RF-002

# 計算複雑性に基づいたパレート効率的な複数財交換ルール

## A complexity approach for Pareto efficient exchange with multiple indivisible goods

藤田 悦誌 * Etsushi Fujita　レスカ ジュリアン* Julien Lesca　苑田 尭久* Akihisa Sonoda　東藤 大樹* Taiki Todo　横尾 真* Makoto Yokoo

## 1 序論

戦略的な行動をするエージェントの集団に対して，集団としての意思決定方式 (メカニズム) を導入すると，何らかの社会的な結果が得られる．社会的に望ましい結果を得られるようにメカニズムを設計することは，メカニズムデザイン (制度設計) と呼ばれ，ミクロ経済学，ゲーム理論の一分野として活発に研究が行われている [6, 9, 12].

金銭による補償を用いることなく，参加者の保有する財を再分配する問題は交換問題と呼ばれる．現実での交換問題の例は多く存在し，住宅市場における住宅交換，腎臓移植における患者とドナーのマッチング等が挙げられる．本研究では，各参加者が複数の非分割財を保有し，財の組合せ（バンドル）に対する選好順序を持つ交換問題に適用可能な交換ルール（メカニズム）の設計に着目する．

交換ルールに望まれる性質として，(i) 個人合理性，(ii) パレート効率性，(iii) 戦略的操作不可能性，が挙げられる．個人合理性は交換に参加することで損しないことを保証する性質であり，パレート効率性は社会的余剰の観点で最適な結果が得られることを保証する性質である．また，戦略的操作不可能性は参加者が虚偽の選好を表明する誘因を持たないことを保証する性質である．しかしながら，これらの性質を満たす交換ルールであっても，参加者や財の数に関して計算量が指数的に増加するならば，計算コストは非常に大きくなり，実用的ではない．したがって，参加者や財の数に関して多項式時間で計算可能である交換ルールが望まれる．

盛んに研究されてきた交換問題の一つに，住宅交換 [10] が挙げられる．住宅交換においては，参加者は 1 財のみ保有し，参加者が財に対して厳密な選好順序を持つ．Gale の *top-trading-cycles* (TTC) アルゴリズムに基づいた交換ルールは個人合理性，パレート効率性，戦略的操作不可能性を同時に満たす唯一の交換ルールであり [5]，多項式時間で計算可能である．したがって，住宅交換に対して，TTC に基づいた交換ルールは非常に優れた交換ルールとされる．

住宅交換の自然な拡張として，参加者が複数の財を保有する交換問題が考えられる．しかしながら，文献 [11] の結果によれば，2 財以上保有する参加者が存在する場合，個人合理性，パレート効率性，戦略的操作不可能性を同時に満たす交換ルールは存在しない．したがって，参加者が複数財を保有する交換問題に対して，非常に優れた交換ルールは存在しない．さらに，文献 [1] によれば，加法的選好順序ドメインのもとであっても，P ≠ NP ならば，パレート効率的かつ多項式時間で計算可能である交換ルールは存在しないことが示されている．

また，インターネットを介した財の再分配を実現する場合，選好順序だけでなく，保有している財も私的情報と考えるのが自然である．さらに，交換ルールは実際の参加者を観測できないと考えられる．したがって，参加者は財の隠蔽や一人の参加者が複数のアカウントを用いて複数の参加者であるかのように振舞う名義の分割が可能となる．このような不正行為に対して頑健なメカニズムを議論することは重要な課題として認知されている．とくにオークションの研究分野においては，名義の分割（架空名義入札）に対して頑健なオークションメカニズムがすでにいくつか提案されてきた [13]．しかしながら，交換問題において，このような不正行為に対して頑健な交換ルールについての議論はほとんどなされていなかった．

本論文では，多項式時間で計算可能な交換ルールを設計するため，経済学において盛んに研究されている辞書式選好順序ドメイン [8] に着目する．辞書式選好順序ドメインのもとで，個人合理性とパレート効率性を同時に満たし，多項式時間で計算可能な交換ルールを設計する．さらに，戦略的操作不可能性の代わりとして，文献 [7] と同様，自身の効用を増加させる虚偽の選好の計算複雑性に関して検討を行う．より詳細には，設計したルールに関して，P ≠ NP ならば，参加者の効用を増加させる虚偽の選好を計算する多項式時間アルゴリズムは存在しないことを示す．計算コストを考慮する際，そのような虚偽の選好を求める問題が計算困難ならば，参加者は虚偽の選好表明を行わないと考えられる．また，虚偽の選好表明による効用の増加の限界に関しても議論する．

さらに，本論文では，財の隠蔽や名義の分割に関する検討も行う．より詳細には，設計した交換ルールに関して，以下を示す: (i) 財の隠蔽で得られるバンドルは名義の分割でも得ることができる，(ii) 名義の分割で得られるバンドルは虚偽の選好表明でも得ることができる．さらに，そのような不正行為の変換は多項式時間で計算可能であることを示す．したがって，設計したルールに関して，自身の効用を増加させる名義の分割も計算困難と考えられる．また，効用の増加の限界に関して，虚偽の選好表明より効用を増加できないことを示す．

* 九州大学大学院システム情報科学府

## 2 準備

### 2.1 モデル

潜在的な参加者の集合を $\mathcal{N}$, 財の集合を $K$，バンドルに対する厳密な選好順序のドメインを $\mathscr{R}$ とする．交換問題は組 $(N, e, R)$ で定義される．$N \subseteq \mathcal{N}$ であり，実際の参加者の集合を表す．便宜のため，$N = \{1, \ldots, n\}$ とする．割当 $x = (x_1, \ldots, x_n)$ は以下の条件を満たすバンドルの組である: (i) $\bigcup_{i \in N} x_i \subseteq K$，(ii) 任意の参加者 $i, j (\neq i) \in N$ に関して，$x_i \cap x_j = \emptyset$．ここで，$x_i$ は 参加者 $i \in N$ に対するバンドルの割当を表す．割当の集合を $\mathcal{X}_N$ とし，$\mathcal{X} = \bigcup_{N \subseteq \mathcal{N}} \mathcal{X}_N$ とする．$e \in \mathcal{X}_N$ であり，初期保有バンドルの組を表す．$R = (R_1, \ldots, R_n) \in \mathscr{R}^n$ であり，選好順序の組を表す（$R_i$ は参加者 $i \in N$ の選好順序を表す）．バンドル $L, L' \subseteq K$ に関して，参加者 $i \in N$ が $L$ を $L'$ より厳密に好むことを $LP_iL'$, 同等以上に好むことを $LR_iL'$ で表す．参加者 $i \in N$, 選好順序 $R_i' \in \mathscr{R}$ に関して，$(R_1, \ldots, R_{i-1}, R_i', R_{i+1}, \ldots, R_n)$ を $(R_i', R_{-i})$ で表す．交換問題の集合を $\mathcal{E}$ で表す．

### 2.2 選好順序

**定義 1** (加法的選好順序)**.** 式（1）を満たす関数 $v_i : K \to \mathbb{R}_+$ が存在する選好順序 $R_i \in \mathscr{R}$ を加法的選好順序という．

$$\forall L, L' \subseteq K, LR_iL' \Leftrightarrow \sum_{k \in L} v_i(k) \geq \sum_{k \in L'} v_i(k). \tag{1}$$

加法的選好順序ドメインを $\mathscr{A}$ で表す．さらに，$\mathscr{R} = \mathscr{A}$ のときの交換問題の集合を $\mathcal{E}_{\mathscr{A}}$ で表す．

