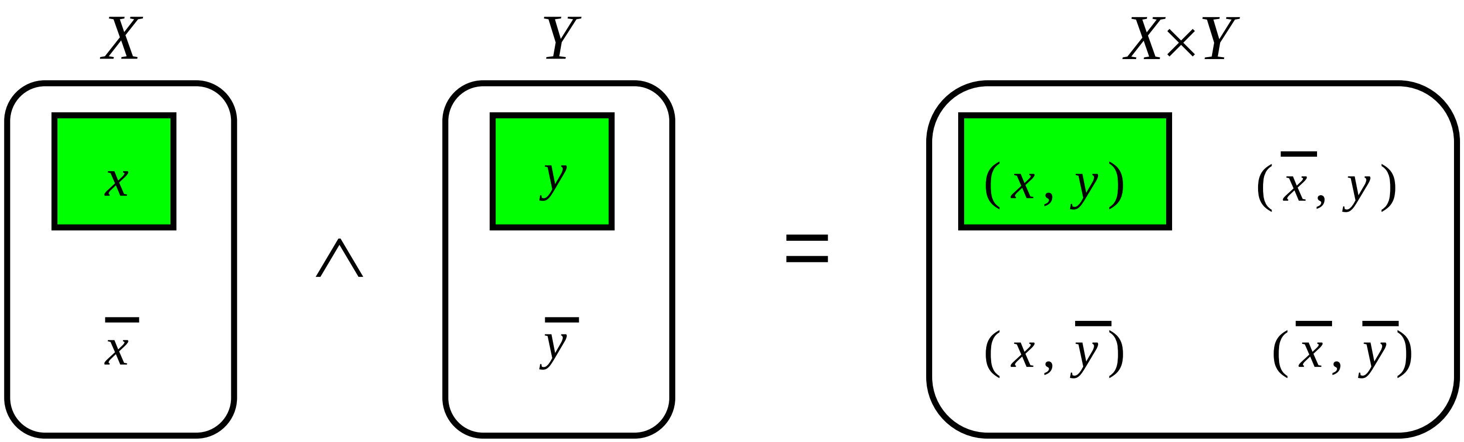
Cartesian product of frames

- Multiplication assumes a Cartesian product.
- Product set has Cardinality = $|X| \cdot |Y|$.
- Coarsening needed as part of computation.



Binomial multiplication

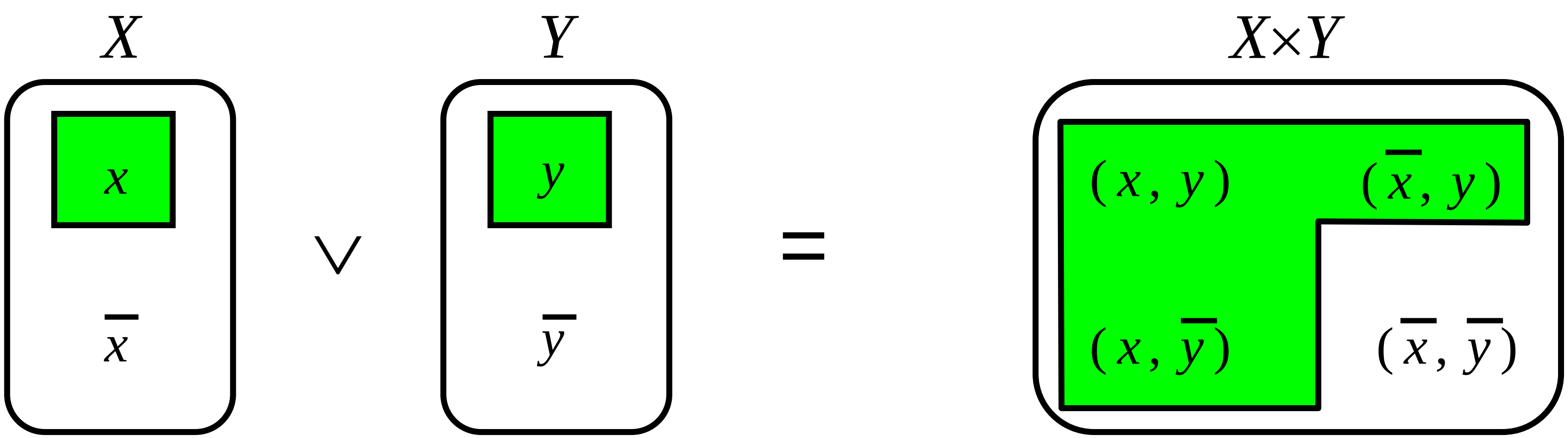
- Notation:
- Probability version: $p(x \wedge y) = p(x) \cdot p(y)$
- Commutative and associative.
- Corresponds to AND and probability product.



$$\omega^{A}_{x \wedge y} = \omega^{A}_{x} \cdot \omega^{A}_{y}$$

Binomial comultiplication

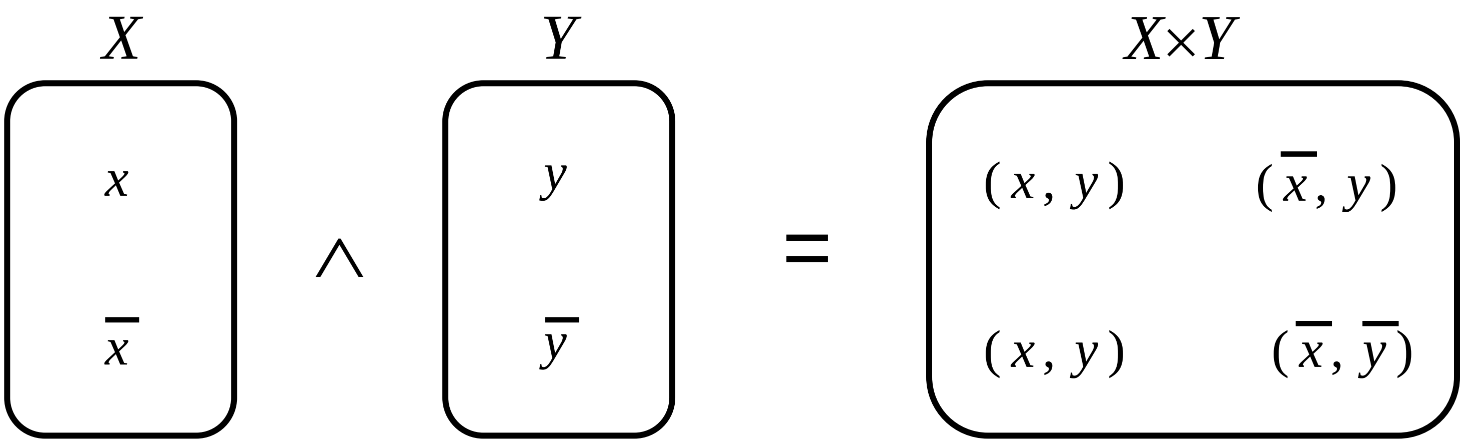
- Notation:
- Probability version: $p(x \vee y) = p(x) + p(y) - p(x)p(y)$
- Commutative and associative.
- Corresponds to OR and probability coproduct.



$$\omega^{A}_{x \vee y} = \omega^{A}_{x} \sqcup \omega^{A}_{y}$$

Multinomial multiplication

- Notation: $\omega^{A}_{X\times Y} = \omega^{A}_{X} \cdot \omega^{A}_{Y}$
- Probability version: matrix multiplication
- Commutative and associative.

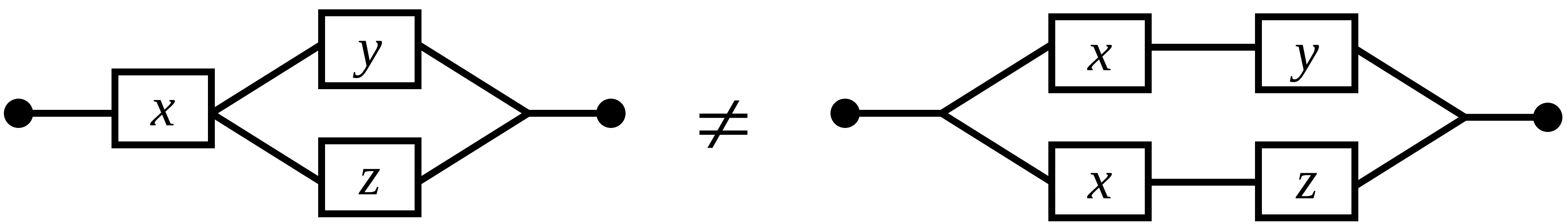


Non-distributivity of products

Multiplication is non-distributive on comultiplication

for opinions: $\omega_{x \wedge (y \vee z)} \neq \omega_{(x \wedge y) \vee (x \wedge z)}$

and for probabilities $p(x \wedge (y \vee z)) \neq p((x \wedge y) \vee (x \wedge z))$



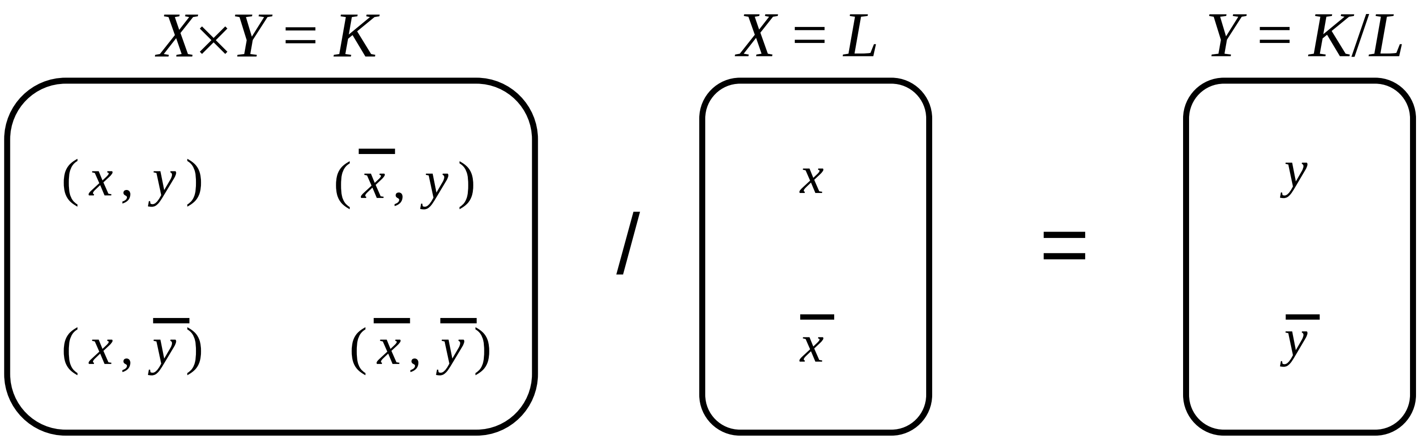
Only applicable for binary logic: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Algebraic properties

- Product: $\mathrm{E}(\omega_{x \wedge y}) = \mathrm{E}(\omega_x)\mathrm{E}(\omega_y)$
- Coproduct: $\mathrm{E}(\omega_{x \vee y}) = \mathrm{E}(\omega_x) + \mathrm{E}(\omega_y) - \mathrm{E}(\omega_x)\mathrm{E}(\omega_y)$
- Complement: $\mathrm{E}(\omega_{\bar{x}}) = 1 - \mathrm{E}(\omega_x)$
- De Morgan 1: $\omega_{\overline{x \wedge y}} = \omega_{\bar{x} \vee \bar{y}}$
- De Morgan 2: $\omega_{\overline{x \vee y}} = \omega_{\bar{x} \wedge \bar{y}}$

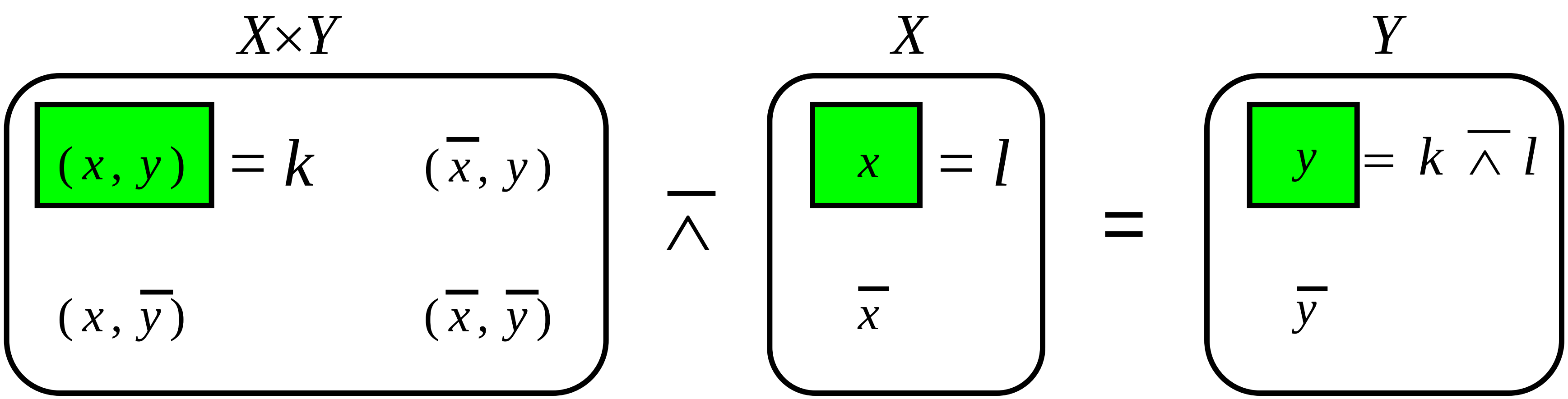
Cartesian quotient of frames

- Division assumes a pre-existing Cartesian product K
- Quotient set has Cardinality = $|K|/|L|$
- Coarsening needed as part of computation



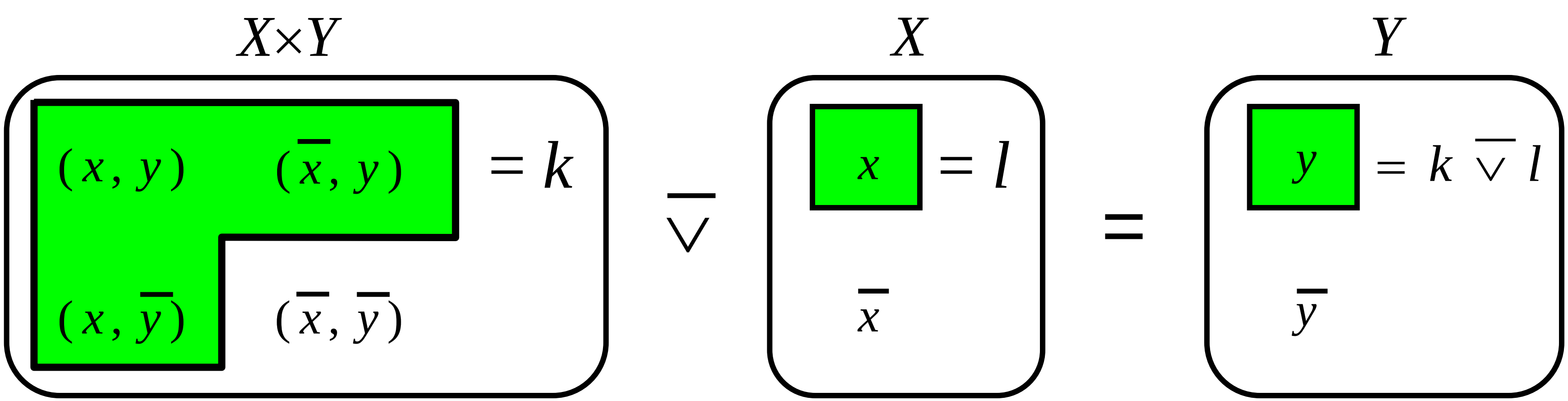
Division

- Notation: $\omega^{A}_{k \overline{\wedge} l} = \omega^{A}_{k} / \omega^{A}_{l}$
- Probability version: $\mathrm{P}(\, k \overline{\wedge} l\,) = \mathrm{P}(\, k\,)/\mathrm{P}(\, l\,)$
- Corresponds to UN-AND and probability division



