大阪薬科大学紀要 Vol. 14（2020 年 3 月 29 日発行）

ヒトが生成する置換の統計的性質 II

永田誠，　武井由智

Statistical properties of human-generated permutations II

Makoto Nagata[1)], Yoshinori Takei[2)]

[1)]*Osaka University of Pharmaceutical Sciences, 4-20-1, Nasahara, Takatsuki-shi, Osaka 569-1094, Japan*
[2)]*National Institute of Technology, Akita College, 1-1, Iijimabunkyocho, Akita-shi, Akita 011-8511, Japan*
(Received October 31, 2019; Accepted December 6, 2019)

– **Article** –

ヒトが生成する置換の統計的性質 II

永田 誠, 武井 由智

Statistical properties of human-generated permutations II

Makoto NAGATA[1)], Yoshinori TAKEI[2)]

[1)] *Osaka University of Pharmaceutical Sciences, 4-20-1, Nasahara, Takatsuki, Osaka 569-1094, Japan*
[2)] *National Institute of Technology, Akita College, 1-1, Iijimabunkyocho, Akita, Akita 011-8511, Japan*
(Received October 31, 2019; Accepted December 6, 2019)

Abstract We report a further analysis of the distributions of human-generated permutations we studied previously. In our previous study, a questionnaire was performed in which each of approximately 1000 participants was directed to generate randomly a permutation of degree 6, for each of 4 different ways of presenting a permutation. To characterize the resulting distributions, in this paper, we focus on several classes of permutations induced from arithmetic progressions modulo the degree of the permutation. It turns out that, for all the 4 different presentation ways, the number of the human-generated permutations that belong to a specific class of permutations induced from arithmetic progressions is remarkably large. We also demonstrate that, even though the distribution of data obtained from the human-generated permutations is distorted so that it is indistinguishable from the distribution of random samples in terms of the total variation distance from the uniform distribution, the disproportionate rate is still effective to differentiate these two distributions.

Key words — arithmetic progression; human-generated; permutation; symmetric group; total variation distance;

1 はじめに

nを自然数とする．本稿ではn次の置換$\sigma : i \mapsto \sigma(i), i = 1, 2, \ldots, n$を

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

あるいは単に$\sigma = (\sigma(1)\sigma(2)\cdots\sigma(n))$で表す. 例えば

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

を(654321)で表す.

次のようなことを考えよう．太郎と花子の二人それぞれに，720個の置換からなる6次対称群S_6から6個の置換を無作為に選ぶよう依頼する．このとき，太郎の選んだ6個の置換は(243561), (152463), (623514), (531624), (453612), (641352)であった．これらの置換を見る限り，太郎は依頼通りに6個の置換を無作為に選んでそうである．少なくとも，無作為に選んでないと疑う理由は見当たらない．

一方，花子が選んだ6個の置換は(123456), (234561), (345612), (456123), (561234), (612345)であった．すぐに気付くであろう．花子の6個の置換の「数の並び」はすべて1から6までを順次並べそれをずらした(シフトした)ものになっている．果たしてこれら6個の置換は本当にS_6から無作為に選ばれたものなのだろうか．

e-mail: [1)]nagata@gly.oups.ac.jp, [2)]ytakei@akita-nct.ac.jp

花子が「これら6個の置換を無作為に選んだ」と主張したとしても，その主張は信用できるだろうか．

太郎と花子に対するこの印象の違いはどこからくるのか．(S_6から非復元抽出で)無作為に6個の置換を選ぶという条件の下では，太郎の6個が選ばれる確率も花子の6個が選ばれる確率も共に189492294437160 分の1である．どちらもその6個が選ばれる確率は極めて小さく，太郎の6個が選ばれる確率と花子の6個が選ばれる確率はまったく同じなのである．それにも関わらず無作為に6個を選んだかどうかでは，太郎の6個には疑いが生じず，花子の6個は疑わしいのである．

太郎の6個と花子の6個では明白な違いがある．それは「数の並び」である．太郎の数の並びには特に恣意的なものは感じない．しかし花子の数の並びは作為的なものを感じるのである．「1から6までを順次並べてずらしたもの」を花子は故意に選んだようにみえるのである．「数の並び」で印象が異なるのだ．

前回のアンケート調査報告[1]のテーマのひとつに，アンケートで回答された置換たちが6次対称群S_6上一様分布からの出力と思えるかどうかを全変動距離等を用いて考察する，というものがあった．S_6上の分布の一様性を議論する以上，各々の置換を区別せず同質のものとして扱うことが前提となる．従ってそこで用いた一様分布からの全変動距離は，個々の置換の「数の並び」については考慮していない．個々の置換の「数の並び」がどのようなものかについては，[1, 第4.1節]で多少述べてはいるものの，詳細には議論しなかった．

以上を踏まえ，次を本稿の目的とする．置換の数の並びに着目し，ある特定の数の並び方をしている置換の集合に注目する．それらの置換の集合を通して，前回[1]のアンケート結果からヒトの集団が生成する置換の特徴を探る．またその応用として，全変動距離では一様分布からの出力と区別がつかない(例えば，[1]で報告されたアンケートの設問IとIIIの回答の置換の積のような)データに対するアプローチを考察する．

2 定義

平易な言葉で説明すると，n次の置換とはn文字の並び替え，となるだろう．前節でもそのように置換を文字の並び替えだと考えている．しかし厳密には，n次の置換はn個の要素からなる集合を始域，終域とする全単射写像のことである．例えば始域，終域が順序関係や構造の全くない単なるn点集合の場合，置換であるその全単射写像に「並び方」という概念はない．このような場合は，置換をn文字の並び替え，と称したときの「並び替え」が何を意味するのかが不明となる．つまり置換をn文字の並び替えと称する以上は，文字を「並べる」段階で何かしらの順序構造が前提として仮定されてなくてはならない．そこで本稿では，我々が既に用いている(そしてこれは標準的な記法である)ように，n次の置換をn個の整数$\{1,2,\ldots,n\}$の並び替えだとみなす．すなわち始域と終域を$\{1,2,\ldots,n\}$とし，この集合の要素は整数，つまり整数の大小関係や，さらには整数の四則演算等の代数構造は既にあるものとして，これを始域と終域とした全単射写像をn文字の並び替え，すなわちn次の置換とする．このことを前提として，前節では置換σの標準的な表示である$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$の下段の列$(\sigma(1)\sigma(2)\cdots\sigma(n))$をみて，花子は疑わしい，となったのである．注意であるが，花子の疑わしさは，この$(\sigma(1)\sigma(2)\cdots\sigma(n))$の「数の並び」にある．全単射写像である置換$\sigma$というよりは，その$\sigma(1)$から$\sigma(n)$までを左から右へと一列に並べた$(\sigma(1)\sigma(2)\cdots\sigma(n))$の「数の並び」が疑わしさの原因なのである．従って，置換σとその「数の並び」は区別しなければならない．本稿では置換$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$の下段の列$(\sigma(1)\sigma(2)\cdots\sigma(n))$で置換$\sigma$を表しているが，その「数の並び」に注目している場合は，数列の記法$\{\sigma(i)\}_{i=1}^{n}$や$(\sigma(1),\sigma(2),\ldots,\sigma(n))$を用いることにする．

まとめておこう．$[n]$で整数1からnまでの集合$\{1,\ldots,n\}$を表す．$[n]$から$[n]$への全単射(すなわちn次の置換)σを考え，この置換σに付随す

る数の並び(数列)を$\{\sigma(i)\}_{i=1}^{n}$で表す.

さて，置換に付随する数列が，(花子のような)作為的なものと思われるのはどのような場合なのだろうか．例えば列$\{\sigma(i)\}_{i=1}^{6}=(1,2,3,4,5,6)$や$\{\tau(i)\}_{i=1}^{6}=(6,5,4,3,2,1)$は$i=1,2,\ldots,6$に対して

$$\sigma(i)=i,\quad \tau(i)=(5i\text{を}6\text{で割った余り})+1$$

と表すことができる．このように，$i=1,2,\ldots,n$に対して「iの値で場合分けすることなく，$\sigma(i)$はiを用いて与えられる」(これを，列を与える手続きがある，と呼ぼう)ことが具体的に提示されると，我々は列$\{\sigma(i)\}_{i=1}^{n}$が作為的なものだと感じるのだろう．要するに，その列を与える手続きが具体的に提示されるという事実が，作為的であることの証拠となり得るのである．

一方で，例えば$\{\sigma(i)\}_{i=1}^{6}=\{1,4,6,5,3,2\}$は円周率の十進数表記を考えると，$i=1,2,\ldots,6$に対して

$$\sigma(i)=\text{円周率の小数第}(5233+i)\text{位の数}$$

と与えることができる．つまりこの$\{\sigma(i)\}_{i=1}^{6}$には列を与える手続きがあり，このように円周率を用いてその手続きが具体的に提示されているのだが，しかし，このような複雑なものを提示されると今度は逆に「この手続きは強引に探した(そうなっているのを偶然みつけた)ものではなかろうか」という疑惑が生じかねない．つまり，提示された手続きがあまりに複雑だと，その複雑さが逆に作為的なものであるという証拠の妥当性を損なってしまう恐れがある．結局，作為的な数の並びと感じられるにはある程度の単純な手続きをもつ列の方が好ましいのであろう．そこで，iの値で場合分けすることなく，$\sigma(i)$はiを用いて「単純に」与えられる具体的なもの，を考えてみる．もっとも単純なものは定数列，つまり$\sigma(i)=$定数であろう．しかしこれだと$\{\sigma(i)\}_{i=1}^{n}$が置換に付随する数の並びにならない．置換に付随する数の並びになり得るもっとも単純なものとしては，a,bを定数として$\sigma(i)=a(i-1)+b$と与えられるもの，つまり等差数列があるだろう．我々はこの等差数列に着目したいのだが，置換に付随する数の並びは，1以上n以下の数しか現れないという制限がある．一方で等差数列の連続したn項を考えると一般には1以上n以下の範囲には収まらない．そこで1以上n以下に収めるために(先の$\{\tau(i)\}_{i=1}^{6}=(6,5,4,3,2,1)$で示したように)「$n$で割った余り+1」という操作を追加して，等差数列をnで割った余り+1，と表示される数の並びをもつ置換を考えることにする．

繰り返しになるが，n次の置換は整数の集合$[n]$から$[n]$への全単射写像とする．以下，$\mathrm{Mod}(m,n)$で整数mをnで割った余りを表すこととし，有理整数環，実数体をそれぞれ$\mathbb{Z},\mathbb{R}$で表す.

2.1 AP族の置換

以下で定義するAP型，NAP型，AAP型，及び，逆置換がそれらの型になる置換をAP族(arithmetic progression family)と呼ぶことにする．本稿ではAP族の置換を単純な手続きをもつ数の並びをもつ代表的なものであると考える．AP族の性質など数学的な考察は付録Aにまわし，ここでは定義及びその簡単な性質を述べることにする．

2.1.1 AP型の置換

定義: $\exists\, a,b\in\mathbb{Z}$ s.t. $\forall\, i=1,\ldots,n$に対して

$$\sigma(i)=\mathrm{Mod}(a(i-1)+b,n)+1$$

を満たすn次の置換σを AP型(arithmetic progression type)と呼ぶことにする．

つまり，AP型は公差a, 初項bの等差数列を由来とする数の並びをもつ置換である．a,bを指定したいときは$\langle a,b\rangle$-AP型と書く．すなわち，n次の置換σが$\langle a,b\rangle$-AP型であるとは「$a,b\in\mathbb{Z}$であり，$\forall\, i=1,\ldots,n$に対して$\sigma(i)=\mathrm{Mod}(a(i-1)+b,n)+1$であるとき」をいう．

例えば既に[2]等にも取り上げられているように，このAP型の置換は付随する数の並びが列を与える手続きをもつもののうちでもっと

も単純で自然なものであろう．n次のAP型の置換は空間$\mathbb{Z}/n\mathbb{Z}$上のアフィン変換と考えられ，付録Aで記したように容易な考察でn次のAP型の置換全体がS_nの部分群であることがわかる．また，n次のAP型の置換は全部で$n \times \phi(n)$個[1]あることもわかる．特にnが素数のとき，n次のAP型の置換は全部で$(n^2 - n)$個とそれなりの個数がある．従って，AP型は群論的にも個数的にも魅力ある置換たち，ということになってくるのだろうが，一方でnが素数でないと個数が少ないことがあり，特に$\phi(n) = 2$となるnではn次のAP型は$2n$個しかない．例えば$n = 6$のとき，$\phi(6) = 2$であるから，6次のAP型の置換は全部で$2 \times 6 = 12$個である．我々はこの後に「ヒトが生成する(6次の)置換」の特徴を説明する置換の集合を考察したいのであるが，6次の置換は全部で720個あることを踏まえるとたった12個の置換だけで「ヒトが生成する(6次の)置換」の特徴を説明するというのは難しそうである．そこでAP型の定義を緩めた次の置換を考える．

2.1.2 NAP型の置換

実数αに対してαを超えない最大の整数を$\lfloor\alpha\rfloor$で表す.[2]

定義: $\exists\, \alpha, \beta \in \mathbb{R}$ s.t. $\forall\, i = 1, \ldots, n$に対して

$$\sigma(i) = \mathrm{Mod}(\lfloor\alpha(i-1) + \beta\rfloor, n) + 1$$

を満たす置換σを NAP型(nearly arithmetic progression type)と呼ぶことにする．

つまり公差α, 初項βの等差数列を土台とするのだが，このα, βは実数である．実数値の数列を(それらが非負の場合では)小数点以下を切り捨てて整数にしたものがNAP型である．α, βを指定したいときは$\langle\alpha, \beta\rangle$-NAP型と書く．従って$\langle a, b\rangle$-AP型の置換は$\langle a, b\rangle$-NAP型である．

NAP型とAP型には大きな違いはない思われるかもしれないがそうではない．AP型の置換は(公差a, 初項bが整数であるため)その個数等の基本的な性質はよくわかり，それらは付録Aに述べた．一方で，n次のNAP型の置換は(公差α, 初項βが実数であるため)全部でいくつあるのか，特にNAP型の置換を具体的に列挙，提示する方法が今のところよくわからない．例えば6次の置換の場合，NAP型は全部で60個ありそれらすべてを列挙することは可能である．しかし計算機を使わずに紙と鉛筆だけで6次のNAP型すべてを探しだそうとすると(現状では)大変な作業が必要である．計算機を使ったとしても，ある大きさ以上のnに対してはn次のNAP型の置換はいくつあるのかすらわからない．計算機を使ってnの多項式時間内でn次のNAP型の置換すべてを列挙する方法は付録Aに記した．

