質と量の組を用いたトラストの多値拡張

真野 健[1]　櫻田 英樹[1]　塚田 恭章[1]

概要：CSS2015 において我々は，質と量の組を用いたトラストとその合成演算を定式化し，基本性質を証明した．また，トラスト計算プロトコルを提案し，その基本性質を用いてその正しさを示した．本稿では，同様な議論が適用可能な定式化のバリエーションのひとつとして，質の多値化を考える．多値論理を援用することで，2 値の場合の同様に多値化されたトラスト計算の正しさを証明できる．

キーワード：トラスト，メトリック，多値

Many-Valued Extention of Trust using Pair of Quality and Quantity

Ken Mano[1]　Hideki Sakurada[1]　Yasuyuki Tsukada[1]

Abstract: In CSS2015, we presented a formulation of a trust and its composition operators using a pair of quality and quantity, and proved their basic properties. We also proposed a trust computation protocol, and proved its correctness using the properties. In this paper we present a variation of the formulation where the quality is many-valued. By employing many-valued logic, we can establish the correctness of many-valued trust computation in the same way as in the two-value case.

Keywords: trust, metric, many-value

1. はじめに

CSS2015 において我々は，質と量の組を用いたトラストとその合成演算を定式化し，基本性質を証明した [3]．また，トラスト計算プロトコルを提案し，その基本性質を用いてその正しさ (健全性，安定性) を証明した．本稿では，同様な議論が適用可能な定式化のバリエーションのひとつとして，質の多値化を考える．

質の多値化にはさまざまなアプローチが考えられるが，ここでは多値論理を援用する．まず，多値論理の真理値表からトラストの直列合成を定義する方法を例示する．次に (質が 2 値の場合において) プロトコルの正しさの証明に必要な性質を明示し，多値化された質がそれを満たすことを示す．それによって，多値化された質を用いたプロトコルの正しさの証明を得られる．

本稿の構成は以下の通りである．2 節では，本稿の問題設定と基本的な結果について説明する．3 節では，その多値拡張について述べる．4 では，2 節で述べられた主張の証明を示すが，これらは 3 節で提示される解釈のもと演算や関係を再解釈することで，多値版の証明にもなっている．

2. 質と量の組を用いたトラストの定式化

本節では，本稿の問題設定と基本的な結果を，[3] にもとづいて説明する．

トラスト値を質と量の組として定義する．任意の人 A, B について，A の B に対するトラストを $t_{AB} = (p_{AB}, q_{AB})$ と定義する．p_{AB} をトラスト t_{AB} の質と呼び，$p_{AB} \in [0, 1]$ と仮定する．q_{AB} は非負実数であり，トラスト t_{AB} の量と呼ぶ．

2 つのトラスト $t_{AC} = (p_{AC}, q_{AC})$ と $t_{BC} = (p_{BC}, q_{BC})$ の並列合成は以下のように定義される[*1]：

[1] 日本電信電話株式会社 NTT コミュニケーション科学基礎研究所.
NTT Communication Science Laboratories, NTT Corporation.

[*1] [3] ではトラストの和と順序に $+$, $\leq$ を用いていたが，本稿では混乱を避けるため $\uplus$, $\preceq$ を用いる．

$$t_{AC} \uplus t_{BC} = \left(\frac{q_{AC} \cdot p_{AC} + q_{BC} \cdot p_{BC}}{q_{AC} + q_{BC}}, q_{AC} + q_{BC} \right).$$

つまり，量は単なる足し算，質は量で重み付けした平均である．ただし，$(0,0) \uplus (0,0) = (0,0)$ と定める．並列合成は，得られた 2 つのトラスト情報の併合を表す．$\uplus$ は結合的かつ可換的であり，$0 \uplus t = t$ を満たす．

2 つのトラスト $t_{BC} = (p_{BC}, q_{BC})$ と $t_{AB} = (p_{AB}, q_{AB})$ の直列合成は以下のように定義される:

$$t_{AB} * t_{BC} = (p_{AB} \cdot p_{BC},\ min(q_{AB}, q_{BC})).$$

直列合成は，トラスト情報の伝聞による劣化を表す．$*$ は結合的かつ可換的であり，$0 * t = 0$ を満たす．

基礎トラスト付値 T は，相異なる人の対からトラストへの関数である．$T(A,B)$ は T における A から B への基礎トラストを表し，t^T_{AB} とも書く．T が文脈から明らかな場合は，これまで通り単に t_{AB} と書く．B の総基礎トラスト t_B を以下のように B に対する基礎トラストの総和として定義する:

$$t_B = \sum_{P \in \mathcal{P} - \{B\}} t_{PB}.$$

トラスト t の質を $p(t)$，量を $q(t)$ と表す．トラスト上情報の多寡を表現する二項関係を定義する．この関係の背後にある直観は，“部分的かつ劣化した方が情報が少ない”ということである．トラスト t が t' より情報が少ないことを表す関係 $t \preceq t'$ を，合成演算を用いて以下のように定義する:

$$t \preceq t' \ \text{ iff } \ \exists t_1, t_2\ t \uplus t_1 = t_2 * t'.$$

補題 2.1 $\preceq$ は以下の性質を満たす．

(1) 反射性: $t \preceq t$.
(2) 推移性: $t \preceq t'$ かつ $t' \preceq t''$ ならば $t \preceq t''$.
(3) 反対称性: $t \preceq t'$ かつ $t' \preceq t$ ならば $t = t'$.
(4) 減少性: $t * t' \preceq t'$.
(5) 単調性: $t \preceq t'$ ならば $t'' \uplus t \preceq t'' \uplus t'$.
(6) 準分配性: $t * (t' \uplus t'') \preceq t * t' \uplus t * t''$.
(7) 追越性: $t \preceq_{\Delta t} t'$ ならば，$t'' \uplus t \preceq_{\Delta t} t'' \uplus t'$ かつ $t'' * t \preceq_{\Delta t} t'' * t'$.

