局所的にAND構造を持つ位数3の可換半群の分類証明とカードベースプロトコルへの適用

須賀 祐治[1,a)]

概要：2 者間の AND 演算によるマッチングはカードベースプロトコルにおける一般的なアプリケーションであり，気まずくならない告白ができることが知られている．2 者間の秘密計算によって AND 演算出力が 0 である場合，入力が 0 だったのか 1 だったのかを秘匿できる意味で，相手に入力がバレないことから気まずくならないとされている．
本稿は 0,1 という 2 択の入力を持つ通常の AND 演算を拡張し，0 でも 1 でもない第 3 の値「不定」を入力可能な拡張 AND プロトコルを考える．プロトコルの連続性を考えると推移律を満たすように設計したほうがよく，実際には位数 3 の半群の分類問題を扱う必要がある．局所的に AND 構造を持つように制約条件を設けて完全分類を試み，自明な例と同型を除いて 7 つに集約できることが分かった．これらには Bochvar や Lukasiewicz による 3 値論理の事例も含まれている．さらに，この分類の中から現時点で考案されているカードベースプロトコルへの事例についても取り上げる．構成例は裏面の識別不可能性を持つ同一カードを用いており，一般的なエンコーディングルールとは異なるカードプロトコルである．

キーワード：カードベースプロトコル，非コミット型プロトコル, Five Card Trick, 可換半群

A classification proof for commutative three-element semigroups with local AND structure and its application to card-based protocols

Yuji Suga[1,a)]

Abstract: The matching situation with AND operations between two parties is a common application in card-based protocols, and it is known to provide a non-embarrassing confession of love. This means that the other party does not know whether the input was 0 or 1, which is said to avoid embarrassment. In this paper, we consider an extended AND protocol that extends the usual AND operations with two input choices, 0 and 1, to allow the input of a third value, "indefinite," which is neither 0 nor 1. Considering the continuity of the protocols, it is better to design it to satisfy the transitivity law, and in practice, we need to deal with the classification of three-element semigroups. We attempted a complete classification with restrictions to have a local AND structure, and found that except for trivial examples and considerations of the algebraic isomorphism, we could reduce the classification to only seven cases. These include cases of three-valued logic by Bochvar and Lukasiewicz respectively. We also discuss some examples applied to the card-based protocols that have been devised. The examples are based on the same pattern cards with indistinguishability on the backside, which is another card protocol different from the general encoding rules.

Keywords: Card-based protocols, Non-committed protocols, Five Card Trick, Commutative semigroups

1. はじめに

カードベースプロトコルのうち非コミット型のプロトコルを扱う．一般的なカードベース暗号では 1 ビット入力を

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan
[a)] suga@iij.ad.jp

2 種類 2 枚のカードが用いられる [1]．例えば，ユーザによる 1 ビット入力は以下の一般的なエンコーディングルールに従う：$\boxed{\clubsuit}\boxed{\heartsuit}=0$, $\boxed{\heartsuit}\boxed{\clubsuit}=1$.

出力がコミット型であるとは，プロトコル停止時に得られる結果が，入力のエンコーディングルールに基づいた形式であることを指す．一方で非コミット型であるとは，プロトコル停止時に利用されたカードを開示するなどして結果を得る方式である．

さらに本稿の制約として，上記のようなスートのみが記載されたカードではなく，表面裏面ともに全く同じ絵柄であるカード（例えば名刺や麻雀牌）を用いることを考える（文献 [2] において水木らは絵柄の上下関係を生かしたメリットとデメリットについて考察されている）．このときカードの上下配置の違いを用いて，それぞれ（一般的なカードプロトコルで用いられる）異なるスートと対応づけることができる．つまり $\boxed{\downarrow}$を $\boxed{\clubsuit}$と，$\boxed{\uparrow}$を $\boxed{\heartsuit}$と同一視することもできる．スートを表現するメモ書きをしないでも，同一カードの束を用いてプロトコルを構成することができる点も一つのメリットである．

