# Qualitative Algebra for Trust Management in e-Services

**COST ECON@Tel**

**Rennes, May 9-10, 2011**

Denis Trček

Laboratory of E-media

Faculty of Computer and Information Science

University of Ljubljana, Slovenia / EU

University of Ljubljana

# Talk Outline

- Why this talk?
  - Already identifiable links to ECON@Tel.
  - Future work related to post ECON@Tel work.
- What is trust?
- Existing trust management solutions.
- What kind of ergonomic grounds can be used for its support (management) and justification for qualitative algebra?
- Application areas (computational / mathematical economics), future work.

# The importance of the area

- The EU commissioner Viviane Reding often exposes the problem of “lack of trust” in e-services.
- Andy Wyckoff of OECD has exposed the problem of lack of trust in the internet in general.
- Lack of trust in the web has clear economical implications.

# Getting to the core of trust…

- Some definitions of trust.
  - Trust is assured reliance on the character, ability, strength, or truth of someone or something (Merriam-Webster dictionary).
  - Trust is an assessment that is driven by experience, shared through a network of people interactions and continually remade each time the system is used (Dorothy J. Denning).

# Trust management methodologies

- Bayes theorem as the basis.
  - The posterior probability of a hypothesis H after observing datum D is given by
    - p(H | D) = p(D | H) * p(H) / p(D), where p(H) is the prior probability of H before D is observed, p(D|H) is the probability that D will be observed when H is true, and p(D) is the unconditional probability of D.
    - Similarly:

$$p(A \mid (B,C)) = p(A,B,C) \,/\, p(B,C) = \ldots =$$

$$= p(B \mid (A,C)) * p(A \mid C) \,/\, p(B \mid C)$$

# Trust management methodologies

- Theory of evidence (ToE).
  - Theory of evidence starts with a set of possible states, called a *frame of discernment* $\Theta$. Within $\Theta$, exactly one state is assumed to be true at any time.
  - A *basic probability assignment, BPA* (*called also belief mass*) is a function $m: 2^{\Theta} \rightarrow [0,1]$, where with each substate $x \in 2^{\Theta}$ $m(x)$ is associated, such that $m(x) \geq 0$, $m(\emptyset)=0$, and $\sum_{x \in 2^{\Theta}} m(x)=1$.
  - A belief mass $m_{\Theta}(x)$ expresses the belief assigned to the set $x$ (as a whole) and does not express any belief in subsets of $x$.

# Trust management methodologies

- ToE and Jøsang's logic / algebra.
  - Example:
    - Assume that $m(\{T\}) = 0.8$, $m(\{\neg T\}) = 0$, and $m(\{T, \neg T\}) = 0.2$.
    - Then $bel(\{T, \neg T\})=m(\{T\}) + m(\{\neg T\}) + m(\{T, \neg T\})$;
    - $bel(\{T\})=m(\{T\})=0.8$, and $bel(\{\neg T\})=m(\{\neg T\}) = 0$.
  - Jøsang defines trust $\omega$ as a triplet $(b, d, u)$, where $b$ stands for belief, $d$ for disbelief and $u$ for uncertainty, such that

$$b(x) = \sum_{y \subseteq x} m(y), \qquad d(x) = \sum_{x \cap y = \emptyset} m(y),$$

$$u(x) = 1 - (b(x) + d(x)), \qquad x, y \in 2^{\Theta}$$

# Trust management methodologies

(from Josang A., An Algebra for Assessing Trust in Certification Chains, NDSS'99, ISOC 1999)

- Jøsang's logic / algebra.
  - Its main contribution are various operators.
  - An example - consensus:

**Definition 4 Consensus**
*Let $\omega_p^A = \{b_p^A, d_p^A, u_p^A\}$ and $\omega_p^B = \{b_p^B, d_p^B, u_p^B\}$ be opinions respectively held by agents $A$ and $B$ about the same binary statement $p$. Then the consensus opinion held by an imaginary agent $[A, B]$ representing both $A$ and $B$ is defined by:*

$$\begin{aligned} \omega_p^{A,B} &= \omega_p^A \oplus \omega_p^B \\ &= \{b_p^{A,B},\ d_p^{A,B},\ u_p^{A,B}\} \end{aligned}$$

