A Proof Of Mashikov's Lemma

kai Onuma

2016 年 3 月 19 日

1 Preparation

定義 1.1 (準備)**.** 本稿では以下の記号を用いる.

- $\mathbb{N} = \{$ 自然数全体 $\}$
- $\mathbb{R} = \{$ 実数全体 $\}$
- $m \in \mathbb{N}$ について $[1, m] = \{1, 2, \ldots, m\}$
- 集合 A と $k \in [1, |A|]$ について $\binom{A}{k} = \{B \subset A \mid |B| = k\}$
- 集合 A, B について $A \setminus B = A \cap B^c$
- $r \in \mathbb{R}$ について $\lfloor r \rfloor = \max\{x \in \mathbb{N} \mid x \leq r\}$

定義 1.2. 集合 A, B について $f : A \to B$ を写像とする. このとき

- f が**単射**である $\iff$ $\forall x, y \in A, x \neq y$ について $f(x) \neq f(y)$
- f が**全射**である $\iff$ $\forall b \in B$ について $\exists a \in A$ s.t. $f(a) = b$
- f が**全単射**である $\iff$ f が単射かつ全射

次に写像に関する基本的な命題をあげておく.

命題 1.3. 集合 A, B について全射 $f : A \to B$ が存在するとき,

$$|A| \geq |B|$$

Proof. f, A について

$$f(A) = \{f(a) \mid a \in A\}$$

とすると $B \supset f(A)$, f が全射であることから $B \subset f(A)$ より $B = f(A)$ なので

$$\begin{aligned}
|B| &= |f(A)| \\
&= \left| \bigcup_{a \in A} \{f(a)\} \right| \\
&\leq \sum_{a \in A} |\{f(a)\}| \qquad (1) \\
&= \sum_{a \in A} 1 \\
&= |A|.
\end{aligned}$$

□

系 1.4. 集合 A, B について全単射 $f : A \to B$ が存在するとき,

$$|A| = |B|$$

Proof. 命題 1.3 の証明中の (1) 式の不等号を等号にすればよい. □

2 Mashikov Inequation

$A \subset \mathbb{N}$ について，

$$\mathrm{S}(A) = \sum_{x \in A} x$$

とし，また $X \subset \mathbb{N}, k \in [1, |X|]$ について，

$$\mathcal{M}(X, k) = \left\{ \mathrm{S}(A) \mid A \in \binom{X}{k} \right\}$$

とする．

命題 2.1. [Mashikov Inequation]
$X \subset \mathbb{N}, k \in [1, |X|]$ について

$$\mathrm{m}(X, k) = |\mathcal{M}(X, k)|$$

としたとき次の不等式が成立する．

$$\mathrm{m}(X, k) \leq \binom{|X|}{k}$$

この不等式を**マシコフ不等式 (Mashikov Inequation)** と呼び，

$$\text{マシコフ不等式において等号が成立} \iff S : \binom{X}{k} \to \mathcal{M}(X, k) \text{ が単射}.$$

Proof. $S : \binom{X}{k} \to \mathcal{M}(X, k)$ は全射なので不等式は明らか．以下，等号成立条件について証明する．
$(\Leftarrow)$ については，$S : \binom{X}{k} \to \mathcal{M}(X, k)$ が単射を仮定すると，$S : \binom{X}{k} \to \mathcal{M}(X, k)$ は全単射となるので成立．また，$\exists P, Q \in \binom{X}{k}, P \neq Q$ s.t. $S(P) = S(Q)$ を仮定すると，

$$\begin{aligned}
\mathrm{m}(X, k) &= |\mathcal{M}(X, k)| \\
&= \left| \left\{ \mathrm{S}(A) \mid A \in \binom{X}{k} \right\} \right| \\
&= \left| \left\{ \mathrm{S}(A) \mid A \in \binom{X}{k} \setminus \{Q\} \right\} \right| \\
&\leq \left| \binom{X}{k} \setminus \{Q\} \right| \\
&= \left| \binom{X}{k} \right| - |\{Q\}| \\
&< \binom{|X|}{k}
\end{aligned}$$

より，対偶をとれば

$$\mathrm{m}(X,k)=\binom{|X|}{k}\Rightarrow\forall A,B\in\binom{X}{k},A\neq B \text{ について } S(A)\neq S(B)$$
$$\Rightarrow S:\binom{X}{k}\to\mathcal{M}(X,k) \text{ が単射}$$

が示される．したがって，

$$\text{マシコフ不等式において等号が成立} \iff S:\binom{X}{k}\to\mathcal{M}(X,k) \text{ が単射}.$$

□

以下，$m\in\mathbb{N}$ について

$$X(m)\in\binom{\mathbb{N}}{m}$$

とする．

命題 2.2. $m\in\mathbb{N}$, $X(m)\in\binom{\mathbb{N}}{m}$ について，

$$m(X(m),\lfloor m/2\rfloor)=\binom{m}{\lfloor m/2\rfloor}\Rightarrow\forall k\in[1,m] \text{ について } \mathrm{m}(X(m),k)=\binom{m}{k}.$$