同一カード利用のメリットでもありデメリットとしては，各プレイヤー（プロトコルに入力するユーザ）に配布されるカードから入力できるバリエーションが拡がる点が挙げられる．例えば Five Card Trick や SCIS2022 で提案された 3 値入力可能な拡張 Five Card Trick では 2 枚のカードを配布することとなる．このとき，オリジナルの Five Card Trick では $\boxed{\clubsuit}\boxed{\heartsuit}=0$, $\boxed{\heartsuit}\boxed{\clubsuit}=1$ の 2 通りの入力のみが可能であるが，拡張版では同一カード 2 枚を用いて $\boxed{\downarrow}\boxed{\downarrow}$, $\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\downarrow}$, $\boxed{\uparrow}\boxed{\uparrow}$の 4 通りの入力が可能となる．これは大きなメリットではあるが，一方でエンコーディングルールを逸脱した入力が可能であることが指摘されており [16]，入力を制御する（例えば 4 つのバリエーションから 3 つに制限する）その他の施策が必要となっている．

1.1 本稿の貢献

裏面の識別不可能性を持つ同一カードを用いるカードプロトコルにおいて，特に 3 値入力可能な拡張 Five Card Trick が実装可能な代数的構造について着目する．具体的には Bochvar の 3 値論理や Lukasiewicz の 3 値論理における実装 [15] のベースとなった位数 3 の可換半群で，かつ AND 演算の構造を局所的に持つ可換半群の分類とその証明を与える．ビルディングブロックとして 2 者間の拡張 AND 演算プロトコルを用い非コミットメント型ではなくコミットメント型にいずれ移り変わることを想定すると，複数のプロトコルを連続して実行することが望まれる．そのため演算としては推移律を満たす必要があることから．可換半群を取り扱うこととなる．

2. 実装可能な非コミットメント型カードプロトコルの事例

出力がコミット型であるとは，プロトコル停止時に得られる結果が，入力のエンコーディングルールに基づいた形式であることを指す．一方で非コミット型であるとは，プロトコル停止時に利用されたカードを開示するなどして結果を得る方式である．

2.1 オリジナル Five-Card Trick

2 ユーザによる非コミットメント型として知られる Five-card trick [3] はハートとクラブ 2 種類のカードが用いられている．

Five-card trick は 2 ユーザ間で AND 演算を行うプロトコルである．2 入力を $a,b\in\{0,1\}$ としたとき $\boxed{?}\boxed{?}(=\bar{a})$ $\boxed{\heartsuit}$ $\boxed{?}\boxed{?}(=b)$ として 5 枚のカードを並べてランダムカット（巡回置換を c_5 としたとき，恒等置換 id と c_5, c_5^2, c_5^3, c_5^4 の 5 通りから等確率で選択してカード束に処理する操作）を行う．ここで $\boxed{?}$は裏面にして入力したことを示しており $\bar{a}$ は a の否定 (negation) である．

ランダムカットを行う際には中央の $\boxed{\heartsuit}$も $\boxed{?}$とし，5 枚とも裏面に向けてシャッフルする．出力は 5 枚のカードをすべて開示することで得られる．3 枚の $\boxed{\heartsuit}$が連続して並んで出力されたとき $a\wedge b=1$，それ以外は $a\wedge b=0$ となる．以下は 5 枚のカードの初期状態を示しており，これらの 5 枚のカードが巡回置換によりシャッフルされることから，出力時に 3 枚の $\boxed{\heartsuit}$が連続して並んでいる場合のみが $a\wedge b=1$ となることが分かる．さらに，$a\wedge b=0$ となる 3 つのケースについてはすべて同一視されるため，出力だけを見ても入力 a,b がどのような値だったかについて認識できない点が本プロトコルのポイントである．

(a,b)	sequence
(0,0)	♡ ♣ ♡ ♣ ♡
(0,1)	♡ ♣ ♡ ♡ ♣
(1,0)	♣ ♡ ♡ ♣ ♡
(1,1)	♣ ♡ ♡ ♡ ♣

表 1 Five-Card Trick 初期入力状態

Five-Card Trick は，カード入力時の一般置換（このケースでは b を入力の際にカードを倒置して置いているため 5 枚のカード全体として $\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}$ の置換を行っていると考える）とランダムカットのみで構成されるシンプルなプロトコルである．