**定義 2** (辞書式選好順序)**.** 式（1）を満たす全単射 $v_i : K \to \{2^l \mid l \in \{0, 1, \ldots, |K| - 1\}\}$ が存在する加法的選好順序 $R_i \in \mathscr{A}$ を辞書式選好順序という．

辞書式選好順序ドメインを $\mathscr{L}$ で表す．さらに，$\mathscr{R} = \mathscr{L}$ のときの交換問題の集合を $\mathcal{E}_{\mathscr{L}}$ で表す．また，辞書式選好順序 $R_i$ は $K$ の順列に対応付けられるので，$\alpha, \beta, \gamma$ を財として，$R_i : \alpha \succ \beta \succ \gamma \succ \cdots$ のように表す．

### 2.3 交換ルールの性質

交換ルールは以下の条件を満たす関数 $f : \mathcal{E} \to \mathcal{X}$ である: 任意の $E = (N, e, R) \in \mathcal{E}$ に関して，$\bigcup_{i \in N} e_i = \bigcup_{i \in N} f_i(E)$. ここで，$y = f(E)$ とするとき，$y_i$ を $f_i(E)$ で表す．

**定義 3** (個人合理性)**.** 以下の条件を満たす交換ルール $f$ は個人合理性を満たすという: 任意の $E = (N, e, R) \in \mathcal{E}$ に関して，$\forall i \in N, f_i(E) R_i e_i$ が成り立つ．

すなわち，個人合理性を満たす交換ルールは以下を保証する: 各参加者は初期保有バンドルより同等以上に好むバンドルを得る．したがって，各参加者は個人合理性を満たす交換ルールに参加しない誘因を持たない．

**定義 4** (パレート効率性)**.** 参加者の集合 $N \subseteq \mathcal{N}$, 割当 $x, y \in \mathcal{X}_N$ に関して，以下の条件を満たすとき，$x$ は $y$ にパレート弱支配されるという: (i) $\forall i \in N, y_i R_i x_i$, (ii) $\exists j \in N, y_j P_j x_j$. 以下の条件を満たす交換ルール $f$ はパレート効率性を満たすという: 任意の $E = (N, e, R) \in \mathcal{E}$, $\bigcup_{i \in N} y_i = \bigcup_{i \in N} e_i$ を満たす 任意の $y \in \mathcal{X}_N$ に関して，$f(E)$ は $y$ にパレート弱支配されない．

すなわち，パレート効率性を満たす交換ルールの出力について，以下が保証される: 各参加者の効用を減少させることなく，ある参加者の効用を増加させる割当は存在しない．

**定義 5** (戦略的操作不可能性)**.** 以下の条件を満たす交換ルール $f$ は戦略的操作不可能性を満たすという: 任意の $E = (N, e, R) \in \mathcal{E}$, $i \in N$, $R_i' \in \mathscr{R}$ に関して，$E' = (N, e, (R_i', R_{-i}))$ とするとき，$f_i(E) R_i f_i(E')$.

各参加者の選好順序を私的情報と考える場合，真の選好順序の組が交換ルールに入力されるとは限らない．しかし，戦略的操作不可能性を満たす交換ルールを用いる場合，各参加者は虚偽の選好を表明する誘因を持たない．

Sönmez [11] の結果によれば，辞書式選好順序ドメインのもとであっても，個人合理性，パレート効率性，戦略的操作不可能性を同時に満たす交換ルールは存在しない．本論文では個人合理性とパレート効率性を満たす交換ルールに着目する．

## 3 Augmented Top-Trading-Cycles Rule

本章では，以下の性質を持つ交換ルールを設計する: (i) 個人合理性，(ii) パレート効率性，(iii) 多項式時間で計算可能．

各参加者が厳密な選好順序を持つ場合，以下の TTC アルゴリズムをもとにした単一財交換ルール（各参加者がただ 1 つの財を保有する場合のみ適用可能な交換ルール）は (i)〜(iii) を満たすことが知られている．

**定義 6** (Top-Trading-Cycles)**.** バンドル $L \subseteq K$，$L$ に対する線形順序の組 $(\succ_k)_{k \in L}$ に関して，Gale の *top-trading-cycles(TTC)* アルゴリズム $\tau$ は以下のように動作する．

1. 有向グラフ $G = (L, \{(k, k') \mid k, k' \in L, \forall k'' \in L \setminus \{k'\}, k' \succ_k k''\})$ を計算する．
2. $G$ のサイクルを構成する辺の集合を $C$ とする．各 $(k, k') \in C$ に関して，$k$ に $k'$ を割り当て，$L \leftarrow L \setminus \{k\}$ とする．
3. $L = \emptyset$ ならば，終了．そうでなければ，1. に戻る．

財 $k \in L$ に対する TTC アルゴリズムによる割当を $\tau_k(L, (\succ_{k'})_{k' \in L})$ で表す．

本論文では，参加者が複数財を保有する場合にも適用できるように TTC アルゴリズムを拡張した *augmented top-trading-cycles (ATTC)* ルール†を提案する．

**定義 7** (Augmented Top-Trading-Cycles)**.** $E = (N, e, R) \in$

† 設計する交換ルールの計算アルゴリズムに関して，本論文の興味の対象外である．したがって，アルゴリズムではなくルールと呼ぶ．

$\mathcal{E}$ に関して，$L = \bigcup_{i \in N} e_i$ とする．$k \in e_i$ に関して，$\succ_k$ を $R_i$ と整合する $L$ に対する線形順序とする（i.e., $\forall k', k'' \in L$, $\{k'\} P_i \{k''\} \Leftrightarrow k' \succ_k k''$）．*augmented top-trading-cycles (ATTC)* ルール $\varphi$ は以下で定義される．

$$\varphi_i(E) = \bigcup_{k \in e_i} \tau_k(L, (\succ_{k'})_{k' \in L}).$$

すなわち，選好順序が $R_i$ である参加者 $i$ に関して，$i$ の保有する財に $R_i$ と整合する線形順序を与える．その後，TTC アルゴリズムにより財の割当を行い，$i$ が保有していた財に割り当てられた財を $i$ が得るという交換ルールである．

TTC アルゴリズムは多項式時間アルゴリズムであるため，ATTC ルールは多項式時間で計算可能である．本論文では ATTC ルールを TTC アルゴリズムにより計算すると仮定する．次章以降で，ATTC ルールの性質について述べる．

## 4 パレート効率性

本章では ATTC ルールがパレート効率性を満たす選好順序のドメインについて議論する．

### 4.1 加法的選好順序

以下の例が示すように，加法的選好順序ドメインのもとで ATTC ルールはパレート効率性を満たさない．

**例 1.** $E = (N, e, R) \in \mathcal{E}_{\mathscr{A}}$, $N = \{1, 2\}$, $e_1 = \{\alpha, \beta\}$, $e_2 = \{\gamma\}$ とし，$R_1$, $R_2 \in \mathscr{A}$ は以下の関数 $v_1, v_2$ により与えられる加法的選好順序とする:

$$v_1(\alpha) = 2, v_1(\beta) = 4, v_1(\gamma) = 8,$$
$$v_2(\alpha) = 2, v_2(\beta) = 4, v_2(\gamma) = 5.$$

このとき，$\varphi(E) = (\{\alpha, \beta\}, \{\gamma\})$ となる（交換を行わない）が，$\varphi(E)$ は割当 $(\{\gamma\}, \{\alpha, \beta\})$ にパレート弱支配される．