Codivision

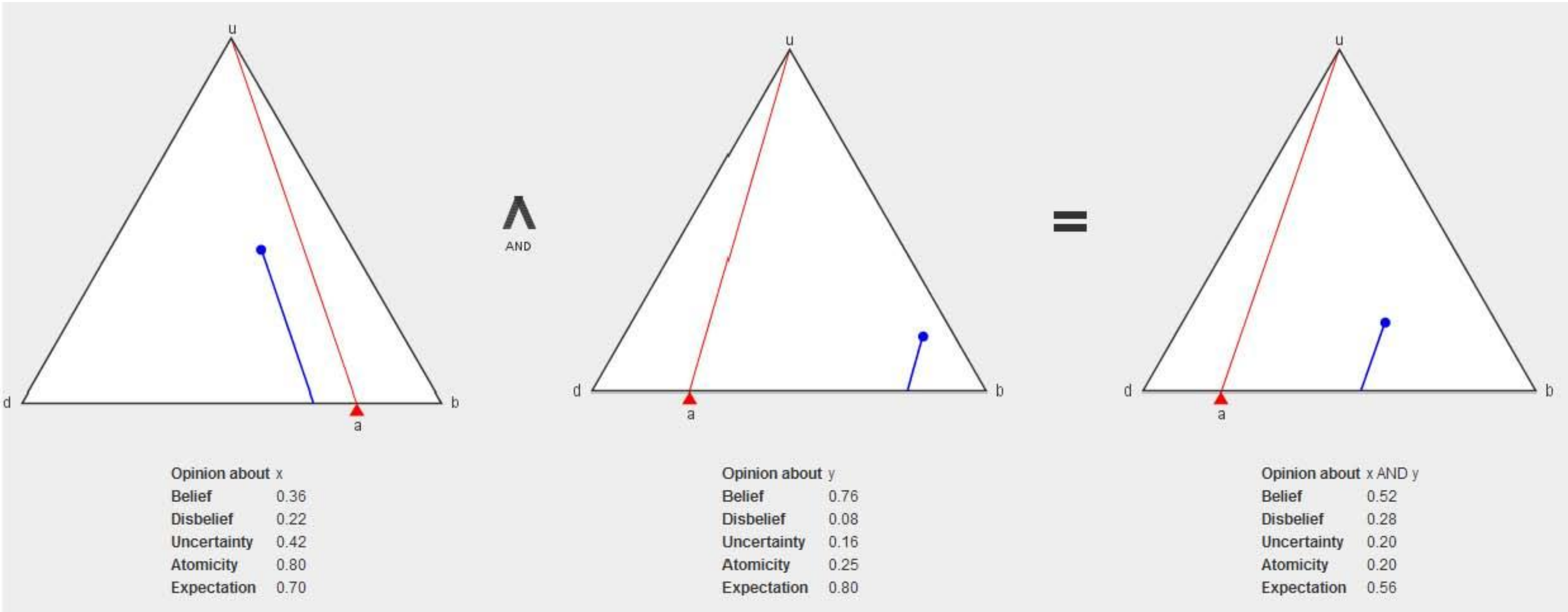
- Notation: $\omega^{A}_{k \overline{\vee} l} = \omega^{A}_{k} \,\bar{\sqcup}\, \omega^{A}_{l}$
- Probability version: $P(k \overline{\vee} l) = (P(k) - P(l))/(1 - P(l))$
- Corresponds to UN-OR and probability codivision



Truth table; Products and quotients

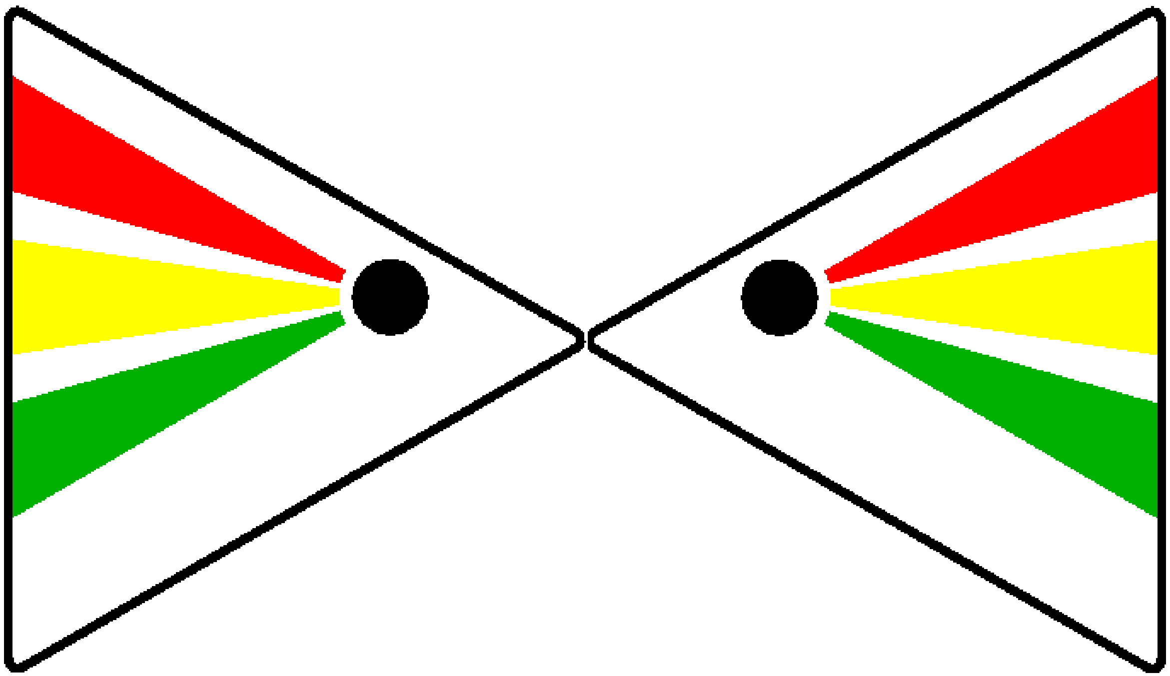
x	y	AND product $x \wedge y$	OR coproduct $x \vee y$	UN-AND quotient $x \overline{\wedge} y$	UN-OR coquotient $x \overline{\triangledown} y$
F	F	F	F	T or F	F
F	T	F	T	F	undefined
T	F	F	T	undefined	T
T	T	T	T	T	T or F

Online demo of SL operators



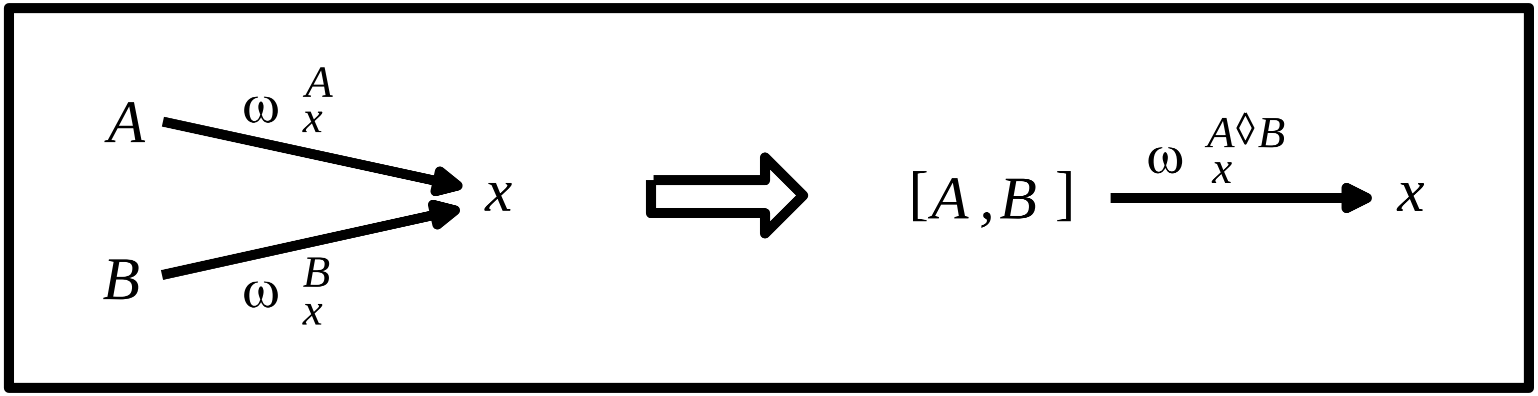
http://persons.unik.no/josang/sl/

Fusion in Subjective Logic



Opinion fusion

- Notation: $\omega_x^{A \Diamond B} = \omega_x^A \oplus \omega_x^B$
- Cumulative fusion
- Averaging fusion
- Reduced to weighted average i.c.o. dogmatic opinions.



Cumulative Fusion

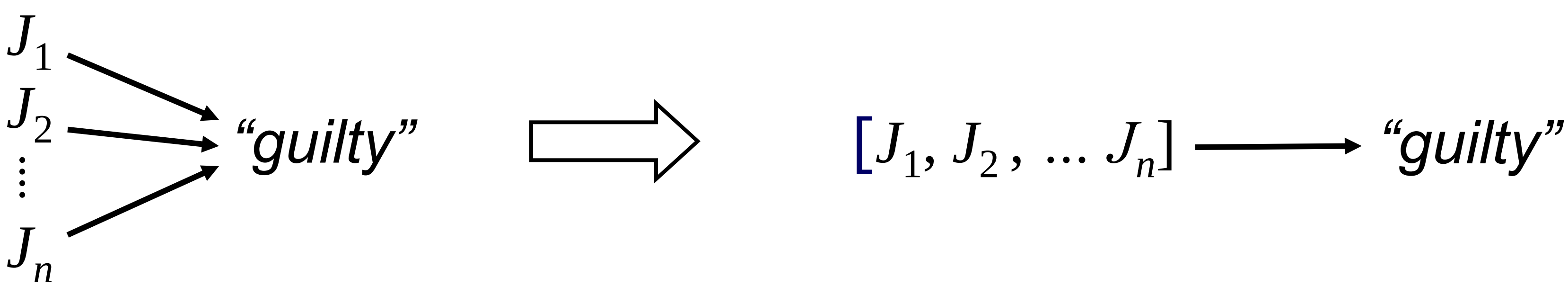
- Accumulates evidence from different sources
- Symbol: $\oplus$
- Sum of Dirichlet evidence vectors
  1. Convert opinions to Dir/Beta: $\omega \rightarrow \mathrm{Dir}(p \mid \vec{r}, \vec{\alpha})$
  2. Add evidence vectors $\vec{r}$ to get cumulative Dir/Beta
  3. Convert Dir/Beta to opinion $\mathrm{Dir}(p \mid \vec{r}, \vec{\alpha}) \rightarrow \omega$
- Commutative and associative.
- Applicable to situations where collected evidence is independent
  - E.g. observed over different time periods

Averaging Fusion

- Average of evidence from different sources
- Symbol: $\underline{\oplus}$
- Average of Dirichlet evidence vectors
  1. Convert opinions to Dir/Beta: $\omega \rightarrow \mathrm{Dir}(p \mid \vec{r}, \vec{\alpha})$
  2. Take average of evidence vectors $\vec{r}$ to produce an average Dir/Beta
  3. Convert Dir/Beta to opinion $\mathrm{Dir}(p \mid \vec{r}, \vec{\alpha}) \rightarrow \omega$
- Commutative, but not associative.
- Applicable to situations where collected evidence is dependent
  – E.g. same event observed by different observers

Example: Reaching a verdict

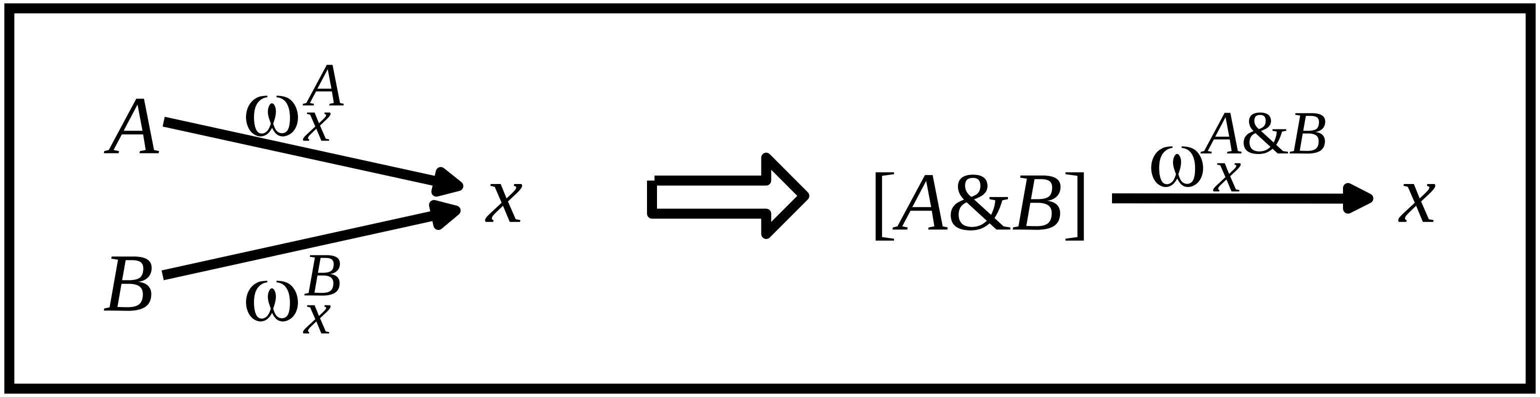
- $J_1, J_2, \ldots J_n$ are n jury members.
- "guilty" is a binary statement.
- $[J_1, J_2, \ldots J_n]$ denotes the whole jury.
- ω_{BRD} is a politically defined threshold value for *"Beyond Reasonable Doubt"*.



$$\omega^{J_1 \Diamond J_2 \Diamond \cdots \Diamond Jn}_{\text{"guilty"}} > \omega_{\text{BRD}} \quad ?$$

Constraint Combination

- Notation: $\omega_x^{A\&B} = \omega_x^A \odot \omega_x^B$
- Commutative
- No corresponding binary logic operator
- Can not be applied for conflicting dogmatic opinions.