2.2 上下シャッフルの導入と Three Card Trick

Five Card Trick と同様に 2 者の AND 演算プロトコルを考える．一般的なカードプロトコルにおいては 2 種類のスート各 1 枚の計 2 枚が配布され，2 枚のカードで 1 ビットを表現する．そのため配布される最小枚数は 2 枚である．一方で，表面裏面ともに全く同じ絵柄であるカードを用いる場合には 1 枚のカードを上下関係，つまり 2 種類の方向 $\boxed{\downarrow}\boxed{\uparrow}$で入力可能なことから 1 ビットを 1 枚で表現可能である．そのため配布される最小枚数は 1 枚であり，1 枚のカードを配布した際の AND プロトコルが構成できれば，枚数としては optimal な方式であると言える．

例えば$\boxed{\downarrow}$= 0, $\boxed{\uparrow}$= 1 というエンコーディングルールを適用しようとする場合 5 Card Trick のような入力，つまり真ん中のエクストラカードを $\boxed{\uparrow}$とし，両側から各ユーザが a, b 1 枚ずつの裏面入力を行うと初期状態として以下のような配置となる．仮にこれを Three Card Trick と呼ぶこととする．

(a, b)	sequence
(0,0)	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$
(0,1)	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$
(1,0)	$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$
(1,1)	$\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$

表 2 Three-Card Trick 初期入力状態

Five Card Trick と同じように入力を撹乱するため 3 枚カードをランダムカットのカード処理を行うが，出力時には $a \wedge b = 1$ のときのみ エクストラカードを含めて $\boxed{\uparrow}$が 3 枚並んでいることが分かる．一方で Five Card Trick において $a \wedge b = 0$ となる 3 つのケースはすべて同一視できていたが表 2 のように $\boxed{\uparrow}$となるカードの枚数が異なることから同一視できず，このままでは入力 a, b を秘匿できない．

そのため次のテクニックを用いる．アイデアとしてはランダム 2 等分カット [5] を勘弁に実装する方式で用いられている方式によく似通っており，上下関係をランダムに入れ替えること（この操作を上下シャッフルと呼ぶ）を考える．ひとつの方法としてはランダムカット後のカード束にさらにエクストラカード 1 枚を用いて 3 枚のカードのうちの 1 枚めの表面を秘匿し，放り投げる等して上下関係を入れ替えた後にエクストラカードを抜き去るという方式が考えられる．ここは様々な実装方式があると考えるが，いずれにせよ上下シャッフルは $\boxed{\downarrow}$と $\boxed{\uparrow}$が入れ替わることを意味しており Three Card Trick では以下のように初期入力状態が変化することとなる．

表 2 と 表 3 の状態をすべて見比べたとき，ランダムカット→上下シャッフル後の状態は $\boxed{\uparrow}$となるカードが 0,1,2,3 枚のいずれかとなり，$a \wedge b = 1$ のときは $\boxed{\uparrow}$が 0,3 枚の

(a, b)	sequence
(0,0)	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$
(0,1)	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$
(1,0)	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}$
(1,1)	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$

表 3 Three-Card Trick にて上下シャッフル後の初期配置

いずれかである．さらに $a \wedge b = 0$ のときは $\boxed{\uparrow}$が 1,2 枚であり，かつ 入力 a, b が秘匿された状態で出力を得ることができる．つまり $\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$, $\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$の 6 通りはすべて同一視されることから本プロトコルの安全性（入力の秘匿性）を確保していることが分かる．また，Three Card Trick は入力カード枚数として optimal な AND 演算プロトコルを実現していることが分かる．

同一視できる 3 枚組に関して以下のタイプに分類することができる．

Type	同一視されるカード組
2	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$, $\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$
3	$\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$, $\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$

表 4 ランダムカット→上下シャッフル後の分類（3 枚組）

Type 名は上下シャッフルによる操作を含め「何枚 $\boxed{\uparrow}$ カードが連続するか」最大の値を示す．例えば$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$は上下シャッフル（180 度回転）によって$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$となることから Type-2 にカテゴライズされる．また，$\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$は上下シャッフルにより $\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$と同一視されることから Type-3 に分類される．

3. 3 値入力と 3 値論理

Five-Card Trick に限らずカードベースプロトコルの多くは 2 値 True(1), False(0) を入力することが想定されている．例えば 2 人による AND プロトコルは「気まずくならない告白」ができるとされており，実際プレーヤー A が True を入力して False という結果を得たとしても，相手のプレイヤー B には A が True を入力したことがバレることがない，という側面で気まずくならない点を保証している．