Proof. まず $k=l\leq\lfloor m/2\rfloor$ について証明する．$\mathrm{m}(X(m),l)=\binom{m}{l}$ が成立すると仮定する．$l-1<l$ より，$\exists t\in X(m)$ s.t. $t\in\binom{X(m)}{l}\setminus\binom{X(m)}{l-1}$．$\mathrm{m}(X(m),l-1)<\binom{m}{l-1}$ とすると，$\mathcal{M}(X(m),k)$ の定義より，$\exists A,B\in\binom{X(m)}{l-1}$ s.t. $A\neq B$,$\mathrm{S}(A)=\mathrm{S}(B)$．このとき，

$$\begin{aligned}\mathrm{S}(A\cup\{t\})&=\mathrm{S}(A)+t\\&=\mathrm{S}(B)+t\\&=\mathrm{S}(B\cup\{t\})\end{aligned}$$

$A\cup\{t\},B\cup\{t\}\in\binom{X(m)}{l}$ より $\mathrm{m}(X(m),l)<\binom{m}{l}$ となるため矛盾．よって $\mathrm{m}(X(m),l-1)=\binom{m}{l-1}$．したがって，帰納法により $\forall k\leq\lfloor m/2\rfloor$ について $\mathrm{m}(X(m),k)=\binom{m}{k}$．次に $k>\lfloor m/2\rfloor$ について証明する．$k=m$ の場合は明らかなので，$k=\lfloor m/2\rfloor+l$ $(l\in[1,m-\lfloor m/2\rfloor-1])$ とする．$A,B\in\binom{X(m)}{k}$,$A\neq B$ について $|X(m)\setminus A|=|X(m)\setminus B|=m-k=m-\lfloor m/2\rfloor-l\leq\lfloor m/2\rfloor$ であるため

$$\begin{aligned}\mathrm{S}(A)&=\mathrm{S}(X(m))-\mathrm{S}(X(m)\setminus A)\\&\neq\mathrm{S}(X(m))-\mathrm{S}(X(m)\setminus B)\\&=\mathrm{S}(B)\end{aligned}$$

A, B は任意であった．よって $k > \lfloor m/2 \rfloor$ について $\mathrm{m}(X(m), k) = \binom{m}{k}$.
したがって，

$$m(X(m), \lfloor m/2 \rfloor) = \binom{m}{\lfloor m/2 \rfloor} \Rightarrow \forall k \in [1, m] \text{ について } \mathrm{m}(X(m), k) = \binom{m}{k}$$

□

以下，$X(m) \in \binom{\mathbb{N}}{m}$ について，$\mathrm{m}(X(m), \lfloor m/2 \rfloor) = \binom{m}{\lfloor m/2 \rfloor}$ が成立しているとする．
$X \subset \mathbb{N}$ について

$$G(X) = \left\{ \mathrm{S}(A) - \mathrm{S}(B) \mid A \in \binom{X}{\lfloor |X|/2 \rfloor}, B \in \binom{X}{\lfloor |X|/2 \rfloor - 1} \right\}$$

と定義する．
このとき次の命題が成り立つ．

命題 2.3. $X(m)$, $t \in G(X(m)) \setminus X(m)$ について，

$$\mathrm{m}\left(X(m) \cup \{t\}, \left\lfloor \frac{m+1}{2} \right\rfloor \right) < \binom{m+1}{\lfloor \frac{m+1}{2} \rfloor}.$$

Proof. $t \in G(X(m))$ より，$\exists A \in \binom{X(m)}{\lfloor m/2 \rfloor}, \exists B \in \binom{X(m)}{\lfloor m/2 \rfloor - 1}$ s.t. $t = \mathrm{S}(A) - \mathrm{S}(B)$. A, B について $\mathrm{S}(A) = \mathrm{S}(B) + t$. $\lfloor m/2 \rfloor + \lfloor m/2 \rfloor < m + 1$ より，$\exists u \in X(m) \cup \{t\}$ s.t. $u \notin A \cup B \cup \{t\}$. このとき，

$$\begin{aligned} \mathrm{S}(A \cup \{u\}) &= \mathrm{S}(A) + u \\ &= \mathrm{S}(B) + t + u \\ &= \mathrm{S}(B \cup \{t, u\}). \end{aligned}$$

$A \cup \{u\}, B \cup \{t, u\} \in X(m) \cup \{t\}$ より，

$$\mathrm{m}\left(X(m) \cup \{t\}, \left\lfloor \frac{m+1}{2} \right\rfloor \right) < \binom{m+1}{\lfloor \frac{m+1}{2} \rfloor}.$$