ただし Δt はトラストであり，

$$t \preceq_{\Delta t} t' \ \text{ iff } \ t' \preceq t \uplus \Delta t \ \wedge \ q(t) \preceq q(t')$$

である． ∎

トラスト計算手順 f とは，基礎トラスト付値 T と相異なる人 A，B を与えられて，停止したら計算されたトラストを出力する手順である．$f(T,A,B)$ は入力 T，A，B に対する可能な出力の全体集合を表す．

定義 2.2 B に対する計算されたトラスト t は，$t \preceq t_B$ のとき健全であるという． ∎

基礎トラスト付値 T における t_{EF} への付値を Δt だけ増やしたものを $T \uplus_{EF} \Delta t$ と書く．トラスト集合上の前順序 $\sqsubseteq$ を以下のように定義する:

$$\mathcal{T} \sqsubseteq \mathcal{T}' \ \text{ iff } \ \forall t \in \mathcal{T}\ \exists t' \in \mathcal{T}'\ t \preceq t'.$$

さらに，トラスト集合 $\mathcal{T}$ とトラスト t に対して，演算 $\mathcal{T} \uplus t$ を以下のように定義する:

$$\mathcal{T} \uplus t = \{t' \uplus t \mid t' \in \mathcal{T} \cup \{0\}\}.$$

定義 2.3 トラスト計算手順 f は，任意の相異なる人 A，B について以下の 2 つの条件を満足するとき，安定であるという．

(1) T における B の総基礎トラストが 0 ならば，$f(T,A,B) \sqsubseteq \{0\}$.
(2) 任意の相異なる人 E, F とトラスト Δt について，$f(T \uplus_{EF} \Delta t, A, B) \sqsubseteq f(T,A,B) \uplus \Delta t$. ∎

人を頂点とする有向グラフ (各辺は，トラストする側からされる側へ向かう) を考え，その上でトラストの計算手順を考える．重複勘定のない手順を表現するために，線形項を定義する．相異なる人の対 A，B に対して，基礎トラスト記号と呼ばれる定数記号 $\tilde{t}_{AB}$ を導入し，それと $\uplus$ および $*$ から構成される項を考える．

定義 2.4 A, B, C を相異なる任意の頂点として，A-B 線形項と，それらが表すグラフ (有向辺の集合) を以下のように定義する:

(1) $\tilde{t}_{AB}$ は A-B 線形項 であり， A-B 辺の単一要素集合を表す．
(2) A-B 線形項 $S_1, \cdots, S_n$ $(n \geq 1)$ が，それらの表すグラフが互いに有向辺を共有しないならば $S_1 \uplus \cdots \uplus S_n$ は A-B 線形項 であり，$S_1 \cup \cdots \cup S_n$ を表す．
(3) S が B-C 線形項 であり，S の表すグラフに A が現れないとき，$\tilde{t}_{AB} * S$ は A-C 線形項であり，S が表すグラフに A-B 辺を加えたものを表す． ∎

補題 2.5 任意の A-B 線形項 S と基礎トラスト付値 T について，$[S]^T \preceq t_B$. ∎

これら合成演算と線形項を用い，トラストがネットワーク上に分散的に配置された状況において，それらを集計する以下のようなプロトコル (基本プロトコルと呼ぶ) を考える．やり取りされるメッセージは以下のとおりである．

要求 トラストを計算したい対象 C と，要求が辿ってきた人の列 P の組 $\langle C, P \rangle$.
応答 計算されたトラスト s と，それを計算するのに用いた線形項 S の組 $\langle s, S \rangle$.

A が C を直接知らない場合は，$t_{AC} = 0$ とする．A が D から $\langle C, P \rangle$ という要求を受け取ったら，以下のことを順に行う:

(1) $t_{AC} \neq 0$ ならば，応答 $\langle t_{AC}, \tilde{t}_{AC} \rangle$ を 自分自身に送る．
(2) 以下の 3 条件を満たす $B_1, \cdots, B_n$ を非決定的に選ん

で，要求 $\langle C, P \cdot A\rangle$ を送る:

- B_i は自分自身でも C でもない.
- t_{AB_i} が 0 でない.
- B_i が P に含まれない.

(3) 応答を待てるだけ待つ.

(4) 得られた応答の中から，その第 2 要素である線形項が互いに同じ基礎トラスト記号を含まないよう $\langle s_{B'_1C}, S_{B'_1C}\rangle, \cdots, \langle s_{B'_kC}, S_{B'_kC}\rangle$ を非決定的に選び (ひとつも選ばなかったら，すぐに終了)，組 $\langle t_{AB'_1} * s_{B'_1C} \uplus \cdots \uplus t_{AB'_k} * s_{B'_kC}, \tilde{t}_{AB'_1} * S_{B'_1C} \uplus \cdots \uplus \tilde{t}_{AB'_k} * S_{B'_kC}\rangle$ を D に返して終了．ただし $B'_i = A$ の場合，$t_{AB'_i} * s_{B'_iC}$ は $s_{B'_iC}$ を，$\tilde{t}_{AB'_i} * S_{B'_iC}$ は $S_{B'_iC}$ を表すものとする．

自分が C に対するトラスト計算セッションを開始したいなら，自分自身に要求 $\langle C, \lambda\rangle$ を送る (λ は空列).

補題 2.6 基本プロトコルの参加者が線形項の構成において嘘をつかないとする．任意の参加者 A が要求 $\langle C, P\rangle$ に対して応答 $\langle s, S\rangle$ を返すとき，S は A-C 線形項である．∎

基本プロトコルを用いて，トラスト計算手順を以下のように定める．入力 T, A, B を与えられたら，

(1) T に従って各人の保持する基礎トラストを定める[*2].

(2) A が B に対するトラスト計算セッションを開始する.

(3) A が応答を受け取ったら，その第一要素を出力する.

各伝達者の嘘をトラスト上の関数として表せると仮定する．参加者 B がトラストを A に伝えるときにつく嘘を表す関数を B の A に対する嘘関数と呼び L_{AB} で表す．B が計算されたトラスト s を A に送る時，実際に A に送られるのは $L_{AB}(s)$ である．そのとき，L_{AB} には以下の不等式が成り立つと仮定する:

$$t_{AB} * L_{AB}(s) \preceq s.$$

すなわち，B の A に対する任意の嘘は，“$t_{AB} * \_$” の適用によってキャンセルできるということであり，これを嘘の上限仮定と呼ぶ.