このような事情を踏まえ，本稿では着目する置換をこのNAP型及びその逆置換までとする．つまり，AP型の定義を緩めて拡張を考えるのはNAP型を限度としこれ以上は拡げない.[3]言い換えれば，(作為的だと思われる)列を与える手続きが具体的に提示される数の並びをもつ置換，はNAP型及びその逆置換がNAP型であるものに限定する．

ここで，逆置換も含める理由を述べておこう．二つ理由がある．一つ目は，AP型がS_nの部分群をなすからである．つまりAP型というクラスは逆置換という操作で閉じている．このAP型の拡張としてNAP型を考えたいのだが，するとその逆置換がNAP型となる置換も，AP型の拡張という意味では同一のクラスと見なした方が対称性という観点からは自然であるからである．

二つ目の理由は置換の記法にある．我々は置換に付随する数の並びを考えているのであった．先に置換σを$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$と書いたのだが，本来この記法は「上段の$i$の下が$\sigma(i)$」という記法，つまり，$[n] = \{i_1, \ldots, i_n\}$として$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$と書かれるものであり，この特殊なケースが

[1] $\phi(n)$はオイラー関数($[n]$のうちでnと互いに素のものの個数)とする．例えばnが素数ならば$\phi(n) = n - 1$である．
[2] $\lfloor\cdots\rfloor$を床関数と呼ぶ．
[3] 付録AでNAP型を含むpNAP型を考察することになるが，6次の置換ではNAP型と pNAP型は一致する．

$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ である．置換σを一般の形の$\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$と書いてしまうと，何が置換$\sigma$の「数の並び」なのかわからないが，$(i_1, i_2, \ldots, i_n)$を$(1, 2, \ldots, n)$とした$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$の場合と，$(i_1, i_2, \ldots, i_n)$を$(\sigma^{-1}(1), \sigma^{-1}(2), \ldots, \sigma^{-1}(n))$とした$\sigma = \begin{pmatrix} \sigma^{-1}(1) & \sigma^{-1}(2) & \cdots & \sigma^{-1}(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$の場合には整数の集合$[n]$の順序に対応した「数の並び」が現れる．今までは前者の$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$の下段の数の並び$\{\sigma(i)\}_{i=1}^n$だけを考えていたが，後者の$\sigma = \begin{pmatrix} \sigma^{-1}(1) & \sigma^{-1}(2) & \cdots & \sigma^{-1}(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$の場合なら置換$\sigma$に付随する数の並びは上段の$(\sigma^{-1}(1), \sigma^{-1}(2), \ldots, \sigma^{-1}(n))$，つまり$\{\sigma^{-1}(i)\}_{i=1}^n$が「数の並び」となろう．要するに，置換$\sigma$の記法から「数の並び」を考えるときには$\{\sigma(i)\}_{i=1}^n$だけではなく，$\{\sigma^{-1}(i)\}_{i=1}^n$も考慮しなくてはならないのである．$\sigma$に対する数の並びとして列$\{\sigma^{-1}(i)\}_{i=1}^n$を考えるとき，この列が等差数列由来のNAP型の条件を満たすということは，σ^{-1}がNAP型の置換ということである．よってσはNAP型の逆置換である．結局，NAP型を考えるならばその逆置換がNAP型，つまりNAP型の逆置換も考えなくてはならない.[4]

nが素数のときはAP型は個数的にも群論的にも着目すべき魅力ある対象となるのだが，nが素数でないときは個数の観点からその魅力が随分と減ってしまう．そのために我々はNAP型を持ち出したのだが，公差と初項を実数に拡げてしまったため，少し扱いにくいものになってしまった．そこでNAP型から扱いやすいものを掬い上げてみよう．

2.1.3 AAP型の置換

(a, n)を整数aとnの最大公約数とする．

定義: $\exists\, a, b \in \mathbb{Z}$ s.t. $\forall\, i = 1, \ldots, n$に対して

$$\sigma(i) = \mathrm{Mod}(\lfloor a(i-1) + \frac{(a,n)}{n}(i-1) + b \rfloor, n) + 1$$

を満たす置換σを AAP$^{(+)}$型(adjusted arithmetic progression (plus) type),

$$\sigma(i) = \mathrm{Mod}(\lfloor a(i-1) + \frac{(a,n)}{n}(n-i) + b \rfloor, n) + 1$$

を満たす置換σを AAP$^{(-)}$型(adjusted arithmetic progression (minus) type) と呼ぶことにする．AAP$^{(+)}$型或いはAAP$^{(-)}$型のいずれか置換であるとき，単にAAP型と呼ぶことにする．

a, bを指定したいときはそれぞれ$\langle a, b\rangle$-AAP$^{(+)}$型, $\langle a, b\rangle$-AAP$^{(-)}$型と書くことにすると，$\langle a, b\rangle$-AAP$^{(+)}$型は$\langle a + \frac{(a,n)}{n}, b\rangle$-NAP型，$\langle a, b\rangle$-AAP$^{(-)}$型は$\langle a - \frac{(a,n)}{n}, b + \frac{(a,n)}{n}(n-1))\rangle$-NAP型であることがわかる．つまり，AAP型の置換はNAP型である．またAP型の置換はAAP型である.[5]またAAP$^{(+)}$型の置換はすべて具体的に与えることができ，n次のAAP$^{(+)}$型は全部で$(n^2 - n)$個あることがわかる．AAP$^{(-)}$型も同様である．また「AAP$^{(+)}$型且つAAP$^{(-)}$型」であることとAP型であることは同値である．さらにnが素数ならばAAP$^{(+)}$型全体とAAP$^{(-)}$型全体は一致し，このときAAP型はAP型であることもわかる．これら諸性質については付録Aに記す．まとめると，AAP型:=(AAP$^{(+)}$型或いはAAP$^{(-)}$型)として

$$\text{AP型} \subset \text{AAP型} \subset \text{NAP型}$$

$$\text{AP型} = \text{AAP}^{(+)}\text{型} \cap \text{AAP}^{(-)}\text{型}$$

$$n\text{が素数のときは}\ \ \text{AP型} = \text{AAP型}$$

ということになる．従ってAAP型が意義を持つのはnが素数でないときに限る．先に，AP

[4] これは次の様に考えても良い．(例えば[1]でのアンケートの設問Iのように) 仮に$(2, 4, 6, 1, 3, 5)$という数列を，左から右に一列に並んだマス目に書いていく方法は二通りある．並んだマス目の順に$2, 4, 6, 1, 3, 5$と書いていく方法と，並んだマス目の2番目，4番目，6番目，1番目，3番目，5番目の順に$1, 2, 3, \ldots, 6$を書いていく方法である．マス目に書かれた数の並びを置換と考えるとき，後者の場合は前者の場合の逆置換となっている．つまり，$(2, 4, 6, 1, 3, 5)$という一つの数列から二つの置換が考えられ，一方は他方の逆置換になっている．

[5] 詳細は付録A参照のこと．

型はnが素数のときは個数もそこそこあり，着目する置換の集合として魅力があるのだが，$n=6$のケースのように個数が少ないときがあり，その場合は着目する置換の集合としての魅力が減ってしまう，と述べた．その個数が少ない理由は，$(a,n)\neq 1$のときに$\{\mathrm{Mod}(a(i-1)+b,n)+1\}_{i=1}^{n}$が置換に付随する数の並びにならないからである．そこで，補正項を付け，床関数$\lfloor\cdots\rfloor$を利用することによって，そのような$(a,n)\neq 1$となるaでも置換に付随する数の並びになるように改良したものがAAP型である．例を挙げておこう．$n=6$で$a=2,b=0$のときの$\langle 2,0\rangle$-AP型は存在しない．なぜなら数列$\{\mathrm{Mod}(2(i-1)+0,6)+1\}_{i=1}^{6}=(1,3,5,1,3,5)$は置換に付随する数の並びにならないからである．しかし$(1,3,5,1,3,5)$の左から4,5,6番目の項(右側の$(1,3,5)$)にそれぞれ1を加えた$(1,3,5,2,4,6)$は置換に付随する数の並びとなる．この類いの補正をしたのがAAP型である．実際$a=2,b=0$の$\langle 2,0\rangle$-AAP型の置換の数の並びは$\{\mathrm{Mod}(\lfloor a(i-1)+\frac{(a,n)}{n}(i-1)\rfloor,n)+1\}_{i=1}^{6}=\{\mathrm{Mod}(\lfloor 2(i-1)+\frac{1}{3}(i-1)\rfloor,6)+1\}_{i=1}^{6}=(1,3,5,2,4,6)$である．

一般にn次のAAP型(またはNAP型)の置換全体はS_nの部分群にならない．特に，AAP型(resp. NAP型)及びその逆置換の中からの任意の二つの置換の積はAAP型(resp. NAP型)になるとは限らない．しかしその積がAAP型(resp. NAP型)になる場合が多い．これに関しては後半の第4.3.2節で述べることにする．

ここで6次の置換でのAP型，NAP型，AAP型及びその逆置換の個数を記しておく．

6次のAP型は全部で12個．AP型の逆置換は同数の12個で，これらは集合として一致する．

6次のNAP型は全部で60個であり,[6]NAP型且つNAP型の逆置換となっているもの(つまりσもσ^{-1}もNAP型となる置換σ)は22個ある．

AAP型を持ち出した理由からは，AAP$^{(+)}$型とAAP$^{(-)}$型は個別に考慮する必然性は見当たらない．本稿では，AAP$^{(+)}$型かAAP$^{(-)}$型のいずれかになっている場合にAAP型と呼び，(AAP$^{(+)}$型かAAP$^{(-)}$型を区別せずに)AAP型を考えるのが自然であるという立場を取るが，個数に関しては一応区別して記しておく．6次のAAP$^{(+)}$型は全部で30個，AAP$^{(+)}$型且つAAP$^{(+)}$型の逆置換となっているもの(つまりσもσ^{-1}もAAP$^{(+)}$型)は14個ある．AAP$^{(-)}$型に関する個数についても全く同様である．

6次のAAP型は全部で48個，AAP型且つAAP型の逆置換となっているもの(つまりσもσ^{-1}もAAP型となる置換σ)は20個ある．

以下，6次のAP型，NAP型，AAP型, AAP$^{(+)}$の置換の集合を

$$AP:=\{\sigma\in S_6\ ;\ \sigma\ \text{はAP型}\}$$

$$NAP:=\{\sigma\in S_6\ ;\ \sigma\ \text{はNAP型}\}$$

$$AAP:=\{\sigma\in S_6\ ;\ \sigma\ \text{はAAP型}\}$$

$$AAP^{(+)}:=\{\sigma\in S_6\ ;\ \sigma\ \text{はAAP}^{(+)}\text{型}\}$$

($AAP^{(-)}$も同様)と書く．従って，

$$AAP=AAP^{(+)}\cup AAP^{(-)}$$

$$AP=AAP^{(+)}\cap AAP^{(-)}$$

である．以下，置換の集合Sに対して，記法

$$S_{\mathrm{inv}}:=\{\sigma^{-1}\ ;\ \sigma\in S\}$$

$$S_{\cup}:=S\cup S_{\mathrm{inv}},\quad S_{\cap}:=S\cap S_{\mathrm{inv}}$$

を用いる．これらの記法を用いるとそれぞれの置換の個数が次の表になる．

6次のAP族の個数[7]

	AP	NAP	AAP	$AAP^{(+)}$	$AAP^{(-)}$
S	12	60	48	30	30
S_{inv}	〃	〃	〃	〃	〃
$S_{\cap}$	〃	22	20	14	14
$S_{\cup}$	〃	98	76	46	46

3　ヒトが生成する置換とAP族

本稿では[1]で報告したアンケート(平成30年6月実施)の結果を「ヒトが生成する置換」のデータとして利用する．先ずはそのアンケー

[6]NAP型の逆置換はNAP型と同じ60個である．他の型の逆置換の個数もその型の個数と同じである．
[7]SにはAP, NAP, AAP, $AAP^{(+)}$, $AAP^{(-)}$のいずれかが入る.「〃」は「同上」の意味である．

トを簡単に復習しておこう．実際に用いたアンケートは[1, 付録A]にあるもので，設問Iから設問IVまでの異なる4つの質問と，学年と性別を尋ねる質問の合計5つの質問で構成されている．そこでは設問IからIVの合計4通りの方法で，6次の置換をそれぞれひとつずつ「ランダムに」生成する[8]ようになっている．約1600人を対象にしたアンケートで1040部の回答を得たが，各設問の回答の中には6次の置換とみなせないもの(無効回答)も含まれている．例えば，設問Iでは6次の置換とみなせる有効回答数は1033である．詳細は[1]を参照して頂きたい．

さて(ランダムに，という指示があるアンケートの回答である)ヒトの集団が生成する置換たちには，作為的だと思われる数の並びをもつ置換のAP族がどの程度含まれているのであろうか．つまり先の太郎と花子の例でいえば，ヒトの集団は太郎と花子のどちらに近いのか．この節では[1]で行ったアンケートの各設問I,II,III,IVの回答に対して，AP族がどのくらいの票を獲得しているかを述べる．以下，票数とはその置換を回答している部数の意味とする．例えば，アンケートの設問Iでは置換(123456)と回答したのが47部あり，(654321)と回答したのが41部あるので，設問Iでは(123456)は47票，(654321)は41票，ということになる．さらにS_6の部分集合Aに対して，Aの各要素での票の総和をAの票数ということにする．例えば，6次のAP型は全部で12個で，$AP = \{(123456), (165432), (216543), (234561), (321654), (345612), (432165), (456123), (543216), (561234), (612345), (654321)\}$ である．そしてそれぞれの置換の設問Iの回答の票数は，この置換の順に$47, 0, 1, 7, 4, 2, 3, 1, 4, 0, 2, 41$ である．この和は112なので，設問IでのAPの票数は112票，ということになる．設問Iでの有効回答数は1033であるので，単純に1033をS_6の個数720で割ると1.4347である．AP型は12個なのでこれを12倍して17.217．つまり要素の個数が(APと同じの)12個のS_6の部分集合の票数は(平均的には)17.217辺りだろうと思われるが，APは112票である．APは(要素の個数が12の部分集合のなかで)票数が極めて多いものだと思われる[9]．

