# Mining Pool 集合の代数的構造について

相　模　裕　一

## 序

現在，ブロックチェーン上のコンセンサス・アルゴリズムについては，PoW（Proof of Work），PoS（Proof of Stake），PoI（Proof of Importance），PoC（Proof of Consensus）等が用いられているが，それぞれメリット，デメリットを有する。ここでは，ビットコインに用いられている PoW について，検討を行うこととする。PoW については，計算量に要する消費電力が膨大であり社会的費用が高いことが大きな問題であるが，依然最も有効なアルゴリズムである。PoW の Mining 計算の競争ではハッシュパワーで勝敗が決せられるので，個人の PC（ノード）での参加でビットコインを取得することは不可能である。通常はグループ（Pool）に所属し，協働でマイニングを行っている。

ここではノードの数と Mining Pool の集合について Pool 間を移転する写像を構成し，ブロックチェーンのマイニングに関して代数的（群論）解析を行う。ここで PoW に関わる人数ではなくノードの数を扱うのは，１人で複数のノードを持つ場合があり，参加人数とノード数が一致しないからである。

Mining Pool 集合（族）については，より根源的な内的構造を見るために，ブロックチェーン上の群構造を分析することにする。ブロックチェーンの代数的分析では唯一 Dongfang Zhao［5］が発表されているが，ここでは群の生成と演算を変え，［5］とは異なる結論を得ている。

本稿の構成は以下の通りである。まず１節では，単純なケースを用いて PoW を行う Pool の集合に群構造を導入する。続く２節において，モデルを一般化する。３節ではシラーの定理より部分群の存在とその重要性を示し，ケーリーの定理より，ここで構成した群に同型の置換群（対称群）とりあげ，Stirling の定理より群の位数を求める。４節の最後において，PoS との関係について触れることにする。

## 1　単純なケース

まずここでは, 単純なケースについて説明しよう。ブロックチェーン上の３個のノードに対して，２個の Pool があるとする。C＝{$C_0$，$C_1$} を Pool の集合とする。３個のノードはそれぞれ Pool 移転写像（略して$\varphi$-map）を持っていると仮定しよう。$\varphi$-map については，以下のように定義しよう。

ノード１については，$\varphi_1(C_0)=C_0$，$\varphi_1(C_1)=C_1$と設定しよう。これはノード１は $C_0$ にいた場合は $C_0$に留まり，$C_1$にいた場合は $C_1$に留まることを意味する。ノード２については，$\varphi_2(C_0)=C_1$，$\varphi_2(C_1)=C_0$ ，ノード３については，$\varphi_3(C_0)=C_1$，$\varphi_3(C_1)=C_1$ と仮定する。これはノード２は，移転を必ず行い，ノード３は常に $C_1$を選択することを意味している。記号の簡略化を行い，ノード１の$\varphi_1(C_0)=C_0$を$\varphi_1(00)$，$\varphi_1(C_1)=C_1$ を$\varphi_1(11)$とする。同様にノード２は$\varphi_2(01)$，$\varphi_2(10)$，ノード３は$\varphi_3(01)$，$\varphi_3(10)$ としよう。３個のノードが $C_0$にいた場合を（000），ノード１が $C_1$，ノード２と３が $C_0$ にいた場合を（100）と記すことにする。すなわち，横ベクトルの第１要素をノード１の位置，第２要素をノード２の位置，第３要素をノード３の位置とする。上記の$\varphi$-map より，（000）は（011）となり，（100）は（111）へ移転することになる。

３ノードの所属する Pool の組合せ集合 C の要素は以下のように８ケースある。
C＝{（000）（100）（010）（001）（110）（101）（011）（111）} ここで，以下のような写像を考えよう。

$f:\mathrm{C}\to\mathrm{C}$　　$f=\langle\varphi_1(00),\ \varphi_1(11)|\varphi_2(01),\ \varphi_2(10)|\varphi_3(01),\ \varphi_3(10)\rangle$