定理 2.7 基本プロトコルを用いて定められるトラスト計算手順を f とする.

(1) f の実行中，プロトコルの参加者が応答の第一要素を決定するときにおいてのみ，上限仮定の範囲内で嘘をつくとする．そのとき，f によって計算されたトラストは健全.

(2) プロトコルの参加者が嘘をつかないならば，f は安定.

3. 質の多値化

前節の定式化では，質を信頼するか否かの 2 値の割合で表現している．これを，3 値に拡張することはできるだろうか．例えば，信頼する/信頼しない/分からないの 3 値を考え，それぞれの割合でトラストの質を表現することを考える．トラストの合成を定義するためには，いくつかの“問い” に答える必要がある．例えば，A が B から C に対するトラストの情報を受け取ったとしよう.

問 1. B が C を信頼しないと言い，A は B を信頼しないとする．そのとき，A は C を信頼する／信頼しない／分からない？

問 2. B が C を信頼しないと言い，A は B を信頼できるか分からないとする．そのときは？

問 3. B が C を信頼できるか分からないと言い，A は B を信頼しないとする．そのときは？

問 4. B が C を信頼しないと言い，A は B を信頼するとする．そのときは？

問 5. B が C を信頼すると言い，A は B を信頼しないとする．そのときは？

ここでは，問 1 に対して A は C を “信頼しない”，問 2 に対して “分からない” と答えるとする．すると $*$ の可換性から，問 3 の答えは “分からない” でなければならない．また，問 4 の答えは “信頼しない” が最も妥当だと考えられるが，そのとき同じく可換性から，問 5 の答えは “信頼しない” でなくてはならない．これらの答えを表にまとめると表 1 のようになる:

そのとき 3 値の質を持つトラストを，例えば $((p_T, p_F), q)$ という質と量の組として以下のように定義できる．ただし，p_T は信頼する割合，p_F は信頼しない割合を表し，$p_T, p_F, p_T + p_F \in [0,1]$ と仮定する．並列合成は，2 値の場合と同様重み付き平均とする:

$$((p_T, p_F), q) \uplus ((p'_T, p'_F), q') = \left(\left(\frac{p_T \cdot q + p'_T \cdot q'}{q + q'}, \frac{p_F \cdot q + p'_F \cdot q'}{q + q'}\right), q + q'\right).$$

ただし量が 0 のとき質は $(0,0)$ とし，$((0,0),0)$ を 0 と書く．さらに，$0 \uplus 0 = 0$ と定める．直列合成は，表 1 にもとづき以下のように定義する:

$$((p_T, p_F), q) * ((p'_T, p'_F), q') = ((p_T \cdot p'_T,\ p_T \cdot p'_F + p_F \cdot p'_T + p_F \cdot p'_F), min(q, q')).$$

以下では，前節で示した健全性と安定性がこのような多値化においても成り立つことを示す．そのためには，演算や関係の基本性質が多値化によって保存されていることを示せばよい.

非負実数の対を非負ベクトルと呼ぶ．非負ベクトル上の演算と関係を以下のように定義する．任意の非負ベクトル (r_T, r_F)，(r_T, r_F) と非負実数 q について，

$$q \cdot (r_T, r_F) = (r_T, r_F) \cdot q = (q \cdot r_T, q \cdot r_F),$$
$$(r_T, r_F)/q = (r_T/q, r_F/q),$$

[*2] T から各人の基礎トラストを定めるというのは現実的ではないが，定式化の都合でこのような説明になっている．実際には各人の基礎トラストが所与であり，形式的な入力 T がそれらによって決定されると考える.

	B は C を信頼する	信頼しない	分からない
A は B を信頼する	信頼する	信頼しない	分からない
信頼しない	信頼しない	信頼しない	分からない
分からない	分からない	分からない	分からない

表 1 多値化されたトラストの直列合成

$(r_T, r_F) + (r'_T, r'_F) = (r_T + r'_T, r_F + r'_F)$,
$(r_T, r_F) \cdot (r'_T, r'_F) = (r_T \cdot r'_T, r_F \cdot r'_T + r_T \cdot r'_F + r_F \cdot r_F)$
$(r_T, r_F) \in [0,1]$ iff $r_T, r_F, r_T + r_F \in [0,1]$.

$p \in [0,1]$ なる非負ベクトル p を，多値化された質と呼ぶ．多値化された質 $(0,0)$ を 0，$(1,0)$ を 1 と書く．非負ベクトル上の関係 $\leq$ を以下のように定義する:

$$r \leq r' \text{ iff 非負ベクトル } r_1 \text{ と 多値化された質 } p_2 \text{ が存在して } r + r_1 = p_2 \cdot r'.$$

さらに，非負ベクトル上の関係 $\ll$ を以下のように定義する:

$$(r_T, r_F) \ll (r'_T, r'_F) \text{ iff } r_T \leq r'_T \wedge r_F \leq r'_F.$$

補題 3.1 任意の非負ベクトル $r = (r_T, r_F)$, $r' = (r'_T, r'_F)$, $r'' = (r''_T, r''_F)$ について，以下が成り立つ．
(1) $r \leq r'$ iff 多値化された質 p_2 が存在して $r \ll p_2 \cdot r'$.
(2) $r \ll r'$ ならば $r'' + r \ll r'' + r'$.
(3) $r \ll r'$ ならば $r'' \cdot r \ll r'' \cdot r'$.
(4) 任意の多値化された質 p, p' について，$r \ll p \cdot r'$ かつ $r' \ll p' \cdot r$ ならば $r = r'$.
(5) 任意の多値化された質 p について，$r \ll r' + p \cdot r''$ ならば多値化された質 p' が存在して $r \ll p' \cdot (r' + r'')$

証明 (1) と (2) と (3) は明らか．

(4) $p = (p_T, p_F)$, $p' = (p'_T, p'_F)$ とする．仮定から，$p_T, p_F, p_T + p_F, p'_T, p'_F, p'_T + p'_F \in [0,1]$ である．2 つに場合分けする．

まず $r_T > 0$ の場合．$r_T \leq p_T \cdot r'_T$ かつ $r'_T \leq p'_T \cdot r_T$ より，$r_T \leq r'_T$ かつ $r'_T \leq r_T$．よって $r_T = r'_T$，したがって $p_T = p'_T = 1$．よって $p_F = p'_F = 0$ なので，$r_F = r'_F$.