以下，置換(123456)をidで表す．

3.1 AP族の票数

以下の表のSにはAP, NAP, AAPのいずれかが入る．例えば，下の最初の表「票数　設問I」での表中のNAPと$S_\cap$の交わりの数値 150 の意味は，設問Iの回答データで，SをNAPとして$S_\cap = S \cap S_{\mathrm{inv}}$の票数，つまり$NAP \cap NAP_{\mathrm{inv}}$の票数が150という意味である．

票数　設問I

	AP	NAP	AAP
S	112	215	193
S_{inv}	〃	202	188
$S_\cap$	〃	150	148
$S_\cup$	〃	267	233

票数　設問II

	AP	NAP	AAP
S	95	168	141
S_{inv}	〃	147	133
$S_\cap$	〃	107	107
$S_\cup$	〃	208	167

票数　設問III

	AP	NAP	AAP
S	99	192	180
S_{inv}	〃	190	179
$S_\cap$	〃	130	125
$S_\cup$	〃	252	234

[8]アンケートではすべての設問で「ランダムに」の類いの指示をしている．

[9]設問Iの回答では(123456)が47票，(654321)が41票であり，この2つの置換で88票あることになる．88票はAP型の総票数112の78.571%に相当する．この2つの置換を除いた残りの10個のAP型の置換の票数は$112 - 88 = 24$票ということになる．単純計算では1つの置換は平均$1033/720 = 1.4347$票とるので，単純に10倍して考えれば(無作為に選んだ)10個の置換の票数は14.347票くらいであろう．従って24票でも大きいことになるのだが，しかし本節の興味は「AP族という等差数列に由来する数の並びをもつ置換がヒトに選ばれやすいか否か」である．数の並びが等差数列に由来する置換(123456)や(654321)を除外してしまうのは適切ではないであろう．しかしながら，(123456)はすべての設問で圧倒的な票数を誇る一番人気の置換である．そこで本稿では，[1]でそうしたように，(123456)の圧倒的多数の票数によるマスキング現象が起こる可能性を考慮して，(123456)を除外した考察も行う．一方で(654321)は設問I,II,IVでは票数二位の置換であるが，設問IVでは票数三位の置換と1票差しかなく，また設問IIIでの票数は同着五位である．本稿では(654321)を除外した考察は行わない．

票数　設問IV

	AP	NAP	AAP
S	208	268	262
S_{inv}	〃	277	272
$S_\cap$	〃	239	235
$S_\cup$	〃	306	299

次の表は，その集合のとる票数の期待値と標準偏差をまとめたものである．例えば表「期待値/標準偏差　設問I」での表中のNAPと$S_\cap$の交わりの数値 31.564/12.782 の意味は，設問Iの回答データで，SをNAPとして$S_\cap = S \cap S_{\mathrm{inv}}$(すなわち$NAP \cap NAP_{\mathrm{inv}}$)の要素の個数22と等しい$S_6$の部分集合を無作為に選んだときの票数，の期待値が31.564であり，その標準偏差が12.782という意味である．期待値と標準偏差の計算方法は付録Bに述べた．

期待値/標準偏差　設問I

	AP	NAP	AAP
S	17.217/9.5085	86.083/20.528	68.867/18.527
S_{inv}	〃	〃	〃
$S_\cap$	〃	31.564/12.783	28.694/12.206
$S_\cup$	〃	140.60/25.469	109.04/22.822

期待値+標準偏差　設問II

	AP	NAP	AAP
S	16.467/7.9347	82.333/17.130	65.867/15.461
S_{inv}	〃	〃	〃
$S_\cap$	〃	30.189/10.667	27.444/10.186
$S_\cup$	〃	134.48/21.254	104.29/19.045

期待値/標準偏差　設問III

	AP	NAP	AAP
S	17.133/7.3618	85.667/15.894	68.533/14.344
S_{inv}	〃	〃	〃
$S_\cap$	〃	31.411/9.8972	28.556/9.4501
$S_\cup$	〃	139.92/19.719	108.51/17.669

期待値/標準偏差　設問IV

	AP	NAP	AAP
S	15.500/23.846	77.500/51.483	62.000/46.464
S_{inv}	〃	〃	〃
$S_\cap$	〃	28.417/32.059	25.833/30.611
$S_\cup$	〃	126.58/63.874	98.167/57.235

以下の表は，各設問でのAP族の各型の票数の偏差値，すなわち「(票数－期待値)÷標準偏差」である．例えば表「票数の偏差値　設問I」での表中のNAPと$S_\cap$の交わりの数値+9.2649とは，設問Iの回答データで，SをNAPとして$S_\cap = S \cap S_{\mathrm{inv}} = NAP \cap NAP_{\mathrm{inv}}$の票数150からその期待値31.564を引き，標準偏差12.783で割った値である．[10]

票数の偏差値　設問I

	AP	NAP	AAP
S	+9.9683	+6.2800	+6.7001
S_{inv}	〃	+5.6467	+6.4302
$S_\cap$	〃	+9.2649	+9.7745
$S_\cup$	〃	+4.9628	+5.4317

票数の偏差値　設問II

	AP	NAP	AAP
S	+9.8975	+5.0008	+4.8596
S_{inv}	〃	+3.7749	+4.3422
$S_\cap$	〃	+7.2005	+7.8106
$S_\cup$	〃	+3.4593	+3.2929

票数の偏差値　設問III

	AP	NAP	AAP
S	+11.121	+6.6903	+7.7708
S_{inv}	〃	+6.5645	+7.7011
$S_\cap$	〃	+9.9613	+10.206
$S_\cup$	〃	+5.6838	+7.1020

票数の偏差値　設問IV

	AP	NAP	AAP
S	+8.0725	+3.7003	+4.3044
S_{inv}	〃	+3.8751	+4.5196
$S_\cap$	〃	+6.5686	+6.8331
$S_\cup$	〃	+2.8089	+3.5089

多くの偏差値が非常に大きな値になっている．例えば，設問Iの回答データでのSがNAPの$S_\cap = NAP_\cap$の偏差値は+9.2649である．もし，要素の個数が($NAP_\cap$の要素の個数と等しい)22のS_6の部分集合の票数の分布，が正規分布に従っているならば，要素の個数が22の集合でその票数が150以上のものの割合，すなわち偏差値+9.2649以上になる確率[11]は10^{-20}より小さく，ほぼ0である．しかし，実際には付録Bに述べたように正規分布に従っているわけではない．設問Iの回答データに対して，要素の個数が22のS_6の部分集合でその票数が150以上となるものの個数は(計算機を用いて数えると)3879441424914051097858913622697172 1個ある．要素が22の部分集合は全部で$\binom{720}{22} = 467524309903018460404470082728097266866400$個あるので，設問Iの回答データに対して，要

[10]表の数値で計算すると9.2651になるが，期待値31.564の正確な値31.56388…と標準偏差12.783の正確な値12.78327…を用いて計算すると9.264928…になる．

[11]Mathematicaによる値は，9.7630×10^{-21}である．

素の個数が22の部分集合でその票数が150以上のものの割合は8.2978×10^{-8}ということになる．その割合，すなわち，それぞれの設問の回答データを用いた場合に偏差値がその値以上となる確率を，以下では簡単に「偏差値以上となる確率」と呼ぶ．偏差値以上になる確率をまとめると次の表になる．

偏差値以上となる確率　設問I

	AP	NAP	AAP
S	9.2893×10^{-6}	7.3921×10^{-7}	8.8587×10^{-7}
S_{inv}	〃	1.6285×10^{-5}	3.2402×10^{-6}
$S_{\cap}$	〃	8.2978×10^{-8}	3.4763×10^{-8}
$S_{\cup}$	〃	1.0231×10^{-5}	6.8619×10^{-6}

偏差値以上となる確率　設問II

	AP	NAP	AAP
S	4.1931×10^{-7}	7.0266×10^{-5}	2.0877×10^{-4}
S_{inv}	〃	1.8542×10^{-3}	7.5910×10^{-4}
$S_{\cap}$	〃	9.3401×10^{-6}	3.1824×10^{-6}
$S_{\cup}$	〃	1.8064×10^{-3}	3.9157×10^{-3}

偏差値以上となる確率　設問III

	AP	NAP	AAP
S	1.5136×10^{-10}	4.4775×10^{-8}	1.4085×10^{-9}
S_{inv}	〃	7.6346×10^{-8}	1.9283×10^{-9}
$S_{\cap}$	〃	4.9340×10^{-11}	4.3259×10^{-11}
$S_{\cup}$	〃	3.9998×10^{-7}	1.7625×10^{-9}

偏差値以上となる確率　設問IV

	AP	NAP	AAP
S	5.0680×10^{-4}	3.9862×10^{-3}	1.0165×10^{-3}
S_{inv}	〃	1.3336×10^{-3}	2.2946×10^{-4}
$S_{\cap}$	〃	4.5386×10^{-5}	4.8368×10^{-5}
$S_{\cup}$	〃	1.2643×10^{-2}	1.2991×10^{-3}

これらの表の値は，条件を満たす部分集合の個数を(計算機を用いて)数え上げ，その値から得られたものである．それら部分集合の個数の詳細の値は付録Cに記した．実はこれらの値を求めるのは容易ではない．フェラーズ図形を利用するなど数え方に工夫をしているものの，これらの計算には最新型のPCを用いても相当の時間がかかっている．今回のデータでは数週間で計算できたが，大きなデータになればさらに時間がかかるであろう．このような時間的コストを考慮すると，一般論としては個数を数えて正確な確率を求めるよりは，票数の偏差値を計算しその偏差値が大きければ稀である(確率が小さい)とみなす，という方が実用的だと思われる．[12]

次に各設問の回答データのidの票数を0票に置き換えたものを考える．以下これを「id除外」と称する．この「id除外」を考える理由は[1, 第4.2.1節]でも述べた通り，idの票が圧倒的に多いために(idの票の多さによる)マスキング現象が起こる可能性に配慮したからである．以下，先と同様なものを順に記す．

票数　設問I(id除外)

	AP	NAP	AAP
S	65	168	146
S_{inv}	〃	155	141
$S_{\cap}$	〃	103	101
$S_{\cup}$	〃	220	186

票数　設問II(id除外)

	AP	NAP	AAP
S	58	131	104
S_{inv}	〃	110	96
$S_{\cap}$	〃	70	70
$S_{\cup}$	〃	171	130

票数　設問III(id除外)

	AP	NAP	AAP
S	72	165	153
S_{inv}	〃	163	152
$S_{\cap}$	〃	103	98
$S_{\cup}$	〃	225	207

票数　設問IV(id除外)

	AP	NAP	AAP
S	28	88	82
S_{inv}	〃	97	92
$S_{\cap}$	〃	59	55
$S_{\cup}$	〃	126	119

期待値/標準偏差　設問I(id除外)

	AP	NAP	AAP
S	16.433/7.5047	82.167/16.202	65.733/14.623
S_{inv}	〃	〃	〃
$S_{\cap}$	〃	30.128/10.089	27.389/9.6336
$S_{\cup}$	〃	134.21/20.102	104.08/18.013

[12]正規分布に従っているならば(偏差値が+1.645を超える確率は5%以下，+1.96を超える確率は2.5%以下であるから)偏差値が+1.645や+1.96を超えるのは稀だとみなそう，となるだろうが，当然正規分布でなければ偏差値+1.645や+1.96以上が稀と言えるかどうかはわからない．すなわち，偏差値がいくつ以上ならば「稀と言える」かは確率分布や推測統計を利用する目的に依存する．しかし，チェビチェフの不等式によれば一般に偏差値が−5以下或いは+5以上となる確率は(如何なる分布でも)$5^{-2} = 4\%$以下である．従って(確率分布が不明でも)偏差値が+5を超えれば稀であるとみなしてよさそうである．勿論，本稿で用いたデータについては偏差値が+5を超える確率は4%より遙かに小さい．

期待値/標準偏差　設問II(id除外)

	AP	NAP	AAP
S	15.850/6.4905	79.250/14.013	63.400/12.647
S_{inv}	〃	〃	〃
$S_{\cap}$	〃	29.058/8.7259	26.417/8.3318
$S_{\cup}$	〃	129.44/17.385	100.38/15.578

期待値/標準偏差　設問III(id除外)

	AP	NAP	AAP
S	16.683/6.5939	83.417/14.236	66.733/12.848
S_{inv}	〃	〃	〃
$S_{\cap}$	〃	30.586/8.8650	27.806/8.4645
$S_{\cup}$	〃	136.25/17.662	105.66/15.827

期待値/標準偏差　設問IV(id除外)

	AP	NAP	AAP
S	12.500/6.6181	62.500/14.288	50.000/12.895
S_{inv}	〃	〃	〃
$S_{\cap}$	〃	22.917/8.8974	20.833/8.4955
$S_{\cup}$	〃	102.08/17.727	79.167/15.884

票数の偏差値　設問I(id除外)

	AP	NAP	AAP
S	+6.4715	+5.2976	+5.4891
S_{inv}	〃	+4.4953	+5.1472
$S_{\cap}$	〃	+7.2227	+7.6411
$S_{\cup}$	〃	+4.2680	+4.5481

票数の偏差値　設問II(id除外)

	AP	NAP	AAP
S	+6.4941	+3.6931	+3.2103
S_{inv}	〃	+2.1944	+2.5777
$S_{\cap}$	〃	+4.6920	+5.2310
$S_{\cup}$	〃	+2.3904	+1.9011

票数の偏差値　設問III(id除外)

	AP	NAP	AAP
S	+8.3890	+5.7308	+6.7143
S_{inv}	〃	+5.5903	+6.6365
$S_{\cap}$	〃	+8.1686	+8.2928
$S_{\cup}$	〃	+5.0250	+6.4031

票数の偏差値　設問IV(id除外)

	AP	NAP	AAP
S	+2.3421	+1.7847	+2.4815
S_{inv}	〃	+2.4146	+3.2570
$S_{\cap}$	〃	+4.0555	+4.0218
$S_{\cup}$	〃	+1.3492	+2.5077

偏差値以上となる確率　設問I(id除外)