このようなシチュエーションを考えた場合，果たしてプレイヤーは 0 か 1 の 2 つの選択しか認めないのであろうか．相手に好意を寄せているのかどうかは 2 値ではなく，中間的な気持ちである「どちらでもない」「自分の気持ちが分からない」を排除してよいのか，という課題を考える [14]．そこでカードプロトコルにおいて 0 でも 1 でもない第 3 の値を入力できるようにすることが可能にする．

3.1 3 値論理のバリエーション

第 3 の値を入力するとして 入力 a, b に対して $a \wedge b$ の真偽表としてどれを用いるかという問題を考える．従来の 2 値論理における AND 真偽表は以下となる．

$a\backslash b$	0	1
0	0	0
1	0	1

これに対して第 3 の値 θ を入れた際に様々な考え方が存在する．一例として，より代数的な考慮に基づいた Lukasiewicz の 3 値論理における AND 真偽表は以下となる．

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	θ
1	0	θ	1

0, 1 をそれぞれ体におけるゼロ元，単位元として考えたときのストレートフォワードな方式である．特に $\theta^2 = \theta$ を満たすように構成されている点に留意する．Kleene による 3 値論理においても AND 演算に関しては同じ真偽表を持つことが知られている．

次に Bochvar の 3 値論理における AND 真偽表を示す．

$a\backslash b$	0	θ	1
0	0	θ	0
θ	θ	θ	θ
1	0	θ	1

オリジナル Five Card Trick で実現される AND 演算プロトコルでは「気まずくならない告白」が実現されるが，さらに「気持ちが揺らいでいる」ことも分かる，という観点で，ゲーム理論の側面としても面白い構造を持っていることが分かる．具体的には a または b のどちらかが θ を入力しただけで AND 演算の結果が θ となる点が面白い．しかし，これは秘密計算としては条件をバイオレーションしており，例えばプレイヤー A の入力が 0 または 1 のときには，マッチングがうまくいかない場合，プレイヤー B にその入力を秘匿することができるが，θ を入力してしまうと，入力が漏れてしまう．本稿ではこれをセキュリティ要件を満たさないという立場ではなく，このリスクを許容してプレイヤーは入力することを前提とする，という立ち位置で議論していく．

4. 位数 3 の可換半群の分類

ビルディングブロックとして 2 者間の拡張 AND 演算プロトコルを用い，複数のプロトコルを連続して実行することを想定すると，この拡張演算は推移律を満たす必要がある．さらに AND 演算は可換であることから，位数 3 の可換半群がここで扱うべき対象となる．計算機による数え上げではなく手による証明を試みる．そのうち，以下のような自明な事例のように全く同じ挙動となる状況については「自明」として扱い，分類からは排除する方針とする．

AND-$(0,0,0)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	0	0
1	0	0	1

上記例では θ は 1 に対して 0 と全く同じ演算結果になることから自明な例として分類表からは排除する．

分類の方針としては，半群は可換であることから（AND 演算は可換であるから）以下のように AND-(a,b,c) s.t $a, b, c \in 0, 1, \theta$ の真偽表が存在するかどうかについて証明することとなる．

AND-(a,b,c):

$a\backslash b$	0	θ	1
0	0	a	0
θ	a	b	c
1	0	c	1

4.1 AND-$(0,0,c)$ の存在性

$b = \theta^2 = 0$ であることから $c^2 = (1 \cdot \theta)^2 = 0^2 \cdot \theta^2 = 0 \cdot 0 = 0$ となる．そのため $1 \cdot \theta = 0$ または $1 \cdot \theta = \theta$ となる．前者は

AND-$(0,0,0)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	0	0
1	0	0	1

となり自明な事例．後者は

AND-$(0,0,\theta)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	0	θ
1	0	θ	1

となり，半群を満たす．実際
$(1 \cdot \theta) \cdot 0 = \theta \cdot 0 = 0, 1 \cdot (\theta \cdot 0) = 1 \cdot 0 = 0$
と矛盾がない．