例 1 は ATTC ルールがパレート効率性を満たさないことを示しているにすぎない．一般には，初期保有バンドルの組に対して，パレート改善される割当が存在しなくなるまで，パレート改善する割当を繰り返し計算することで，パレート効率的な割当を得ることができる．しかしながら，文献 [1] の結果によれば，加法的選好順序ドメインのもとでパレート改善する割当の存在を判定する問題は NP 完全であることが示されている．したがって，パレート効率的な割当を多項式時間で計算するアルゴリズムは存在しないと考えられる．

### 4.2 辞書式選好順序

前節の結果より，加法的選好順序ドメインのもとで，ATTC ルールはパレート効率性を満たさたない．しかしながら，加法的選好順序ドメインのサブドメインである辞書式選好順序ドメインのもとでは，以下の定理が成り立つ．

**定理 1.** 辞書式選好順序ドメインのもとで，ATTC ルールはパレート効率性を満たす．

**証明.** 交換問題 $E = (N, e, R) \in \mathcal{E}_{\mathscr{L}}$ に関して，$x = \varphi(E)$ とする．$x$ は 割当 $y \in \mathcal{X}_N$ にパレート弱支配されると仮定する．

$t \in \{1, 2, \ldots\}$ に関して，ATTC ルールの $t$ 回目のラウンドで財が割り当てられる参加者の集合を $S^t$ とし，参加者 $i \in S^t$ に割り当てられる財を $g_i^t$ とする．ここで，1 回のラウンドで 2 個以上の財が同一の参加者に割り当てられることはないことに注意されたい．命題 $H^t$ を $\forall i \in S^t, g_i^t \in y_i$ とし，数学的帰納法より，$H^1, H^2, \ldots$ が真であることを示す．

**■基底段階** ATTC ルール，辞書式選好順序の定義より，参加者 $i \in S^1$ に関して，$g_i^1 \notin y_i$ ならば，$x_i P_i y_i$ が成り立つ．これは $x$ は $y$ にパレート弱支配されるという仮定に反する．したがって，$g_i^1 \in y_i$ が成り立ち，$H^1$ は真である．

**■帰納段階** $H^1, \ldots, H^{t-1}$ が真と仮定し，$H^t$ が真であることを示す．ATTC ルールの定義より，参加者 $i \in S^t$, $\{k\} P_i \{g_i^t\}$ を満たす財 $k \in \bigcup_{i \in N} e_i$ に関して，$g_j^{t'} = k$ なる $t' < t, j \in N$ が存在する．よって，帰納法の仮定より，$j \neq i$ ならば $k \notin y_i$ を満たす．したがって，$g_i^t \notin y_i$ ならば，$x_i P_i y_i$ が成り立つ．これは $x$ は $y$ にパレート弱支配されるという仮定に反する．したがって，$g_i^t \in y_i$ が成り立ち，$H^t$ は真である．

$H^1, H^2, \ldots$ が真であることから，$x_i = y_i$ が成り立つ．これは $x$ は $y$ にパレート弱支配されるという仮定に反する．したがって，$x$ は任意の割当にパレート弱支配されない． □

また，ATTC ルールの定義より，辞書式選好順序ドメインのもとで，ATTC ルールは個人合理性を満たす．しかしながら，ATTC ルールは個人合理性とパレート効率性を満たす唯一の交換ルールでない．したがって，本研究のモデルにおいて，ATTC ルールは優れたルールの一つにすぎない．

## 5 虚偽の選好表明

文献 [11] の示した結果より，辞書式選好順序ドメインのもとであっても，ATTC ルールは戦略的操作不可能性を満たさない．本章では，ATTC ルールにおける虚偽の選好表明の誘因について議論する．

また，以下のように記法の簡単化を行う: 交換問題 $E = (N, e, R)$, 選好順序 $R_i' \in \mathscr{R}$ に関して，交換問題 $E' = (N, e, (R_i', R_{-i}))$ を $(R_i' \mid E)$ で表す．

### 5.1 効用を増加させる虚偽の選好の計算複雑性

計算コストを考慮する際，自身の効用を増加させる虚偽の選好を求める問題が計算困難ならば，参加者は虚偽の選好表明を行わないと考えられる．そこで，本節では ATTC ルールにおける自身の効用を増加させる虚偽の選好の計算複雑性について議論する．具体的には，ATTC ルールにおいて，$\mathrm{P} \neq \mathrm{NP}$ ならば自身の効用を増加させる虚偽の選好を求める問題を解く多項式時間アルゴリズムは存在しないことを示す．

**定義 8** (ATTC 効用増加問題)**.**

**入力** $E = (N, e, R) \in \mathcal{E}_{\mathscr{L}}$, $i \in N$.
**出力** 以下の条件を満たす $R_i' \in \mathscr{L}$:

$$\varphi_i(R_i' \mid E) P_i \varphi_i(E).$$

ただし，そのような $R_i'$ が存在しないならば “None”.

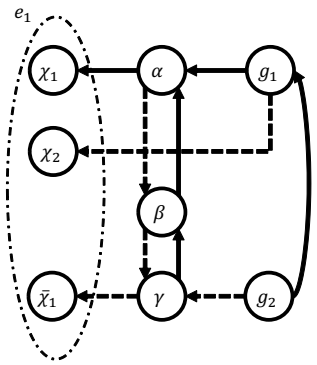


図 1　ATTC 効用増加問題の例

**例 2.** $E = (N, e, R) \in \mathcal{E}_{\mathscr{L}}$, $N = \{1, \ldots, 6\}$,

$$
\begin{array}{ll}
e_1 = \{\chi_1, \chi_2, \bar{\chi}_1\}, & R_1 : g_1 \succ g_2 \succ \chi_2 \succ \bar{\chi}_1 \succ \cdots \\
e_2 = \{\alpha\}, & R_2 : \chi_1 \succ \beta \succ \cdots \\
e_3 = \{\beta\}, & R_3 : \alpha \succ \gamma \succ \cdots \\
e_4 = \{\gamma\}, & R_4 : \beta \succ \bar{\chi}_1 \succ \cdots \\
e_5 = \{g_1\}, & R_5 : \alpha \succ \chi_2 \succ \cdots \\
e_6 = \{g_2\}, & R_6 : g_1 \succ \gamma \succ \cdots
\end{array}
$$

とする．図 1 はこの交換問題を表しており，実線の矢印は始点の財を保有する参加者が終点の財を最も好むことを表す．同様に，破線の矢印は 2 番目に好むことを表す．

参加者 1 が真の選好順序 $R_1$ を表明した場合，$g_1, \chi_2, \bar{\chi}_1$ を得る．参加者 1 が虚偽の選好順序 $R_1' : \chi_1 \succ g_1 \succ g_2 \succ \cdots$, を表明した場合，$g_1, g_2, \chi_1$ を得る．したがって，$R_1'$ はこの問題に対する出力である．

例 2 において，$\chi_1$ を $g_1$ と交換すると，$\bar{\chi}_1$ は $g_2$ と交換できない．一方，$\chi_1$ を 自身と交換するよう虚偽の選好表明を行うことで，$\bar{\chi}_1$ を $g_2$ と交換することができ，$g_1$ と $g_2$ を得ることができる．このように，ATTC 効用増加問題は SAT と関連性を持つ．