	AP	NAP	AAP
S	9.5757×10^{-4}	1.3323×10^{-5}	2.0527×10^{-5}
S_{inv}	〃	2.6817×10^{-4}	7.1991×10^{-5}
$S_{\cap}$	〃	5.3448×10^{-6}	2.6363×10^{-6}
$S_{\cup}$	〃	9.9344×10^{-5}	8.9163×10^{-5}

偏差値以上となる確率　設問II(id除外)

	AP	NAP	AAP
S	5.0379×10^{-5}	1.0921×10^{-3}	4.0160×10^{-3}
S_{inv}	〃	2.6041×10^{-2}	1.3995×10^{-2}
$S_{\cap}$	〃	4.7383×10^{-4}	1.8760×10^{-4}
$S_{\cup}$	〃	1.5157×10^{-2}	4.1491×10^{-2}

偏差値以上となる確率　設問III(id除外)

	AP	NAP	AAP
S	3.4389×10^{-8}	8.4597×10^{-7}	3.7986×10^{-8}
S_{inv}	〃	1.4257×10^{-6}	5.1632×10^{-8}
$S_{\cap}$	〃	4.3477×10^{-9}	4.4438×10^{-9}
$S_{\cup}$	〃	4.0370×10^{-6}	2.6554×10^{-8}

偏差値以上となる確率　設問IV(id除外)

	AP	NAP	AAP
S	3.9715×10^{-2}	5.4213×10^{-2}	1.8013×10^{-2}
S_{inv}	〃	1.8580×10^{-2}	4.1993×10^{-3}
$S_{\cap}$	〃	2.0179×10^{-3}	2.3814×10^{-3}
$S_{\cup}$	〃	1.0112×10^{-1}	1.4135×10^{-2}

これらの結果について，先ずは個数を正確に数えて得られた「偏差値以上になる確率」の数値をみてみよう．idを含む回答データについて，設問Iでは小さい順に$AAP_{\cap}$, $NAP_{\cap}$, NAPであり，APは7位である．IIでは，AP, $AAP_{\cap}$, $NAP_{\cap}$の順，IIIでは，$AAP_{\cap}$, $NAP_{\cap}$, APの順，IVでは，$NAP_{\cap}$, $AAP_{\cap}$, AAP_{inv}の順であり，APは4位である．id除外の回答データについては，設問Iでは小さい順に$AAP_{\cap}$, $NAP_{\cap}$, NAPであり，APは最下位の9位である．IIでは，AP, $AAP_{\cap}$, $NAP_{\cap}$の順，IIIでは，$NAP_{\cap}$, $AAP_{\cap}$, $AAP_{\cup}$の順でAPは4位，IVでは，$NAP_{\cap}$, $AAP_{\cap}$, AAP_{inv}の順でAPは7位である．

$NAP_{\cap}$と$AAP_{\cap}$はすべてのケースで確率の小ささで3位以内であり，すべての場合でその確率が0.25%より小さい．この結果より$NAP_{\cap}$と$AAP_{\cap}$は顕著に多くの票を取る置換の集合といえるだろう．一方でAPは確率の小ささで1位をとるケースやその数値として小さい確率をとる場合もあるのだが，例えばid除外の設問IVのケースのときは確率3.9715%であり，すべてのケースで顕著に小さいとはいいにくい．第2.1.1節の最後で案じた通りに，APですべてを説明しようとするのはやはり難しいようである．すべてのケースで確率が顕著に小さい，すなわち票数が顕著に多いということに関してはAPよりは$NAP_{\cap}$や$AAP_{\cap}$の方が優れていよう．

次に偏差値をみてみよう．idを含む回答デー

タについて，IからIVまですべての設問で値が大きい順にAP, $AAP_{\cap}$, $NAP_{\cap}$である．id除外の回答データについては，設問Iでは大きい順に$AAP_{\cap}$, $NAP_{\cap}$, APである．IIとIIIでは，AP, $AAP_{\cap}$, $NAP_{\cap}$の順，IVでは$NAP_{\cap}$, $AAP_{\cap}$, AAP_{inv}の順でAPは7位である．

id除外の回答データではAPが一番大きいのは設問II,IIIの2つだけあり，またIVではAPの偏差値は+2.3421で，極めて大きな数値とは言えない．偏差値に関しても，すべてのケースで安定して大きな偏差値となるのは$AAP_{\cap}$と$NAP_{\cap}$である．

ここで$AAP_{\cap}$の置換20個を挙げておく．

id, (135246), (142536), (165432), (216543), (234561), (246135), (321654), (345612), (362514), (415263), (432165), (456123), (531642), (543216), (561234), (612345), (635241), (642531), (654321)

$NAP_{\cap}$はこれに(154326), (623451) を加えたものである．

今度は逆に小さくない確率，大きくない偏差値のものをみてみよう．2.5%を超えるようなそれ程小さな確率でないものは，idを含む回答データではひとつもなく，id除外のデータでは設問IIで$AAP_{\cup}$の4.1492%, IVでAPの3.9715%, NAPの5.4213%, $NAP_{\cup}$の10.112%である．偏差値については，偏差値が2.0以下となるものはidを含む場合は1つもなく，id除外の場合は設問IIで$AAP_{\cup}$, 設問IVでNAP, $NAP_{\cup}$である．

想像の域を超えないが，$NAP_{\cup}$, $AAP_{\cup}$は集合の要素の個数が大きすぎるために確率が小さくなりにくく，また偏差値が大きくなりにくいと思われる．今回のアンケートの回答データを見る限りではあるが「AP族の(AP, NAP, AAP等の)集合は，要素の個数が大きくならない方が票の多さでその顕著性が出るのだが，一方で要素の個数が小さすぎると(APのように)すべてのデータに対してはその顕著性が薄れてしまう」ようである．

以上のアンケートの回答の解析から，次の様にまとめられるだろう：

「ランダムに」という指示の下でヒトが生成する6次の置換について，4種類の生成方法及びそれらからid除外したものすべてのデータで，AP族の$AAP_{\cap}$と$NAP_{\cap}$に著しい偏りがある．

また，NAPとAAPについて，SとS_{inv}では設問I,II,IIIはSの方が確率は小さく偏差値が大きい．一方でIVはS_{inv}の方が偏差値が大きい．IVは他の設問と違って「並び替え」というものを想像しにくいことを考えると「並び替えの作業」で置換を生成するような場合はNAP_{inv}よりNAP, AAP_{inv}よりAAPの方がヒトに好まれるようである．

[1]での結果によれば，アンケートの設問すべてに対して回答データは(idを含む場合とid除外した場合の共に)，全変動距離からは一様分布からの出力とは思えないのであった．今回さらに分かったことは，AP族，特にその置換と逆置換の両方の数の並びが作為的だと思われる$AAP_{\cap}$または$NAP_{\cap}$の票数が異常に多いということである．先の「太郎か花子か」という論点では，ヒトが生成する6次の置換についてはどの回答データに関しても「花子に近い」となるのであろう．

3.2 選ばれにくい置換

[1]のアンケートの回答で一票も取らない置換は設問I,II,III,IVの順で259個，265個，276個，371個ある．ちなみにすべての回答データでAPのすべての置換[13]が必ずしも票を取るわけでもない．例えば，設問I,II,IVではAP型の(165432)は一票も取らず，設問IIIではAP型の(321654)は一票も取っていない．アンケートの質問の仕方で，AP型での人気の置換も異なってくるということになろう．

一方で設問IからIVまでのすべての回答(有効回答数3979)をみてみると，一票も取らないという置換は30個ある．その30個のうち，$NAP_{\cup}$の置換は(425361)の1個だけであった．[14]$NAP_{\cup}$はすべてのAP族を含む集合であるから，4つの設問をあわせると一票も取らないAP族の置換は1個ということになる．ちなみに，要素の個数が98個(すなわち$NAP_{\cup}$と同じ要素の個数)の

[13] $AAP_{\cap}$や$NAP_{\cap}$はAPを含むことに注意する．
[14] この置換はAAP_{inv}に属しAPに属さない．

S_6の部分集合を無作為に選ぶとき「特定の30個の置換がその部分集合に何個含まれるか」の期待値(理論値)は4.0833個である．$NAP_\cup$では1個なので，その意味ではAP族，つまり$NAP_\cup$は「ヒトに選ばれにくい置換たち」ではなさそうである．

4 応用

この節では「ヒトが生成する置換はAP族に偏りがある」ことの応用を述べる．

4.1 置換の積

[1]で報告した置換の積に関する結果を復習しておく．設問I(id除外)と設問III(id除外)の置換を，同じ回答者で積をとったデータ[15]

$$D^{\mathrm{I,III}} := (\sigma_i^{\mathrm{I}} \circ \sigma_i^{\mathrm{III}} \ ; \ \sigma_i^{\mathrm{I}}, \sigma_i^{\mathrm{III}} \in S_6 \setminus \{\mathrm{id}\})_{i=1,\ldots,1040}$$

は，($D^{\mathrm{I,III}}$と同じ大きさの969個の復元無作為標本をS_6から抽出したときのデータと)一様分布からの全変動距離の理論値からの隔たりが小さく[1, 第4.3.4節]，それらの値から判断すると，データ$D^{\mathrm{I,III}}$はS_6の一様分布に従った出力と区別がつかないのであった．

4.1.1 $D^{\mathrm{I,III}}$でのAP族の票数

データ$D^{\mathrm{I,III}}$について，AP族の票数と期待値と標準偏差，偏差値，及びその偏差値以上になる確率を以下の表に記す．

票数　$D^{\mathrm{I,III}}$

	AP	NAP	AAP
S	41	104	91
S_{inv}	〃	117	94
$S_\cap$	〃	58	55
$S_\cup$	〃	163	130

期待値/標準偏差　$D^{\mathrm{I,III}}$

	AP	NAP	AAP
S	16.150/4.1490	80.750/8.9574	64.600/8.0842
S_{inv}	〃	〃	〃
$S_\cap$	〃	29.608/5.5779	26.917/5.3260
$S_\cup$	〃	131.89/11.113	102.28/9.9583

票数の偏差値　$D^{\mathrm{I,III}}$

	AP	NAP	AAP
S	+5.9894	+2.5956	+3.2656
S_{inv}	〃	+4.0469	+3.6367
$S_\cap$	〃	+5.0900	+5.2729
$S_\cup$	〃	+2.7992	+2.7833

偏差値以上となる確率　$D^{\mathrm{I,III}}$

	AP	NAP	AAP
S	1.8250×10^{-6}	7.5936×10^{-3}	1.3767×10^{-3}
S_{inv}	〃	1.0177×10^{-4}	4.5856×10^{-4}
$S_\cap$	〃	9.7235×10^{-6}	6.2180×10^{-6}
$S_\cup$	〃	3.8999×10^{-3}	4.3816×10^{-3}

$D^{\mathrm{I,III}}$に対しても，確率はAP, $AAP_\cap$, $NAP_\cap$の順で小さい．また偏差値も同様にAP, $AAP_\cap$, $NAP_\cap$の順で大きい．集合AP, $AAP_\cap$, $NAP_\cap$は票数が極めて多いという意味で$D^{\mathrm{I,III}}$に対してもこれらが顕著な集合であることがわかる．

4.1.2 一様分布からの出力のAP族

一様分布に従った出力での期待値及び標準偏差をまとめておく．6次対称群S_6の任意の部分集合をひとつ考え，これをAとする．$i = 1, 2, \ldots, N$に対して，S_6からひとつの標本(置換)を無作為抽出してその置換がAに属しているとき$X_i = 1$, Aに属していないとき$X_i = 0$とする確率変数X_iを考える．$p = |A|/|S_6|$とおけば，X_iはベルヌーイ分布$\mathrm{B}(1, p)$に従っており，故にYを，S_6からN個復元無作為抽出したときのAに属している置換の個数，とすれば$Y = \sum_{i=1}^{N} X_i$であり，これは二項分布$\mathrm{B}(N, p)$に従う．よってYの期待値$E[Y]$はNp, Yの標準偏差$SD[Y]$は$\sqrt{Np(1-p)}$である．

さて，$D^{\mathrm{I,III}}$のデータの個数は969個であるから，$N = 969$として，AをそれぞれのS, S_{inv},$S_\cap$,$S_\cup$(Sは AP, NAP, AAPのいずれか)で計算するとAの票数の期待値と標準偏差[16]は

期待値/標準偏差　一様分布

	AP	NAP	AAP
S	16.150/3.9851	80.750/8.6035	64.600/7.7649
S_{inv}	〃	〃	〃
$S_\cap$	〃	29.608/5.3576	26.917/5.1156
$S_\cup$	〃	131.89/10.674	102.28/9.5649

[15]アンケート回答者に番号$i (i = 1, 2, \ldots, 1040)$を振って，$\sigma_i^{\mathrm{I}}$は回答者番号$i$の設問Iの回答した置換，$\sigma_i^{\mathrm{III}}$は回答者番号$i$の設問IIIの回答した置換とする．設問IまたはIIIで置換となっていない回答は除外する．詳細は[1]参照のこと．

[16]期待値は第4.1.1節の期待値と同じ値になる．標準偏差は異なる．

となる．もし，$D^{\mathrm{I,III}}$が一様分布からの出力だとすると，各AP族の票数の偏差値は

票数の偏差値　$D^{\mathrm{I,III}}$

	AP	NAP	AAP
S	+6.2358	+2.7024	+3.3999
S_{inv}	〃	+4.2134	+3.7863
$S_{\cap}$	〃	+5.2993	+5.4898
$S_{\cup}$	〃	+2.9143	+2.8978

となり，特にAP, $AAP_{\cap}$, $NAP_{\cap}$の集合は極めて票数が多いことがわかる．

全変動距離を用いた考察では$D^{\mathrm{I,III}}$は一様分布からの出力と区別がつかなかったのであるが，しかし，このAP, $AAP_{\cap}$, $NAP_{\cap}$の票数の異常な多さを見ると，$D^{\mathrm{I,III}}$を一様分布からの出力とみなすには無理があるようである．

4.2　全変動距離が小さい偽装データ

[1]のアンケートの回答データは，ある単純な方法のデータ改変で，その一様分布からの全変動距離を小さくすることができる．従ってそれら改変されたデータ(偽装データ)は全変動距離の値からでは一様分布からの出力と区別がつかないことになる．