4.2 AND-$(\theta, 0, c)$ の存在性

前節と同様の議論で $1 \cdot \theta = 0$ または $1 \cdot \theta = \theta$ となる．前者は $(1 \cdot \theta) \cdot 0 = 0 \cdot 0 = 0$, $1 \cdot (\theta \cdot 0) = 1 \cdot \theta = 0$ と，ここでは矛盾がないが，$a \cdot c = (0 \cdot \theta) \cdot (1 \cdot \theta) = (0 \cdot 1) \cdot \theta^2 = 0 \cdot b$ であるから $a \cdot c = (0 \cdot \theta) \cdot (1 \cdot \theta) = \theta \cdot 0 = \theta$, $a \cdot c = 0 \cdot b = 0$ となり矛盾する．

後者は半群の条件を満たし

AND-$(\theta, 0, \theta)$:

$a\backslash b$	0	θ	1
0	0	θ	0
θ	θ	0	θ
1	0	θ	1

は半群である．

4.3 AND-$(1, 0, c)$ の存在性

前節と同様の議論で $1 \cdot \theta = 0$ または $1 \cdot \theta = \theta$ となる．前者は $(1 \cdot \theta) \cdot 0 = 0 \cdot 0 = 0$, $1 \cdot (\theta \cdot 0) = 1 \cdot 1 = 1$ と矛盾する．また $a \cdot c = (0 \cdot \theta) \cdot (1 \cdot \theta) = (0 \cdot 1) \cdot \theta^2 = 0 \cdot b$ であるから後者は $a \cdot c = (0 \cdot \theta) \cdot (1 \cdot \theta) = 1 \cdot \theta = \theta$, $a \cdot c = 0 \cdot b = 0$ となり矛盾する．つまり AND-$(1, 0, c)$ は存在しない．

4.4 AND-$(0, \theta, c)$ の存在性

同様に議論すると全ての c に対して半群となることが分かった．

AND-$(0, \theta, 0)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	0
1	0	0	1

AND-$(0, \theta, \theta)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	θ
1	0	θ	1

AND-$(0, \theta, 1)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	1
1	0	1	1

4.5 AND-(θ, θ, c) の存在性

同様に

のみが半群となる．

AND-(θ, θ, θ):

$a\backslash b$	0	θ	1
0	0	θ	0
θ	θ	θ	θ
1	0	θ	1

4.6 AND-$(1, \theta, c)$ の存在性

同様に議論すると AND-$(1, \theta, c)$ は存在しない．

4.7 AND-$(0, 1, c)$ の存在性

同様に議論すると

AND-$(0, 1, \theta)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	1	θ
1	0	θ	1

は半群であるが，以下は半群の条件を満たすが自明な例となる（θ が 0 に対して 1 と同様の役割であるため）．

AND-$(0, 1, 1)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	1	1
1	0	1	1

4.8 AND-$(\theta, 1, c)$ の存在性

同様に議論すると $c^2 = (1 \cdot \theta)^2 = 1\dot{1} = 1$ であるため $c = \theta$ または $c = 1$ となるが両方とも矛盾するため AND-$(\theta, 1, c)$ は存在しない．

4.9 AND-$(1, 1, c)$ の存在性

同様に議論すると $c^2 = (1 \cdot \theta)^2 = 1\dot{1} = 1$ であるため $c = \theta$ または $c = 1$ となるが両方とも矛盾するため AND-$(1, 1, c)$ は存在しない．

以上の議論により全ての a, b, c に対して可換半群の存在性証明を与えることとなった．結果として自明なものを除外して 7 種類に分類することができることが分かった．

5. 分類結果とカードプロトコルの実装について

前章の証明により位数 3 で局所的に AND 構造を持つ可換な半群は以下の 7 種類に分類することができることが分かった.