*where*

$$\begin{cases} b_p^{A,B} = (b_p^A u_p^B + b_p^B u_p^A)/(u_p^A + u_p^B - u_p^A u_p^B), \\ d_p^{A,B} = (d_p^A u_p^B + d_p^B u_p^A)/(u_p^A + u_p^B - u_p^A u_p^B), \\ u_p^{A,B} = (u_p^A u_p^B)/(u_p^A + u_p^B - u_p^A u_p^B). \end{cases}$$

□

# Trust management methodologies

- Game theoretic approaches:
  - A game consists of a set of players, a set of actions that are realizations of certain strategies available to the players, and a set of payoffs for each strategy.
  - Let $N$ be the set of players in the game, $A$ the set of action profiles, $A_i$ the set of actions available to player $i$, and $u_i$ player $i$'s utility function.

# Trust management methodologies

- Problems of the existing methodologies.
  1. Agents are not (always) rational.
  2. If they are rational they (may) have problems with the basic notion of probability.
  3. Even if they do not have problems with the basic probability, they will likely not understand sophisticated mathematics.
  4. Is trust $\omega$ really something like ($b$, $d$, $u$)?
  5. In case of trust they may no preferences.
  6. If they have preferences, these may not be transitive.

version 1.3
no. 12

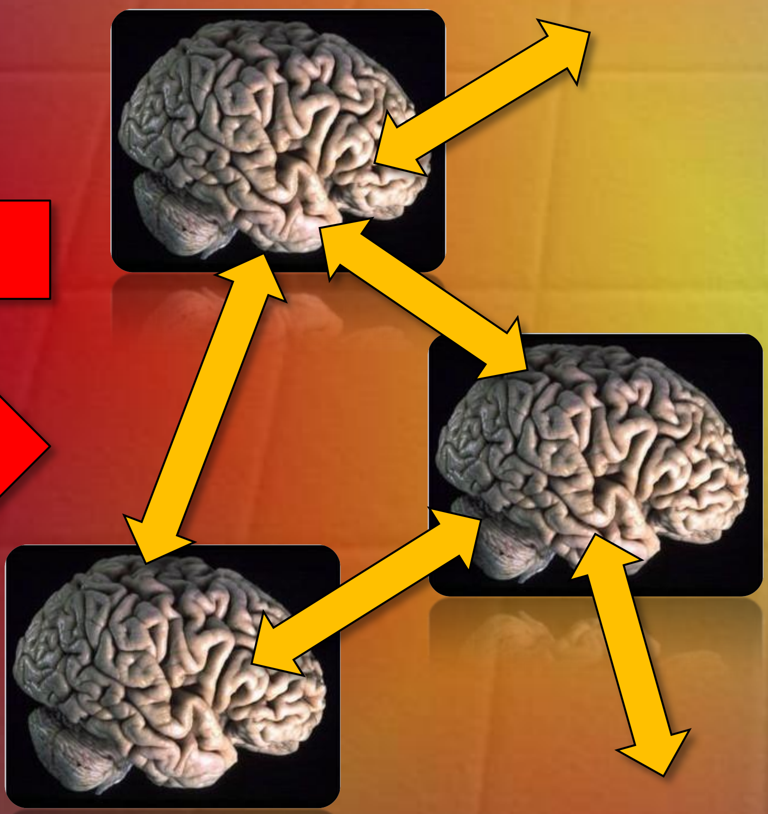
# Qualitative Algebra – Modelling approach

$$A = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & \cdots & \alpha_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n,1} & \alpha_{n,2} & \cdots & \alpha_{n,n} \end{bmatrix}$$

$$\Omega = \{\Uparrow, \Downarrow, \upharpoonleft, \downharpoonright, \rightsquigarrow, \leftrightarrow, \odot, \updownarrow\}$$

$$QAD = \langle \Lambda, \mathbf{A}_\Gamma, \Theta_\Gamma, \Omega \rangle$$

• • •



**math. model** **real world**

# Trust Managmenet and Qualitative Algebra

- Qualitative algebra:
  - At the very beginning this was indeed a group (some 5 years ago).
  - To closer model the reality, it was modified and we ended up with semi-group.
  - Last improvements have actually resulted in a mathematical structure that is not of algebraic nature.
- Qualitative assessment dynamics–QAD.