次に $r_T = 0$ の場合．$r_T = 0 \leq p_T \cdot r'_T$ かつ $r'_T \leq p'_T \cdot r_T = 0$ から，$r'_T = 0$．さらに，$r_F \leq (p_T + p_F) \cdot r'_F$ かつ $r'_F \leq (p'_T + p'_F) \cdot r_F$ より，$r_F \leq r'_F$ かつ $r'_F \leq r_F$，よって $r_F = r'_F$.

(5) $p = (p_T, p_F)$ とする．一般性を損なうことなく，$p_T + p_F = 1$ と仮定できる ($p_T + p_F < 1$ ならば，$1 - p_T$ を新たに p_F と置いても仮定は成り立つから)．すると仮定から，

$$r_T \leq r'_T + p_T \cdot r''_T,$$

$$\begin{aligned} r_F &\leq r'_F + p_T \cdot r''_F + (1 - p_T) \cdot r''_T + (1 - p_T) \cdot r''_F \\ &= r'_F + p_T \cdot r''_F + r''_T - p_T \cdot r''_T + r''_F - p_T \cdot r''_F \\ &= r'_F + r''_T + r''_F - p_T \cdot r''_T. \end{aligned}$$

このとき，

$$r'_T + p_T \cdot r''_T = p'_T \cdot (r'_T + r''_T)$$

$$\begin{aligned} r'_F + r''_T + r''_F - p_T \cdot r''_T = (r'_T + r''_T) + (r'_F + r''_F) \\ - p'_T \cdot (r'_T + r''_T) \end{aligned}$$

を満たす $p'_T \in [0,1]$ が存在するなら，$p' = (p'_T, 1 - p'_T)$ と置けば良い．実際上の 2 式は同値であり，p'_T について解くと，

$$p'_T = \frac{r'_T + p_T \cdot r''_T}{r'_T + r''_T}$$

となる．$p'_T \in [0,1]$ より $p'_T \in [0,1]$ である．よって結論は成り立つ． ∎

補題 3.2 任意の非負ベクトル r, r', r'' について，以下の性質が成り立つ．
(1) $0 \cdot r = r \cdot 0 = 0$ (0 は多値化された質).
(2) $1 \cdot r = r$ (1 は多値化された質).
(3) $r \cdot (r' \cdot r'') = r' \cdot (r \cdot r'')$.
(4) $r \cdot (r' + r'') = r \cdot r' + r \cdot r''$.
(5) $r \leq r$.
(6) $r \leq r'$ かつ $r' \leq r''$ ならば，$r \leq r''$.
(7) $r \leq r'$ かつ $r' \leq r$ ならば，$r = r'$.
(8) 任意の多値化された質 p について $p \cdot r \leq r$.
(9) 任意の実数 $q \in [0,1]$ について $q \cdot r \leq r$.
(10) $r \leq r'$ ならば，$r'' + r \leq r'' + r'$.

証明 (1) と (2) は明らか．(3) と (4) は，定義にしたがって式を展開すれば確かめられる．(5) は $\leq$ の定義において $r_1 = 0$，$p_2 = 1$ と置けばよい．(6) は補題 3.1 の (1) と (3) から導かれる．(7) も同補題の (1) と (4) から導かれる．(8) は $r_1 = 0$，$p_2 = p$ とおけばよい．(9) も $r_1 = 0$，$p_2 = (q, 0)$ とおけばよい．

(10) については，補題 3.1 の (1) から多値化された質 p_2 が存在して，$r \ll p_2 \cdot r'$．よって同補題の (2) から，$r'' + r \ll r'' + p_2 \cdot r'$．そのとき同補題 の (5) から，多値化された質 p'_2 が存在して，$r'' + r \ll p'_2 \cdot (r'' + r')$．よってふたたび同補題の (1) から $r'' + r \leq r'' + r'$. ∎

上記性質からさらに，$r \leq r'$ ならば $r'' \cdot r \leq r'' \cdot r'$，$0 \leq r$ などが導かれる．

補題 3.3 上記の多値化されたトラストについて，補題 2.1 に対応する性質が成り立つ．

証明　次節の 2 値版の補題 2.1 の証明に現れる質に関する演算と関係を，上記のものに置き換えて再解釈することで，多値版の対応する証明が得られる．∎

次節では，前節の基本プロトコルの健全性や安定性の証明も示されているが，その証明は演算の具体的定義によらず，補題 2.1 で確立した性質にのみ依存している．したがって，多値化された質のトラストを用いた基本プロトコルの健全性と安定性も成立する．

この問題にはさらにバリエーションが考えられるが，ここではそのいくつかを検討する．まず，問 3 や問 5 で上記以外の選択をする，すなわち $*$ の可換性を認めないという場合である．例えば表 2 のように，信頼しないのは A が B を信頼し，かつ B は C を信頼する場合のみとする合成を考えよう．この表にもとづく直列合成は，

$$((p_T, p_F), q) * ((p'_T, p'_F), q') = ((p_T \cdot p'_T,\ p_T \cdot p'_F), min(q, q'))$$

である．実は健全性や安定性を導くのに $*$ の結合性や可換性は必須ではない．その代わり，補題 2.1 の (4) の減少性とともに以下の (4′) が，そして (6) の準分配性の代わりに以下の (6′) が成り立てば良い．

(4′)　右減少性: $t' * t \preceq t'$.

(6′)　右準分配性: $(t' \uplus t'') * t \preceq t' * t \uplus t'' * t$.