Example constraint combination

- Alice, Bob and Clark want to go to the cinema together
- Options are: *"Black Dust", "Gray Matter" and "White Powder"*

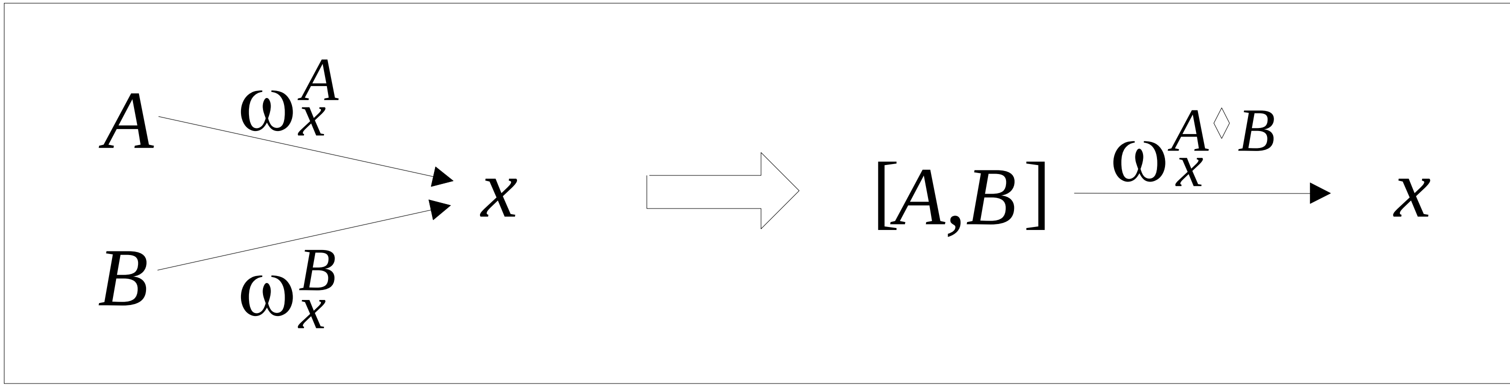
	Preferences of:			Results of preference combinations:	
	Alice	Bob	Clark	(Alice & Bob)	(Alice & Bob & Clark)
	ω_{Θ}^{A}	ω_{Θ}^{B}	ω_{Θ}^{C}	$\omega_{\Theta}^{A\&B}$	$\omega_{\Theta}^{A\&B\&C}$
$b(BD) =$	0.99	0.00	0.00	0.00	0.00
$b(GM) =$	0.01	0.01	0.00	1.00	1.00
$b(WP) =$	0.00	0.99	0.00	0.00	0.00
$b(GM \cup WP) =$	0.00	0.00	1.00	0.00	0.00

Table 4. Combination of film preferences

- They can only agree on watching: "*Gray Matter*"

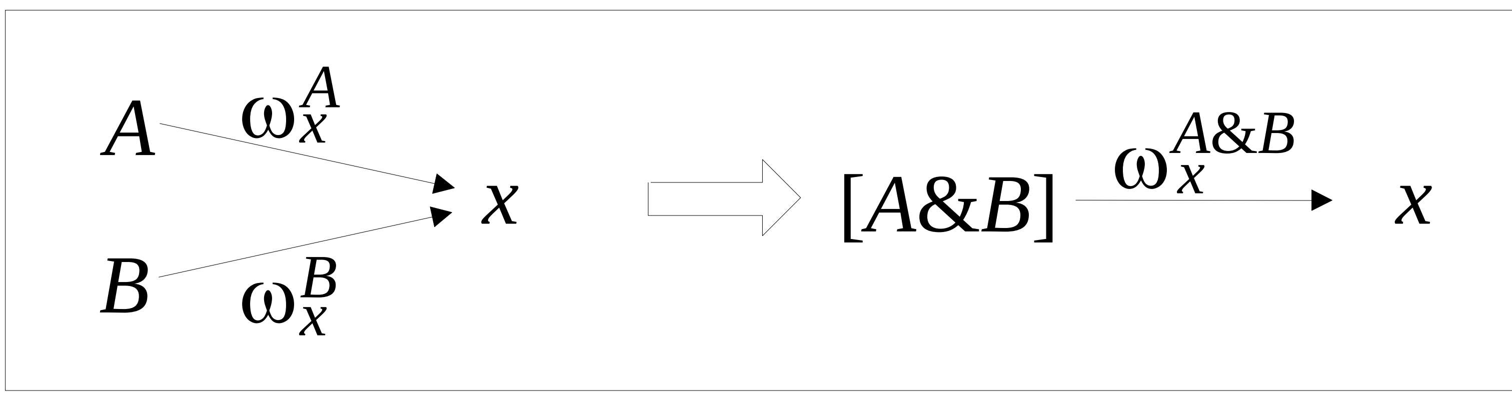
Comparing Fusion and Constraining

Fusion



- Jurors A and B reach a consensus about truth of x

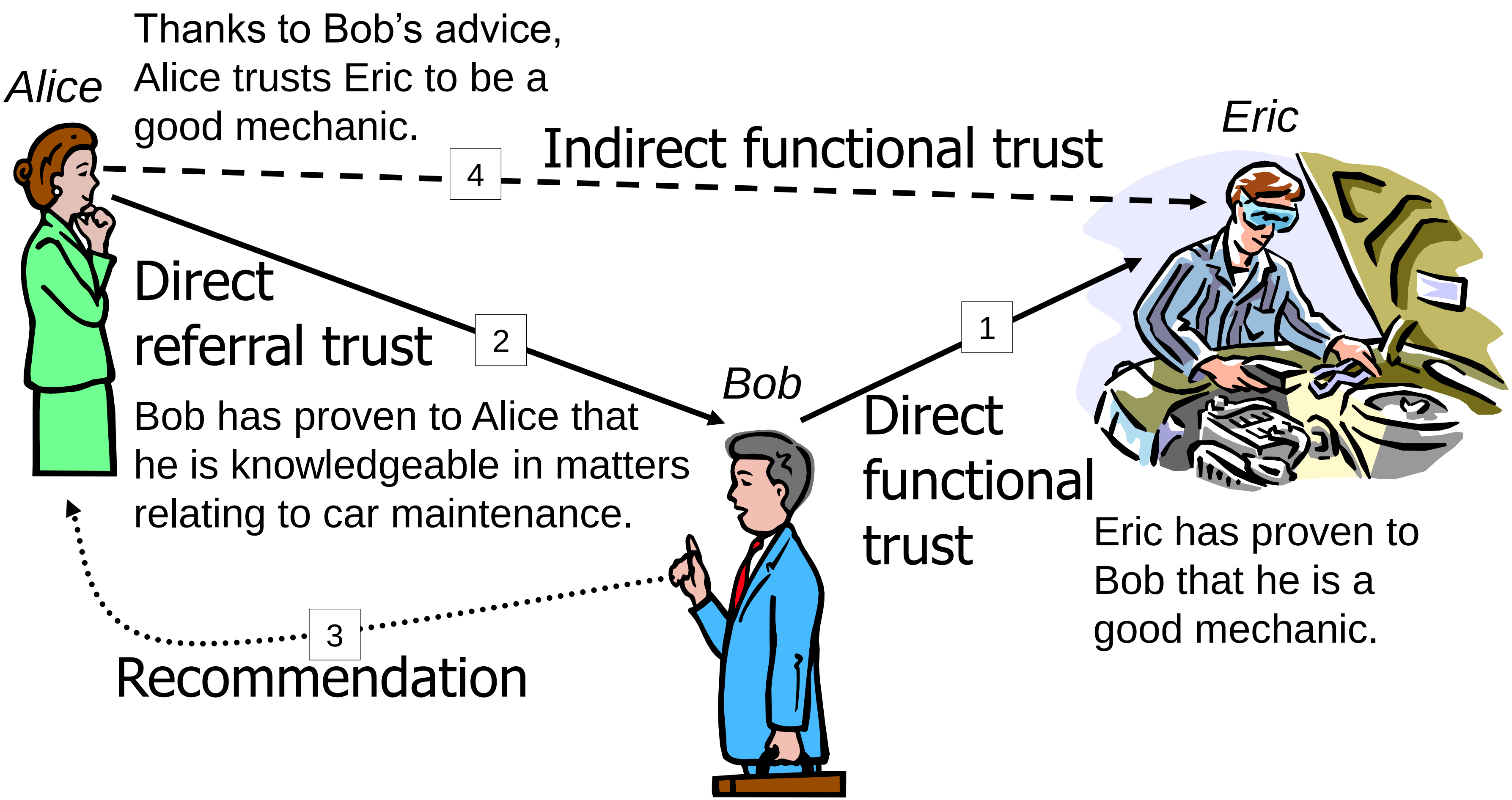
Constraining



- Agents A and B agree on whether x is a good choice

Trust modelling

Trust transitivity



Trust scope

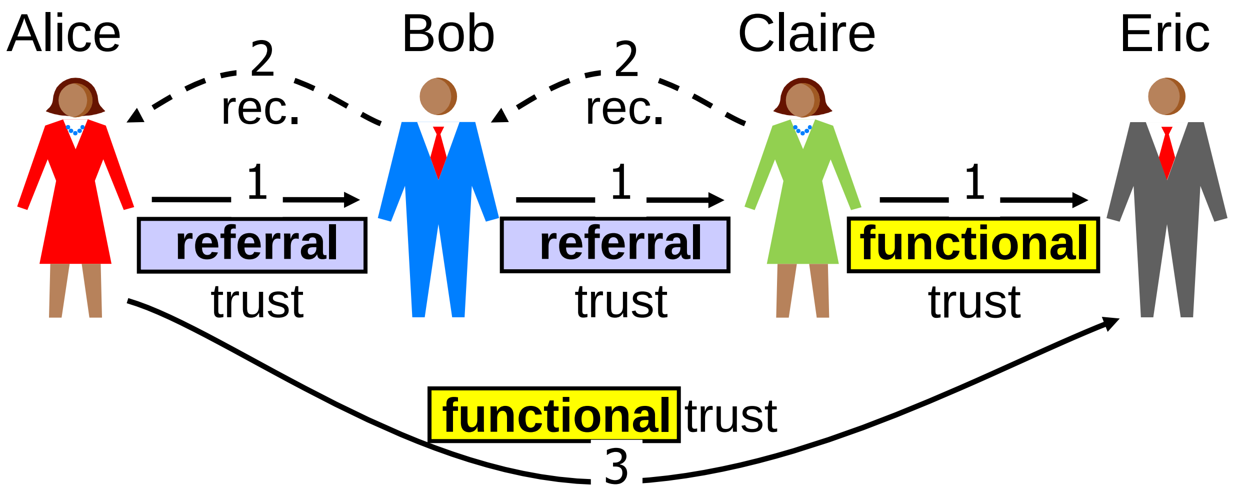
- The trust **scope** defines the specific purpose(s) of trust assumed in a given trust relationship.
- In other words, the trusted party is relied upon to have certain qualities, and the **scope** defines the trusting party's view of what those qualities are.
- Aka: Trust purpose, trust context, subject matter

Types of Trust

- **Direct** Trust as a result of direct experience
- **Indirect** Trust as a result of recommendations (i.e. indirect knowledge)

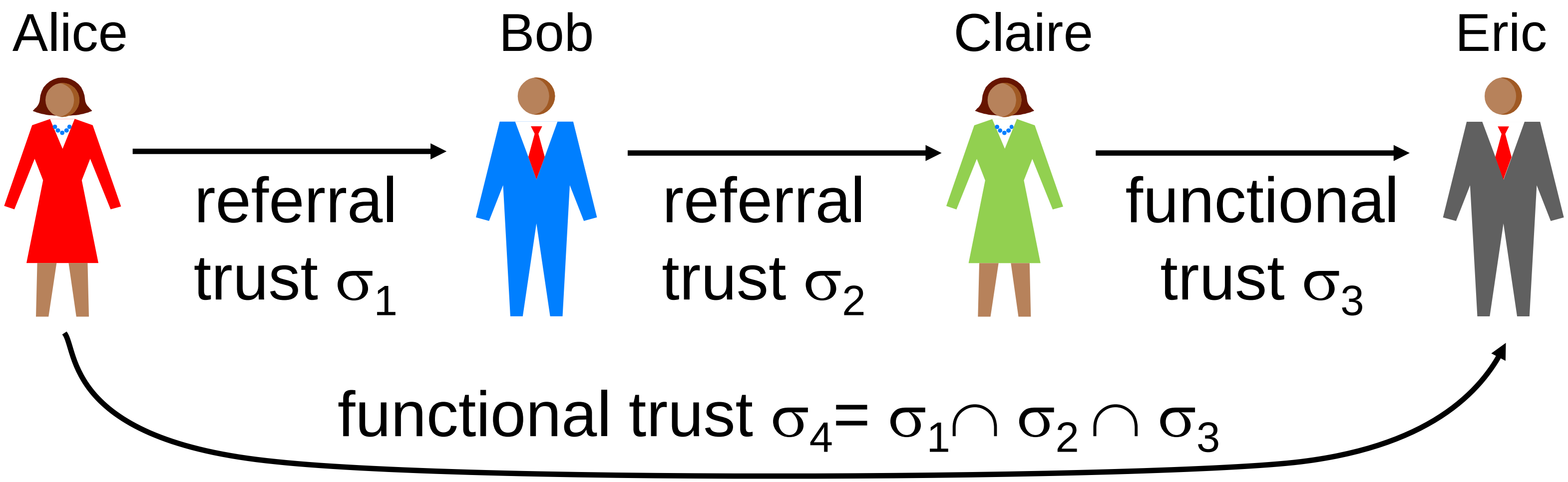
- **Functional** Trusting entity x for scope σ (e.g. “to be a good car mechanic”)
- **Referral** Trusting x to recommend for scope σ (e.g. “to be reliable at recommending car mechanics)

Functional trust derivation requirement



- Derivation of functional trust through a transitive path, requires that the last trust arc represents functional trust, and all previous trust arcs represent referral trust.