よく知られた NP 完全問題である Monotone 3-SAT [2] に関して，例 2 を一般化することで，ATTC 効用増加問題の計算複雑性を示す．

**定義 9** (Monotone 3-SAT)**.**

**入力**　変数の集合 $U$, $U$ に関する節の集合 $C = \{c_1, \ldots, c_m\}$. ただし，各節の含むリテラルの数は 3 であり，各節の含むリテラルはすべて正リテラルまたは負リテラルである．

**出力**　$C$ の各節を充足する $U$ の各変数に対する真理値割当が存在するならば “Yes”，そうでなければ “No”．

**定理 2.** P $\neq$ NP ならば，ATTC 効用増加問題を解く多項式時間アルゴリズムは存在しない．

**証明.** ATTC 効用増加問題を解く多項式時間アルゴリズム $A$ が存在すると仮定する．背理法より，NP 完全である Monotone 3-SAT を解く多項式時間アルゴリズムが存在するならば，定理は示される．

■Monotone 3-SAT から ATTC 効用増加問題への変換

節 $c_r \in C$ は $c_r^1 \vee c_r^2 \vee c_r^3$ で表されるとする．$\overrightarrow{\infty} = (\infty, \infty)$ とする．簡単のため, リテラル $\lambda$ に関して, $\lambda$ が正リテラルならば真となる述語を $\rho(\lambda)$ とし，さらに，以下の関数を導入する:

$$
first(\lambda) = \underset{(r,l) \in \{(r',l') \mid c_{r'}^{l'} = \lambda\} \cup \{\overrightarrow{\infty}\}}{\arg\min} r,
$$

$$
next(\lambda, r'') = \underset{(r,l) \in \{(r',l') \mid c_{r'}^{l'} = \lambda, r' > r''\} \cup \{\overrightarrow{\infty}\}}{\arg\min} r.
$$

各 $r \in \{1, \ldots, m\}$ に関して，財 $g_r$ を導入する．各 $r \in \{1, \ldots, m\}$, $l \in \{1, 2, 3\}$ に関して, 財 $k_r^l$, $p_r^l$, $\pi_r^l$, $\chi_r^l$ を導入する．$\rho(c_r^l)$ が真, $\rho(c_{r'}^{l'})$ が偽となるような各 $r, r' \in \{1, \ldots, m\}$, $l, l' \in \{1, 2, 3\}$ に関して，財 $\alpha_{r',l'}^{r,l}$, $\beta_{r',l'}^{r,l}$, $\gamma_{r',l'}^{r,l}$ を導入する．各 $r \in \{1, \ldots, m\}$, $l \in \{1, 2\}$ に関して, 財 $q_r^{l,l+1}$ を導入する．参加者 $i$ を導入し，$e_i = \{\chi_r^l \mid r \in \{1, \ldots, m\}, l \in \{1, 2, 3\}\}$ とする．$\chi_r^l$ 以外の各財に対応した参加者を導入し，$i$ 以外の参加者は対応する財のみ保有する．

以降，選好順序を組で表す．例えば，$R_j : \alpha \succ \beta \succ \gamma \succ \cdots$ を $(\alpha, \beta, \gamma)$ で表す．さらに，財 $k$ を保有する参加者の選好順序を $R(k)$ で表す．各参加者の選好順序を以下で定める:

$$
R(g_r) = \begin{cases} (k_1^1, k_1^2, k_1^3, g_1) & \text{if } r = 1 \\ (g_{r-1}, k_r^1, k_r^2, k_r^3, g_r) & \text{if } r \in \{2, \ldots, m\}, \end{cases}
$$

$$
R(k_r^l) = \begin{cases} (p_r^l, k_r^l) & \text{if } first(\neg c_r^l) = \overrightarrow{\infty} \\ (\alpha_{r',l'}^{r,l}, k_r^l) & \text{if } first(\neg c_r^l) = (r', l') \neq \overrightarrow{\infty} \wedge \rho(c_r^l) \\ (\gamma_{r,l}^{r',l'}, k_r^l) & \text{if } first(\neg c_r^l) = (r', l') \neq \overrightarrow{\infty} \wedge \neg\rho(c_r^l), \end{cases}
$$

$$
R(\alpha_{r',l'}^{r,l}) = \begin{cases} (p_r^l, \beta_{r',l'}^{r,l}, \alpha_{r',l'}^{r,l}) & \text{if } next(c_{r'}^{l'}, r') = (r'', l'') = \overrightarrow{\infty} \\ (\alpha_{r'',l''}^{r,l}, \beta_{r',l'}^{r,l}, \alpha_{r',l'}^{r,l}) & \text{if } next(c_{r'}^{l'}, r') = (r'', l'') \neq \overrightarrow{\infty}, \end{cases}
$$

$$
R(\beta_{r',l'}^{r,l}) = (\alpha_{r',l'}^{r,l}, \gamma_{r',l'}^{r,l}, \beta_{r',l'}^{r,l}),
$$

$$
R(\gamma_{r',l'}^{r,l}) = \begin{cases} (\beta_{r',l'}^{r,l}, p_{r'}^{l'}, \gamma_{r',l'}^{r,l}) & \text{if } next(c_r^l, r) = \overrightarrow{\infty} \\ (\beta_{r',l'}^{r,l}, \gamma_{r',l'}^{r'',l''}, \gamma_{r',l'}^{r,l}) & \text{if } next(c_r^l, r) = (r'', l'') \neq \overrightarrow{\infty}, \end{cases}
$$

$$
R(p_r^l) = \begin{cases} (\pi_r^1, q_r^{1,2}, p_r^1) & \text{if } l = 1 \\ (q_r^{1,2}, \pi_r^2, q_r^{2,3}, p_r^2) & \text{if } l = 2 \\ (q_r^{2,3}, \pi_r^3, p_r^3) & \text{if } l = 3, \end{cases}
$$

$$
R(q_r^{l,l+1}) = \begin{cases} (p_r^1, p_r^2, q_r^{1,2}) & \text{if } l = 1 \\ (p_r^2, p_r^3, q_r^{2,3}) & \text{if } l = 2, \end{cases}
$$

$$
R(\pi_r^l) = \begin{cases} (\chi_1^l, \pi_1^l) & \text{if } r = 1 \\ (g_{r-1}, \chi_r^l, \pi_r^l) & \text{if } r \in \{2, \ldots, m\}, \end{cases}
$$

$$
R_i = (g_1, \ldots, g_m, \chi_m^1, \chi_1^2, \chi_1^3, \chi_2^2, \chi_2^3, \ldots, \chi_m^2, \chi_m^3).
$$

図 2 は変換された交換問題を表しており，実線の矢印は始点の財を保有する参加者が終点の財を最も好むことを表す．同様に，破線の矢印は 2 番目に好むこと，点線の矢印は 3 番目に好むこと，一点鎖線の矢印は 4 番目に好むことを表す．

以上より，与えられた Monotone 3-SAT から ATTC 増加問題への変換が定義された．財の数は $O(m^2)$ より，この変換は多項式時間で計算可能であることに注意されたい．