表 3 の直列合成の場合，右減少性，右準分配性を含む必要な基本性質が成り立つので，前節の基本プロトコルの健全性と安定性が導かれる．

もちろん，このような表に基づいて定義される直列合成のすべてが望ましい性質を持つわけでない．そのような例のひとつが，表 3 のように問 1 に “信頼する” と答える，いわば二重否定を肯定と解釈する場合である．この表にもとづくと，直列合成の定義は

$$((p_T, p_F), q) * ((p'_T, p'_F), q') = \\ ((p_T \cdot p'_T + p_F \cdot p'_F,\ p_T \cdot p'_F + p_F \cdot p'_T), min(q, q'))$$

となる．上記のような合成は，[1] などで用いられている．しかしこの場合，単調性が成立しない．例えば多値化された質 $(0.5, 0.5)$ と $(0, 1)$ を考える．上記の定義に則ると，$(0.5, 0.5) + 0 = (0.5, 0.5) \cdot (0, 1)$ なので $(0.5, 0.5) \leq (0, 1)$ であるが，にもかかわらず $(1, 0) + (0.5, 0.5) \leq (1, 0) + (0, 1)$ とはならない．むしろ，$(1, 1) + 0 \leq (0.5, 0.5) \cdot (1.5, 0.5)$ から $(1, 0) + (0, 1) \leq (1, 0) + (0.5, 0.5)$ である．つまり質の和の単調性が成り立たないため，トラストの並列合成の単調性も成り立たない．

最後に，4 値以上を考える場合である．実は本節でひとつめに示した表は，ウカシェヴィッチの 3 値論理 [2] における論理積の真理値表となっている[*3]．ウカシェヴィッチは一般に n 値の多値論理を提示しているが，これは任意の有限全順序集合を意味領域とするようなブール代数の拡張とみなすことができる．よって，例えばショッピングサイトでの評価のように星 1 つ〜星 5 つのそれぞれの重みで表現されたトラストがあったとき，それを 5 値のウカシェヴィッチ論理に対応づけて積演算を定義することで，健全かつ安定なトラスト計算手順が得られる．

4. 証明

本節では，2 節で述べられた主張の証明を示す．これらは 3 節で提示される解釈のもと演算や関係を再解釈することで，多値版の証明にもなっている．トラスト t に対して，$p(t) \cdot q(t)$ を t の勝ち星と呼び，$w(t)$ と表す．

補題 4.1　$\exists t_1, t_2\ t \uplus t_1 = t_2 * t'$ であるとき，一般性を損なうことなく $q(t_2) = q(t')$ と仮定できる．

証明　$\exists t_1, t_2\, t \uplus t_1 = t_2 * t'$ と仮定する．$t \uplus t'_1 = t'_2 * t'$ であって，かつ $q(t'_2) = q(t')$ であるような t'_1，t'_2 が存在することを示す．

$q(t_2) > q(t')$ ならば，$t'_1 = t_1$，$t'_2 = (p(t_2), q(t'))$ と置くと，$t_2 * t' = (p(t_2) \cdot p(t'), q(t')) = t'_2 * t'$ となり条件を満たす．もし $q(t_2) < q(t')$ ならば，$q(t \uplus t_1) = q(t_2)$．そこで，$t'_1 = t_1 \uplus (p(t \uplus t_1), q(t') - q(t_2))$，$t'_2 = (p(t_2), q(t'))$ と置くと，

$$\begin{aligned} & t \uplus t'_1 \\ &= t \uplus t_1 \uplus (p(t \uplus t_1), q(t') - q(t_2)) \\ &= (p(t \uplus t_1), q(t')) \\ &= (p(t_2) \cdot p(t'), min(q(t'), q(t')) = t'_2 * t' \end{aligned}$$

となり条件を満たす．∎

補題 4.2　$t \preceq t'$ iff $q(t) \leq q(t')$ かつ $w(t) \leq w(t')$.

証明　[only-if part] 仮定から，t_1，t_2 が存在して，$t \uplus t_1 = t_2 * t'$.[*4]補題 4.1 より，一般性を損なうこと無く $q(t_2) = q(t')$ と仮定できる．そのとき，量と質それぞれに以下が成り立つ:

$$q(t) + q(t_1) = q(t'),$$

$$(q(t) \cdot p(t) + q(t_1) \cdot p(t_1))/q(t') = p(t2) \cdot p(t').$$

量についての条件は，上式から明らかに成り立つ．質についても，

$$\begin{aligned} & q(t) \cdot p(t) \\ &\leq q(t) \cdot p(t) + q(t_1) \cdot p(t_1) \\ &= q(t') \cdot p(t2) \cdot p(t') \\ &\leq q(t') \cdot p(t') \end{aligned}$$

[*3] “信頼する”，“信頼しない”，“分からない” を，それぞれウカシェヴィッチの 3 値論理の *true*，*possible*，*false* に対応させる．なお，問 2 の答えを “信頼しない” とした場合は，“信頼する”，“信頼しない”，“分からない” をそれぞれ *true*，*false*，*possible* に対応させる．

[*4] 質が 2 値の場合は，$t_1 = 0$ と取ることができる．

	B は C を信頼する	信頼しない	分からない
A は B を信頼する	信頼する	信頼しない	分からない
信頼しない	分からない	分からない	分からない
分からない	分からない	分からない	分からない

表 2 非対称な多値化の直列合成

	B は C を信頼する	信頼しない	分からない
A は B を信頼する	信頼する	信頼しない	分からない
信頼しない	信頼しない	信頼する	分からない
分からない	分からない	分からない	分からない

表 3 二重否定を肯定と解釈する多値化の直列合成

なので成り立つ.

[if part] 量についての仮定から, $q(t')-q(t)\geq 0$ なので, $q=q(t')-q(t)$ と置く. また勝ち星についての仮定から, p_1, p_2 が存在して $p_2\in[0,1]$ かつ $q(t)\cdot p(t)+p_1=p_2\cdot q(t')\cdot p(t')$.

そのとき, $q(t)+q=q(t')$ より,

$$q(t)\cdot p(t)+q\cdot(p_1/q)=(q(t)+q)\cdot p_2\cdot p(t').$$

両辺を $q(t)+q$ で割ると,

$$\frac{q(t)\cdot p(t)+q\cdot(p_1/q)}{q(t)+q}=p_2\cdot p(t').$$

よって $t\uplus((p_1/q),q)=(p_2,q(t'))*t'$ なので結論は成り立つ. ∎

補題 2.1 の証明 (1) $t_1=0$, $t_2=(1,q(t))$ と取ると, $t\uplus t_1=t_2*t$.

(2) 補題 4.2 より明らか.