□

系 2.4. $X(m)$ について，

$$\mathrm{m}\left(X(m) \cup \{v\}, \left\lfloor \frac{m+1}{2} \right\rfloor \right) = \binom{m+1}{\lfloor \frac{m+1}{2} \rfloor} \Rightarrow v \notin X(m) \cup G(m).$$

Proof. 命題 2.3 の対偶をとればよい． □

3 Mashikov's Lemma

補題 3.1. [Mashikov's Lemma]
$m \in \mathbb{N}$ にたいして，$k(m)$ を以下のように定義する．

- $k(1) = 1, k(2) = 2, k(3) = 3$
- $m > 3$ について $k(m) = \sum_{i=1}^{\lfloor m/2 \rfloor} k(m-i) - \sum_{j=1}^{\lfloor m/2 \rfloor - 1} k(j) + 1$

このとき $K(m) = \{k(i) \mid i \in [1, m]\}$ とすると，

$$\mathrm{m}(K(m), \lfloor m/2 \rfloor) = \binom{m}{\lfloor m/2 \rfloor}.$$

Proof. $m \leq 3$ については，$\mathrm{m}(K(m), \lfloor m/2 \rfloor)$ は明らか．$m \geq 3$ について $\mathrm{m}(K(m), \lfloor m/2 \rfloor)$ が成立するとする．このとき，

$$K(m+1) = K(m) \cup \{k(m+1)\}$$

であるが，

$$\begin{aligned}
k(m+1) &= \sum_{i=1}^{\lfloor \frac{m+1}{2} \rfloor} k(m+1-i) - \sum_{j=1}^{\lfloor \frac{m+1}{2} \rfloor - 1} k(j) + 1 \\
&= \max \left\{ S(A) \mid A \in \binom{K(m)}{\lfloor \frac{m+1}{2} \rfloor} \right\} - \min \left\{ S(B) \mid B \in \binom{K(m)}{\lfloor \frac{m+1}{2} \rfloor - 1} \right\} + 1 \\
&= \max G(K(m+1)) + 1
\end{aligned}$$

より

$$k(m+1) \notin G(K(m+1)).$$

したがって，命題 2.3 より，

$$\mathrm{m}\left(K(m+1), \left\lfloor \frac{m+1}{2} \right\rfloor \right) = \binom{m+1}{\lfloor \frac{m+1}{2} \rfloor}.$$

m についての帰納法により，全ての $m \in \mathbb{N}$ について

$$\mathrm{m}(K(m), \lfloor m/2 \rfloor) = \binom{m}{\lfloor m/2 \rfloor}.$$

□

例 3.2. $m = 10$ とすると，

$$K(10) = \{1, 2, 3, 5, 8, 14, 25, 47, 89, 173\}$$

であり，$\mathrm{m}(K(10), 5) = 252 = \binom{10}{5}$ となる．

4 Mashikov Problem

定義 4.1 (Mashikov Property). X が

$$\mathrm{m}(|X|, \lfloor |X|/2 \rfloor) = \binom{|X|}{\lfloor |X|/2 \rfloor}$$

を満たすとき，X は**マシコフ条件 (Mashikov Property)** をみたすという．また，

$$\mathcal{F}_M = \left\{ X \subset \mathbb{N} \mid \mathrm{m}(|X|, \lfloor |X|/2 \rfloor) = \binom{|X|}{\lfloor |X|/2 \rfloor} \right\}$$

で定義される $\mathcal{F}_M$ を**マシコフ族 (Mashikov Family)** とよぶ．

例 4.2. $\forall m \in \mathbb{N}$ において

$$\{2^i \mid i \in [1, m] \cup \{0\}\} \in \mathcal{F}_{\mathcal{M}}.$$

$m \in \mathbb{N}$ について $\mathcal{F}_M^{(m)} = \{A \in \mathcal{F}_M \mid |A| = m\}$ とする．

Mashikov Problem

$m \in \mathbb{N}$ について

$$\mu(m) = \min \left\{ \max X \mid X \in \mathcal{F}_{\mathcal{M}}^{(m)} \right\}$$

が存在するか確かめよ．存在する場合はその値を求めよ．

例 4.3. $m = 10$ のとき，例 3.2, 例 4.2 より

$$173 \in \left\{ \max X \mid X \in \mathcal{F}_{\mathcal{M}}^{(m)} \right\}$$
$$2^9 = 512 \in \left\{ \max X \mid X \in \mathcal{F}_{\mathcal{M}}^{(m)} \right\}.$$

例 4.4. 補題 3.1, 例 4.3 より $m \in \mathbb{N}$ について

$$m \leq \mu(m) \leq k(m)$$

が成り立つ．

2016 年 3 月時点で上記のマシコフ問題[*1]の結論は出ておらず，解決が急がれるところである．

[*1] 2016 年に **A.Mashikov** により $\mu(m) = 2^{m-1}$ と予想されていたが，例 4.2, 例 4.3 から分かる通り，$m > 2$ については誤りであることが知られている．