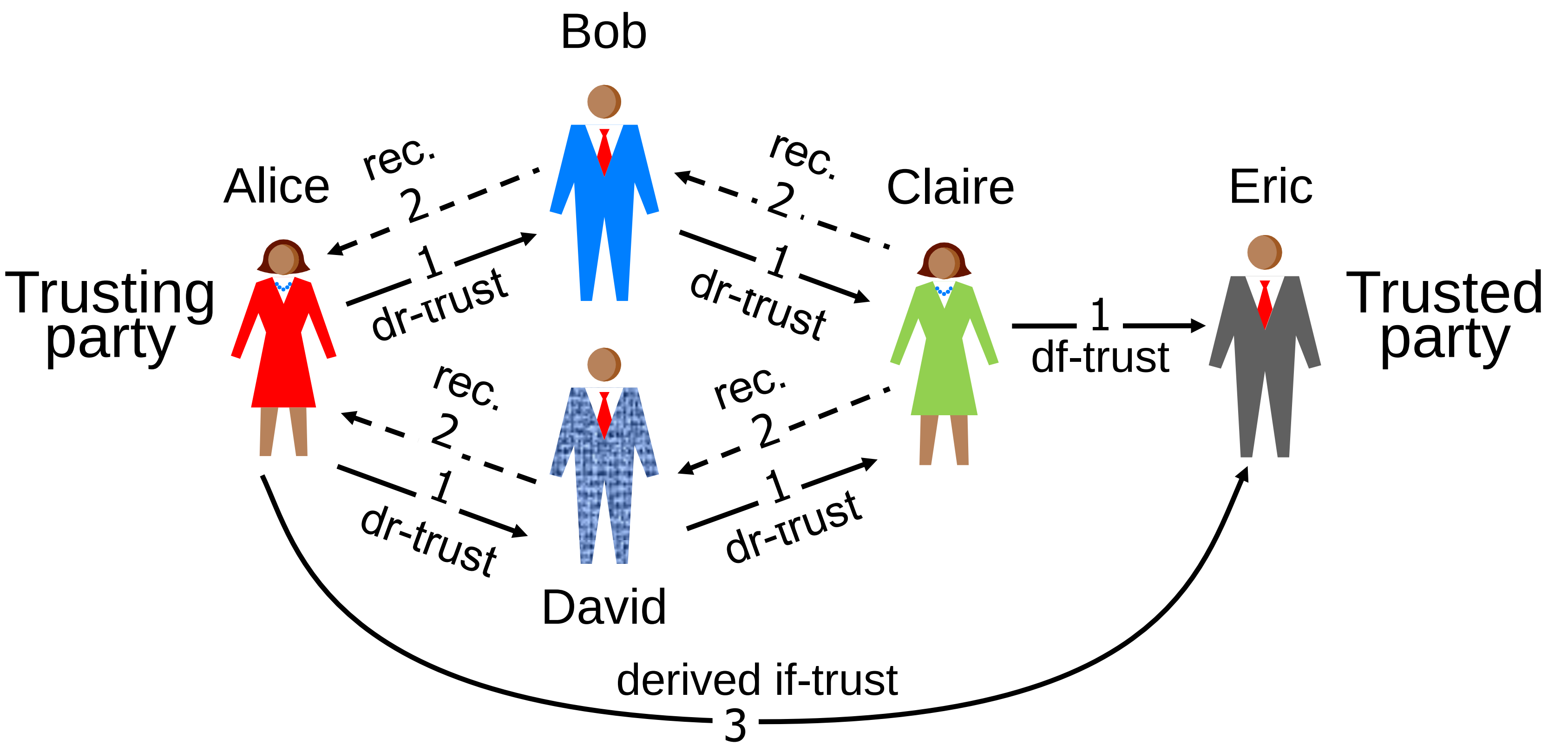
Trust scope consistency requirement



- A valid transitive trust path requires that there exists a trust scope which is a common subset of all trust scopes in the path. The derived trust scope is then the largest common subset.

Trust network building blocks

Combination of serial and parallel trust paths



Notation:
(implicit scope)

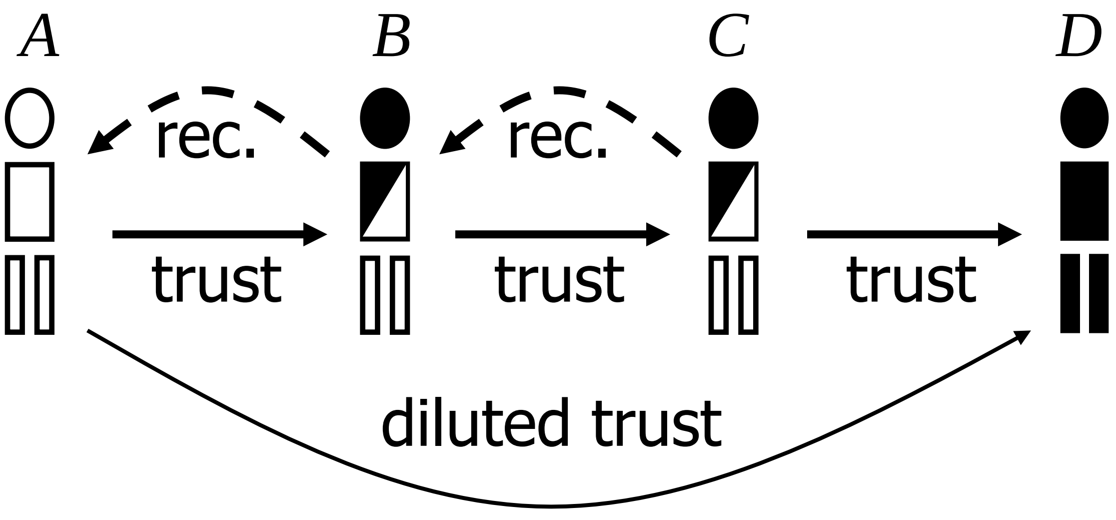
$$[A, E] = (([A,B] : [B,C]) \Diamond ([A,D] : [D,C])) : [C,E]$$

Additional aspects of trust

- Trust measure: μ
  - Binary (e.g. “Trusted”, “Not trusted”)
  - Discrete (strong-, weak-, trust or distrust)
  - Continuous (percentage, probability, belief)
- Time: τ
  - Time stamp when trust was assessed and expressed. Very important as trust generally weakens with temporal distance.

Trust transitivity characteristics

Trust is diluted in a transitive chain.

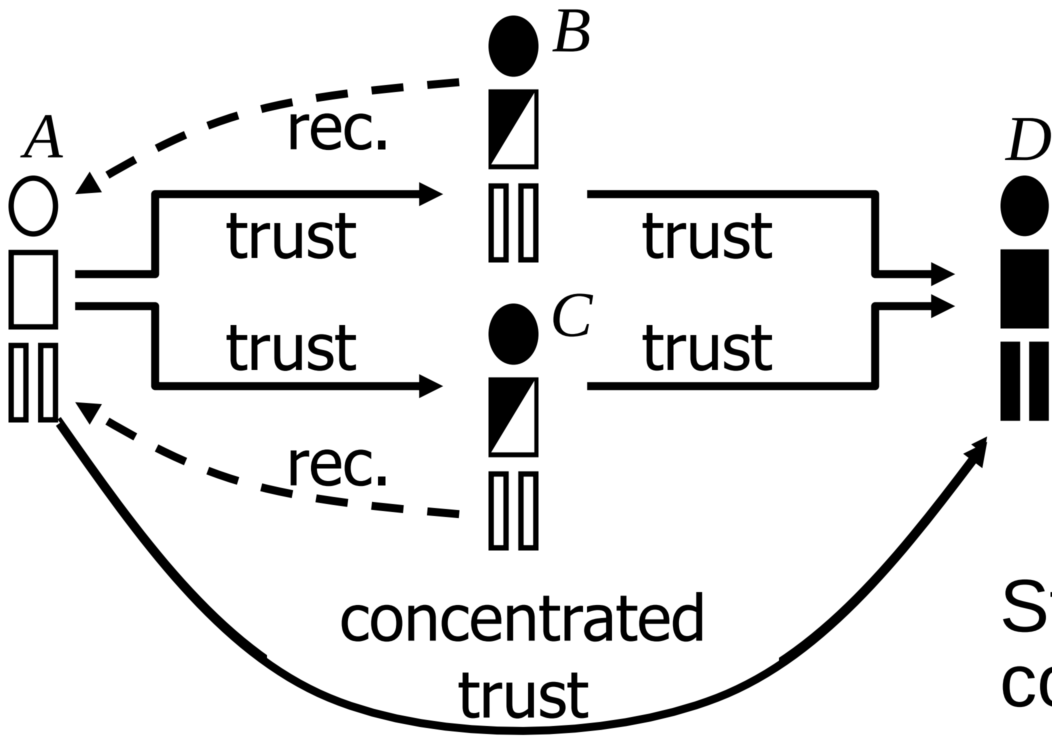


Computed with transitivity operator of SL

Graph notation: $[A, D] = [A, B] : [B, C] : [C, D]$

Explicit notation: $[A, D, \text{if}\sigma] = [A, B, \text{dr}\sigma] : [B, C, \text{dr}\sigma] : [C, D, \text{df}\sigma]$

Trust fusion characteristics

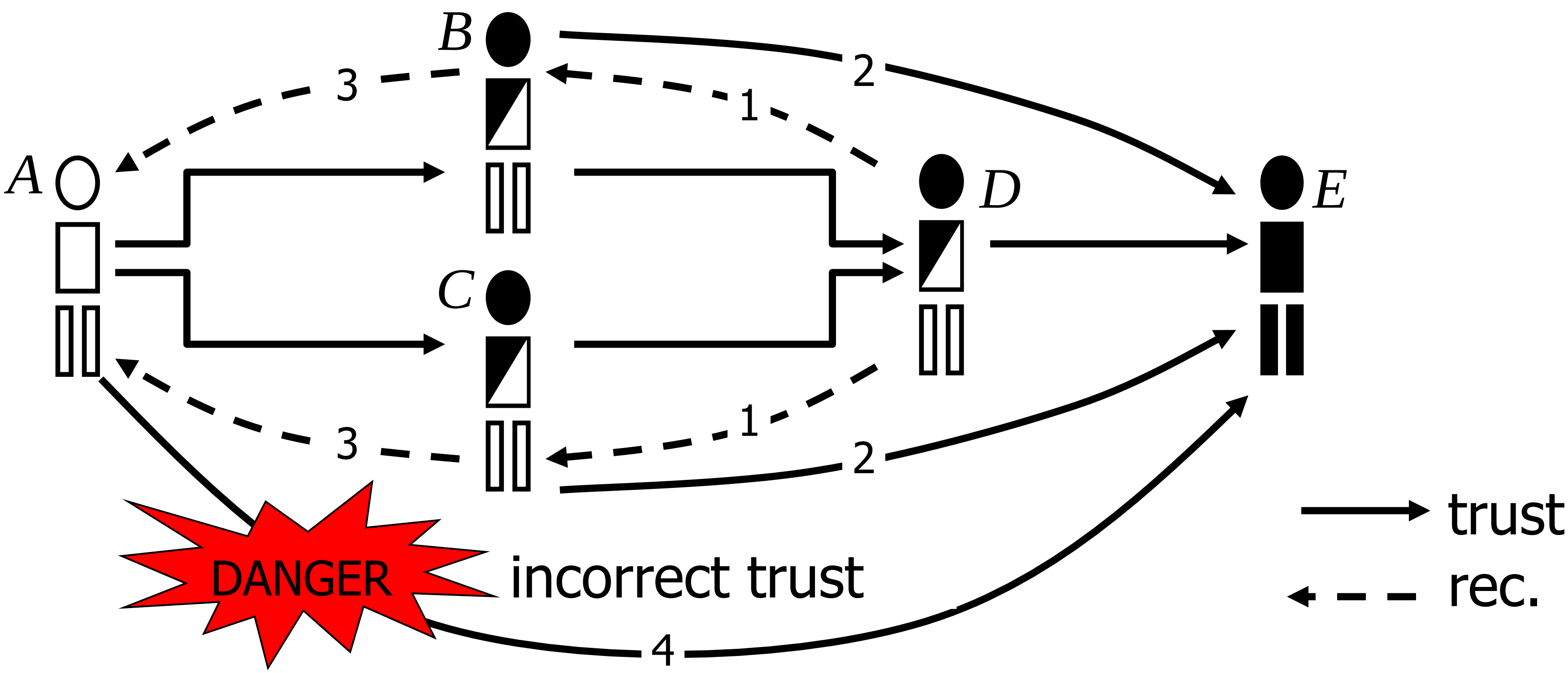


Strengthens trust confidence

Computed with the fusion operator of subjective logic

Graph notation: $[A, D] = ([A, B] : [B, D]) \Diamond ([A, C] : [C, D])$

Indirect referral trust

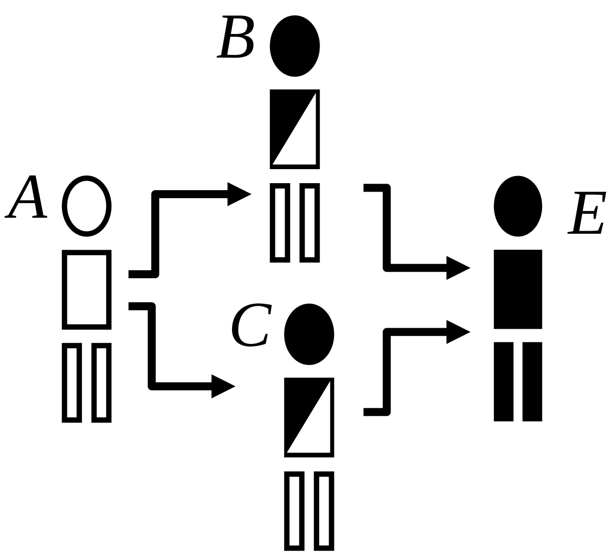


Perceived $([A, B] : [B, E]) \Diamond ([A, C] : [C, E])$

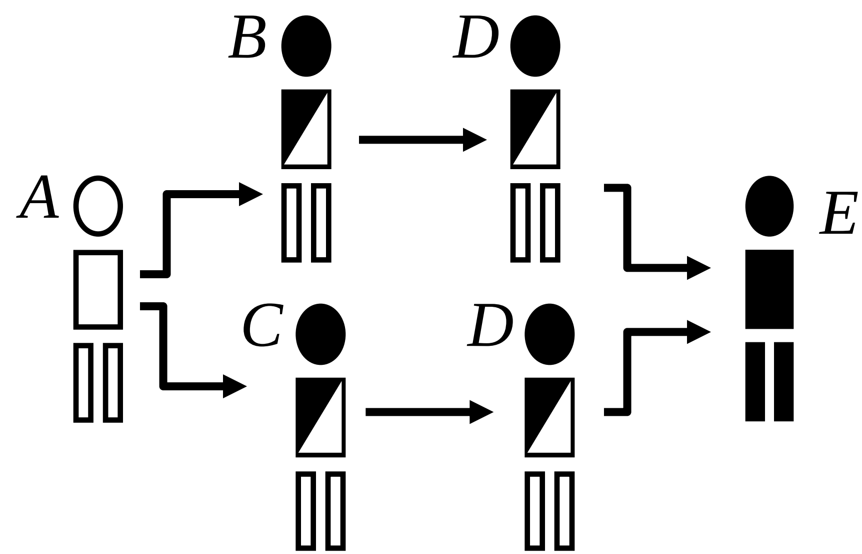
Reality: $([A, B] : [B, D] : [D, E]) \Diamond ([A, C] : [C, D] : [D, E])$

Hidden and perceived topologies

Perceived topology:



Hidden topology:

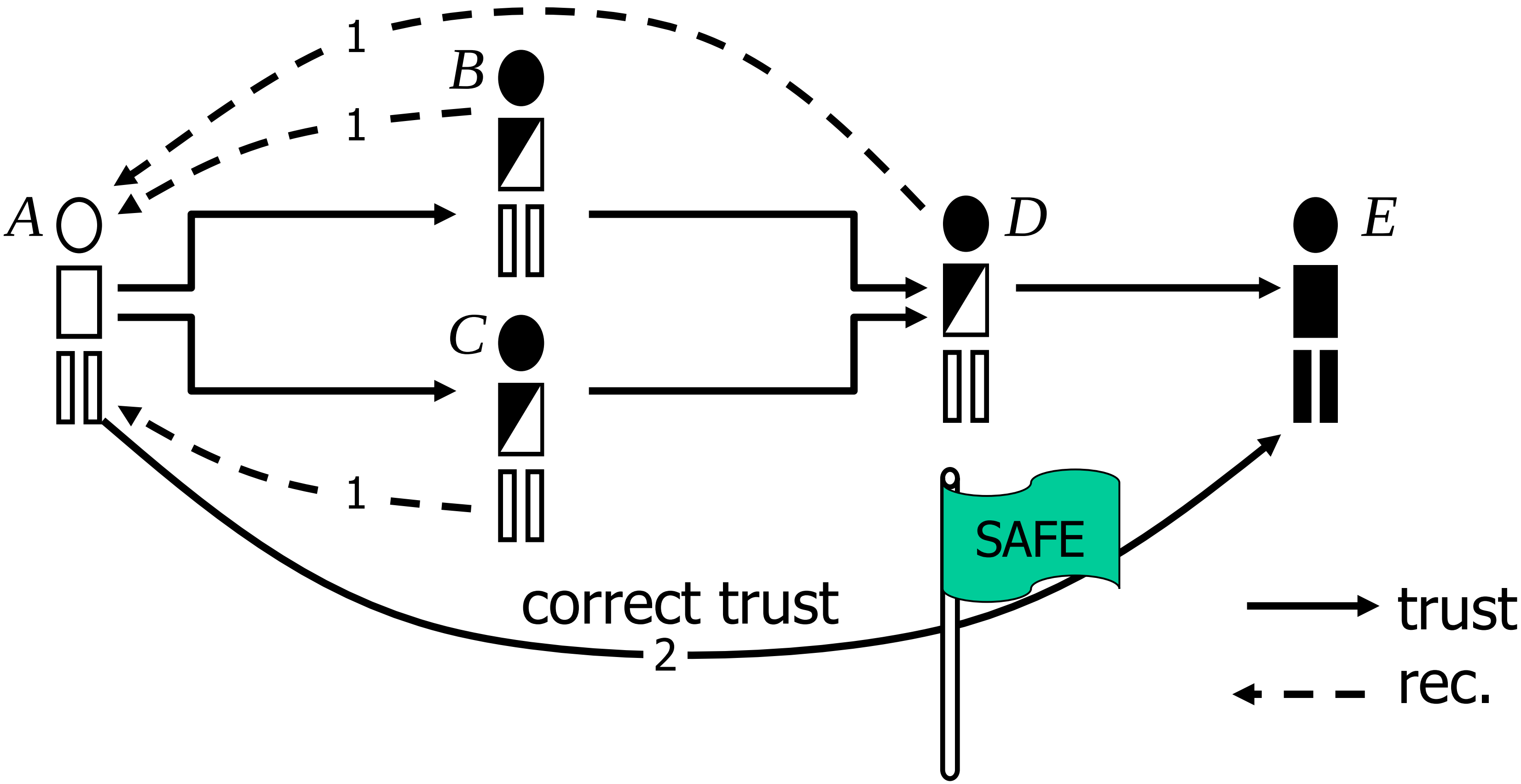


$$([A, B] : [B, E]) \ \lozenge \ ([A, C] : [C, E])$$

$$\neq \ ([A, B] : [B, D] : \mathbf{[D, E]}) \ \lozenge \ ([A, C] : [C, D] : \mathbf{[D, E]})$$

(D, E) is taken into account twice

Correct indirect referral trust

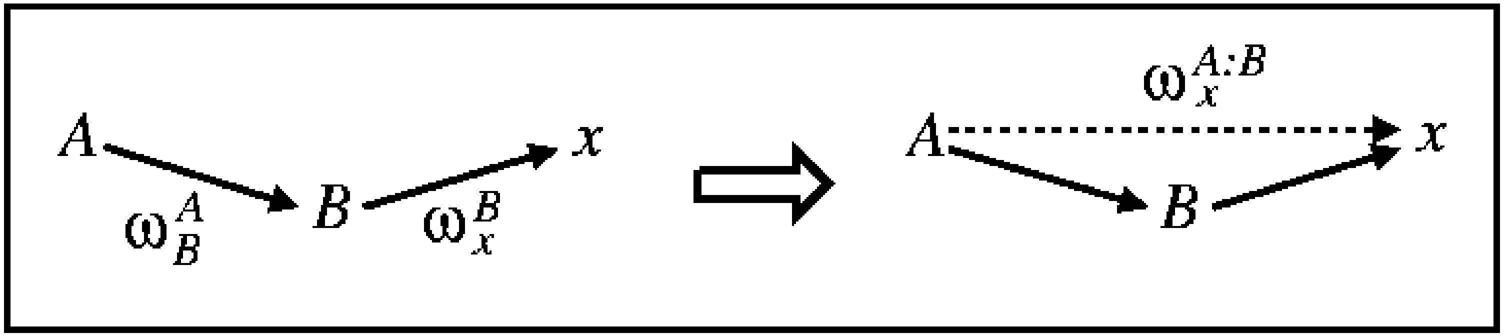


Perceived and_real topologies are equal:

$$(([A, B] : [B, D]) \lozenge ([A, C] : [C, D])) : [D, E]$$

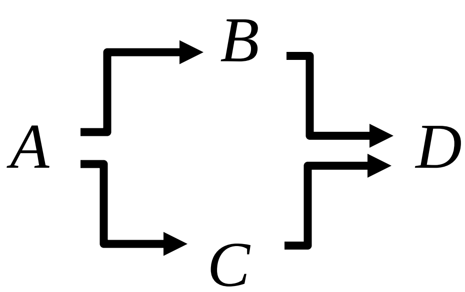
Trust transitivity in SL

- Notation: $\omega_x^{A:B} = \omega_B^A \otimes \omega_x^B$
- Associative and non-commutative.
- Operator for transitive belief
- No correspondence to logic or probability.



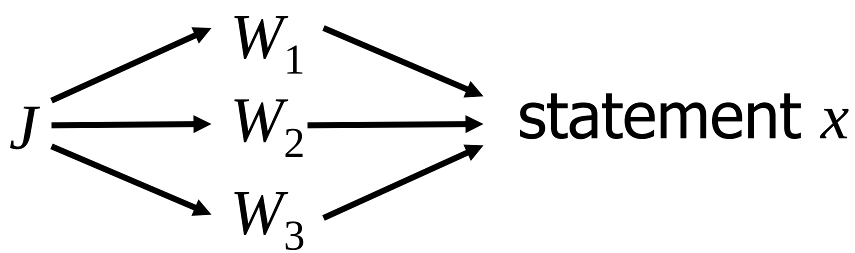
Trust notation with subjective logic

- Agent A trust agent B for trust scope σ
  - Explicit notation: $\omega^{A}_{B(\sigma)}$
  - Implicit notation: ω^{A}_{B} (implicit trust scope)
- Example: $([A, B] : [B, D]) \lozenge ([A, C] : [C, D])$
  - SL notation: $(\omega^{A}_{B} \otimes \omega^{B}_{D}) \oplus (\omega^{A}_{C} \otimes \omega^{C}_{D})$



Example: Weighing testimonies

- Computing beliefs about statements in court.
- J is the judge.
- W_1, W_2, W_3 are witnesses providing testimonies.

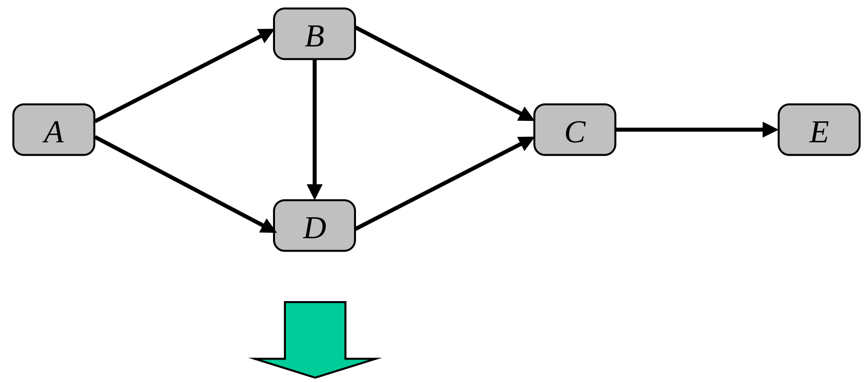


$$\omega_x^{(J:W_1)\Diamond(J:W_2)\Diamond(J:W_3)}$$

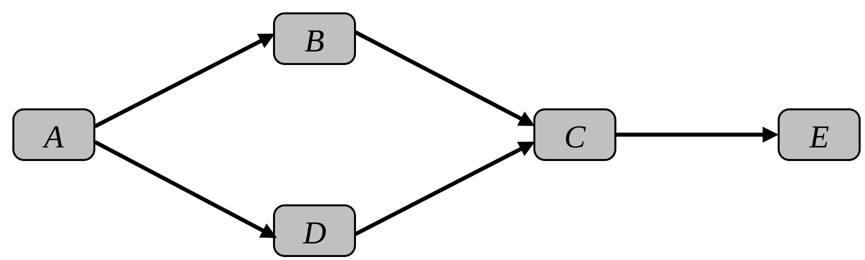
Trust network analysis with subjective logic

- Subjective logic can be used to analyse Directed Series Parallel Graphs (DSPG)
- Complex networks must be simplified

Original graph:
(non-DSPG)



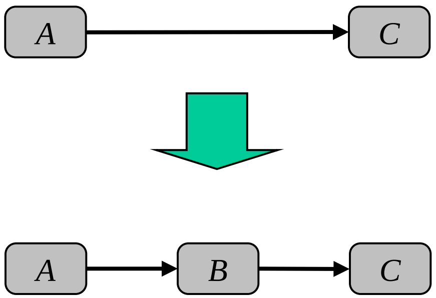
Simplified graph 1:
(DSPG graph)



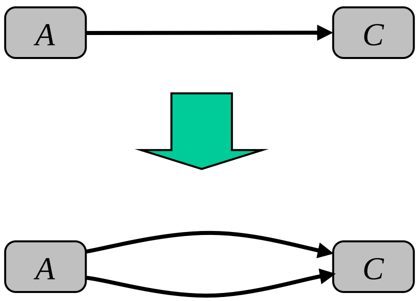
Building Directed Series-Parallel Graphs

- Repeatedly apply
  - Series graph composition
  - Parallel graph composition

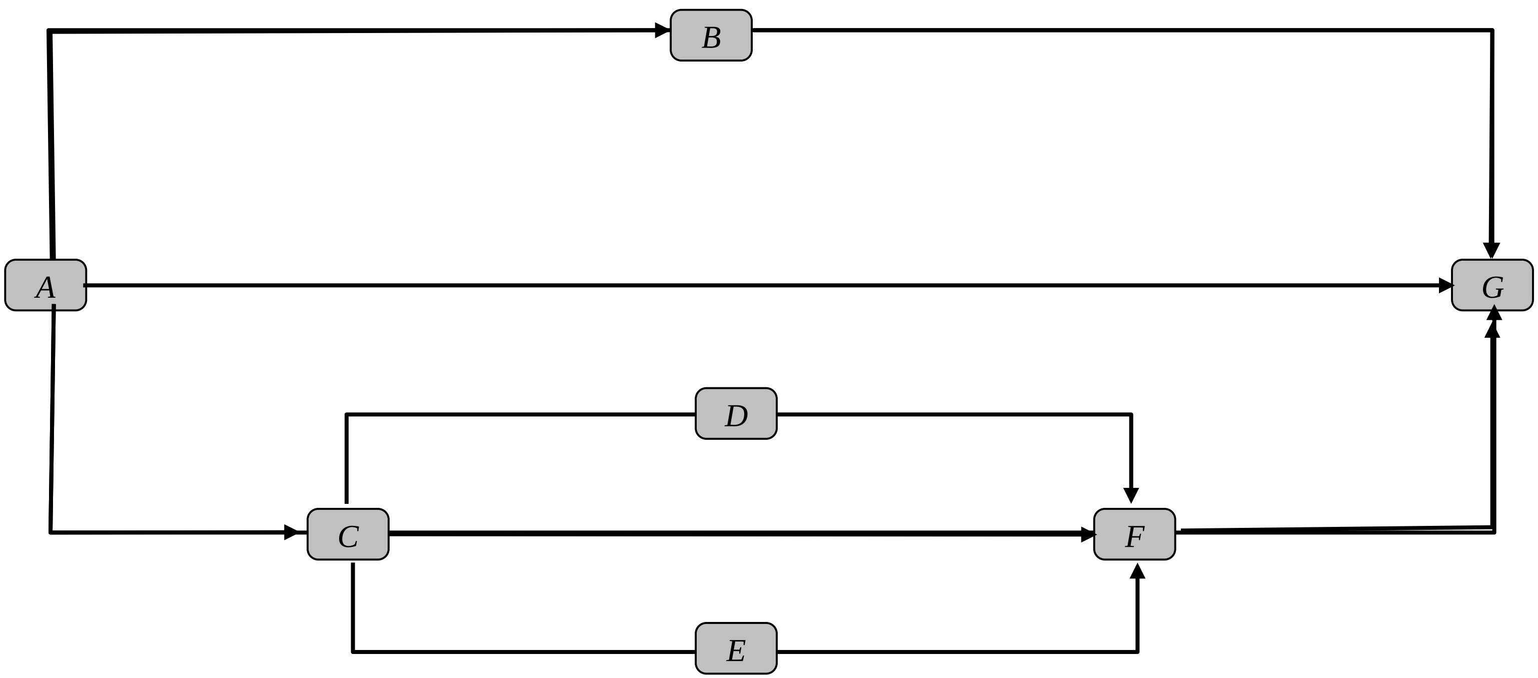
Series graph composition:



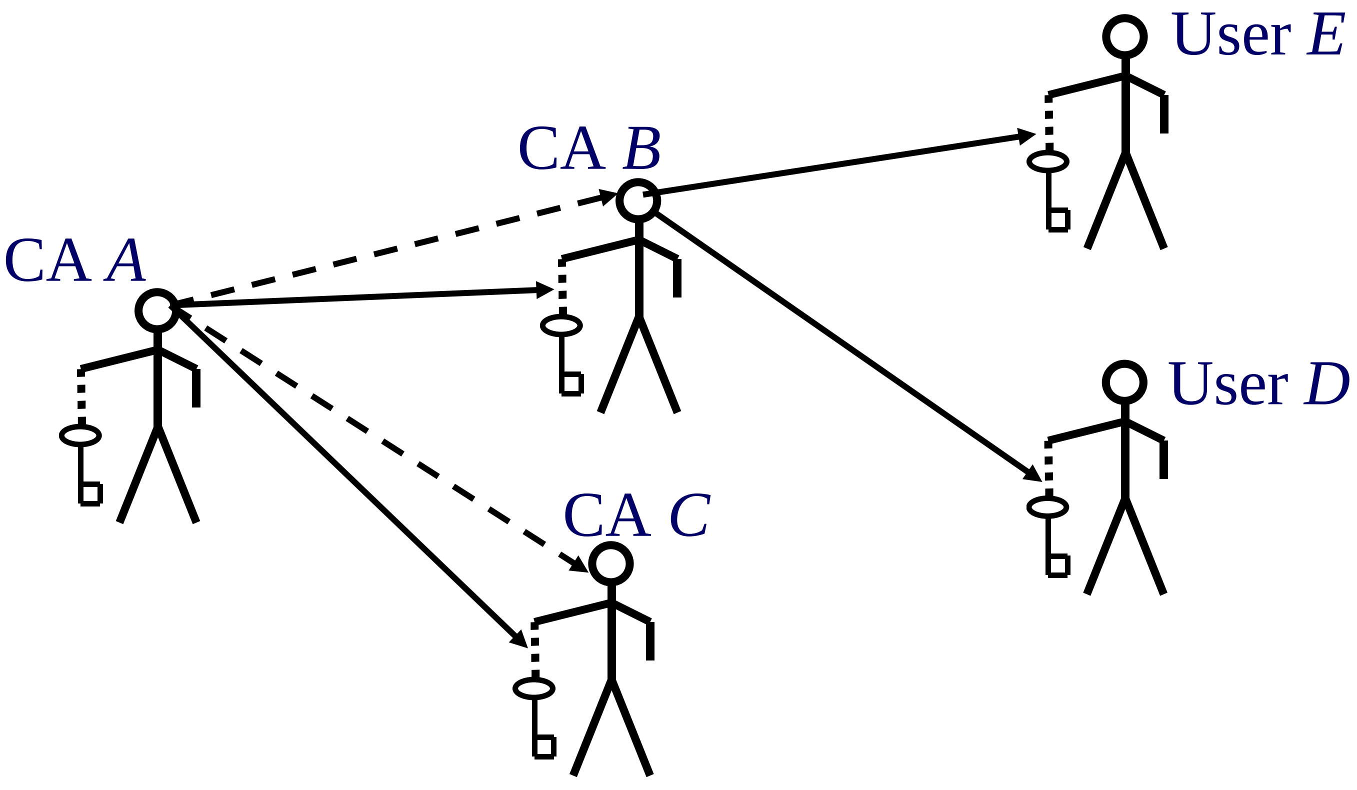
Parallel graph composition:



Example DSPG composition



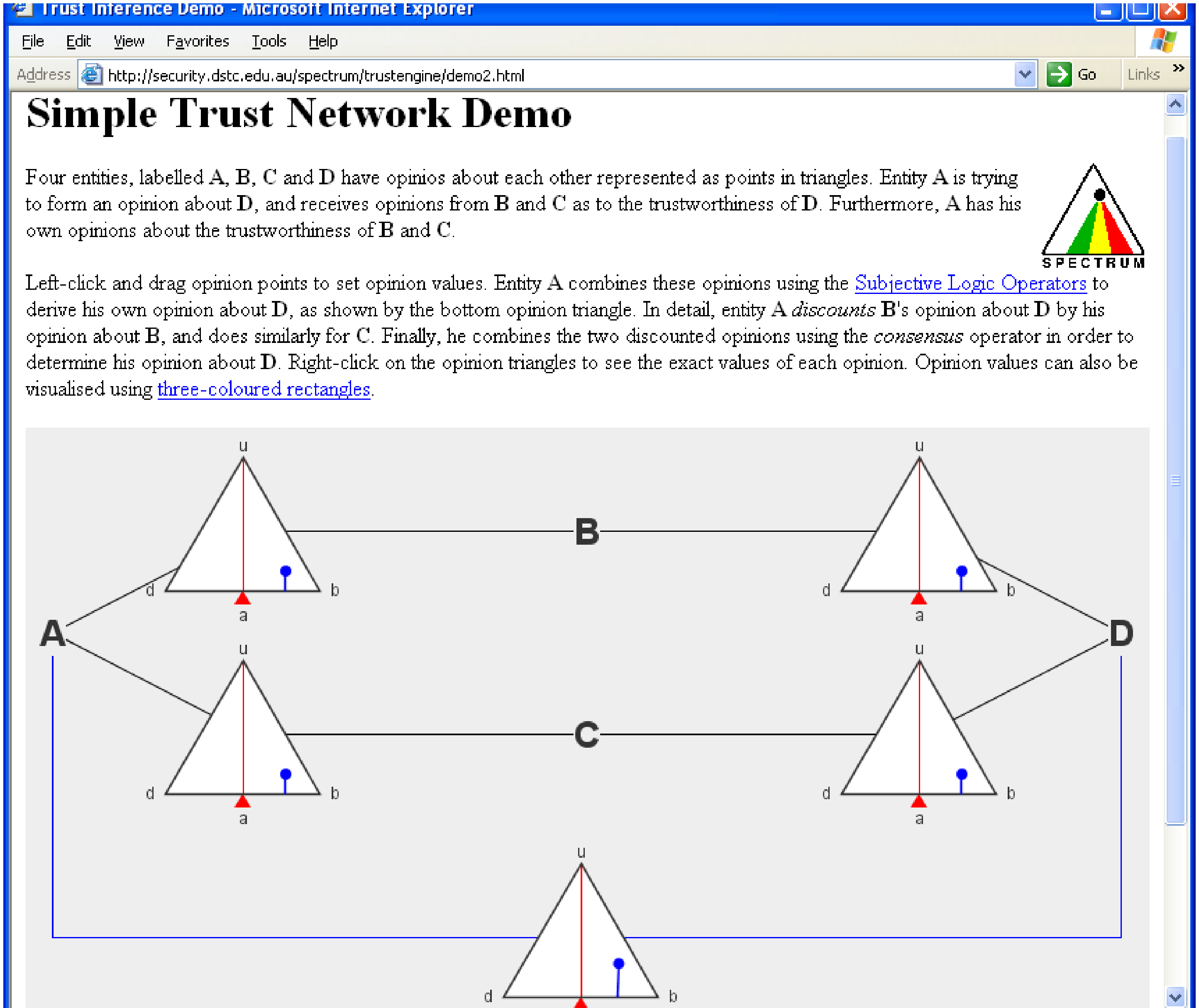
PKI and trust transitivity



Trust in public keys (explicit through certificate chaining)

Trust in CA's (implicitly expressed through policies)

Computational trust with subjective logic



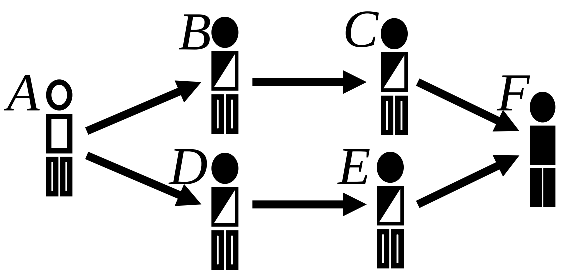
http://persons.unik.no/josang/sl/

Trust model exercise 1

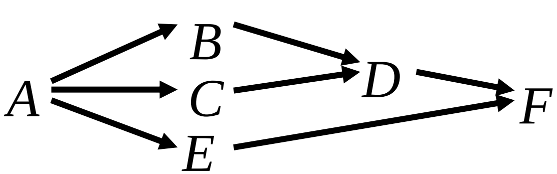
Write the trust expressions corresponding to the trust networks.

Try to write both network notation and subjective logic notation.

1.a)

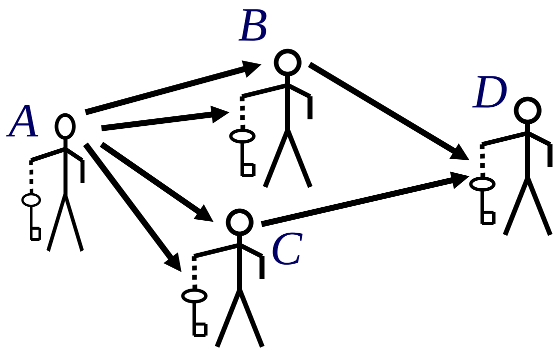


1.b)



Trust model exercise 2

- Write subjective logic expression corresponding to the certificate network below.



$$\omega^{A}_{B} = \omega^{A}_{(\mathrm{rel}(B) \wedge (\mathrm{aut}(\mathrm{k}_B))}$$

$$\omega^{A}_{C} = \omega^{A}_{(\mathrm{rel}(C) \wedge (\mathrm{aut}(\mathrm{k}_C))}$$

$$\omega^{A}_{\mathrm{aut}(\mathrm{k}_D)} =$$

Trust model exercise 3

Draw the trust network corresponding to the following expression:

$$(((\omega_B^A \otimes (\omega_D^B \otimes \omega_F^D) \oplus (\omega_E^B \otimes \omega_F^E)) \oplus (\omega_C^A \otimes \omega_F^C)) \otimes \omega_G^F) \oplus \omega_G^A$$

Solutions to trust model exercises

- 1a:

$$\omega^{A}_{F} = (\omega^{A}_{B} \otimes \omega^{B}_{C} \otimes \omega^{C}_{F}) \oplus (\omega^{A}_{D} \otimes \omega^{D}_{E} \otimes \omega^{E}_{F})$$

- 1b:

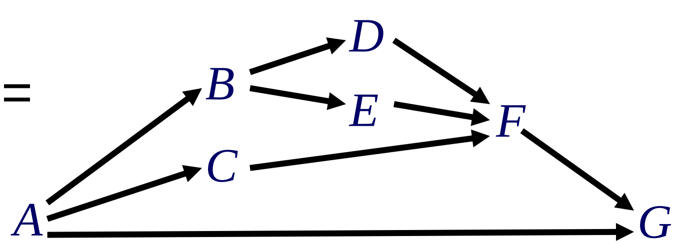
$$\omega^{A}_{F} = (((\omega^{A}_{B} \otimes \omega^{B}_{D}) \oplus (\omega^{A}_{C} \otimes \omega^{C}_{D})) \otimes \omega^{D}_{F}) \oplus (\omega^{A}_{E} \otimes \omega^{E}_{F})$$

- 2:

$$\omega^{A}_{\text{aut}(k_D)} = ((\omega^{A}_{\text{rel}(B)} \cdot \omega^{A}_{\text{aut}(k_B)}) \otimes \omega^{B}_{\text{aut}(k_D)}) \oplus ((\omega^{A}_{\text{rel}(C)} \cdot \omega^{A}_{\text{aut}(k_C)}) \otimes \omega^{C}_{\text{aut}(k_D)})$$

- 3:

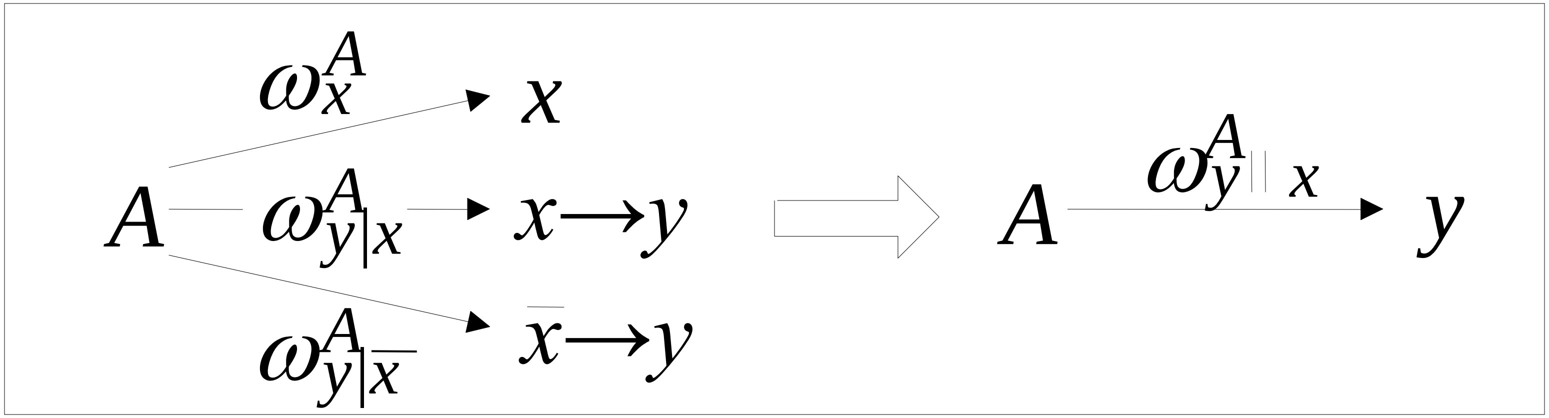
$$\omega^{A}_{G} =$$



Bayesian belief reasoning

Conditional deduction

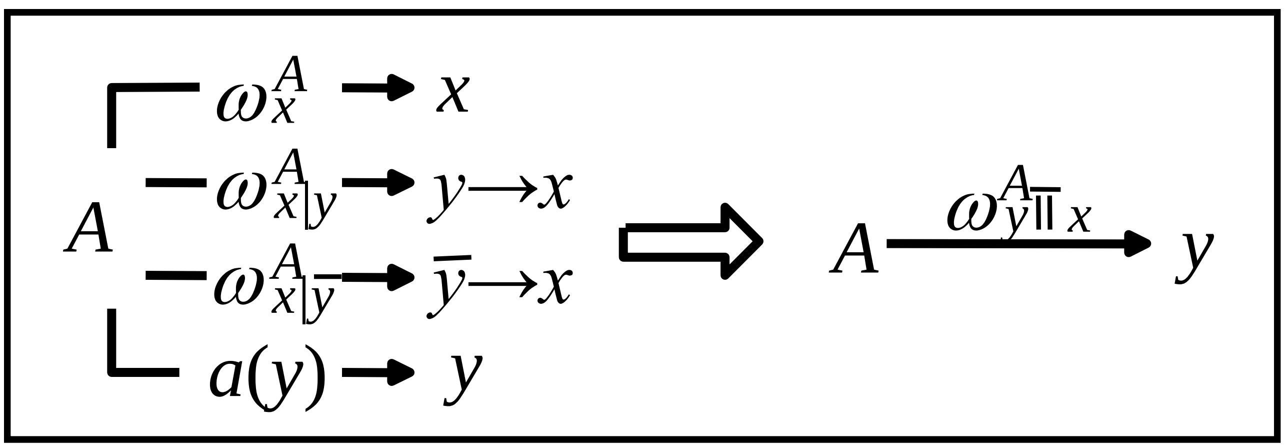
- Notation: $\omega^{A}_{y\|x} = \omega^{A}_{x} \circledcirc (\omega^{A}_{y|x}, \omega^{A}_{y|\bar{x}})$
- Probability: $p(y\|x) = p(x) \cdot p(y|x) + p(\bar{x}) \cdot p(y|\bar{x})$
- Corresponds to MODUS PONENS and conditional inference.
- Ternary operator



Conditional abduction

- Notation:
- Corresponds to MODUS TOLLENS and reverse conditional inference.
- Quaternary operator

$$\omega^{A}_{\bar{y}\|x} = \omega^{A}_{x} \,\bar{\circledcirc}\, (\omega^{A}_{x|y}, \omega^{A}_{x|\bar{y}}, a(y))$$



About evidence ...

Causal evidence
directly influences the likelihood of one or more hypotheses.