(3) $t\preceq t'$ かつ $t'\preceq t$ と仮定する. 補題 4.2 より $q(t)\leq q(t')$, $q(t)\cdot p(t)\leq q(t')\cdot p(t')$, かつ $q(t')\leq q(t)$, $q(t')\cdot p(t')\leq q(t)\cdot p(t)$. そのとき $q(t)=q(t')$. よって $p(t)\leq p(t')$ かつ $p(t')\leq p(t)$, したがって $p(t)=p(t')$.

(4) $t_1=0$, $t_2=t$ と置くと, $t*t'\uplus t_1=t_2*t'$.

(5) $t\preceq t'$ と仮定する. 補題 4.2 より $q(t)\leq q(t')$ かつ $q(t)\cdot p(t)\leq q(t')\cdot p(t')$. よって, $q(t'')+q(t)\leq q(t'')+q(t')$ かつ $q(t'')\cdot p(t'')+q(t)\cdot p(t)\leq q(t'')\cdot p(t'')+q(t')\cdot p(t')$. よってふたたび補題 4.2 より $t''\uplus t\preceq t''\uplus t'$.

(6) 補題 4.2 より以下の 2 つが証明できればよい:

(a) $q(t*(t'\uplus t''))\leq q(t*t'\uplus t*t'')$, すなわち $min(q(t),q(t')+q(t''))\leq min(q(t),q(t'))+min(q(t),q(t''))$.

(b) $w(t*(t'\uplus t''))\leq w(t*t'\uplus t*t'')$, すなわち $min(q(t),q(t')+q(t''))\cdot p(t)\cdot(q(t')\cdot p(t')+q(t'')\cdot p(t''))/(q(t')+q(t''))\leq min(q(t),q(t'))\cdot p(t)\cdot p(t')+min(q(t),q(t''))\cdot p(t)\cdot p(t'')$.

一般性を失うことなく, $q(t')\leq q(t'')$ と仮定できる. 以下の 4 つに場合分けする.

[$q(t)\leq q(t')$ の場合]

(a) $q(t)\leq q(t)+q(t)$ より成り立つ.

(b) $q(t)\cdot p(t)\cdot(q(t')\cdot p(t')+q(t'')\cdot p(t''))/(q(t')+q(t''))$
$=(q(t)\cdot p(t)\cdot q(t')\cdot p(t')+q(t)\cdot p(t)\cdot q(t'')\cdot p(t''))/(q(t')+q(t''))$
$=q(t)\cdot p(t)\cdot p(t')\cdot(q(t')/(q(t')+q(t'')))+q(t)\cdot p(t)\cdot p(t'')\cdot(q(t'')/(q(t')+q(t'')))$
$\leq q(t)\cdot p(t)\cdot p(t')+q(t)\cdot p(t)\cdot p(t'')$.
よって成り立つ.

[$q(t')<q(t)\leq q(t'')$ の場合]

(a) $q(t)\leq q(t')+q(t)$ より成り立つ.

(b) $q(t)\cdot p(t)\cdot(q(t')\cdot p(t')+q(t'')\cdot p(t''))/(q(t')+q(t''))$
$=q(t')\cdot p(t)\cdot p(t')\cdot(q(t)/(q(t')+q(t'')))+q(t)\cdot p(t)\cdot p(t'')\cdot(q(t'')/(q(t')+q(t'')))$
$\leq q(t')\cdot p(t)\cdot p(t')+q(t)\cdot p(t)\cdot p(t'')$.
よって成り立つ.

[$q(t'')<q(t)\leq q(t')+q(t'')$ の場合]

(a) $q(t)\leq q(t')+q(t'')$ より成り立つ.

(b) $q(t)\cdot p(t)\cdot(q(t')\cdot p(t')+q(t'')\cdot p(t''))/(q(t')+q(t''))$
$=q(t')\cdot p(t)\cdot p(t')\cdot(q(t)/(q(t')+q(t'')))+q(t'')\cdot p(t)\cdot p(t'')\cdot(q(t)/(q(t')+q(t'')))$
$\leq q(t')\cdot p(t)\cdot p(t')+q(t'')\cdot p(t)\cdot p(t'')$.
よって成り立つ.

[$q(t')+q(t'')<q(t)$ の場合]

(a) $q(t')+q(t'')\leq q(t')+q(t'')$ より成り立つ.

(b) $(q(t')+q(t''))\cdot p(t)\cdot(q(t')\cdot p(t')+q(t'')\cdot p(t''))/(q(t')+q(t''))$
$=q(t')\cdot p(t)\cdot p(t')+q(t'')\cdot p(t)\cdot p(t'')$.
よって成り立つ.

(7) $t\preceq_{\Delta t}t'$ と仮定する. 補題 4.2 より, $q(t)\leq q(t')\leq q(t)+q(\Delta t)$ かつ $w(t')\leq w(t\uplus\Delta t)$ である.

まず, $t''\uplus t\preceq_{\Delta t}t''\uplus t'$ を示す. 補題 4.2 より, $q(t''\uplus t)\leq q(t''\uplus t')\leq q(t''\uplus t\uplus\Delta t)$ および $w(t''\uplus t)\leq w(t''\uplus t')$ を示せばいい.

前者は仮定から明らか. 後者は, $p(t')\cdot q(t')\leq p(t)\cdot q(t)+p(\Delta t)\cdot q(\Delta t)$ ならば, $p(t'')\cdot q(t'')+p(t')\cdot q(t')\leq p(t'')\cdot q(t'')+p(t)\cdot q(t)+p(\Delta t)\cdot q(\Delta t)$ なので成り立つ.

次に, $t''*t\preceq_{\Delta t}t''*t'$ を示す. やはり補題 4.2 の量と勝ち星による特徴づけを用いる. t'' として, 以下の 2 つの場

合を考えれば十分である．

(a) $q(t'') \geq max(q(t), q(t'))$.

(b) $p(t'') = 1$.