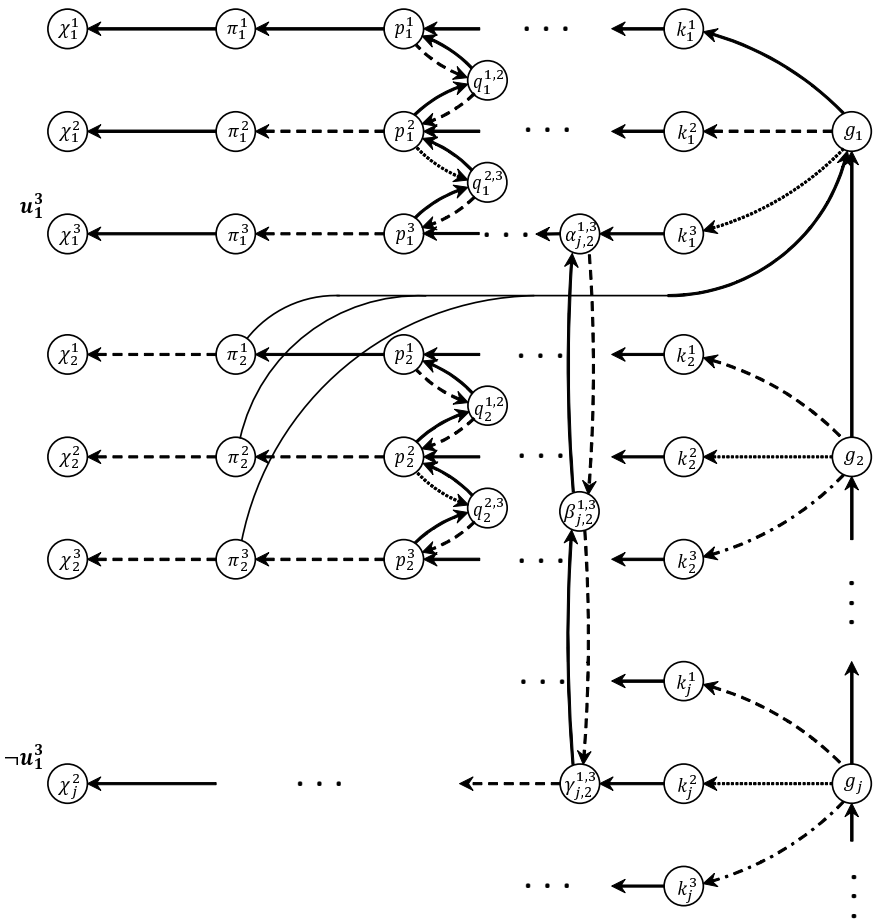


図 2　Monotone 3-SAT から ATTC 効用増加問題への変換

**■変換の対応関係**　前述の変換に関して，変換前と変換後の問題の対応について議論する．具体的には，$\varphi_i(E) = \{g_1, \ldots, g_{m-1}, \chi_m^1, \chi_1^2, \chi_1^3, \chi_2^2, \chi_2^3, \ldots, \chi_m^2, \chi_m^3\}$ を満たす交換問題 $E$ を入力とする変換後の ATTC 効用増加問題に関して，以下を示す: 変換後の ATTC 効用増加問題が出力 $R_i'$ を持つならば，そのときに限り，変換前の Monotone 3-SAT の出力は “Yes” である．辞書式選好順序であることから，変換後の ATTC 効用増加問題の出力 $R_i'$ に関して，$\{g_1, \ldots, g_m\} \subseteq \varphi_i(R_i' \mid E)$ を満たす．また，一般性を失うことなく，$c_1, \ldots, c_z$ を正リテラルのみ含む節とし，$c_{z+1}, \ldots, c_m$ を負リテラルのみ含む節と仮定する．

変換前の Monotone 3-SAT の出力を “Yes” と仮定する．このとき，各節を充足する各変数に対する真理値割当が存在する．真を割り当てる変数の集合を $U'$，偽を割り当てる変数の集合を $\bar{U}'$ で表す．各 $u' \in U'$, $\bar{u}' \in \bar{U}'$ に関して，$c_r^l = \neg u'$ または $c_r^l = \bar{u}'$ であるような $(r,l)$ の集合を $\mathcal{I}^-$ で表す．さらに $\{\chi_r^l \mid (r,l) \in \mathcal{I}^-\}$ を $L = \{\kappa_1, \ldots, \kappa_{|\mathcal{I}^-|}\}$ で表す．$R_i' : \kappa_1 \succ \cdots \succ \kappa_{|\mathcal{I}^-|} \succ g_1 \succ \cdots \succ g_m \succ \cdots$ とするとき，$\varphi_i(R_i' \mid E) P_i \varphi_i(E)$ が成り立つことを示す．

ATTC の定義より，$\kappa_1, \ldots, \kappa_{|\mathcal{I}^-|}$ は自身と交換される．$g_1$ から $\chi_1^1$ に至るパスが存在することから，$c_1^1$ が真のとき，$\chi_1^1$ が $g_1$ と交換される．$c_1^1$ が偽のとき，$\chi_1^1$, $\pi_1^1$ の順で自身と交換される．さらに，$p_1^1$ は $q_1^{1,2}$ と交換され，$\alpha_{r,l}^{1,2}$ は $\beta_{r,l}^{1,2}$ と交換される．したがって，$k_1^1$ は自身と交換され，$g_1$ から $\chi_1^2$ に至るパスが現れる（$q_1^{1,2}$ が存在しないため，$p_1^2$ は $\pi_1^2$ を最も好むようになることに注意されたい）．よって，$c_1^2$ が真のとき，$\chi_1^2$ が $g_1$ と交換される．同様に，$c_1^2$ が偽のとき，$\chi_1^3$ が $g_1$ と交換される．各節を充足する真理値割当であることから，$\chi_1^1$, $\chi_1^2$, $\chi_1^3$ のいずれかが $g_1$ と交換される．$g_1$ が存在しないため，$g_2$ は $g_1$ を最も好み，$\pi_2^l$ は $\chi_2^l$ を最も好む．したがって，$g_1$ と同様に，$\chi_2^1$, $\chi_2^2$, $\chi_2^3$ のいずれかが $g_2$ と交換される．$g_3, \ldots, g_z$ についても同様である．$c_{z+1}^l$ が真のとき，$c_{z+1}^1 = \neg c_r^l$ を満たす $(r,l)$ に関して，$\chi_r^l$ は自身と交換されることから，$\alpha_{z+1,1}^{r,l}$ は $\beta_{z+1,1}^{r,l}$ と交換される．したがって，$\gamma_{z+1,1}^{r,l}$ は $p_{z+1}^1$ または $\gamma_{z+1,1}^{next(\neg c_r^l, r)}$ を最も好むため，$g_{z+1}$ から $\chi_{z+1}^1$ に至るパスが存在し，$\chi_{z+1}^1$ は $g_{z+1}$ と交換される．$c_{z+1}^2, c_{z+1}^3$ に関しても同様である．$c_r^l$ に関しても同様である（$r \in \{z+2, \ldots, m\}$, $l \in \{1,2,3\}$）．以上より，$\{g_1, \ldots, g_m\} \subseteq \varphi_i(R_i' \mid E)$ が成り