AND-$(0,0,\theta)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	0	θ
1	0	θ	1

AND-$(\theta,0,\theta)$:

$a\backslash b$	0	θ	1
0	0	θ	0
θ	θ	0	θ
1	0	θ	1

AND-$(0,\theta,0)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	0
1	0	0	1

AND-$(0,\theta,\theta)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	θ
1	0	θ	1

AND-$(0,\theta,1)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	1
1	0	1	1

AND-(θ,θ,θ):

$a\backslash b$	0	θ	1
0	0	θ	0
θ	θ	θ	θ
1	0	θ	1

AND-$(0,1,\theta)$:

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	1	θ
1	0	θ	1

5.1 AND-$(0,\theta,\theta)$ の実装

SCIS2022 にて AND-$(0,\theta,\theta)$, AND-$(\theta,0,\theta)$, AND-$(0,0,\theta)$ の 3 方式について Five Card Trick と同様な操作で実装できることが示されている．ここでは特に AND-$(0,\theta,\theta)$ の実装について述べる．

エンコーディングルールとして以下を適用する：$\boxed{\downarrow}\boxed{\uparrow}=0$, $\boxed{\uparrow}\boxed{\downarrow}=\theta$, $\boxed{\downarrow}\boxed{\downarrow}=1$. このとき真ん中にエクストラカード $\boxed{\uparrow}$を置いてその左側に a の negation, 右側に b を入力した場合，バリエーションとして表 5 の 9 パターンが得られる．ここで negation は左右を入れ替えたカードを入力することとする．Five Card Trick では 補数の入力を意味していたが，Five Card Trick においても negation は 2 枚のカードの左右を入れ替える操作と考えれば全く同じ操作であると考えることができる．

(a,b)	sequence
(0,0)	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$
(0,1)	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$
(1,0)	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$
(1,1)	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$
$(0,\theta)$	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$
$(\theta,0)$	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$
$(1,\theta)$	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$
$(\theta,1)$	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$
(θ,θ)	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$

表 5 AND-$(0,\theta,\theta)$ 実装の初期状態

このときランダムカットと上下シャッフルと行うことにより $(a,b)=(1,1)$ のときのみ $\boxed{\uparrow}$が 1 または 4 枚のパターンが現れる．また $(a,b)=(\theta,\theta),(\theta,1),(1,\theta)$ の場合 $\boxed{\uparrow}$または $\boxed{\downarrow}$が 3 枚連続現れ，これらの 3 パターンは全て同一視される．さらにそれ以外の 5 パターンは例えば $\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$等が現れ，この形式がランダムカットと上下シャッフルした状態のいずれかに一致するため同一視される．

このことから注意深く分類すると

$a\backslash b$	0	θ	1
0	0	0	0
θ	0	θ	θ
1	0	θ	1

という真偽表が得られることから Five Card Trick に上下シャッフル操作を追加するだけで AND-$(0,\theta,\theta)$ を実装できることが分かる．

表 4 と同様に，ランダムカット→上下シャッフル後の分類を行うと以下となる．

タイプ	同一視されるカード組
2	↑↓↑↓↓, ↓↑↓↓↑, ↑↓↓↑↓, ↓↓↑↓↑, ↓↑↓↑↓, ↓↑↑↓↑, ↓↑↓↑↑, ↑↓↑↑↓, ↑↓↓↑↓, ↑↑↓↑↓, ↑↓↑↓↑, ↑↑↓↓↓, ↑↓↓↓↑
3	↓↓↓↑↑, ↓↓↑↑↓, ↓↑↑↓↓, ↑↑↑↓↓, ↑↑↓↓↑, ↑↓↓↑↑, ↓↓↑↑↑, ↓↑↑↑↓, ↑↑↓↑↑, ↑↓↑↑↑
4	↓↓↓↓↑, ↓↓↓↓↓, ↓↓↑↓↓, ↓↑↓↓↓, ↑↓↓↓↓, ↑↑↑↑↓, ↑↑↑↓↑, ↑↑↓↑↑, ↑↓↑↑↑, ↓↑↑↑↑

表 6 ランダムカット→上下シャッフル後の分類（5 枚組）

タイプ 5 に分類される↑↑↑↑↑, ↓↓↓↓↓は出現せず，上記のように $2^5 - 2 = 30$ 通りが出現することとなる．

さきほどの真偽表にて上記タイプ（3,4,5 のいずれか）を当てはめると以下となる．ただし a の入力としては negation を表記している，つまり実際のカード入力であることに注意する．

$\overline{a}\backslash b$	↓↑	↑↓	↓↓
↑↓	Type-2	Type-2	Type-2
↓↑	Type-2	Type-3	Type-3
↓↓	Type-2	Type-3	Type-4