実際, 任意の t'' は $(1, q(t'')) * (p(t''), max(q(t), q(t'), q(t'')))$ と表すことができる．

(a) の場合，不等式の両辺に量の変化はないので，量についてはあきらか．勝ち星については，$p(t'') \cdot p(t') \cdot q(t') \leq p(t'') \cdot p(t) \cdot q(t) + p(t'') \cdot p(\Delta t) \cdot q(\Delta t) \leq p(t'') \cdot p(t) \cdot q(t) + p(\Delta t) \cdot q(\Delta t)$ より成り立つ．

(b) の場合，両辺の質に変化はない．量に関して，3 つに場合分けをする．

$[q(t') \leq q(t'')$ の場合]

$q(t'' * t) = q(t)$，$q(t'' * t') = q(t')$ である．よって量についての条件は $q(t') \leq q(t) + q(\Delta t)$ より成り立つ．勝ち星についても $p(t') \cdot q(t') \leq p(t) \cdot q(t) + p(\Delta t) \cdot q(\Delta t)$ より成り立つ．

$[q(t) \leq q(t'') \leq q(t')$ の場合]

$q(t'' * t) = q(t)$，$q(t'' * t') = q(t'')$ である．$q(t) \leq q(t'') \leq q(t') \leq q(t) + q(\Delta t)$ より, 量についての条件は成り立つ．勝ち星も $p(t') \cdot q(t'') \leq p(t') \cdot q(t') \leq p(t) \cdot q(t) + p(\Delta t) \cdot q(\Delta t)$ より成り立つ．

$[q(t'') \leq q(t)$ の場合]

$q(t'' * t) = q(t''), q(t'' * t') = q(t'')$ である．$q(t'') \leq q(t'') \leq q(t'') + q(\Delta t)$ より量についての条件は成り立つ．勝ち星については，$q(t'') \leq q(t) \leq q(t')$ なので，$q(t'')/q(t') < q(t'')/q(t) \leq 1$ である．そのとき，

$$\begin{aligned} & p(t') \cdot q(t'') \\ &= (q(t'')/q(t')) \cdot p(t') \cdot q(t') \\ &\leq (q(t'')/q(t')) \cdot (p(t) \cdot q(t) + p(\Delta t) \cdot q(\Delta t)) \\ &\leq (q(t'')/q(t)) \cdot (p(t) \cdot q(t) + p(\Delta t) \cdot q(\Delta t)) \\ &= p(t) \cdot q(t'') + (q(t'')/q(t)) \cdot (p(\Delta t) \cdot q(\Delta t)) \\ &\leq p(t) \cdot q(t'') + p(\Delta t) \cdot q(\Delta t) \end{aligned}$$

よって成り立つ．∎

補題 2.5 の証明　(概略) S の中の $\tilde{t}_{PP'} * s_{P'B}$ という形の任意の部分項で最外のものをひとつ選んで $s_{P'B}$ で置き換えたものを S' とすると，単調性と減少性から $[S]^T \preceq [S']^T$ である．これを繰り返してすべての $*$ を除去すると，$\bar{S} = \tilde{t}_{P_1 B} \uplus \cdots \uplus \tilde{t}_{P_n B}$ という形の和が残るが，線形性と単調性から $[\bar{S}]^T \preceq t_B$．よって，$[S]^T \preceq t_B$．∎

補題 2.6 の証明　(概略) S の構成に関する帰納法による．帰納段階において，プロトコル の (4) で “線形項が互いに同じ基礎トラスト記号を含まないように” B'_i を選ぶことから，線形項の定義の (2) にある条件 “それらの表すグラフが互いに有向辺を共有しない” が満足される．また，プロトコルの (2) で “P に含まれない” 相手を選んで要求を送ることから，線形項の定義の (3) にある条件 “S の表すグラフに A が現れない” が満足される．∎

定理 2.7 の証明　1. (概略) 出力 s を決定した際に A が受け取った応答を $\langle s, S \rangle$ とする．仮定より，参加者は S の構成において嘘はつかない．プロトコルの任意の参加者 C, D に対して関数記号 $\tilde{L}_{CD}$ を導入し，その解釈を D の C に対する嘘関数とする．S 中の $*$ の適用は “$\tilde{t}_{CD} * \_$” $(C \neq D)$ の形をしているが，それらをすべて “$\tilde{t}_{CD} * \tilde{L}_{CD}(\_)$” に置き換えたものを S^L とすると，$s = [S^L]^T$ である．そのとき，減少性の代わりに嘘の上限仮定を使うことで，補題 2.5 の証明と同様の議論によって S^L から $*$ と $\tilde{L}_{CD}$ を除去できる．よって s は健全である．

2. 任意の人 A, B について，t_{AB} は $[\tilde{t}_{AB}]^T$ を表し，t^+_{AB} は $[\tilde{t}_{AB}]^{T \uplus_{EF} \Delta t}$ を表すとする．

本証明は，以下の 3 つの状況を考えて，それらの間である性質を満たす模擬が存在することを示すことによって行う．

(a) 付値は $T \uplus_{EF} \Delta t$.

(b) 付値は T，ただし基礎トラストが 0 である相手にもリクエストを送れるようにプロトコルを変更.

(c) 付値は T.

まず (a) の (b) による模擬について述べる．(b) では，プロトコル記述の (1) における “$t_{AC} \neq 0$”，(2) における “t_{AB_i} が 0 でない” という条件を除いた改変プロトコルを用いる．そして以下のように (a) を模擬することを考える．

- (a) のリクエストは，(b) の同一のリクエストで模擬
- (a) のレスポンス $\langle s, S \rangle$ は，(b) のレスポンス $\langle [S]^T, S \rangle$ で模擬 ($s = [S]^{T \uplus_{EF} \Delta t}$ であることに注意)

A, C, D を任意の人とする．(a) において，D が A からレスポンス $\langle s^+_{AC}, S_{AC} \rangle$ を受け取ったとし，$\langle s_{AC}, S_{AC} \rangle$ をそれに対応する (b) のレスポンスとする．

この模擬において，以下の (A)，(B) の論理積として定められる主張 $P(\langle s^+_{AC}, S_{AC} \rangle)$ を成り立つことを示す．

(A) $D \neq A$ かつ $\tilde{t}_{DA}$ が S_{AC} に現れないならば，$t_{DA} * s_{AC} \preceq_{\Delta t} t^+_{DA} * s^+_{AC}$.

(B) $D = A$ ならば，$s_{AC} = s^+_{AC}$.