ここで$f$は各ノードの０または１（$C_0$または $C_1$）における移転の組合せを示している。ノード$i$の$\varphi$-map は以下の行列で示される。第１要素は出発点，第２要素は移転先を表している。

$$\begin{bmatrix}\varphi_i(00) & \varphi_i(01)\\ \varphi_i(10) & \varphi_i(11)\end{bmatrix}\ i=1,2,3$$

$\Omega=\left\{f\middle|f:\mathrm{C}\to\mathrm{C}\right\}$　は写像の集合である。ここで以下のように写像の一般化を行う。

$f_{\langle 0i,\,1j|0k,\,1l|0m,\,1n\rangle}=\langle\varphi_1(0i),\ \varphi_1(1j)|\varphi_2(0k),\ \varphi_2(1l)|\varphi_3(0m),\ \varphi_3(1n)\rangle$

$i,j,k,l,m,n$ は０か１のいずれかを選択するので$2^6=64$個の写像が存在することになる。

そしてΩの２元$f_\alpha$と$f_\beta$について以下の演算⊗を定義すると，(Ω,⊗)は有限群となる。
$f_\alpha = f_{\langle 00,10|01,11|01,10\rangle} = \langle \varphi_1(00),\ \varphi_1(10)|\varphi_2(01),\ \varphi_2(10)|\varphi_3(01),\ \varphi_3(10)\rangle$ と
$f_\beta = f_{\langle 01,10|00,11|00,11\rangle} = \langle \varphi_1(01),\ \varphi_1(10)|\varphi_2(00),\ \varphi_2(11)|\varphi_3(00),\ \varphi_3(11)\rangle$ について
$f_\alpha \otimes f_\beta$ を以下のように定義する。

出発点を（000）とする。すなわち３つのノードが$C_0$に所属していたとする。まず$f_\alpha = f_{\langle 00,10|01,11|01,10\rangle}$ より $f_\alpha(000) = (011)$ となり，$f_\beta = f_{\langle 01,10|00,11|00,11\rangle}$ によって$f_\beta(011)=(111)$となる。すなわち $f_\beta \otimes f_\alpha(000) = (111)$となる。
$f_\beta \otimes f_\alpha = f_\gamma = f_{\langle 01,1j|01,1l|01,1n\rangle} \in \Omega$　なぜなら $f_\gamma(000) = (011)$

また，結合法則：$f_\alpha \otimes (f_\beta \otimes f_\gamma) = (f_\alpha \otimes f_\beta) \otimes f_\gamma$ は明らかである。
しかしながら，$f_\alpha \otimes f_\beta \neq f_\alpha \otimes f_\beta$ より，可換ではない。
ここで$f_e = f_{\langle 00,11|00,11|00,11\rangle}$とすると，任意の$f_\sigma \in \Omega$ に対して $f_\sigma \otimes f_e = f_e \otimes f_\sigma$
よって $f_e$は単位元となる。さらに，
任意の$f_\sigma \in \Omega$ に対して，$f_\sigma \otimes f_\tau = f_\tau \otimes f_\sigma = f_e$となる$f_\tau$の存在はあきらかである。
よって$f_\tau = {f_\sigma}^{-1}$ は，逆元となる。
以上のように，結合法則，単位元，逆元の存在によってΩは群（有限群）となる。

## ２　モデルの一般化

ここでモデルの一般化を試みる。

ブロックチェーン上に N 個のノードが存在し，K 個の Mining Pool があるとする。Mining Pool の集合族を C とする。
$C = \{C_0, C_1, C_2, \cdots, C_{K-1}\}$ となり，$C_0$は Mining Pool に所属しない単独のノードの集まりである。
Pool 移転写像（$\varphi$-map）は次のように拡張される。
$f_{\langle 0i_1, 1i_2, 2i_3 \cdots|0j_1, 1j_2 \cdots|\cdots\rangle} = \langle \varphi_1(0i_1),\ \varphi_1(1i_2),\ \varphi_1(2i_3)\cdots|\varphi_2(0j_1),\ \varphi_2(1j_2),\cdots|\cdots\rangle$
これを以下のように書き換える。N 個のノードの$\varphi$-map の組合せを以下のような写像で定義しよう。