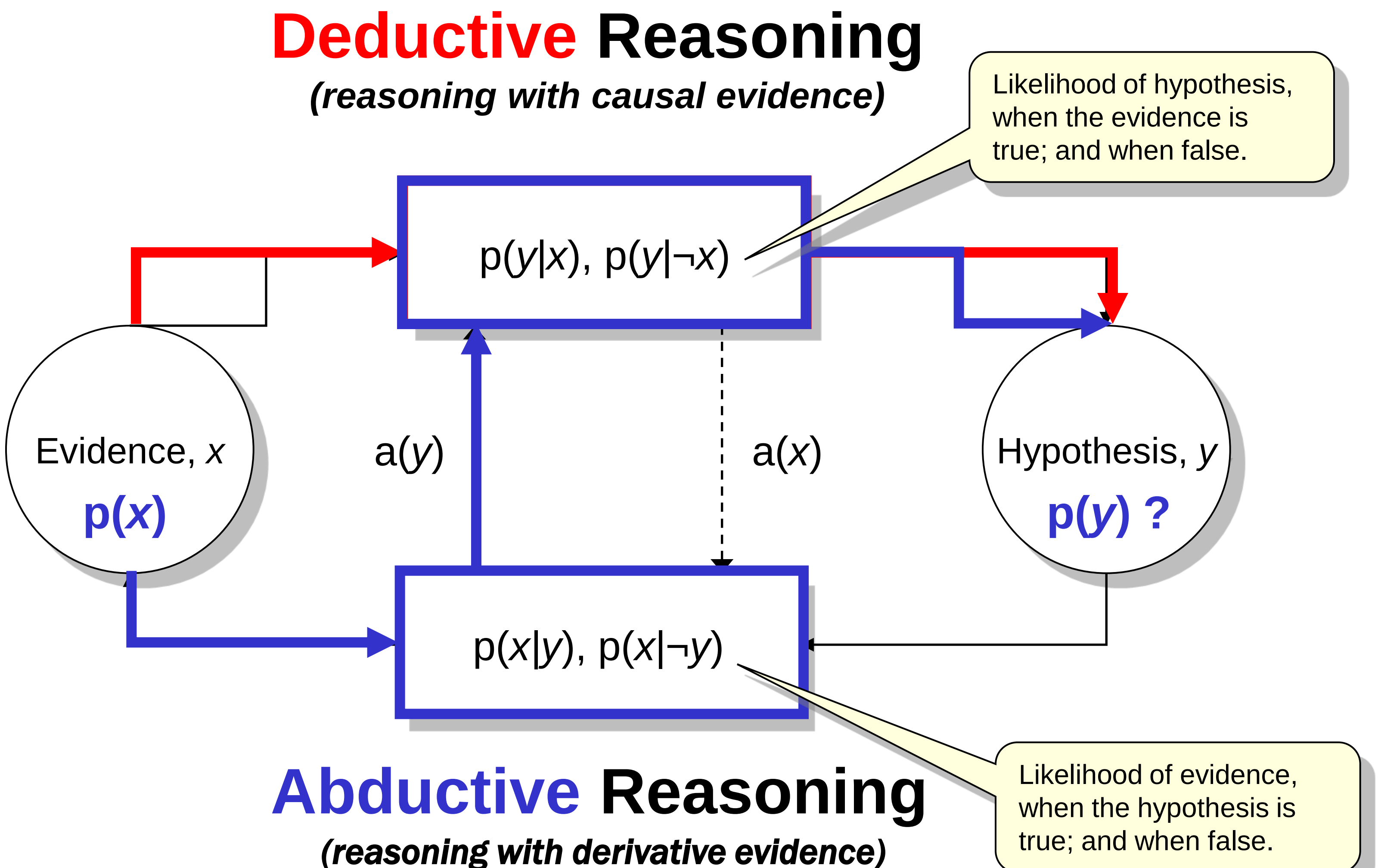
***Deductive* reasoning uses likelihood of each hypothesis‡, for each piece of evidence, i.e. $p(y|x)$ and $p(y|\overline{x})$.**

Derivative evidence
is usually observed in conjunction with one or more hypotheses.

***Abductive* reasoning uses likelihood of evidence‡, for each hypothesis, i.e. $p(x|y)$ and $p(x|\overline{y})$.**

‡ *plus knowledge of the base rates of the hypotheses y and evidence.x*

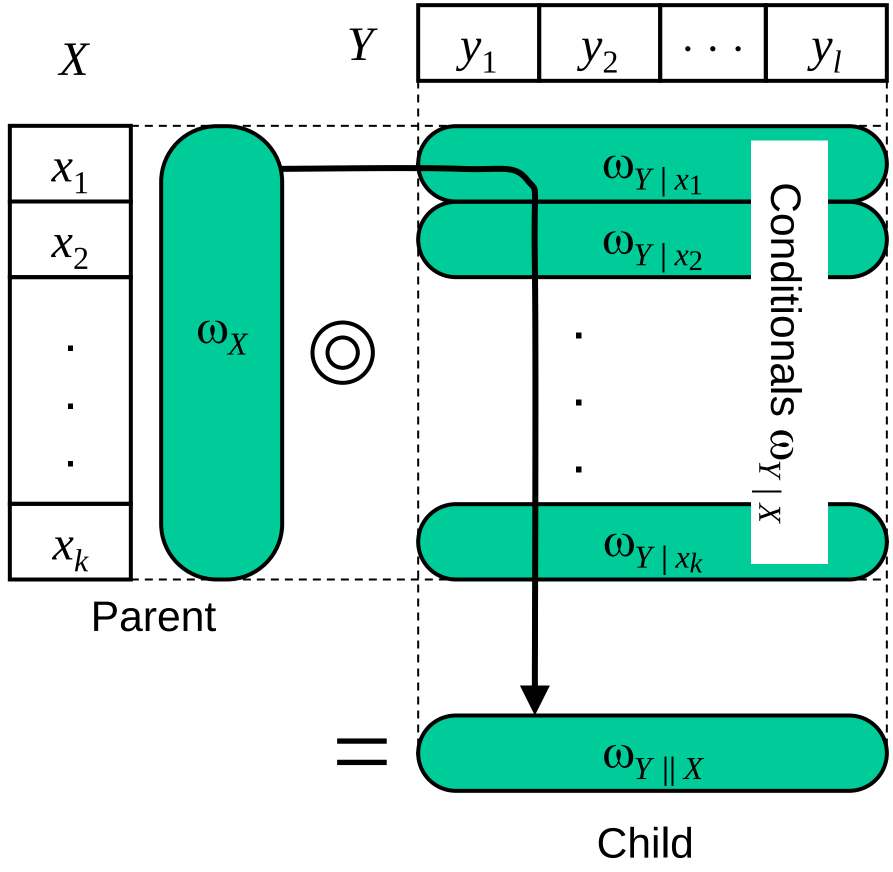
Deductive vs. abductive reasoning



The Base Rate Fallacy

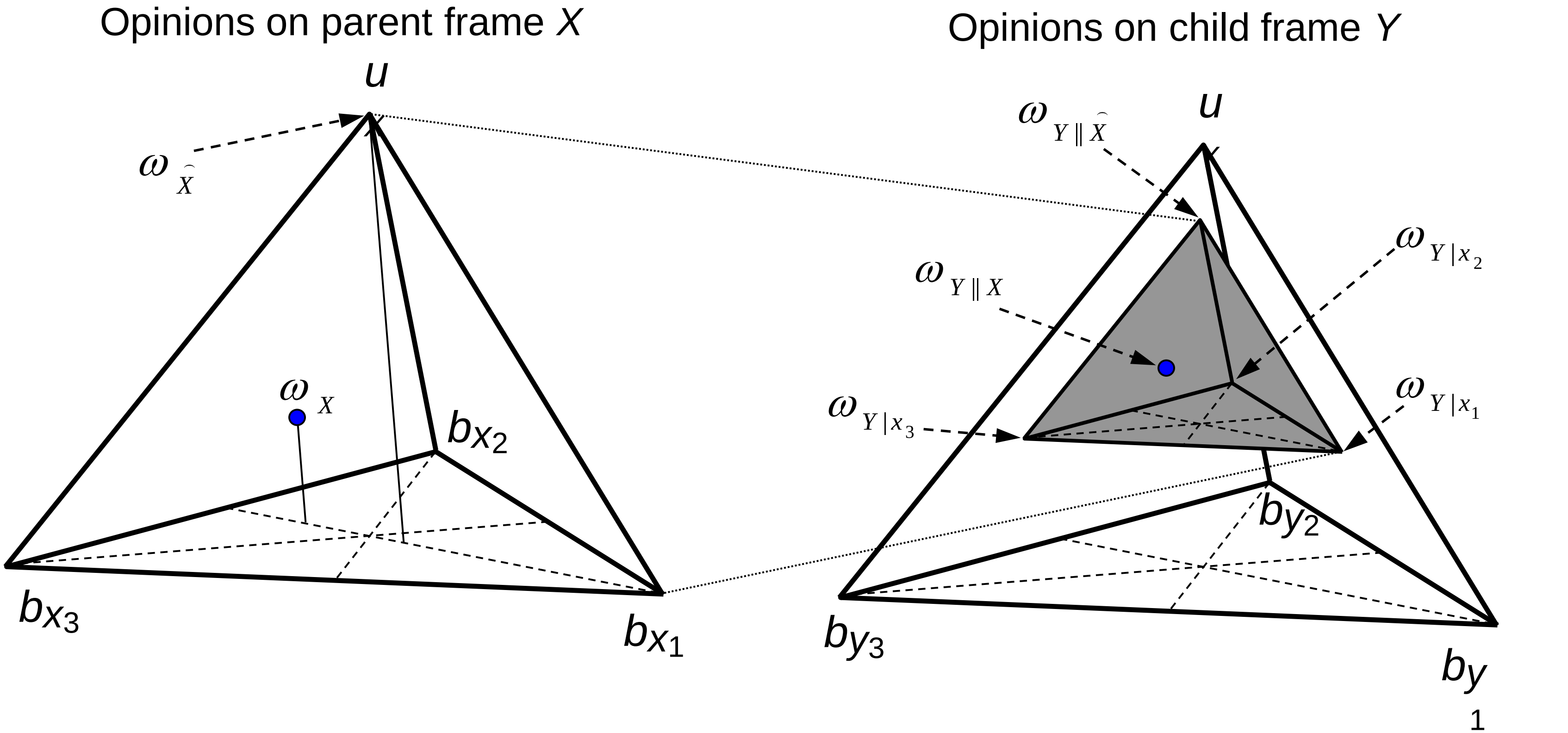
- The **base rate fallacy** is an error that occurs when $p(y||x)$, the conditional probability of some hypothesis y given some evidence x, is assessed without taking account of the "base rate" of y, often as a result of wrongly assuming equality between the two inverse conditionals: $p(y|x) = p(x|y)$.
- The correct type of reasoning where the conditional $p(y|x)$ is correctly derived, is commonly referred to as *abduction*.

Deduction with subjective logic

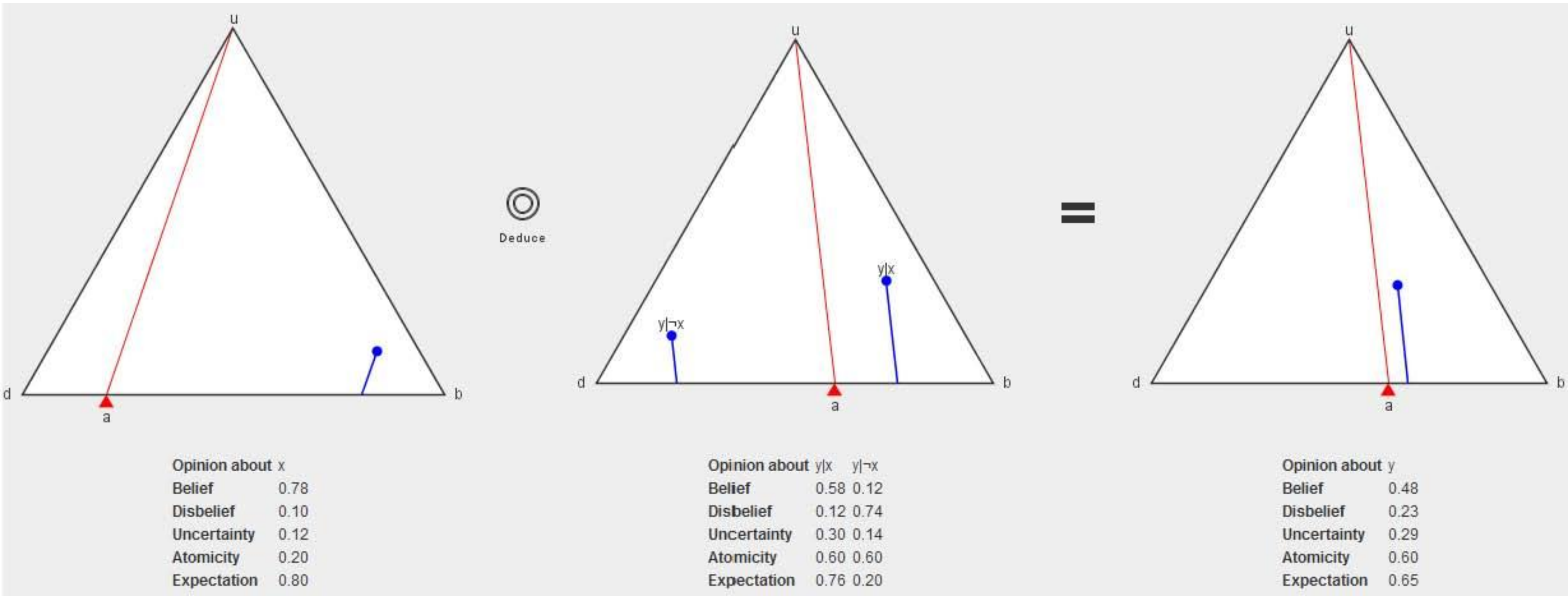


Deduction visualisation

- Evidence pyramid is mapped inside hypothesis pyramid as a function of the conditionals.
- Conclusion opinion is linearly mapped