立ち，$\varphi_i(R'_i \mid E)P_i\varphi_i(E)$ を満たす．

変換後の ATTC 効用増加問題に関して，出力 $R'_i$ が存在すると仮定する．$g_1$ と交換可能な参加者 $i$ の財は $\chi_1^1, \chi_1^2, \chi_1^3$ のいずれかである．$g_1$ を参加者 $i$ の財と交換した場合，$g_2$ と交換可能な参加者 $i$ の財は $\chi_2^1, \chi_2^2, \chi_2^3$ のいずれかである．同様に，$g_1, \ldots, g_{l-1}$ をそれぞれ参加者 $i$ の財と交換した場合，$g_l$ と交換可能な参加者 $i$ の財は $\chi_l^1, \chi_l^2, \chi_l^3$ のいずれかである．必要性と同様の議論により，$\chi_r^l$ が $g_r$ と交換された場合，$c_{r'}^{l'} = \neg c_r^l$ を満たす $(r', l')$ に関して，$\chi_{r'}^{l'}$ は $g_{r'}$ と交換不可能である．以上より，各変数 $u \in U$ に関して，$c_r^l = u$ かつ $\chi_r^l$ が $g_r$ と交換される $(r, l)$ が存在するならば $u$ に真を割り当て，$c_r^l = \neg u$ かつ $\chi_r^l$ が $g_r$ と交換される $(r, l)$ が存在するならば $u$ に偽を割り当てる真理値割当（それ以外の変数に対する割当は任意）は変換前の Monotone 3-SAT を充足する．

■**Monotone 3-SAT を解くアルゴリズム**　存在を仮定したアルゴリズム $A$ を用いて，以下のアルゴリズムを定義する．

1. $U, C$ を入力とする Monotone 3-SAT に関して，論理式 $(c_1^1 \wedge \cdots \wedge c_r^1)$ が恒偽式でないような最大の $r$ を $r'$ とする．$r' = m$ ならば “Yes” を出力し，停止する．そうでなければ $C' = \{c_1, \ldots, c_{r'+1}\}$ とする．
2. $U, C'$ を入力とする Monotone 3-SAT に関して，前述の変換により得られる交換問題を $E_{r'}$ とする．$E_{r'}$ を入力とする ATTC 効用増加問題を アルゴリズム $A$ を用いて解き，$R'_i$ を得る．解が存在しないならば，“No” を出力し，停止する．
3. 交換問題 $(R'_i \mid E_{r'})$ に対する ATTC ルールの手続きにおいて，各 $r \in \{1, \ldots, r'+1\}$ 関して，$g_r$ と交換した財を $\chi_r^l$ とする．各節 $c_r$ に関して，リテラル $c_r^l$ をその節の先頭に移動させ，1. に戻る．

Monotone 3-SAT の定義より，1. の条件を満たすとき，変換前の問題の出力は “Yes” である．ここで，アルゴリズムの動作により，$C$ に含まれる節のリテラルの順序が入れ替わる可能性はあるが，論理式として元の問題と等価であることに注意されたい．2. において，$A$ を用いて解いた問題は変換前の問題の一部の節を充足させる問題である（$\varphi_i(E_{r'}) = \{g_1, \ldots, g_{r'}, \chi_{r'+1}^1, \chi_1^2, \chi_1^3, \ldots, \chi_{r'+1}^2, \chi_{r'+1}^3\}$ を満たすことに注意されたい）．したがって，$A$ を用いて解が存在しないならば，変換前の問題の出力は “No” である．3. において，変換の対応関係の議論より，$\{g_1, \ldots, g_{r'+1}\} \subseteq \varphi_i(R'_i \mid E_{r'})$ を満たす．したがって，各 $r \in \{1, \ldots, r'+1\}$ に関して，$g_r$ と交換される財 $\chi_r^l$ は存在する．さらに，リテラルの順序の入れ替えにより，次のループの 1. で計算される $r'$ は現在のループで計算された $r'$ より大きくなる．以上より，このアルゴリズムは常に停止し，出力も正しい．

Monotone 3-SAT から ATTC 効用増加問題への変換，3. におけるリテラルの交換は多項式時間で計算される．また，ATTC ルールの計算は多項式時間で可能である．ループ回数は高々 $m$ 回であることから，このアルゴリズムは多項式時間アルゴリズムである．

以上より，ATTC 効用増加問題を解く多項式時間アルゴリズムが存在すると仮定すると，Monotone 3-SAT を解く多項式時間アルゴリズムが存在する．　□

定理 2 より，辞書式選好順序ドメインのもとで，ATTC ルールにおける自身の効用を増加させる虚偽の選好を求める問題は計算困難と考えられる．

### 5.2　虚偽の選好表明による効用の増加

本節では，虚偽の選好表明による効用の増加の限界について議論する．以下の定理が示すように，真の選好表明により得られる財のうち最も好む財を $k$ とするとき，いかなる虚偽の選好表明を行っても $k$ より好む財を得ることはできない．

**定理 3.** 任意の交換問題 $E = (N, e, R) \in \mathcal{E}_{\mathscr{L}}$，任意の参加者 $i \in N$，任意の選好順序 $R'_i \in \mathscr{L}$ に関して，$\forall k' \in \varphi_i(E), \{k\}P_i\{k'\}$ を満たす財 $k \in \varphi_i(R'_i \mid E)$ は存在しない:

**証明.** 交換問題 $E$ に関して，参加者 $i \in N$ が財を得る ATTC ルールの最初のラウンドを $r$ とする．$r$ より前のラウンドで割り当てられた財の集合を $K'$ で表す．ATTC ルールの定義より，$r$ 回目のラウンドで参加者 $i$ に割り当てられた財は $K \setminus K'$ に含まれる財のうち，$i$ が最も好む財である．したがって，任意の選好順序 $R'_i \in \mathscr{L}$，任意の財 $k \in K'$ に関して，$k \notin \varphi_i(R'_i \mid E)$ を示せばよい．

交換問題 $\bar{E} \in \mathcal{E}_{\mathscr{L}}$ に関して，ATTC ルールの $t$ 回目のラウンドで構成されるサイクルに含まれる財の集合を $L^t(\bar{E})$ で表す．$t \in \{1, \ldots, r-1\}$ に関して，命題 $H^t$ を以下のように定める: 財 $k \in K'$ に関して，$k \in L^t(E)$ ならばそのときに限り $E'$ に関しても，$k \in L^t(E')$．数学的帰納法より，$H^1, \ldots, H^{r-1}$ が真であることを示す．

■**基底段階**　財 $k \in K'$ を始点とする有向辺は，参加者 $i$ の選好順序に依存しない．したがって，任意の財 $k \in L^1(E)$ に関して，$k \in L^1(E')$ である．また，ATTC の定義より，財 $k \in K'$ を保有する参加者の選好順序 $R_j$ に関して，$\{k'\}P_j\{k\}$ を満たすならば，$k' \in K'$ である．よって，財 $k \notin L^1(E)$ を始点とし，参加者 $i$ が保有する財を終点とする有向辺は存在しない．したがって，$k' \in K'$, $k' \in L^1(E')$ を満たす財 $k'$ に関しても，$k' \in L^1(E)$ が成り立つ．以上より，$H^1$ は真である．

■**帰納段階**　$H^1, \ldots, H^{t-1}$ が真と仮定し，$H^t$ が真であることを示す．$H^1, \ldots, H^{t-1}$ が真であることから，交換問題 $E$ と $E'$ に関して，ATTC ルールの $t$ 回目のラウンド開始時点で割り当てられていない，かつ，$K'$ に含まれる財の集合は等しい．よって，基底段階と同様の議論により，$H^t$ は真である．

$H^1, \ldots, H^{r-1}$ が真であるため，$k \notin \varphi_i(E')$ が成り立つ．　□

辞書式選好順序を持つ参加者のバンドルに対する効用は，最も好む財に大きく依存する．したがって，定理 3 より，最適な虚偽の選好を求めることができたとしても，計算コストに見合うことは多くないと考えられる．