$f_{\langle\overline{1},\overline{2},\cdots,\overline{N}\rangle} = \langle\overline{\varphi_1},\overline{\varphi_2},\cdots\overline{\varphi_N}\rangle$　ここで　$\overline{\varphi_m} = (\overline{\varphi_{m0}},\overline{\varphi_{m1}},\overline{\varphi_{m2}},\cdots,\overline{\varphi_{mk-1}})$ $m \in \{1,2,\cdots,N\}$

$\overline{\varphi_{m0}} = \big(\varphi_m(0i_1),\varphi_m(0i_2),\cdots,\varphi_m(0i_{k-1})\big)$

但し，$\varphi_m(0i_p)$は集合$\{\varphi_m(01),\varphi_m(02)\cdots,\varphi_1(0k-1)\}$から選択される 1 つの要素である。

以上より，ノード$i$ の$\varphi$-map は$k^k$ 個存在し，

集合$F = \left\{f_{\langle\overline{1},\overline{2},\cdots,\overline{N}\rangle}\middle| f_{\langle\overline{1},\overline{2},\cdots,\overline{N}\rangle} : \mathrm{C} \to \mathrm{C}\right\}$については$|F| = k^{kN}$となる。

上述の 3 ノード，2pool のケースと同様に演算⊗ を定義すると$(F,\otimes)$は群になることは明らかである。よって位数は$k^{kN}$となる。

## 3　同型な置換群，対称群について

ここで$k$について素因数分解をおこなうと $k = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$ となる。

$p_i$は素数で　$i < j$ に対して$p_i < p_j$ である。これより

$|F| = k^{kN} = p_1^{\alpha_1 kN} \times p_2^{\alpha_2 kN} \times \cdots \times p_r^{\alpha_r kN}$

これより，シローの定理より$k$が素数ならば，部分群は有さないが，$|F|$が$p_j^{\alpha_j kN}$の約数を持つとき，位数が$p_j^{\alpha_j kN}$の部分群をもつことなる。上述のように$p_1$から$p_r$の場合は，$r$個の部分群を有することを意味している。この部分群の存在は暗号生成問題に重要な示唆を与えていると思われる。またケーリーの定理より任意の（有限）群はある置換群$H$に同型であることより，$(F,\otimes) \cong H \subset S_n$となることが知られている。Dongfang Zhao［5］は，$H = S_{|F|}$としているが，これでは位数が大きくなりすぎてしまう。

$$S_{|F|} = (k^{kN})! \sim \sqrt{2\pi k^{kN}} \cdot \left(\frac{k^{kN}}{e}\right)^{k^{kN}}$$

ここで$k = 2,\ N = 3$ ならば

$|F| = 64$となるが，一方対照群$S_{|F|}$は Stirling's approximation より，

$$\left|S_{|F|}\right| \sim 2^3\sqrt{2\pi} \cdot \left(\frac{2^6}{e}\right)^{64} = \frac{8\sqrt{2\pi}}{e^{64}} \cdot 2^{384} = 1.12337073 \times 10^{89}$$ となる。

これは，$2^{295} = 6.365737426 \times 10^{88}$　　$2^{296} = 1.273147485 \times 10^{89}$　より

$2^{295} < \left|S_{|F|}\right| < 2^{296}$となる。よって$(F,\otimes)$を［5］のように対称群 $S_{|F|}$として分析するのは不可能である。$S_{|F|}$の元の動きに制約を付けた部分群として考える必要がある。問

題は$(F,\otimes)$と同型となるためにどのような制約を課すべきかである。すなわち$(F,\otimes) \cong H$となる部分群では以下のような制約が必要となる。