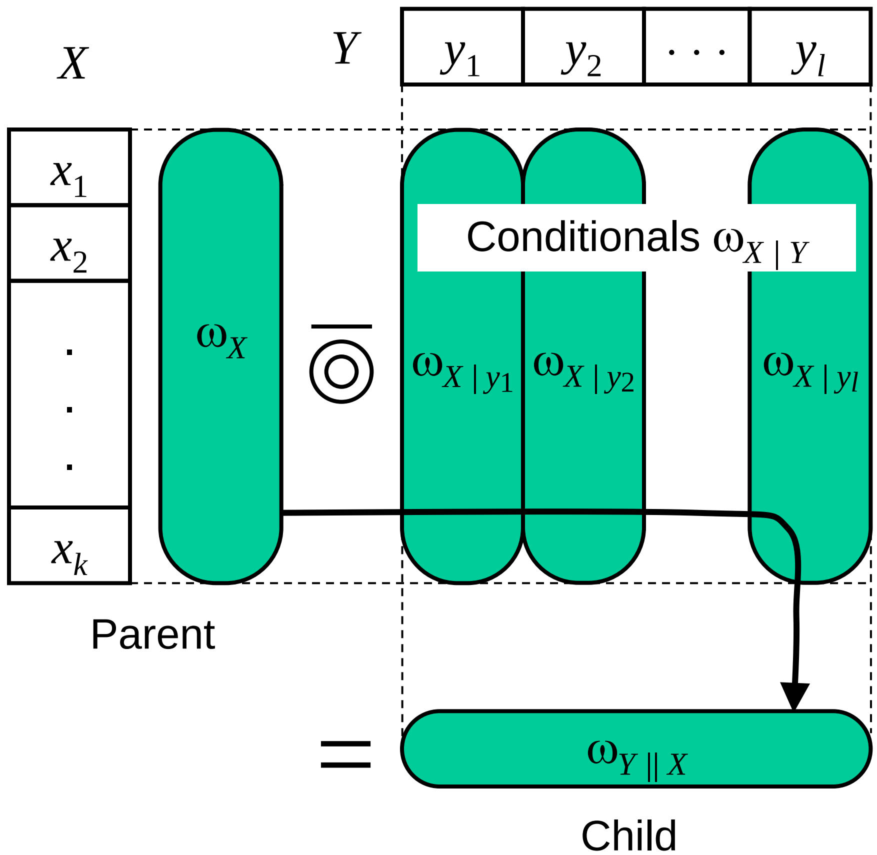


Deduction – online operator demo

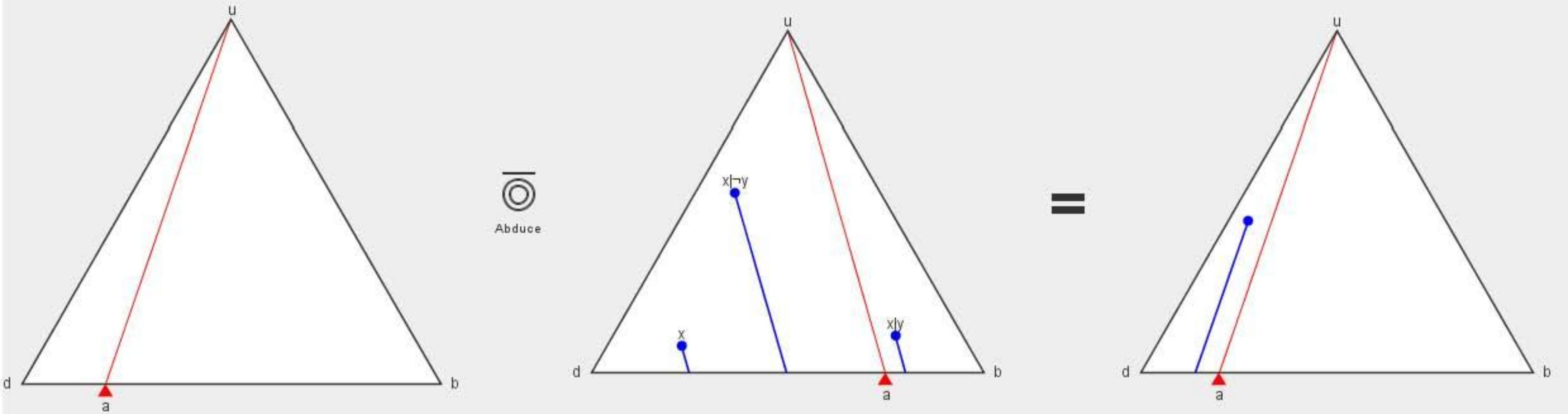


http://persons.unik.no/josang/sl/

Abduction with subjective logic



Abduction – Online operator demo



Opinion about	br(y)
Belief	0.00
Disbelief	0.00
Uncertainty	1.00
Atomicity	0.20
Expectation	0.20

Opinion about	x	x|y	x|¬y
Belief	0.19	0.72	0.10
Disbelief	0.73	0.17	0.37
Uncertainty	0.08	0.11	0.53
Atomicity	0.75	0.75	0.75
Expectation	0.25	0.80	0.50

Opinion about	y
Belief	0.05
Disbelief	0.50
Uncertainty	0.45
Atomicity	0.20
Expectation	0.14

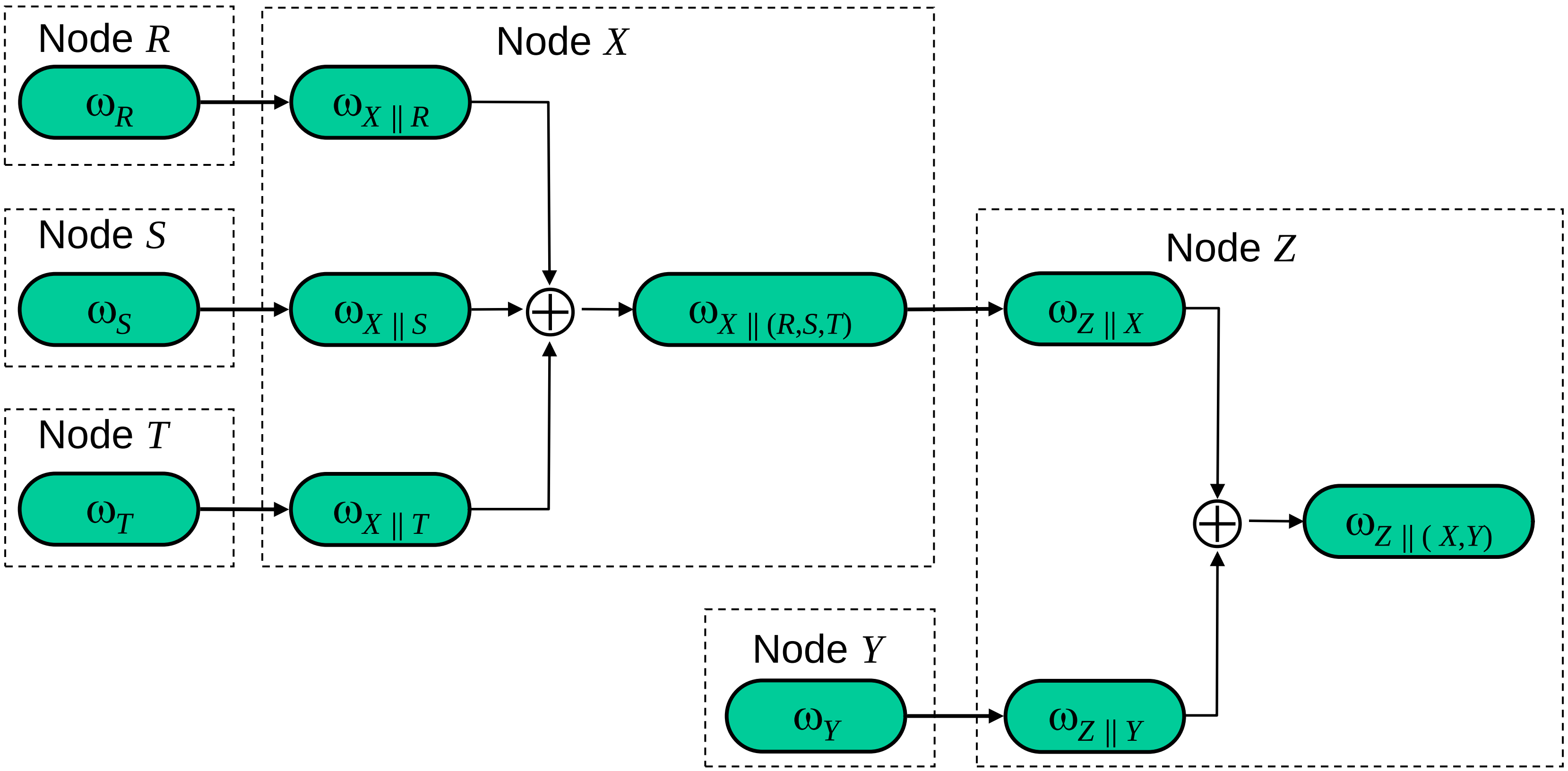
Deduction and abduction notation

- Binomial deduction $\omega_{y\|x} = \omega_x \circledcirc (\omega_{y|x}, \omega_{y|\bar{x}})$
- Multinomial deduction $\omega_{Y\|X} = \omega_X \circledcirc \omega_{Y|X}$
- Binomial abduction $\omega_{y\bar{\|}x} = \omega_x \overline{\circledcirc} (\omega_{x|y}, \omega_{x|\bar{y}}, a_y)$
- Multinomial abduction $\omega_{Y\bar{\|}X} = \omega_X \overline{\circledcirc} (\omega_{X|Y}, \vec{a}_Y)$

Bayesian logic

- Subjective logic represents a calculus for Beta and Dirichlet PDFs
- Analytically correct for 1st moment, i.e. expectation value.
- Approximation for 2nd moment (i.e. variance)
- Analytic or numeric combination of PDFs give high computational complexity
- Subjective logic gives very low computational complexity
- Bayesian logic

Bayesian network representation



Forensic Reasoning Application

- The conditional relationship between observed evidence and malicious actions that produced it can be analysed with abductive reasoning.
- Need to find $\omega_{(\text{action})}$, i.e. opinion about hypothetical malicious action.
- Requires $\omega_{(\text{action} \mid \text{evidence})}$ and $\omega_{(\text{action} \mid \text{no evidence})}$
- Can estimate $\omega_{(\text{evidence} \mid \text{action})}$ and $\omega_{(\text{evidence} \mid \text{no action})}$
- Can derive $\omega_{(\text{action} \mid \text{evidence})}$ and $\omega_{(\text{action} \mid \text{no evidence})}$
- Can then compute the needed $\omega_{(\text{action} \,\|\, \text{evidence})}$

- Forensic analysis with subjective logic works even in the presence of high uncertainty

Exercise: Bayesian networks

1. Draw Bayesian network corresponding to:

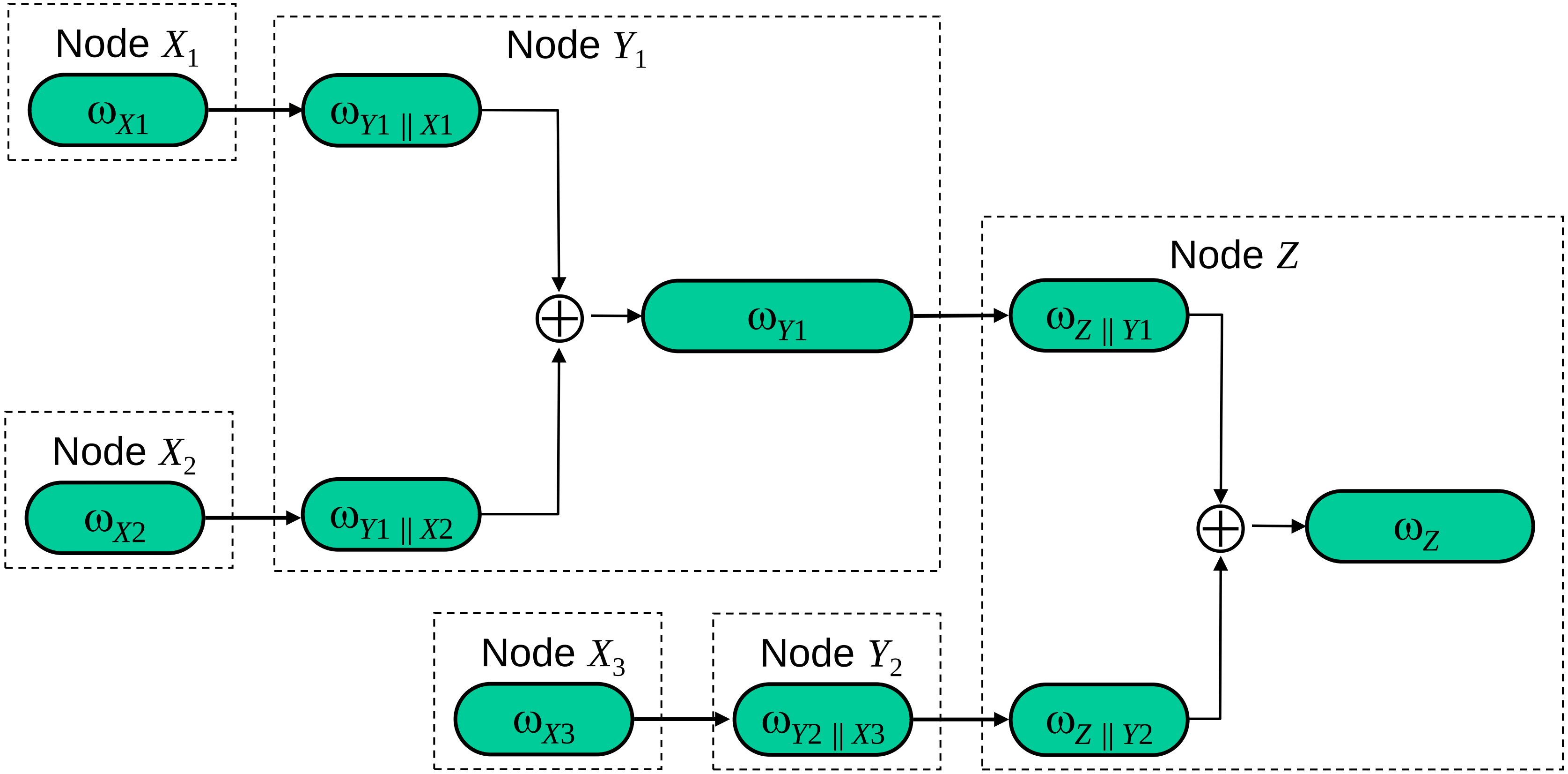
$$\omega_{Z} = \omega_{Z \| Y_1} \oplus \omega_{Z \| Y_2}$$

$$\omega_{Y_1} = \omega_{Y_1 \| X_1} \oplus \omega_{Y_1 \| X_2}$$

$$\omega_{Y_2} = \omega_{Y_2 \| X_3}$$

2. Write SL expressions corresponding to Bayesian network on previous slide

Solution 1 – Bayesian network



Solution 2 – Bayesian network

$$\omega_Z = \omega_{Z \| X} \oplus \omega_{Z \| Y}$$

$$\omega_X = \omega_{X \| R} \oplus \omega_{X \| S} \oplus \omega_{X \| T}$$

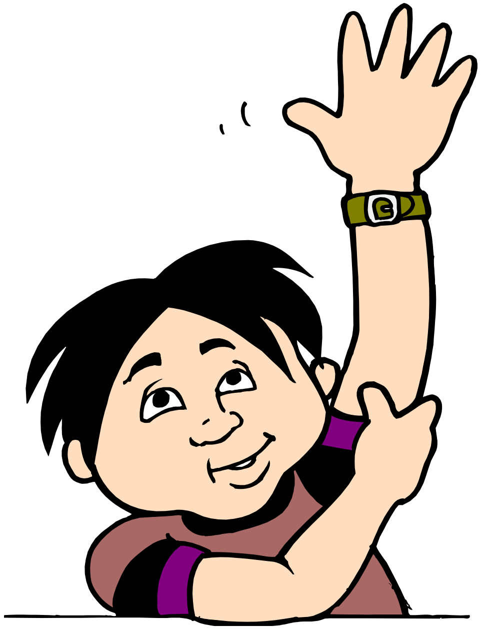
Final remarks

- Subjective logic
  - Compatible with
    - Binary logic
    - Probability models
  - Includes degrees of uncertainty
- Suitable for modelling realistic situations
  - Approximation of complex analytical models
  - Fast computation
  - Suitable for modelling trust networks
  - Analysis of situations with significant uncertainty,
    - Intelligence analysis
    - Possibly suitable for cryptanalysis

References

- Papers and online demo at: http://persons.unik.no/josang/
- Some relevant papers:
  - *Cumulative and Averaging Fusion of Beliefs (2010)*
  - *Conditional Reasoning with Subjective Logic (2008)*
  - *Simplification and Analysis of Transitive Trust Networks* (2006)
  - *Anlysis of Competing Hypotheses using Subjective Logic* (2005)
  - *Conditional Deduction Under Uncertainty* (2005)
  - *Multiplication and Comultiplication of Beliefs* (2004)
  - *The Consensus Operator for Combining Beliefs* (2002)
  - *A Logic for Uncertain Probabilities* (2001)

Thank you for your attention!



Questions?