表 7 AND-$(0, \theta, \theta)$ 実装のタイプ分類

出現として Type-2 が 出力 0, Type-3 が出力 θ, Type-4 が出力 1 に該当することが分かる．

6. まとめと今後について

本稿は 0,1 という 2 択の入力を持つ通常の AND 演算を拡張し，0 でも 1 でもない第 3 の値「不定」を入力可能な拡張 AND プロトコルを考えるにあたり，プロトコルの連続性を考えて推移律を満たすように設計するため，位数 3 の半群の分類問題を扱った．局所的に AND 構造を持つように制約条件を設けて完全分類を試み，自明な例と同型を除いて 7 つに集約できることが分かった．これらには Bochvar や Lukasiewicz による 3 値論理の事例も含まれている．

代数的に良い構造をもつ 3 つの半群（AND-$(0, \theta, \theta)$, AND-$(\theta, 0, \theta)$, AND-$(0, 0, \theta)$）に対してほぼ Optimal と考えられるカードプロトコルが提示されており，十分簡便な実装が実現可能であることも分かった．

Open problems としてそれら以外の 4 つの半群に対して，利用するカード枚数などの指標を用いて，よりよい実装が可能かどうかについて提示しておく．拡張 Five Card Trick では 2 名のプレイヤーにそれぞれ 2 枚のカードを配布しエクストラの 1 枚を加えた 5 枚で実装可能である．この方式に近い形で実装が可能であれば新しい結果として歓迎されると考えられる．

参考文献

[1] 水木, 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 2016 年 9 巻 3 号 pp.179-187, カード組を用いた秘密計算, https://www.jstage.jst.go.jp/article/essfr/9/3/9_179/_article/-char/ja
[2] T. Mizuki, H.Shizuya, Practical Card-Based Cryptography, FUN2014, pp.313-324, 2014.
[3] B. denBoer, More efficient match-making and satisability: the five card trick, EUROCRYPT'89, pp.208-217, 1989.
[4] T. Mizuki and H. Sone, Six-card secure AND and four-card secure XOR, International Workshop on Frontiers in Algorithmics, pp.358-369, 2009.
[5] T. Mizuki, M. Kumamoto and H. Sone, The Five-Card Trick Can Be Done with Four Cards, Asiacrypt2012.
[6] T. Nishida, Y. Hayashi, T. Mizuki and H. Sone, Card-based protocols for any boolean function, TAMC2015.
[7] I. Ueda, A. Nishimura, Y. Hayashi, T. Mizuki and H. Sone, How to implement a random bisection cut, The 5th International Conference on Theory and Practice of Natural Computing (TPNC2016), pp.58-69, 2016.
[8] K. Shinagawa, K. Nuida, T. Nishide, G. Hanaoka and E. Okamoto, Size-Hiding Computation for Multiple Parties, ASIACRYPT2016, 2016.
[9] S. Ruangwises, T. Itoh, Securely Computing the n-Variable Equality Function with 2n Cards, TAMC2020, 2020
[10] S. Ruangwises, T. Itoh, Physical Zero-Knowledge Proof for Numberlink Puzzle and k Vertex-Disjoint Paths Problem, New Generation Computing, 2020.
[11] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, Theoretical Computer Science, Volume 839, pp.135-142, November 2020.
[12] Y. Watanabe, Y. Kuroki, S. Suzuki, Y. Koga, M. Iwamoto, K. Ohta, Card-based majority voting protocols with three inputs using three cards, ISITA2018, pp.218–222, 2018.
[13] K. Shinagawa, K. Nuida, A single shufe is enough for secure card-based computation of any boolean circuit, Discrete Applied Mathematics, Vol.289, pp.248–261, 2021.
[14] 須賀, 0,1, 不定の 3 値入力が可能な AND 演算カードベースプロトコルの初期検討, 第 44 回情報理論とその応用シンポジウム (SITA2021), 4-3-3, 2021.
[15] 須賀, 3 値入力可能な可換半群の条件を満たす非コミットメント型 AND 演算拡張カードベースプロトコルの構成, SCIS2022, 2F4-2, 2022.
[16] 須賀, 3 値入力可能な Five Card Trick における第 4 の未定義値の扱いについて, 情報処理学会研究報告 Vol.2022-CSEC-96, 2022.