4.2.1　回答データの全変動距離を小さくする方法

$D^{\mathrm{I,III}}$で一票も取らない置換は189個である．この個数は，第3.2節の冒頭で述べた設問I,II,III,IVの回答で一票も取らない置換の個数より随分と少ない．どうもこの「一票も取らない置換が少ない」ことが一様分布からの全変動距離が小さくなる理由のひとつのようである．そこで，次のデータ操作(1)と(2)の両方を行うデータ改変方法を方法(M)と名付けよう．

(1) 設問Iの回答データで「一票も取らない置換」の259個のうち151個[17]の置換に一票を加える．但し，この一票加える置換はAP族以外から選ぶ.[18]

(2) 票数が異常に多い置換の票数を減らす.[19]具体的には，8票を超えたものはすべて8票にする.[20]

この方法(M)で設問Iの回答データを改変(偽装)したものを$D^{\mathrm{I}}_{\mathrm{M}}$としよう．この$D^{\mathrm{I}}_{\mathrm{M}}$のデータの個数は1099である．$S_6$から(一様分布に従って)1099個の置換を復元無作為抽出したデータの一様分布からの全変動距離の期待値と標準偏差(理論値[21])は順に0.33152, 0.0080013であり，一方$D^{\mathrm{I}}_{\mathrm{M}}$の一様分布からの全変動距離は0.33153である．この値0.33153は期待値の理論値0.33152に相当に近い．例えばこの値から期待値を引いて標準偏差で割った値(偏差値)は0.0011768である．このデータ$D^{\mathrm{I}}_{\mathrm{M}}$は，一様分布からの全変動距離の値を見る限りは一様分布からの出力と全く区別できない．

4.2.2　AP族の票数

一方で$D^{\mathrm{I}}_{\mathrm{M}}$のAP族の票数は次の様になる．

票数　$D^{\mathrm{I}}_{\mathrm{M}}$

	AP	NAP	AAP
S	40	131	109
S_{inv}	〃	118	104
$S_{\cap}$	〃	66	64
$S_{\cup}$	〃	183	149

先の第4.1.2節と同様に考える．$D^{\mathrm{I}}_{\mathrm{M}}$のデータの個数は1099であるから，$N = 1099$として，第4.1.2節の$A$をそれぞれの$S$, S_{inv}, $S_{\cap}$, $S_{\cup}$(SはAP, NAP, AAPのいずれか)で計算するとAの票数の期待値と標準偏差は

[17]151個の理由は，この個数が設問Iの回答データの改変にとって都合がよいからである．つまり，設問Iの回答データをこの個数でデータ改変したものが，一様分布からの全変動距離が期待値(理論値)により近くなるのである．

[18]この条件はAP族の票を増やさない為である．

[19]一様分布からの出力ならば，異常に票が多い置換が存在する確率は小さいからである．一様分布からの全変動距離が小さくても票数が異常に多い置換があるとそれだけで一様分布からの出力とは思えないということになる．

[20]計算機シュミレーションでは，S_6から1000個の無作為抽出データで9票以上の置換があるのは稀(10万回中1038回の1.038%)である．

[21]一様分布からの全変動距離の期待値と標準偏差に関しては[1]参照のこと．

期待値/標準偏差　一様分布

	AP	NAP	AAP
S	18.317/4.2440	91.583/9.1625	73.267/8.2694
S_{inv}	〃	〃	〃
$S_\cap$	〃	33.581/5.7057	30.528/5.4479
$S_\cup$	〃	149.59/11.368	116.01/10.186

となる．

もし，$D_{\mathrm{M}}^{\mathrm{I}}$が一様分布からの出力だとすると，各AP族の票数の偏差値は

票数の偏差値　$D_{\mathrm{M}}^{\mathrm{I}}$

	AP	NAP	AAP
S	+5.1092	+4.3020	+4.3212
S_{inv}	〃	+2.8831	+3.7165
$S_\cap$	〃	+5.6820	+6.1440
$S_\cup$	〃	+2.9394	+3.2391

となり，特にAP, $NAP_\cap$, $AAP_\cap$の3つは極めて票数が多いことがわかる．従って，第4.1.2節と同じ結論，すなわち，データ$D_{\mathrm{M}}^{\mathrm{I}}$は全変動距離からでは一様分布からの出力と全く区別がつかないのだが，このAP, $NAP_\cap$, $AAP_\cap$の票数の異常な多さから考えると，$D_{\mathrm{M}}^{\mathrm{I}}$を一様分布からの出力とみなすには無理があるようである．

4.3　置換の積(変種)

この小節では，第3節の結果の応用というよりは，それが使えないケース，すなわち，全変動距離が小さいあるデータについて，AP族の票数を調べる方法が「効かない」ものの例を述べる．勿論，そのような例があるからといって直ちに，AP族の票数を調べるのは役に立たない，ということにはならないだろう.[22]この小節のデータは，全変動距離は小さくして，且つ，AP族の票も小さくするような，ヒトが生成する置換のデータを加工する方法の1つの例にもなっている．

4.3.1　積の間に挟む

[1]では$D^{\mathrm{I,III}}$の代わりに，$\tau \in S_6$に対して

$$D_\tau^{\mathrm{I,III}} := (\sigma_i^{\mathrm{I}} \circ \tau \circ \sigma_i^{\mathrm{III}} \ ; \ \sigma_i^{\mathrm{I}}, \sigma_i^{\mathrm{III}} \in S_6)_{i=1,\ldots,1040}$$

を考え，特定のτ(例えば$\tau = (532641)$)のケースでは$D_\tau^{\mathrm{I,III}}$の一様分布からの全変動距離はとても小さいという報告をした．以下，τを(532641)に固定して考える．このときの$D_\tau^{\mathrm{I,III}}$のデータの個数は1022であり，$D_\tau^{\mathrm{I,III}}$の一様分布からの全変動距離は0.33067である．また，S_6から(一様分布に従って)1022個の置換を復元無作為抽出したデータの一様分布から全変動距離の期待値と標準偏差(理論値)は順に0.34309と0.0082571である．よって，$D_\tau^{\mathrm{I,III}}$の一様分布からの全変動距離の偏差値(期待値との差を標準偏差で割ったもの)は-1.5048である.[23]

さらにこの$D_\tau^{\mathrm{I,III}}$のAP族の票数は少ないのである．以下の表はその票数である．

票数　$D_{(532641)}^{\mathrm{I,III}}$

	AP	NAP	AAP
S	11	90	70
S_{inv}	〃	79	62
$S_\cap$	〃	24	19
$S_\cup$	〃	145	113

第4.1.2節と同様に考える．$D_\tau^{\mathrm{I,III}}$のデータの個数は1022であるから，$N = 1022$として，第4.1.2節のAをそれぞれのS, S_{inv}, $S_\cap$, $S_\cup$(Sは AP, NAP, AAPのいずれか)で計算するとAの票数の期待値と標準偏差は

期待値/標準偏差　一様分布

	AP	NAP	AAP
S	17.033/4.0926	85.167/8.8357	68.133/7.9744
S_{inv}	〃	〃	〃
$S_\cap$	〃	31.228/5.5021	28.389/5.2536
$S_\cup$	〃	139.11/10.962	107.88/9.8230

である．もし，$D_\tau^{\mathrm{I,III}}$が一様分布からの出力だとすると，各AP族の票数の偏差値は

票数の偏差値　$D_{(532641)}^{\mathrm{I,III}}$

	AP	NAP	AAP
S	-1.4742	+0.54702	+0.23408
S_{inv}	〃	-0.69793	-0.76913
$S_\cap$	〃	-1.3136	-1.7871
$S_\cup$	〃	+0.53770	+0.52145

[22]全変動距離の値では「パス」してもAP族の票数で「パス」しない例を第4.1節, 第4.2節に挙げたが，だからといって全変動距離の値を調べることは無意味ということにはならないだろう．この小節は全変動距離の値でもAP族の票数でもパスしてしまう例である．そもそもどのような方法でもパスしてしまうデータならば，一様分布からの出力と区別することはできない．

[23]この-1.5048はやや小さいが小さくて怪しいというほどではない．

となる．特に±2.0を超えるような大きな偏差値はひとつもない．つまりAP族の票数からは，$D_\tau^{\mathrm{I,III}}$が一様分布からの出力でないと推測することはできない．[24]

そもそも何故$\tau=(532641)$という特定の置換を積の間に挟むという不自然なことをするのか，という疑問もあろう．結論から言えば、全変動距離が小さくなるように「探してきた」のである．確かに不自然な感はあるのだが，しかしAP族の票数を調べることは万能ではないという具体例を述べることは意義があろう．

4.3.2 $D^{\mathrm{I,III}}$でAP族の票数が多い理由

単に積を取った$D^{\mathrm{I,III}}$にAP族の票数が多い理由は,「AP族は積で閉じる割合が多い」からのようである．

例えばAPはS_6の部分群であるから，当然積で閉じている．また，NAP型(及びAAP型)については($NAP_\cap$(resp. $AAP_\cap$)がその票数の多さに顕著性をもつので) $NAP_\cap$(resp. $AAP_\cap$)に着目すると，積がまた$NAP_\cap$(resp. $AAP_\cap$)である割合が高い．$NAP_\cap$(resp. $AAP_\cap$)の任意の2つの積がまた$NAP_\cap$(resp. $AAP_\cap$)に属する割合の具体的な数値は53.719%(resp. 56.000%)である．この値はid $\in A$となるS_6の部分集合Aで$|A|=|NAP_\cap|$ (resp. $|A|=|AAP_\cap|$)を満たすもの，のAの任意の2つの積がまたAに属する割合の期待値(理論値) 11.850%(resp. 12.483%) より遙かに大きい．従って，[1]のアンケートの回答データのように，AP族の票数が多い2つのデータには，$D^{\mathrm{I,III}}$のようにその積にもAP族の票数が多くなる傾向があるのだと思われる．

一方で$D_\tau^{\mathrm{I,III}}$のように積の間に(id以外の)置換を挟んでしまうと，この「AP族は積で閉じる割合が多い」が活かせないようである．すなわち，設問IとIIIの回答データにはAP族が多いのだけれども，積をとるときにτを掛けて一方の回答データを「平行移動」させてしまったことで「AP族は積で閉じる割合が多い」が役に立たなくなるのだと想像される．

5 まとめ

[1]のアンケートのそれぞれの設問での回答はヒトが生成する(6次の)置換である．これらヒトが生成する置換にはある種の偏りがあるのではないか，という推測が本稿の動機である．[1, 第4.1.3節]のように人気がある置換をいくつか並べてみて，特に対称群や置換の群論的な視点からあれこれと眺めてみたのだが，これといった「法則」は見つからない．そこで群論からの視点ではなく，もっと素朴に置換の「数の並び」に着目してみた．数の並びで最も簡単な規則性であるAP型を考えてみたが，6次のAP型は12個と数が少なく，AP型以外の置換にも人気がある置換がいくつもある．AP型だけで4種類の設問の回答すべてを説明するには難しそうである．そこで公差と初項を実数に拡げてNAP型を持ち出したのだが，NAP型はその置換を列挙するのも容易ではない．そこで(NAP型の部分集合として)AAP型を持ち出した．扱い易さという点ではNAP型よりAAP型の方が優れている．また，ヒトが等差数列を補正しながら置換を作るとすればNAP型よりAAP型の方が負担が少ないであろう．これらNAP型やAAP型，そしてそれらの逆置換を一括りにAP族と呼ぶとき，統計的にAP族はヒトに選ばれやすい置換のようだ，というのが本稿の主張である．[1]のアンケートの回答データから，$NAP_\cap$や$AAP_\cap$は特にヒトに選ばれやすいという結果になった．さらに置換の積のデータ$D^{\mathrm{I,III}}$にも同様なことが言え，[1]での$D^{\mathrm{I,III}}$の全変動距離等に関する結果とあわせると興味あるものになったと思う．第4節の内容からは「ベンフォードの法則とその数値改竄への応用」が連想される．以上はすべてアンケート調査による統計的結果である．一方で数学としてはAP族，特にNAP型の置換に興味

[24] 実は$\tau=(532641)$のときのデータ$D_\tau^{\mathrm{I,III}}$はτが21票ある．一つの置換が21票という異常に大きい票数を獲得するという事実から$D_\tau^{\mathrm{I,III}}$を一様分布からの出力と思うには無理があるとなろう．つまり，一様分布からの全変動距離とAP族の票数の偏差値では一様分布からの出力と区別が付かないのであるが，特定の置換の票数が異常に多い，という(非常にシンプルな)観点から$D_\tau^{\mathrm{I,III}}$は一様分布からの出力ではなさそうだ，ということになる．

があろう．AP型は部分群をなすが，NAP型はそうでなく群論的には由緒正しいものではなさそうである．しかしいわゆるSós置換[3, 4]との関連も観察され，どうやらNAP型の置換はDiophantine近似の分野と関連がありそうである．今後はNAP型の置換やその周辺に関してさらに理解を深めていきたい．

参考文献

[1] ヒトが生成する置換の統計的性質： 永田誠，武井由智　大阪薬科大学紀要 Vol. 13 pp.5–36 (2019)

[2] Min-Wise Independent Permutations : Andrei Z. Broder, Moses Charikar, Alan M. Frieze, Michael Mitzenmacher　J. Comput. Syst. Sci. 60(3), pp.630-659 (2000)

[3] On the distribution mod 1 of the sequence $n\alpha$: Vera. T. Sós　Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Math. 1, pp.127-134 (1958)

[4] Farey fractions and permutations generated by fractional part $\{i\alpha\}$: A. V. Shutov Chebyshevskii Sb., Vol.15(1), pp.195-203 (2014)

付録A

AP族の性質について

AP族に関する性質とその証明を述べる．以下，nは2以上の自然数とし，記号≡は「mod nで合同」を意味する．また，(a,n)は整数aとnの最大公約数の意味とする．混乱を避けるためaとbの組は丸括弧ではなく，山括弧$\langle a,b\rangle$で表す．開区間を指定する場合は丸括弧を用いるが，その場合には開区間$(0,1)$等のように開区間であることを明示する． また$\mathrm{Mod}(m,n)$は整数mをnで割った余りを意味する．

付録A.1　AP型について

命題 AP-1　$a\in\mathbb{Z}$のとき，次の(1)と(2)は同値である．
(1) $\{\mathrm{Mod}(ai,n)\ ;\ i=0,1,\ldots,n-1\}=\{0,1,\ldots,n-1\}$.
(2) aとnは互いに素．すなわち $(a,n)=1$.