$H \cong \left\{\sigma \epsilon S_{|F|} \middle| \sigma(p) = p,\ \sigma(q) = q,\ \cdots,\ \sigma(z) = z\right\}$　ここで$p,\ q,\ \cdots,\ z$の個数を求めることが重要である。しかし，この方法では同型となる部分群を求めることは困難である。例えば上述の３ノード，2pool の場合$|S_4| < |F|(= \Omega) < |S_5|$となってしまう。しかしながらこの場合は$\varphi$-map の構成法に注視すれば以下のように簡単に求められることが分かる。

ノード１についての写像の集合上で構成される群は実は$S_2 \times S_2$と同型である。他の２，３のノードでも同様である。したがって　$F = \Omega \cong S_2 \times S_2 \times S_2 \times S_2 \times S_2 \times S_2$となることが分かる。

確かに$S_n$を同型として分析できることは，容易に正規化群や共役類，類別式を導出できる利点があるので，$(F,\otimes)$と同型になる制約条件を求めることは重要であり，今後の課題である。

## ４　PoS との関係について

ここで本稿の分析と他のコンセンサス・アルゴリズムとの関係について言及しておこう。PoW に対する批判として膨大な計算に伴う電力消費量の高さと認証時間の遅さ（10分間），そして１ブロックに収容される取引量が限定されていることである。（１秒間に最大７トランザクション，通常４トランザクション）さらに，Mining Pool が寡占状態で大手数社が大きなシェアをしめていることに対しても批判が起こっている。

それに対して，PoS は Proof of Stake の略ですなわち資産保有による証明である。コインの保有量と保有期間の掛け算で表される Coinage（コイン年数）が大きいノードほど，マイニングの計算が容易になっており，PoW のような高性能のコンピューター（マイニングマシーン）は不要で，電気代も膨大な高さにならないマイニングである。この PoS ではある一定以上のコインを有することが絶対条件で，コイン年数の高さがコインを増やす決め手となる。

ではこの PoS は前述の Pool 群においてはどのように表されるだろうか？ノード数 N に対して，コイン年数の多い順に番号を付し，１～n までは任意の$\varphi$-map となるが，n より大きいノードでは常に同じ値かデフォルト値に固定することになる。上述の３

ノード，2pool の場合ならば，ノード１と２のみがコイン年数が高いとすると，３ノードの$\varphi$-map は固定値を取ることにすればよい。よって，

$F = \Omega \cong S_2 \times S_2 \times S_2 \times S_2 \times S_2 \times S_2$は$F = \Omega \cong S_2 \times S_2 \times S_2 \times S_2 \times (00) \times (00)$となり，

$|F| = 16$　となる。

より一般的な$k = \alpha,\ N = \beta$についても，同様な議論が成立しよう。この Pool 群の位数は重要と思われる。それは P2P のコンセンサス・アルゴリズムの自由度の大きさを表している。リップルの PoI は，中央集権的証明によりノード$N$に対して，$k = 1$で$|F| = 1$となり Bitcoin の場合の最大値は$|F| = k^{kN}$となる。Pool数$k$の増大はハッシュパワーの指数的増大と消費電力を増大となるので，アナーキーシステムの最大のネックとなっている。

**参考文献**

[1] Julian Debus (2017) Consensus Methods in Blockchain Systems FSBC Working Paper
http://explore-ip.com/2017_Consensus-Methods-in-Blockchain-Systems.pdf
[2] Narayanan, A., Bonneau, J., Felten, E., Miller, A and Goldfeder, S (2016) BITCOIN AND CRYPTOCURERENCY TECHNOLOGIES Princeton University Press.
[3] Satoshi Nakamoto (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System
https://bitcoin.org/bitcoin.pdf
[4] Sothearath SEANG, Dominique TORRE (2008) “Proof of Work and Proof of Stake consensus protocols: a blockchain application for local complementary currencies.”
https://gdre-scpo-aix.sciencesconf.org/195470/document
[5] Dongfang Zhao (2020) “Algebraic Structure of Blockchains: A Group-Theoretical Primer”
https://arxiv.org/abs/2002.05973
[6] 浅野啓三・永尾汎（1965）『群論』岩波書店
[7] 松村英之（1990）『代数学』朝倉書店