# Qualitative Assessment Dynamics (QAD)

- The basic tenets of QAD ($H_1$ - $H_{11}$):
  - More than 30% of users would choose direct trust management.
  - More than 30% of users have problems with conforming to the basic definition of probability when it comes to trust.
  - More than 30% of users would choose qualitative assessment of trust.
  - More than 30% of users would choose five levels ordinal scale for trust assessments.
  - To more than 30% of users trust is not a reflexive relation.

# Qualitative Assessment Dynamics (QAD)

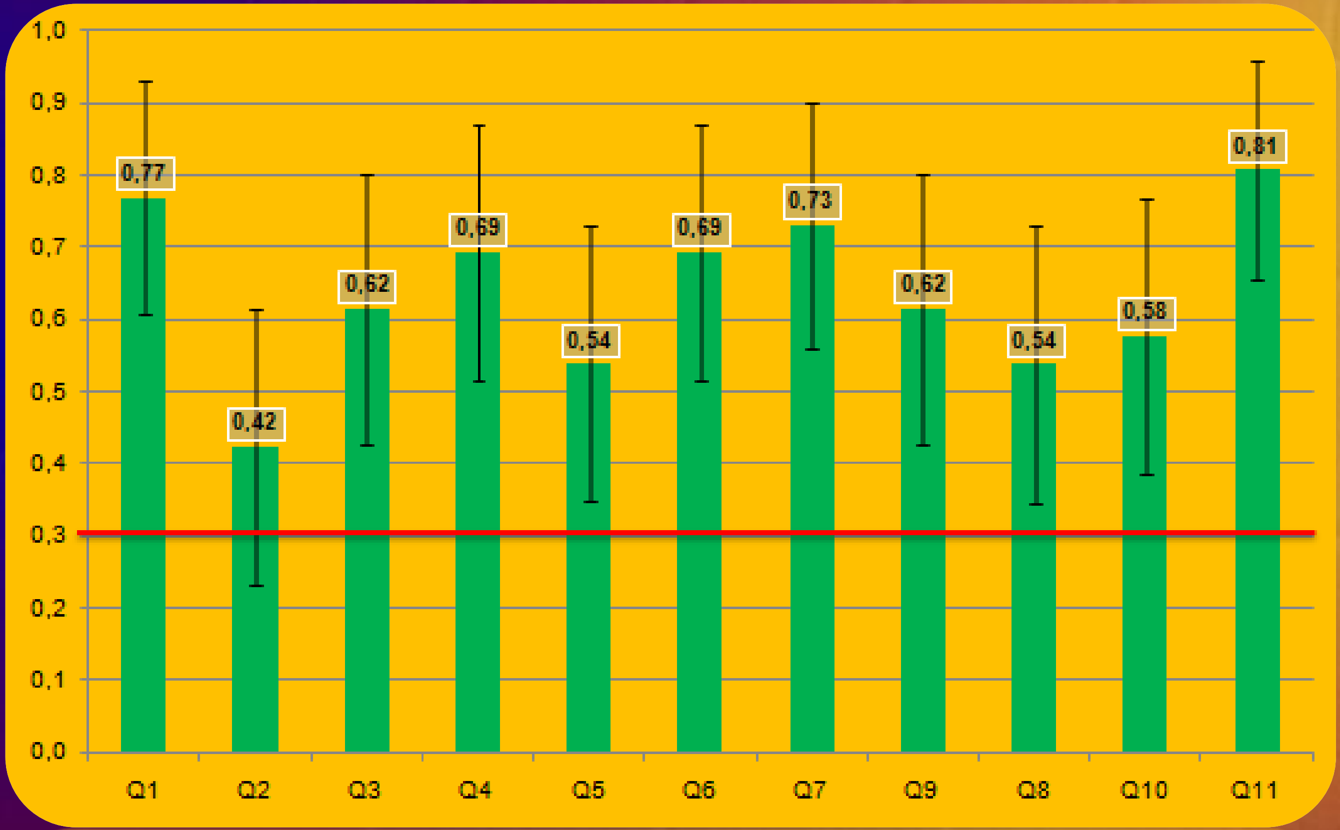
- The basic tenets of QAD ($H_1$ - $H_{11}$):
  - To more than 30% of users trust is not a symmetric relation.
  - To more than 30% of users trust is not a transitive relation.
  - To more than 30% of users that belong to a certain group their assessment may generally differ from that of the group.
  - To more than 30% of users that assess a certain group as a whole this assessment equals to their assessment about the majority of the members of this group.