(証明) (2)のとき，$i,j\in\{0,1,\ldots,n-1\}$ with $i<j$ に対して$ai\equiv aj$と仮定すると，$a(i-j)\equiv 0$ であり，(2)より$i-j\equiv 0$であるが，これは$0\le j<i\le n-1$よりあり得ない．すなわち$ai\not\equiv aj$である．このことは，$i=0,1,\ldots,n-1$に対して$ai \mod n$はすべて異なることを示している．故に(1)が成立する．
(1)のとき，$(a,n)=\ell>1$と仮定する．このとき，$a=a'\ell$, $n=n'\ell$ with $1\le n'\le n-1$ なる $a',n'\in\mathbb{Z}$が存在する．$an'=a'\ell n'=a'n\equiv 0$より，$0<n'\le n-1$で$0=a0\equiv an'$が成立する．従って(1)の等式の左辺の集合の要素の個数は$n-1$以下であるが，その等式の右辺の集合の要素の個数はnなので矛盾．故に(2)が成立する．□

命題 AP-2　次の(1),(2)が成立する．
(1) $\sigma\in S_n$に対して，$\exists\, a,b\in\mathbb{Z}$ s.t. σは$\langle a,b\rangle$-NAP型である，ならば $(a,n)=1$.
(2) $a,b\in\mathbb{Z}$ が $(a,n)=1$を満たすならば，$[n]$から$[n]$への写像$\sigma(i):=\mathrm{Mod}(a(i-1)+b,n)+1$, $i\in[n]$ は全単射写像である．すなわち写像σは$\langle a,b\rangle$-AP型の置換である．

(証明) (1) $a,b\in\mathbb{Z}$なので$\lfloor a(i-1)+b\rfloor=a(i-1)+b$である．よって$\sigma(i)=\mathrm{Mod}(a(i-1)+b,n)+1$であるから，$\{\mathrm{Mod}(ai+b,n)\ ;\ i=0,1,,\ldots,n-1\}=\{\mathrm{Mod}(a(i-1)+b,n)\ ;\ i=1,2,\ldots,n\}=\{\sigma(i)-1\ ;\ i=1,2,\ldots,n\}=\{0,1,\ldots,n-1\}$ である．命題 AP-1より$(a,n)=1$である．
(2) 命題 AP-1より$\{\mathrm{Mod}(a(i-1)+b,n)\ ;\ i=1,2,\ldots,n\}=\{0,1,\ldots,n-1\}$ すなわち$\{\mathrm{Mod}(a(i-1)+b,n)+1\ ;\ i=1,2,\ldots,n\}=\{1,\ldots,n\}$ であり，故に$\sigma(i):=\mathrm{Mod}(a(i-1)+b,n)+1$, $i=1,2,\ldots,n$ は $[n]$から$[n]$への全単射写像である．□

命題 AP-3　n次のAP型の置換は$n\phi(n)$個ある．

(証明) AP型の定義より$\langle a,b\rangle$-AP型と$\langle a+n,b\rangle$-AP型と$\langle a,b+n\rangle$-AP型は同一の置換であることがわかる．故に，集合

$$B := \{\langle a,b\rangle \in [n-1]\times\{0,1,\ldots,n-1\}\ ;\ (a,n)=1\}$$

の要素$\langle a,b\rangle \in B$に対して，(命題 AP-2の(2)より$\langle a,b\rangle$-AP型となる置換が存在することより) それらの異なるAP型の個数がn次のAP型の個数である．特にn次のAP型は$|B|$個以下である．さて，もしも$\langle a,b\rangle,\langle a',b'\rangle \in B$で$\langle a,b\rangle$-AP型と$\langle a',b'\rangle$-AP型が同じ置換であるならば，$i=1,\ldots,n$で$\mathrm{Mod}(a(i-1)+b,n)=\mathrm{Mod}(a'(i-1)+b',n)$である．特に$i=1$で$b=b'$がわかる．さらに$i=2$で$a=a'$がわかる．つまり$\langle a,b\rangle=\langle a',b'\rangle$である．故に$\langle a,b\rangle\neq\langle a',b'\rangle$ならば$\langle a,b\rangle$-AP型と$\langle a',b'\rangle$-AP型は異なる置換である．故に$n$次のAP型は丁度$|B|$個である．以上より$n$次のAP型は全部で$n\phi(n)$個ある．□

命題 AP-4　2つのn次のAP型の置換の積はAP型である．

(証明) $\sigma,\tau\in S_n$をそれぞれ$\langle a,b\rangle$-AP型，$\langle c,d\rangle$-AP型とする．$\tau\circ\sigma(i)=\tau(\sigma(i))=\tau(\mathrm{Mod}(a(i-1)+b,n)+1)=\mathrm{Mod}(c(\mathrm{Mod}(a(i-1)+b,n)+1-1)+d,n)+1=\mathrm{Mod}(c\mathrm{Mod}(a(i-1)+b,n)+d,n)+1$ に注意する．

Claim: $i\in[n]$に対して，$\mathrm{Mod}(c\mathrm{Mod}(a(i-1)+b,n)+d,n)=\mathrm{Mod}(ac(i-1)+bc+d,n)$である．

(Claimを示す．$i\in[n]$に対して，$a(i-1)+b=m_in+r_i$ なる$m_i,r_i\in\mathbb{Z}$ with $0\le r_i<n$をとる．このとき，$\mathrm{Mod}(c\mathrm{Mod}(a(i-1)+b,n)+d,n)=\mathrm{Mod}(cr_i+d,n)$である．一方，$\mathrm{Mod}(ac(i-1)+bc+d,n)=\mathrm{Mod}(c(a(i-1)+b)+d,n)=\mathrm{Mod}(c(m_in+r_i)+d,n)=\mathrm{Mod}(cr_i+d,n)$である．故にClaimが成立する．)

Claimより，$(a,n)=(c,n)=1$のとき$(ac,n)=1$であるから，命題 AP-2より$\tau\circ\sigma$は$\langle ac,bc+d\rangle$-AP型であることがわかる．□

命題 AP-5　AP型の逆置換はAP型である．

(証明) 命題 AP-3の証明で用いた集合Bを利用する．$\langle 1,0\rangle$-AP型が単位置換である．命題 AP-4の証明より$\langle a,b\rangle\in B$に対して，$ac\equiv 1$ 且つ$bc+d\equiv 0$ となる$c,d\in\mathbb{Z}$が存在すればよい．このとき(もし$(c,n)>1$ならば$ac\equiv 1$でないから)$(c,n)=1$であり，命題 AP-2の(2)より$\langle c,d\rangle$-AP型は存在する．さて、$(a,n)=1$より不定方程式$xa+yn=1$の整数解x,yが存在するが，ここで$c=x$, $d=-bc$とおけば，$ac\equiv 1$ 且つ$bc+d\equiv 0$が成り立つ．□

次はAP型の別定義を与える．これは以下の命題 NAP-1，及びpNAP型の定義の前振りとなる．

命題 AP-6　$\sigma\in S_n$に対して，次の(1)と(2)は同値である．

(1) σはn次のAP型である．

(2) 集合$K_\sigma=\{\mathrm{Mod}(\sigma(i)-\sigma(i+1),n)\ ;\ i\in[n-1]\}$に対して，$\exists\, m\in[n-1]$ s.t. $K_\sigma=\{m\}$である．

(証明) (1)とする．命題 AP-3の証明での集合Bを用いると，$\exists\,\langle a,b\rangle\in B$ s.t. σは$\langle a,b\rangle$-AP型である．$i\in[n]$に対して，$ai+b\equiv c_i$ with $0\le c_i\le n-1$とすると，$1\le a\le n-1$に注意して

$$\sigma(i)-\sigma(i+1)=\mathrm{Mod}(a(i-1)+b,n)-\mathrm{Mod}(ai+b,n)=\mathrm{Mod}(c_i-a,n)-c_i=\begin{cases} c_i-a-c_i=-a & \text{if } a\le c_i\\ c_i-a+n-c_i=-a+n & \text{if } c_i<a\end{cases}$$

である．故に$\mathrm{Mod}(\sigma(i)-\sigma(i+1),n)=n-a$であり，$a\in[n-1]$であるから$n-a\in[n-1]$である．$m=n-a$として(2)が成り立つ．

(2)とする．aを$m=n-a$となる整数, すなわち $a=n-m$とする．$\mathrm{Mod}(\sigma(1)-\sigma(2),n)=n-a$より$\sigma(2)\equiv\sigma(1)+a$. 同様にして$i\in[n-1]$で$\mathrm{Mod}(\sigma(i)-\sigma(i+1),n)=n-a$より$\sigma(i+1)\equiv\sigma(i)+a$である．故に$i\in[n]$で$\sigma(i)\equiv a(i-1)+\sigma(1)$, すなわち$\sigma(i)=\mathrm{Mod}(a(i-1)+\sigma(1)-1,n)+1$である．従って$\sigma$は$\langle a,\sigma(1)-1\rangle$-AP型の置換である．□

付録A.2　AAP型について

命題 AAP-1　$a\in[n-1]$, $b\in\{0,1,\ldots,n-1\}$を任意に固定する．$[n]$から$[n]$への写像$f_{a,b}$, $g_{a,b}$を次で定義する：$i\in[n]$に対して，

$$f_{a,b}(i) := \mathrm{Mod}(\lfloor a(i-1)+\frac{(a,n)}{n}(i-1)+b\rfloor,n)+1$$

$$g_{a,b}(i) := \mathrm{Mod}(\lfloor a(i-1) + \frac{(a,n)}{n}(n-i) + b \rfloor, n) + 1$$

このとき，$f_{a,b}$, $g_{a,b}$はそれぞれ$[n]$から$[n]$への全単射写像である．

さらに，a,bが組として異なればそれぞれは異なる写像である．すなわち，$a,c \in [n-1]$, $b,d \in \{0,1,\ldots,n-1\}$が$\langle a,b\rangle \neq \langle c,d\rangle$であれば[25]，写像として$f_{a,b} \neq f_{c,d}$ 且つ $g_{a,b} \neq g_{c,d}$である．

すなわち，n次対称群S_nへの写像

$$f_{\cdot,\cdot} : [n-1] \times \{0,1,\ldots,n-1\} \to S_n, \quad \langle a,b\rangle \mapsto f_{a,b}$$

はwell-def. な単射写像である．$g_{\cdot,\cdot}$ についても同様である．

(証明) $f_{a,b}$, $g_{a,b}$が$[n]$から$[n]$への写像であるのは$\mathrm{Mod}(\cdot,n)$の定義から良いであろう．さて，aとnの最大公約数(a,n)をℓとする．a',n'を$a = a'\ell$, $n = n'\ell$ とすると，$(a',n') = 1$である．$0 \leq i < j < n$なる整数i,jに対して$ai \equiv aj$ であることと$a'\ell(j-i) \equiv 0$ であることは同値であるから$\mathrm{Mod}(ai,n)$, $i = 0,1,\ldots,n-1$は周期n'を持つ．さらにこのn'は基本周期である．なぜなら$0 \leq i < j < n'$で$ai \equiv aj$ ならば$a'\ell(j-i) \equiv 0$ であるから，$\exists\, m \in \mathbb{Z}$ s.t. $a'\ell(j-i) = mn = mn'\ell$ であり$a'(j-i)$はn'の倍数である．$(a',n') = 1$であるから，$j-i$はn'の倍数でなくてはならないが，これは$0 \leq i < j < n'$に矛盾する．

主張の前半を示す．ここで$\frac{(a,n)}{n} = \frac{1}{n'}$より，

- $i = 1,2,\ldots,n'$に対して$\frac{(a,n)}{n}(i-1) = \frac{i-1}{n'}$は0以上1未満である．
- ($\ell \geq 2$の場合)$i = n'+1,\ldots,2n'$に対して$\frac{(a,n)}{n}(i-1)$は1以上2未満である．
- $i = kn'+1,\ldots,(k+1)n'$ $(k = 0,1,\ldots,\ell-1)$ に対して$\frac{(a,n)}{n}(i-1)$はk以上$k+1$未満である．

従って，$i = 1,\ldots,n$に対して$\mathrm{Mod}(\lfloor a(i-1) + \frac{(a,n)}{n}(i-1) \rfloor, n)$の値は

- $i = 1,\ldots,n'$に対しては順に $\mathrm{Mod}(0,n)$, $\mathrm{Mod}(a,n)$, …, $\mathrm{Mod}(a(n'-1),n)$ である．
- ($\ell \geq 2$の場合)$i = n'+1,\ldots,2n'$に対しては順に $\mathrm{Mod}(an'+1,n)$, $\mathrm{Mod}(a(n'+1)+1,n)$, …, $\mathrm{Mod}(a(2n'-1)+1,n)$ であるが，$an' = a'\ell n' = a'n$であるから，これらは順に$\mathrm{Mod}(1,n)$, $\mathrm{Mod}(a+1,n)$, …, $\mathrm{Mod}(a(n'-1)+1,n)$ と等しい．
- $i = kn'+1,\ldots,(k+1)n'$ $(k = 0,\ldots,\ell-1)$に対しては順に $\mathrm{Mod}(akn'+k,n)$, $\mathrm{Mod}(a(kn'+1)+k,n)$, …, $\mathrm{Mod}(a((k+1)n'-1)+k,n)$ であるが，同様に$an' = a'\ell n' = a'n$であるから，これらは順に$\mathrm{Mod}(k,n)$, $\mathrm{Mod}(a+k,n)$, …, $\mathrm{Mod}(a(n'-1)+k,n)$ と等しい．

Claim: $s,t,i,j \in \mathbb{Z}$ with $0 \leq s,t \leq \ell-1$, $0 \leq i < j \leq n'-1$に対して，$ai+s \not\equiv aj+t$である．

(Claimを示す．$ai+s \equiv aj+t$と仮定する．$s = t$のとき，$ai \equiv aj$であり，$a'\ell(i-j) \equiv 0$である．すなわち$\exists\, m \in \mathbb{Z}$ s.t. $a'\ell(i-j) = mn = mn'\ell$ であるから$a'(i-j) = mn'$となり，$a'(i-j)$はn'の倍数である．$(a',n') = 1$より$i-j$はn'の倍数となるが，これは$0 \leq i < j \leq n'-1$に反する．$s \neq t$のときは，$0 \leq s,t \leq \ell-1$の条件より$\ell > 1$であることに注意しておく．このとき，$a'\ell(i-j) \equiv t-s$ であるから$\exists\, m \in \mathbb{Z}$ s.t. $t-s = a'\ell(i-j)+mn = a'\ell(i-j)+mn'\ell$ である．故に$t-s = \ell(a'(i-j)+m)$より$t-s$はℓの倍数であるが，これは$s \neq t$且つ$0 \leq s,t \leq \ell-1$に反する．)