## 6 財の隠蔽と名義の分割

本章では，初期保有バンドルが私的情報であり，真の（実際に参加する）参加者の集合を交換ルールは知ることができないケースを考える．このケースにおいて，参加者は財の隠蔽や名義の分割を行うことが可能であるため，これらの不正行為の影響について議論する．

### 6.1 記法の定義

**財の隠蔽** バンドル $e_i \subseteq K$ に関して，財の隠蔽 $h_i = (e_i^r, e_i^w)$ は以下の条件を満たすバンドルの組である: (i) $e_i^w \subseteq e_i$, (ii) $e_i^r = e_i \setminus e_i^w$. $e_i^r$ は公開するバンドルを表す．$e_i^w$ は隠蔽するバンドルを表す．財の隠蔽の集合を $\mathcal{H}(e_i)$ とする．

**名義の分割** バンドル $e_i \subseteq K$ に関して，$m \in \{1, \ldots, |e_i|\}$ 名義の分割 $s_i = ((e_i^1, R_i^1), \ldots, (e_i^m, R_i^m))$ は以下の条件を満たす組である: (i) $\bigcup_{l=1}^m e_i^l = e_i$, (ii) $\forall l, l' \in \{1, \ldots, m\}, e_i^l \cap e_i^{l'} = \emptyset$, (iii) $\forall l \in \{1, \ldots, m\}, R_i^l \in \mathscr{R}$. $e_i^l$ は $l$ 番目の名義の初期保有バンドルを表し，$R_i^l$ は $l$ 番目の名義の選好順序を表す．$m$ 名義の分割の集合を $\mathcal{S}_m(e_i)$ とし，すべての名義の分割の集合を $\mathcal{S}(e_i)$ とする (i.e., $\mathcal{S}(e_i) = \bigcup_{m=1}^{|e_i|} \mathcal{S}_m(e_i)$).

交換問題 $E = (N, e, R) \in \mathcal{E}$, 参加者 $i \in N$ に関して，以下のように記法の簡単化を行う．

財の隠蔽 $h_i = (e_i^r, e_i^w) \in \mathcal{H}(e_i)$ に関して，$E' = (N, (e_1, \ldots, e_{i-1}, e_i^r, e_{i+1}, \ldots, e_n), R)$ とするとき，$\varphi_i(E') \cup e_i^w$ を $\varphi_i(h_i \mid E)$ で表す．

名義の分割 $s_i = ((e_i^1, R_i^1), \ldots, (e_i^m, R_i^m)) \in \mathcal{S}(e_i)$ に関して，$N' = \{1, \ldots, i-1, (i,1), \ldots, (i,m), i+1, \ldots, n\}$, $e' = (e_1, \ldots, e_{i-1}, e_i^1, \ldots, e_i^m, e_{i+1}, \ldots, e_n)$, $R' = (R_1, \ldots, R_{i-1}, R_i^1, \ldots, R_i^m, R_{i+1}, \ldots, R_n)$ とするとき，交換問題 $(N', e', R')$ を $E(s_i)$ で表す．さらに，$\bigcup_{l=1}^m \varphi_i^l(E(s_i))$ を $\varphi_i(s_i \mid E)$ で表す．ここで，$\varphi(s_i \mid E) = (y_1, \ldots, y_{i-1}, y_i^1, \ldots, y_i^m, y_{i+1}, \ldots, y_n)$ とするとき，$y_i^l$ を $\varphi_i^l(s_i \mid E)$ で表す．また，常に $N' \subseteq \mathcal{N}$ が成り立つとする．

### 6.2 各不正行為の関係

本節では，ATTC ルールにおける，虚偽の選好表明，財の隠蔽，名義の分割の関係を示す．以下の補題を用いて各不正行為の関係を示す．

**補題 1.** バンドル $L \subseteq K$, $L$ に対する線形順序 $(\succ_k)_{k \in L}$ に関して，TTC アルゴリズムにより構築される，あるサイクルに含まれる財の集合を $C$ とする．財 $k \in C$ に関して，$\succ'_k$ を $\succ_k$ と整合する $C$ に対する線形順序とするとき，$\tau_k(L, (\succ_{k'})_{k' \in L})) = \tau_k(C, (\succ'_{k'})_{k' \in C})$ が成り立つ．財 $k \in L \setminus C$ に関して，$\succ'_k$ を $\succ_k$ と整合する $L \setminus C$ に対する線形順序とするとき，$\tau_k(L, (\succ_{k'})_{k' \in L})) = \tau_k(L \setminus C, (\succ'_{k'})_{k' \in L \setminus C})$ が成り立つ．

証明は割愛するが，財 $k \in C$ に関して，成り立つことは明らかである．また，対象のサイクルが構築されるラウンド，あるいはそれ以前のラウンドで構築されるサイクルに含まれる財の集合 $C'$ に関して，財 $k' \in C'$ を始点とし，財 $k \in C$ を終点とする辺が現れることはないため，あらかじめ $C$ に含まれるすべての財を除外しても $C'$ から成るサイクルは構築される．また，対象のサイクルより後に構築されるサイクルに関して，前述の $C'$ から成るサイクルが構築されるため，あらかじめ $C$ に含まれるすべての財を除外されても $C''$ から成るサイクルは構築される．

補題 1 より，TTC アルゴリズムが構築する，あるサイクルに含まれるすべての財をあらかじめ除外し，残りの財と除外された財に対して独立に TTC アルゴリズムを適用しても等価な結果が得られる．

**定理 4.** 任意の交換問題 $E = (N, e, R) \in \mathcal{E}_{\mathscr{L}}$，任意の参加者 $i \in N$, 任意の財の隠蔽 $h_i \in \mathcal{H}(e_i)$ に関して，$\varphi_i(s_i \mid E) = \varphi_i(h_i \mid E)$ を満たす名義の分割 $s_i \in \mathcal{S}(e_i)$ が存在する．

**証明.** $e_i = \{g_i^1, \ldots, g_i^{|e_i|}\}$, $h_i = (e_i^r, e_i^w) \in \mathcal{H}(e_i)$ とする．$l \in \{1, \ldots, |e_i|\}$ に関して，$R_i^l$ を，$g_i^l \in e_i^r$ ならば $R_i^l = R_i$, $g_i^l \in e_i^w$ ならば $R_i^l : g_i^l \succ \cdots$ なる選好順序とする．$s_i = ((\{g_i^1\}, R_i^1), \ldots, (\{g_i^{|e_i|}\}, R_i^{|e_i|})) \in \mathcal{S}_{|e_i|}(e_i)$ とする．このとき，$\varphi_i(s_i \mid E) = \varphi_i(h_i \mid E)$ を満たすことを示す．

参加者 $i$ が名義の分割 $s_i$ を用いる場合，ATTC ルールの 1 回目のラウンドにおいて，財 $k \in e_i^w$ は自己ループを持つ．交換問題 $E(s_i)$ に関して，$e_i^w$ に含まれる財を保有する参加者を除外した交換問題を $E'$ とする．各財 $k \in e_i^w$ に関して，補題 1 を繰り返し用いることで，$\varphi_i(s_i \mid E) = \varphi_i(E') \cup e_i^w$ を得る．$g_i^l \in e_i^r$ を満たす $l \in \{1, \ldots, |e_i|\}$ に関して，$R_i^l = R_i$ より，$\varphi_i(s_i \mid E) = \varphi_i(h_i \mid E)$ を得る． □

**定理 5.** 任意の交換問題 $E = (N, e, R) \in \mathcal{E}_{\mathscr{L}}$，任意の参加者 $i \in N$, 任意の名義の分割 $s_i \in \mathcal{S}(e_i)$ に関して，$\varphi_i(R'_i \mid E) = \varphi_i(s_i \mid E)$ を満たす $R'_i \in \mathscr{L}$ が存在する．

証明は割愛するが，名義の分割 $s_i \in \mathcal{S}(e_i)$ に関して，以下に示す選好順序 $R'_i$ は $\varphi_i(R'_i \mid E) = \varphi_i(s_i \mid E)$ を満たす: $s_i$ を用いた場合に，ATTC ルールの手続きにおいて，参加者 $i$ が得た財を，割り当てられたラウンドが早い順に $g_i^1, \ldots, g_i^{|e_i|}$ (同一のラウンドで複数の財が割り当てられた場合，それらの順序は任意）として，$R'_i : g_i^1 \succ \cdots \succ g_i^{|e_i|}$.