# Qualitative Assessment Dynamics (QAD)

- The basic tenets of QAD ($H_1$ - $H_{11}$):
  - More than 30% of users may occasionally change trust assessment on a non-identifiable basis.
  - In more than 30% of users trust may be initialized on a non-identifiable basis.
- The threshold of 30% was selected to identify “the second most important player” in the IT field (if such population requires certain functionality, it should be supported).

version 1.3
no. 17

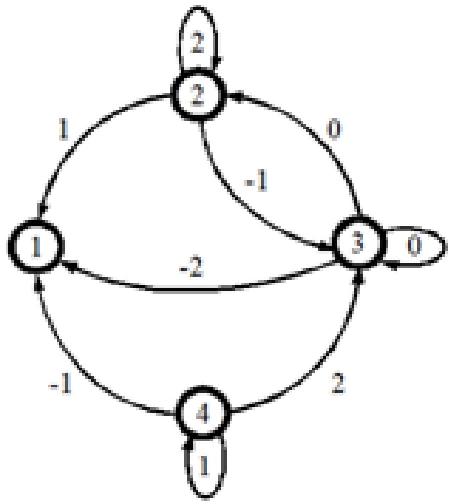
# Qualitative Assessment Dynamics (QAD)




**confidence interval set to 95%, i.e. Z=1.96**

# Qualitative Assessment Dynamics (QAD)

- Formal treatment of trust.




$$\begin{bmatrix} - & - & - & - \\ 1 & 2 & -1 & - \\ -2 & 0 & 0 & 2 \\ -1 & - & 2 & 1 \end{bmatrix}$$

- “Weights” of links: totally distrusted, partially distrusted, undecided, partially trusted and totally trusted.

# Qualitative Assessment Dynamics (QAD)

**a)** $\boldsymbol{\alpha^{-}_{j,i} \neq -}$**:**

- $\Uparrow_j$: $max(\alpha^{-}_{1,i}, \alpha^{-}_{2,i}, \alpha^{-}_{3,i}, \ldots, \alpha^{-}_{j,i}, \ldots, \alpha^{-}_{n,i}) \rightarrow \alpha^{+}_{j,i}$ $\qquad i = 1,2,\ldots,n$
- $\Downarrow_j$: $min(\alpha^{-}_{1,i}, \alpha^{-}_{2,i}, \alpha^{-}_{3,i}, \ldots, \alpha^{-}_{j,i}, \ldots, \alpha^{-}_{n,i}) \rightarrow \alpha^{+}_{j,i}$ $\qquad i = 1,2,\ldots,n$
- $\uparrow_j$: $$\begin{cases} \alpha^{-}_{j,i} \rightarrow \alpha^{+}_{j,i} & if\ \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} \leq \alpha^{-}_{j,i} \\ \lfloor \alpha^{-}_{j,i} + 1 \rfloor \rightarrow \alpha^{+}_{j,i} & otherwise \end{cases}$$
- $\downarrow_j$: $$\begin{cases} \alpha^{-}_{j,i} \rightarrow \alpha^{+}_{j,i} & if\ \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} \geq \alpha^{-}_{j,i} \\ \lceil \alpha^{-}_{j,i} - 1 \rceil \rightarrow \alpha^{+}_{j,i} & otherwise \end{cases}$$
- $\rightsquigarrow_j$: $$\begin{cases} \left\lceil \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} \right\rceil \rightarrow \alpha^{+}_{j,i} & if\ \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} < 0 \\ \left\lfloor \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} \right\rfloor \rightarrow \alpha^{+}_{j,i} & otherwise \end{cases}$$
- $\leftrightarrow_j$: $$\begin{cases} \left\lceil \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} \right\rceil \rightarrow \alpha^{+}_{j,i} & if\ \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} > 0 \\ \left\lfloor \frac{1}{n_1}\sum_{i=1}^{n_1} \alpha^{-}_{i,k} \right\rfloor \rightarrow \alpha^{+}_{j,i} & otherwise \end{cases}$$
- $\odot_j$: $\alpha^{-}_{j,i} \rightarrow \alpha^{+}_{j,i}$ $\qquad i = 1,2,\ldots,n$
- $\updownarrow_j$: $random(-2,-1,0,1,2) \rightarrow \alpha^{+}_{j,i}$ $\qquad i = 1,2,\ldots,n$