従ってClaimより$\mathrm{Mod}(\lfloor a(i-1) + \frac{(a,n)}{n}(i-1) \rfloor, n)$は$i = 1,\ldots,\ell n'(= n)$ですべて異なる．$\mathrm{Mod}(\cdot,n)$の値は$n$通りしかないので，($b = 0$のときの)写像$f_{a,0}$は$[n]$から$[n]$の全単射写像である．$b \in [n-1]$については，$f_{a,0}$を$b$だけ平行移動しているだけであるから，$b \in [n-1]$のときの$f_{a,b}$も$[n]$から$[n]$の全単射写像である．

$g_{a,b}$に関しても同様であるが念のために書いておく．$\frac{(a,n)}{n}(n-i) = \frac{1}{n'}(n'\ell - i) = \ell - \frac{i}{n'}$より

- $i = 1,2,\ldots,n'$に対して$\frac{(a,n)}{n}(n-i)$は$\ell-1$以上ℓ未満である．
- ($\ell \geq 2$の場合)$i = n'+1,2,\ldots,2n'$に対して$\frac{(a,n)}{n}(n-i)$は$\ell-2$以上$\ell-1$未満である．
- $i = kn'+1,\ldots,(k+1)n'$ $(k = 0,1,\ldots,\ell-1)$ に対して$\frac{(a,n)}{n}(n-i)$は$\ell-k-1$以上$\ell-k$未満である．

従って，$i = 1,\ldots,n$に対して$\mathrm{Mod}(\lfloor a(i-1) + \frac{(a,n)}{n}(n-i) \rfloor, n)$の値は

- $i = 1,\ldots,n'$に対しては順に $\mathrm{Mod}(0+\ell-1,n)$, $\mathrm{Mod}(a+\ell-1,n)$, …, $\mathrm{Mod}(a(n'-1)+\ell-1,n)$ である．
- ($\ell \geq 2$の場合)$i = n'+1,\ldots,2n'$に対しては順に $\mathrm{Mod}(an'+\ell-2,n)$, $\mathrm{Mod}(a(n'+1)+\ell-2,n)$, …, $\mathrm{Mod}(a(2n'-1)+\ell-2,n)$ であるが，$an' = a'\ell n' = a'n$であるから，これらは順に$\mathrm{Mod}(\ell-2,n)$, $\mathrm{Mod}(a+\ell-2,n)$, …, $\mathrm{Mod}(a(n'-1)+\ell-2,n)$ と等しい．

[25]繰り返しになるが，組は(,)ではなく⟨ , ⟩という記号を用いている．

• $i = kn'+1, \ldots, (k+1)n'$ $(k = 0, \ldots, \ell-1)$に対しては順に $\mathrm{Mod}(akn'+\ell-k-1, n)$, $\mathrm{Mod}(a(kn'+1)+\ell-k-1, n)$, …, $\mathrm{Mod}(a((k+1)n'-1)+\ell-k-1, n)$ であるが，同様に$an' = a'\ell n' = a'n$であるから，これらは順に$\mathrm{Mod}(\ell-k-1, n)$, $\mathrm{Mod}(a+\ell-k-1, n)$, …, $\mathrm{Mod}(a(n'-1)+\ell-k-1, n)$ と等しい．

従ってClaimより$\mathrm{Mod}(\lfloor a(i-1)+\frac{(a,n)}{n}(n-i)\rfloor, n)$は$i = 1, \ldots, \ell n'(= n)$ですべて異なり，$\mathrm{Mod}(\cdot, n)$の値は$n$通りしかないので，($b = 0$のときの)写像$g_{a,0}$は$[n]$から$[n]$の全単射写像である．$b \in [n-1]$については，$g_{a,0}$を$b$だけ平行移動しているだけであるから，$b \in [n-1]$のときの$g_{a,b}$も$[n]$から$[n]$の全単射写像である．

主張の後半を示す．$b, d \in \{0, 1, \ldots, n-1\}$と$a \in [n-1]$に対して，$\frac{(a,n)}{n} < 1$であるから$f_{a,b}(1) - f_{a,b}(2) = \mathrm{Mod}(b, n) - \mathrm{Mod}(a+b, n) = \mathrm{Mod}(-a, n)$ であり，同様に$c \in [n-1]$, $a \neq c$に対して$f_{c,d}(1) - f_{c,d}(2) = \mathrm{Mod}(d, n) - \mathrm{Mod}(c+d, n) = \mathrm{Mod}(-c, n)$ である．故に$a, c \in [n-1]$で$a \neq c$ならば写像$f_{a,b}$と$f_{c,d}$は異なる．さらに，$a = c \in [n-1]$, $b, d \in \{0, 1, \ldots, n-1\}$ with $b \neq d$に対しては，$f_{a,b}(1) = \mathrm{Mod}(b, n) + 1$, $f_{a,d}(1) = \mathrm{Mod}(d, n) + 1$であるから写像$f_{a,b}$と$f_{a,d}$は異なる．同様にして$b, d \in \{0, 1, \ldots, n-1\}$と$a \in [n-1]$に対して，$\frac{(a,n)}{n} < 1$であるから$g_{a,b}(n) - g_{a,b}(n-1) = \mathrm{Mod}(a(n-1)+b, n) - \mathrm{Mod}(a(n-2)+b, n) = \mathrm{Mod}(a, n)$ であり，また$c \in [n-1]$, $a \neq c$に対して$g_{c,d}(n) - g_{c,d}(n-1) = \mathrm{Mod}(c(n-1)+d, n) - \mathrm{Mod}(c(n-2)+d, n) = \mathrm{Mod}(c, n)$ である．故に$a, c \in [n-1]$で$a \neq c$ならば写像$g_{a,b}$と$g_{c,d}$は異なる．さらに，$a = c \in [n-1]$, $b, d \in \{0, 1, \ldots, n-1\}$ with $b \neq d$に対しては，$g_{a,b}(n) = \mathrm{Mod}(-a+b, n)$, $g_{a,d}(n) = \mathrm{Mod}(-a+d, n)$ であるから写像$g_{a,b}$と$g_{a,c}$は異なる．□

命題 AAP-2 $a, c \in [n-1]$, $b, d \in \{0, 1, \ldots, n-1\}$に対して，命題 AAP-1の写像$f_{a,b}$, $g_{c,d}$について次の(1)と(2)は同値である．

(1) $f_{a,b}$ と $g_{c,d}$が写像として一致する．

(2) $a = c$且つ$b = d$且つ$(a, n) = 1$.

(証明) (2)から(1)を示す．$(a, n) = 1$のとき，$i \in [n]$に対して，$\frac{(a,n)}{n}(i-1)$と$\frac{(a,n)}{n}(n-i)$は共に0以上1未満である．よって$f_{a,b}(i) = \mathrm{Mod}(a(i-1)+b, n)+1$, $g_{c,d}(i) = \mathrm{Mod}(c(i-1)+d, n)+1$ である．$a = c$, $b = d$のとき(1)は成立する．

(1)から(2)を示す．

$(a, n) > 1$且つ$(c, n) = 1$且つ写像として$f_{a,b} = g_{c,d}$とする．$a = a'\ell$, $n = n'\ell$なる整数ℓ, a', n'をとると$a \in [n-1]$よりaはnの倍数でないから，$n' \geq 2$である．$f_{a,b}(1) = \mathrm{Mod}(b, n)+1$, $g_{c,d}(1) = \mathrm{Mod}(d, n)+1$が等しいので，$b \equiv d$である．また，$\frac{(a,n)}{n} = \frac{1}{n'} \leq \frac{1}{2}$より$f_{a,b}(2) = \mathrm{Mod}(\lfloor a + \frac{(a,n)}{n} + b\rfloor, n) = \mathrm{Mod}(\lfloor a + \frac{1}{n'} + b\rfloor, n) = \mathrm{Mod}(a+b, n)+1$, $g_{a,b}(2) = \mathrm{Mod}(c+d, n)+1$ より$a+b \equiv c+d$である．故に$a \equiv c$, $b \equiv d$となり特に$a, c \in [n-1]$より$a = c$である．これは$(a, n) > 1$且つ$(c, n) = 1$に反する．

$(a, n) = 1$且つ$(c, n) > 1$且つ写像として$f_{a,b} = g_{c,d}$とする．$c = c'\ell$, $n = n'\ell$なる整数ℓ, c', n'をとるとcはnの倍数でないので，$n' \geq 2$である．$f_{a,b}(1) = \mathrm{Mod}(b, n)+1$, $g_{c,d}(1) = \mathrm{Mod}(\lfloor d + \frac{(c,n)}{n}(n-1)\rfloor, n)+1 = \mathrm{Mod}(\lfloor d + \frac{1}{n'}(n'\ell-1)\rfloor, n)+1 = \mathrm{Mod}(d+\ell-1, n)+1$ で$f_{a,b} = g_{c,d}$より$b \equiv d+\ell-1$である．また，$n' \geq 2$に注意すると，$f_{a,b}(2) = \mathrm{Mod}(a+b, n)+1$, $g_{a,b}(2) = \mathrm{Mod}(\lfloor c+d+\frac{(c,n)}{n}(n-2)\rfloor, n)+1 = \mathrm{Mod}(\lfloor c+d+\frac{1}{n'}(n'\ell-2)\rfloor, n)+1 = \mathrm{Mod}(c+d+\ell-1, n)+1$より$a+b \equiv c+d+\ell-1$である．故に$a \equiv c$, $b \equiv d+\ell-1$となり，特に$a, c \in [n-1]$ より$a = c$であるから，$(a, n) > 1$且つ$(c, n) = 1$に反する．

$(a, n) > 1$且つ$(c, n) > 1$且つ写像として$f_{a,b} = g_{c,d}$とする．$a = a'\ell_1$, $n = n_1\ell_1$なる整数ℓ_1, a', n_1と$c = c'\ell_2$, $n = n_2\ell_2$なる整数ℓ_2, c', n_2 をとる．$n = 2$の場合，$a = 1$しかあり得ないが，このときは$(a, n) = (1, 2) = 1$となるので考える必要はない．従って$n \geq 3$としてよい．さて，$f_{a,b}(1) = \mathrm{Mod}(b, n)+1$であり，$g_{c,d}(1) = \mathrm{Mod}(\lfloor d + \frac{(c,n)}{n}(n-1)\rfloor, n)+1 = \mathrm{Mod}(\lfloor d + \frac{1}{n_2}(n_2\ell_2-1)\rfloor, n)+1 = \mathrm{Mod}(d+\ell_2-1, n)+1$ であるから，$f_{a,b} = g_{c,d}$より$b \equiv d+\ell_2-1$である．$f_{a,b}(2) = \mathrm{Mod}(\lfloor a+\frac{(a,n)}{n}+b\rfloor, n) = \mathrm{Mod}(\lfloor a+\frac{1}{n_1}+b\rfloor, n) = \mathrm{Mod}(a+b, n)+1$であり，$n_2 \geq 2$より$g_{a,b}(2) = \mathrm{Mod}(\lfloor c+d+\frac{(c,n)}{n}(n-2)\rfloor, n)+1 = \mathrm{Mod}(\lfloor c+d+\frac{1}{n_2}(n_2\ell_2-2)\rfloor, n)+1 = \mathrm{Mod}(c+d+\ell_2-1, n)+1$であるから，$a+b \equiv c+d+\ell_2-1$である．故に$a \equiv c$, $b \equiv d+\ell_2-1$となり，$a, c \in [n-1]$ より$a = c$である．特に$\ell_1 = \ell_2 =: \ell$, $n_1 = n_2 =: n'$ となる．この記号の下では$b \equiv d+\ell-1$と書ける．$f_{a,b}(n'+1) = \mathrm{Mod}(\lfloor a(n'+1-1)+\frac{(a,n)}{n}(n'+1-1)+b\rfloor, n)+1 = \mathrm{Mod}(\lfloor a'\ell n' + \frac{1}{n'}(n') + b\rfloor, n)+1 = \mathrm{Mod}(a'n+1+b, n)+1 = \mathrm{Mod}(1+b, n)+1$. また$g_{c,d}(n'+1) = g_{a,d}(n'+1) = \mathrm{Mod}(\lfloor a(n'+1-1)+\frac{(a,n)}{n}(n-n'-1)+d\rfloor, n)+1 = \mathrm{Mod}(\lfloor \frac{1}{n'}(\ell n'-n'-1)+d\rfloor, n)+1 = \mathrm{Mod}(\lfloor \ell - \frac{n'+1}{n'} + d\rfloor, n)+1 = \mathrm{Mod}(\ell-2+d, n)+1$ である．故に$1+b \equiv \ell-2+d$となり $b \equiv d+\ell-3$である．$b \equiv d+\ell-1$であるから，$-1 \equiv -3$ すなわち $2 \equiv 0$である．$n \geq 3$よりこれはあり得ない．

以上により，写像として$f_{a,b} = g_{c,d}$ならば$(a, n) = (c, n) = 1$が必要である．

$(a, n) = (c, n) = 1$のとき，$\frac{(a,n)}{n} = \frac{(c,n)}{n} = \frac{1}{n}$であるから，$i \in [n-1]$で$f_{a,b}(i) = \mathrm{Mod}(\lfloor a(i-1)+\frac{i-1}{n}+b\rfloor, n)+1 = \mathrm{Mod}(a(i-1)+b, n)+1$であり，$g_{c,d}(i) = \mathrm{Mod}(\lfloor a(i-1)+\frac{n-i}{n}+b\rfloor, n)+1 = \mathrm{Mod}(c(i-1)+d, n)+1$である．よって，$f_{a,b}(1) = \mathrm{Mod}(b, n)+1$であり，$g_{c,d}(1) = \mathrm{Mod}(d, n)+1$より$b \equiv d$である．また，$f_{a,b}(2) = \mathrm{Mod}(a+b, n)+1$であり，$g_{c,d}(2) = \mathrm{Mod}(c+d, n)+1$より$a+b \equiv c+d$である．故に$a \equiv c$である．