証明は S_{AC} の構成に関する帰納法で行う．すなわち，S_{AC} よりも小さい任意の線形項 S を持つレスポンス $\langle s^+, S \rangle$ について $P(\langle s^+, S \rangle)$ が成立すると仮定して，$P(\langle s^+_{AC}, S_{AC} \rangle)$ を導く．

まず (A) について，3 つに場合分けをする．

(A-1) $\tilde{t}_{EF} = \tilde{t}_{DA}$ の場合.

(A-2) $\tilde{t}_{EF}$ が S_{AC} に現れる場合.

(A-3) それ以外の場合.

(A-3) の場合，$t_{DA} * s_{AC} = t^+_{DA} * s^+_{AC}$ なので主張は自

明である．

(A-1) の場合，$t^+_{DA} = t_{DA} \uplus \Delta t$ である．仮定から $\tilde{t}_{DA} = \tilde{t}_{EF}$ は S_{AC} に現れないので，$s_{AC} = s^+_{AC}$．そのとき，

$$q(t_{DA} * s_{AC}) \preceq q((t_{DA} \uplus \Delta t) * s_{AC}),\ \text{かつ}$$
$$(t_{DA} \uplus \Delta t) * s_{AC} \preceq t_{DA} * s_{AC} \uplus \Delta t$$

を言えばいい．

前者は，

$$\begin{aligned} & q(t_{DA} * s_{AC}) \\ &= min(q(t_{DA}), q(s_{AC})) \\ &\preceq min(q(t_{DA} \uplus q(\Delta t)), q(s_{AC})) \\ &= q((t_{DA} \uplus \Delta t) * s_{AC}) \end{aligned}$$

なので成り立つ．後者は，右準分配性，右減少性，単調性から導かれる．すなわち，

$$\begin{aligned} (t_{DA} \uplus \Delta t) * s_{AC} &\preceq t_{DA} * s_{AC} \uplus \Delta t * s_{AC} \\ &\preceq t_{DA} * s_{AC} \uplus \Delta t. \end{aligned}$$

(A-2) の場合，プロトコルの性質から，S_{AC} は以下の形で表現される:

$$S_{AC} = \tilde{t}_{AB_1} * S_{B_1C} \uplus \cdots \uplus \tilde{t}_{AB_n} * S_{B_nC}.$$

線形性から，$\tilde{t}_{EF}$ は $\tilde{t}_{AB_i} * S_{B_iC}$ $(i = 1, \cdots, n)$ のどれか 1 つに現れるので，それを $\tilde{t}_{AB_j} * S_{B_jC}$ とする．$A \neq B_j$ なら帰納法の仮定の (A) から

$$t_{AB_j} * s_{B_jC} \preceq_{\Delta t} t_{AB_j} * s^+_{B_jC},$$

$A = B_j$ なら $\tilde{t}_{AB_j} * S_{B_jC}$ は S_{B_jC} を表すが，帰納法の仮定の (B) から

$$s_{B_jC} \preceq_{\Delta t} s^+_{B_jC}.$$

いずれの場合も，追越性より，

$$t_{DA} * s_{AC} \preceq_{\Delta t} t_{DA} * s^+_{AC}.$$

つぎに (B) について．t_{EF} が S_{AC} に含まれない場合は自明なので，含まれる場合を考える．2 つに場合分けをする．

(B-1)　$S_{AC} = \tilde{t}_{AC}$ の場合．

(B-2)　そうでない場合．

(B-1) の場合，$s_{AC} = t_{AC} = t_{EF}$，$s^+_{AC} = t^+_{AC} = t_{EF} \uplus \Delta t$ である．よって，$s_{AC} \preceq_{\Delta t} s^+_{AC}$．

(B-2) の場合，S_{AC} は $t_{AB_1} * S_{B_1C} \uplus \cdots \uplus t_{AB_n} * S_{B_nC}$ の形で表現され，(A-2) と同様な議論によって $s_{AC} \preceq_{\Delta t} s^+_{AC}$ が導かれる．

次に，(b) と (c) につにて，以下のような模擬を考える．

- プロトコル記述の (1) では，(c) においては単にプロトコルにしたがって処理をする．すなわち，もし $t_{AB} \neq 0$ ならば (c) において $\langle t_{AC}, \tilde{t}_{AC} \rangle$ を送出し，さもなければ (たとえ (b) でレスポンスが送出されていても) 何も送らない．
- (2) で，(b) においてリクエストを送られた相手のうち，(c) において t_{AB_i} が 0 でない相手だけにリクエストを送る．
- (4) で，(b) において選ばれた相手 B'_i からのレスポンスのみを用いて (c) のレスポンスを構成し送出する．ただし，どの B'_i からもレスポンスが得られない場合は，レスポンスは送出しない．

このような模擬において，任意の (b) のレスポンス $\langle s, S \rangle$ に対し以下の 2 つが容易に確かめられる．

- もし (c) に対応するレスポンス $\langle s', S \rangle$ があれば，$s = s'$．
- もし (c) に対応するレスポンスがなければ，$s = 0$．

さて改めて，A, B を任意の人とする．(b) のように変更したプロトコルによるトラスト計算手順を f' と書く．上記 2 つの模擬によって，以下の関係が成立することが言える:

$$f(T \uplus_{EF} \Delta t, A, B) \sqsubseteq \{t' \uplus \Delta t \mid t' \in f'(T, A, B)\},$$

$$f'(T, A, B) \subseteq f(T, A, B) \cup \{0\}.$$

よって全体として，

$$f(T \uplus_{EF} \Delta t, A, B) \sqsubseteq f(T, A, B) \uplus \Delta t. \qquad \blacksquare$$

5. おわりに

量と質の組を用いたトラストの定式化について，質を多値化する拡張を提案した．多値論理を援用することで，2 値の場合の同様にトラスト計算の健全性，安定性を証明できること例示した．

参考文献

[1] J. Huang and D. M. Nicol. A calculus of trust and its application to PKI and identity management. In *IDtrust 2009*, pages 23–37, 2009.

[2] Stanford Encyclopedia of Philosophy. Jan Łukasiewicz. http://plato.stanford.edu/entries/lukasiewicz/.

[3] 真野 健, 櫻田 英樹, and 塚田 恭章. 質と量の組を用いたトラストの定式化. In **コンピュータセキュリティシンポジウム** *2015*, pages 755–762, 2015.