**b)** $\boldsymbol{\alpha^{-}_{j,i} = -}$**:**

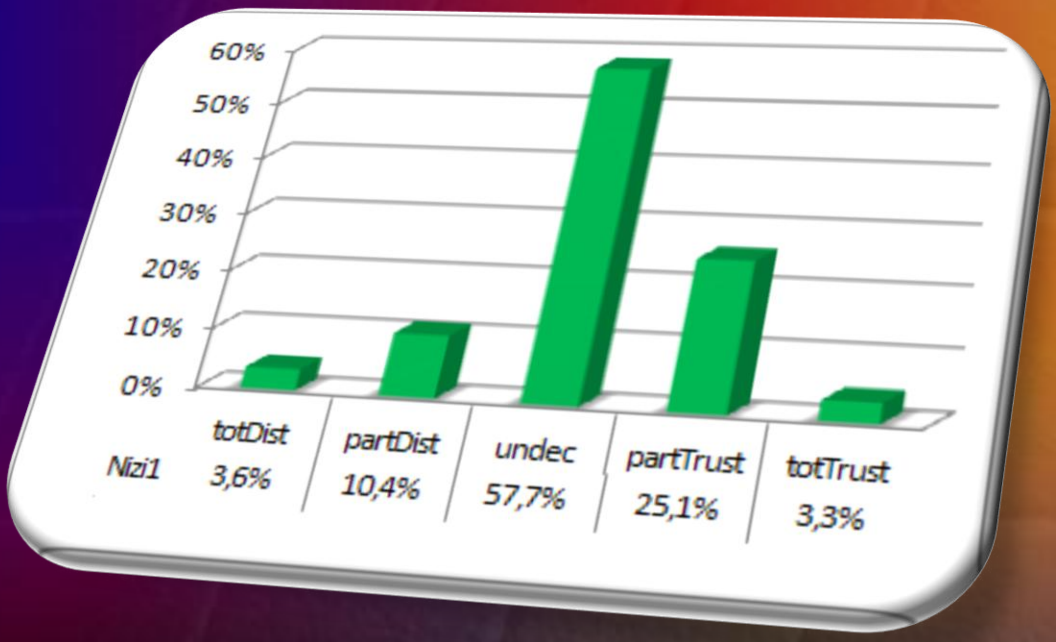
$- \rightarrow \alpha^{+}_{j,i}$ $\qquad i = 1,2,\ldots,n$

# Qualitative Assessment Dynamics (QAD)

- Simulation example.
  - Suppose an example society consists of 10 agents, where all agents are undecided about other agents initially.
  - All agents are initially governed by extreme optimistic operator, except one being assessment hoping (AHO).
  - In each step one agent changes its operator randomly; this agent is randomly chosen as well (all possible values for newly assigned random assessments and operators are equally likely).

# Qualitative Assessment Dynamics (QAD)

- Simulation example.
  - Running 30 simulation runs on this society, each of them taking 100 steps, the following histogram has been obtained.



# Conclusions

- Further development of qualitative algebra (QAD methodology) will cover
  - research of the necessary new operators;
  - experimental verification of existing operators together with new ones.
- Modeling and experimental verification of QAD by including dynamic interactions.
- RM related issues.

version 1.3

no. 23

# References


- D. Trček, Trust Management in the Pervasive Computing Era, IEEE Security & Privacy, June/August, 2011.
- D. Trček, A Formal Apparatus for Modeling Trust in Computing Environments, Mathematical and Computer Modeling, Elsevier, 2008, DOI: 10.1016/j.mcm.2008.05.005.

- More coming soon…