また，補題 1 を繰り返し適用することで，$\varphi_i(R'_i \mid E) = \varphi_i(s_i \mid E)$ が示される．直観的には，名義の分割 $s_i$ を用いる場合と比べ，選好 $R'_i$ を表明することで財を得るラウンドが遅れる可能性があるが，同一のサイクルまたは分割されたサイクル (e.g., サイクル $(k_1, g_i^1, k_2, g_i^2, k_1)$ に関して，$(g_i^1, k_2, g_i^1)$ と $(g_i^2, k_1, g_i^2)$) が構築されるため，等価な結果となる．

定理 4 の $s_i$, 定理 5 の $R'_i$ は多項式時間で計算可能であることに注意されたい．また，1 名義の分割は虚偽の選好表明であることから，任意の虚偽の選好表明と等価な結果を得る名義の分割も存在する．したがって，ATTC ルールにおいて，虚偽の選好表明により得られるバンドルの集合を $M$，財の隠蔽

により得られるバンドルの集合を $H$，名義の分割により得られるバンドルの集合を $S$ とすると，$H \subseteq M = S$ が成り立つ．

### 6.3 計算複雑性と効用の増加

本節では，虚偽の選好表明と同様，自身の効用を増加させる財の隠蔽と名義の分割の計算複雑性について議論する．

定理 2 より，P $\neq$ NP ならば，自身の効用を増加させる選好を求める問題を解く多項式時間アルゴリズムは存在しない．また，定理 5 より，任意の名義の分割 $s_i$ に関して，$s_i$ と等価な結果を得る選好順序 $R_i'$ が存在し，かつ，$R_i'$ は多項式時間で計算可能である．したがって，名義の分割に関しても以下が成り立つ: P $\neq$ NP ならば，自身の効用を増加させる名義の分割を求める問題を解く多項式時間アルゴリズムは存在しない．自身の効用を増加させる財の隠蔽に関しても，P $\neq$ NP ならば，そのような財の隠蔽を求める問題を解く多項式時間アルゴリズムは存在しないと考えている．

財の隠蔽／名義の分割による効用の増加に関して，定理 4, 5 より，虚偽の選好表明による効用の増加の限界を超えることはできない．したがって，定理 3 より，不正行為を行わない場合に得られる最も好む財を $k$ として，いかなる財の隠蔽／名義の分割を行っても，$k$ より好む財を得ることはできない．

## 7 結論

本論文では，参加者が複数の非分割財を保有し，辞書式選好順序を持つ交換問題に適用可能な交換ルールを提案した．提案ルールは個人合理性とパレート効率性を満たし，多項式時間で計算可能であることを示した．また， P $\neq$ NP ならば，提案ルールに関して，参加者の効用を増加させる虚偽の選好を求める多項式時間アルゴリズムは存在しないことを示した．さらに，真の選好表明により得られる最も好む財を $k$ とするとき，いかなる虚偽の選好表明を行っても $k$ より好む財を得ることはできないことを示した．初期保有バンドルが私的情報であり，交換ルールが真の参加者の集合を知ることができない場合，財の隠蔽や名義の分割といった不正行為が考えられるが，これらの不正行為に対してもほぼ同様の結果が得られることを示した．

以下に今後の課題を述べる．本論文で提案した交換ルールは，辞書式選好順序ドメインのもとで，個人合理性とパレート効率性を満たし，多項式時間で計算可能であるが，そのような交換ルールは唯一ではない．したがって，提案した交換ルールの特徴付けが挙げられる．提案した交換ルールの特徴付けを与えるために，提案した交換ルールの持つ他の社会的に優れた性質を解明する必要がある．また，文献 [4, 3] により提案された巨大市場の解析に基づいて，提案した交換ルールに対して不正行為を行う誘因を持つ参加者の割合の平均を評価することも重要であると考えている．

## 謝辞

本研究の遂行にあたり，日本学術振興会科学研究費補助金基盤研究 (S) (課題番号 24220003) の助成を受けました．ここに深く感謝致します．また，非常に有益なコメントを下さった電子情報通信学会 情報・システムソサイエティ人工知能と知識処理（AI）の 2 名の査読者に深く感謝致します．

## 参考文献

[1] Bart de Keijzer, Sylvain Bouveret, Tomas Klos, and Yingqian Zhang. On the complexity of efficiency and envy-freeness in fair division of indivisible goods with additive preferences. In *ADT*, pp. 98–110, 2009.

[2] E Mark Gold. Complexity of automaton identification from given data. *Information and Control*, Vol. 37, No. 3, pp. 302 – 320, 1978.

[3] Nicole Immorlica and Mohammad Mahdian. Marriage, honesty, and stability. In *SODA*, pp. 53–62, 2005.

[4] Fuhito Kojima and Parag A. Pathak. Incentives and stability in large two-sided matching markets. *American Economic Review*, Vol. 99, No. 3, pp. 608–27, June 2009.

[5] Jinpeng Ma. Strategy-proofness and the strict core in a market with indivisibilities. *International Journal of Game Theory*, Vol. 23, No. 1, pp. 75–83, 1994.

[6] ポール・ミルグラム．オークション 理論とデザイン．東洋経済新報社, 2007.

[7] Maria Silvia Pini, Francesca Rossi, K. Brent Venable, and Toby Walsh. Manipulation complexity and gender neutrality in stable marriage procedures. *Autonomous Agents and Multi-Agent Systems*, Vol. 22, No. 1, pp. 183–199, January 2011.

[8] Daniela Saban and Jay Sethuraman. A note on object allocation under lexicographic preferences. *Journal of Mathematical Economics*, Vol. 50, No. 0, pp. 283 – 289, 2014.

[9] 坂井豊貴, 藤中裕二, 若山琢磨．メカニズムデザイン – 資源配分制度の設計とインセンティブ．ミネルヴァ書房, 2008.

[10] Lloyd Shapley and Herbert Scarf. On cores and indivisibility. *Journal of Mathematical Economics*, Vol. 1, No. 1, pp. 23–37, 1974.

[11] Tayfun Sönmez. Strategy-proofness and essentially single-valued cores. *Econometrica*, Vol. 67, No. 3, pp. 677–689, 1999.

[12] 横尾真. オークション理論の基礎 –ゲーム理論と情報科学の先端領域–. 東京電機大学出版局, 2006.

[13] Makoto Yokoo, Yuko Sakurai, and Shigeo Matsubara. The effect of false-name bids in combinatorial auctions: New fraud in internet auctions. *Games and Economic Behavior*, Vol. 46, No. 1, pp. 174–188, 2004.