以上により，写像として$f_{a,b} = g_{c,d}$ならば(2)が成り立つ．□

明らかに$f_{a,b}=f_{a+n,b}=f_{a,b+n}$であり$g_{a,b}=g_{a+n,b}=g_{a,b+n}$であるから，命題 AAP-1と命題 AAP-2，及び命題AP-3より次が成り立つ．

系 AAP-3　n次の置換に対して，次の(1),(2),(3)が成り立つ．
(1) AAP$^{(+)}$型,AAP$^{(-)}$型はぞれぞれ$(n-1)n$個ある．これらの置換は，$a\in[n-1]$, $b\in\{0,1,\ldots,n-1\}$を用いてそれぞれ$\langle a,b\rangle$-AAP$^{(+)}$型，$\langle a,b\rangle$-AAP$^{(-)}$型で与えられる．
(2) 置換σがAAP$^{(+)}$型且つAAP$^{(-)}$型であることと，AP型であることは同値である．
(3) nが素数ならば，$\langle a,b\rangle$-AAP$^{(+)}$型と$\langle a,b\rangle$-AAP$^{(-)}$型は一致して，これは$\langle a,b\rangle$-AP型である．

6次のAAP$^+$型の置換とAAP$^-$型の置換を列挙しておく．
AAP$^+$: (123456),(135246),(142536),(153264),(165432),(216543),(234561),(246351),(253641),(264315),(315426),
(321654),(345612),(351462),(364152),(415263),(426531),(432165),(456123),(462513),(513624),(526314),(531642),
(543216),(561234),(612345),(624135),(631425),(642153),(654321)
AAP$^-$: (123456),(135624),(146352),(153642),(165432),(216543),(234561),(246135),(251463),(264153),(315264),
(321654),(345612),(351246),(362514),(413625),(426315),(432165),(456123),(462351),(513462),(524136),(531426),
(543216),(561234),(612345),(624513),(635241),(642531),(654321)

付録A.3　NAP型について

以下の系 NAP-2, 系 NAP-4は，計算機を用いた結果であり，限定されたnだけの主張であることに注意しておく．

次は命題 AP-6によるAP型の1つの拡張である．

定義　nは2以上の自然数とする．n次の置換$\sigma\in S_n$と集合$K_\sigma=\{\mathrm{Mod}(\sigma(i)-\sigma(i+1),n)\ ;\ i\in[n-1]\}$ に対して$\exists\, m\in[n-2]$ s.t. $K_\sigma\subset\{m,m+1\}$ であるとき(但し$n=2$のときは$m=0$とする)，σをpNAP型(pseudo nearly arithmetic progression type)と呼ぶことにする．すなわち，「$\exists\, m\in[n-1]$ s.t. $K_\sigma=\{m\}$，あるいは$\exists\, m\in[n-2]$ s.t. $K_\sigma=\{m,m+1\}$である」という条件を満たすとき，σをpNAP型と呼ぶ．

注意：数列の差分(のnで割った余り)の集合であるK_σの代わりに，終項と初項の差(のnで割った余り)を加えた集合$\widehat{K}_\sigma=K_\sigma\cup\{\mathrm{Mod}(\sigma(n)-\sigma(1),n)\}$ を考えても構わない. この場合，K_σの要素が1個(すなわちAP型)のときは$\widehat{K}_\sigma$の要素は1個だが，K_σの要素が2個のときは$\widehat{K}_\sigma$の要素は3個となる．[26]

命題 NAP-1　NAP型の置換はpNAP型である．
特に，σが$\langle\alpha,\beta\rangle$-NAP型で，$0<\alpha<n$とすると，集合$K_\sigma=\{\mathrm{Mod}(\sigma(i)-\sigma(i+1),n)\ ;\ i\in[n-1]\}$ は$\{n-\lfloor\alpha\rfloor\}$, $\{n-\lfloor\alpha\rfloor-1\}$, $\{n-\lfloor\alpha\rfloor-1,n-\lfloor\alpha\rfloor\}$のいずれかである．

(証明) $\langle\alpha,\beta\rangle$-NAP型の置換と$\langle\alpha+n,\beta\rangle$-NAP型の置換と$\langle\alpha,\beta+n\rangle$-NAP型の置換は同一であるから，$0\le\alpha<n$, $0\le\beta<n$としても一般性は失わない．$\alpha=0$のときの$\langle\alpha,\beta\rangle$-NAP型は存在しない．何故なら定義より置換にならないからである．従って$0<\alpha<n$ 且つ $0\le\beta<n$の場合のみを考える．
σを$\langle\alpha,\beta\rangle$-NAP型とする．このとき，$i\in[n-1]$に対して

$$\sigma(i)-\sigma(i+1)=\mathrm{Mod}(\lfloor\alpha(i-1)+\beta\rfloor,n)-\mathrm{Mod}(\lfloor\alpha i+\beta\rfloor,n)$$

であるので非負の実数$\gamma_i:=\alpha(i-1)+\beta$ に対して$\mathrm{Mod}(\lfloor\gamma_i\rfloor,n)-\mathrm{Mod}(\lfloor\gamma_i+\alpha\rfloor,n)$ の取り得る値を考える．$\gamma_i=p_i+q_i$, $p_i\in\mathbb{Z}_{\ge0}$, $0\le q_i<1$とし，$\alpha=s+t$, $s\in\mathbb{Z}_{\ge0}$, $0\le t<1$とすると

$$\mathrm{Mod}(\lfloor\gamma_i\rfloor,n)-\mathrm{Mod}(\lfloor\gamma_i+\alpha\rfloor,n)=\mathrm{Mod}(p_i,n)-\mathrm{Mod}(\lfloor p_i+s+q_i+t\rfloor,n)$$

[26]理由：$\sigma(n)-\sigma(1)=-\sum_{i=1}^{n-1}\sigma(i)-\sigma(i+1)$から，$\sigma$がpNAP型のとき数列$\{\mathrm{Mod}(\sigma(i)-\sigma(i+1),n)\}_{i=1}^{n-1}$のうち$m$が$k$個，$m+1$が$n-1-k$個ならば簡単な計算で$\mathrm{Mod}(\sigma(n)-\sigma(1),n)=\mathrm{Mod}(m+1+k,n)$を得る．$k=0,n-1$の場合と，$1\le k\le n-2$の場合を考えればよい．

である．$0 \leq q_i + t < 2$であるから，

$$\mathrm{Mod}(\lfloor p_i + s + q_i + t \rfloor, n) = \begin{cases} \mathrm{Mod}(p_i + s, n) & \text{if } 0 \leq q_i + t < 1 \\ \mathrm{Mod}(p_i + s + 1, n) & \text{if } 1 \leq q_i + t < 2 \end{cases}$$

である．sはiに依存しないことより$\mathrm{Mod}(p_i, n) - \mathrm{Mod}(\lfloor p_i + q_i + s + t \rfloor, n)$ は$\mathrm{Mod}(p_i, n) - \mathrm{Mod}(p_i + s, n) \equiv p_i - (p_i + s) \equiv -s$ の場合と$\mathrm{Mod}(p_i, n) - \mathrm{Mod}(p_i + s + 1, n) \equiv p_i - (p_i + s + 1) \equiv -s - 1$ の場合の二通りしかない．以上より，NAP型の置換σに対して，

$$\mathrm{Mod}(\sigma(i) - \sigma(i+1), n) = \mathrm{Mod}(\mathrm{Mod}(\lfloor \alpha(i-1) + \beta \rfloor, n) - \mathrm{Mod}(\lfloor \alpha i + \beta \rfloor, n), n)$$

は高々$\mathrm{Mod}(-s, n), \mathrm{Mod}(-s-1, n)$の2種類の値しか取り得ない．

$\mathrm{Mod}(-s, n)$の値しか取らない場合は(σは置換なので$-\lfloor \alpha \rfloor = -s \neq 0$である．従って$\lfloor \alpha \rfloor \neq 0$より$1 \leq \alpha < n$であり)集合$K_\sigma = \{\mathrm{Mod}(\sigma(i) - \sigma(i+1), n)\ ;\ i \in [n-1]\}$は$\{\mathrm{Mod}(-\lfloor \alpha \rfloor, n)\} = \{n - s\}$である．$s = \lfloor \alpha \rfloor$は$1 \leq s \leq n-1$であるから$n - s \in [n-1]$である．

$\mathrm{Mod}(-s-1, n)$の値しか取らない場合は(σは置換なので$-\lfloor \alpha \rfloor - 1 = -s - 1 \neq 0$である．従って$\lfloor \alpha \rfloor \neq n-1$より$0 \leq \alpha < n-1$であり)集合$K_\sigma = \{\mathrm{Mod}(\sigma(i) - \sigma(i+1), n)\ ;\ i \in [n-1]\}$は$\{\mathrm{Mod}(-\lfloor \alpha \rfloor - 1, n)\} = \{n - s - 1\}$である．$s = \lfloor \alpha \rfloor$は$0 \leq s \leq n-2$であるから$n - s - 1 \in [n-1]$である．

$\mathrm{Mod}(-s, n), \mathrm{Mod}(-s-1, n)$の2種類の値を取る場合は(同様の議論より$1 \leq \alpha < n-1$であり) $K_\sigma = \{\mathrm{Mod}(-\lfloor \alpha \rfloor, n) - 1, \mathrm{Mod}(-\lfloor \alpha \rfloor, n)\} = \{n - s, n - s - 1\}$である．ここで$2 \leq n - s \leq n-1$, $1 \leq n - s - 1 \leq n-2$である．□

系 NAP-2　6次のNAP型は60個である．

(証明) 先ず，計算機を利用して探すと60個の6次のNAP型が見つかる．例えばMathematica[27]を用いるのであれば，

```
Select[Union[Flatten[Table[Table[
  Mod[Floor[a (i - 1) + b], 6] + 1, {i, 1, 6}], {a, 1, 5, 1/4}, {b, 0, 6, 1/4}], 1]], PermutationListQ]
```

で60個のNAP型の置換が見つかる．よって6次のNAP型は少なくとも60個ある．

一方，6次のpNAP型の置換は丁度60個である．例えばMathematicaを用いるのであれば,[28]

```
n = 6;
Union[Select[Flatten[Table[Table[
  Module[{li}, li = {{i}}; Do[li = Union[
    Map[Append[#, If[Mod[Last[#] - j, n] == 0, n, Mod[Last[#] - j, n]]] &, li],
    Map[Append[#, If[Mod[Last[#] - j - 1, n] == 0, n, Mod[Last[#] - j - 1, n]]] &, li]],
      n - 1]; li], {i, 1, n}], {j, 1, n - 1}], 2], PermutationListQ]]
```

で60個の置換が出力される．従って，命題 NAP-1により，最初に見つかった60個の置換で6次のNAP型すべてを尽くしている．□

6次のNAP型の置換を列挙しておく．
(123456),(134562),(135246),(135624),(142536),(146352),(153264),(153642),(154326),(165432),(216543),(234561),
(245613),(246135),(246351),(251463),(253641),(264153),(264315),(265431),(315264),(315426),(316542),(321654),
(345612),(351246),(351462),(356124),(362514),(364152),(413625),(415263),(421653),(426315),(426531),(432165),
(456123),(461235),(462351),(462513),(512346),(513462),(513624),(524136),(526314),(531426),(531642),(532164),
(543216),(561234),(612345),(623451),(624135),(624513),(631425),(635241),(642153),(642531),(643215),(654321)

NAP型の考え方とは異なる方法でAP型を拡張したpNAP型を持ち出した理由は，nを決めれば理屈の上では計算機を使ってpNAP型の個数は数えられるため，命題 NAP-1に従ってNAP型の個数の評価を調べる手がかりになると考えたからである．系 NAP-2で実際にそのような使い方をしている．

---

[27] Version 11.1を使用した．

[28] この実装例は，pNAP型の定義を満たす置換をもれなく構成するという方法を用いている．$n = 6$ならば，n次の置換すべてをpNAP型かどうかチェックするという素朴な方法でpNAP型を探してもよい．しかしその方法だとnが大きいときは，n次の置換の個数があまりにも多くなり(例えば$n = 18$では$18! = 6402373705728000$個ある)計算機でも実用的な時間で計算が終わらない．

実は，n次のNAP型をすべて列挙するアルゴリズムは存在する．

命題 NAP-3　与えられた自然数nに対して，$O(n^6)$時間内でn次のNAP型の置換のすべてを出力するアルゴリズムが存在する．但し，絶対値が高々n^3の整数の算術演算と出力は単位演算とする．

(証明)　$\alpha,\beta\in\mathbb{R}$ と $i\in[n]$ に対して，

$$F_{\alpha,\beta}(i)=\lfloor\alpha(i-1)+\beta\rfloor,$$
$$G_{\alpha,\beta}(i)=\mathrm{Mod}(F_{\alpha,\beta}(i),n)+1$$

で，$F_{\alpha,\beta}:[n]\to\mathbb{Z}$ と$G_{\alpha,\beta}:[n]\to[n]$ をそれぞれ定義する．定義より，$\langle\alpha,\beta\rangle$-NAP 型の置換 σ とは置換であるような $G_{\alpha,\beta}$ のことである．

$\mathbb{R}^2$ 上の関係

$$\langle\alpha,\beta\rangle\sim\langle\alpha',\beta'\rangle\Leftrightarrow G_{\alpha,\beta}=G_{\alpha',\beta'}$$

を定義する．これは同値関係であるが，$\mathbb{R}^2$ をこの同値関係で分類したときの各同値類からそれぞれ1つ(以上)の代表元を有限回の手続きで列挙すれば，関数として互いに異なる $G_{\alpha,\beta}$ を全て列挙でき，そのうち置換であるものを残せば集合

$$NAP=\{G_{\alpha,\beta}\ ;\ \alpha,\beta\in\mathbb{R},\ G_{\alpha,\beta}\text{は}[n]\text{ 上の置換}\}$$

を列挙できることになる．そこで，同値関係 $\sim$ についての同値類のうち，置換をもたらすものそれぞれを漏れなく(重複はかまわないとし)カバーするような，$\langle\alpha,\beta\rangle$ のなす集合 – これを簡潔に「探索範囲」と呼ぶことにする – をできるだけ小さく作ることを考える．

まず，α の範囲を絞ることを考える．$\langle\alpha+n,\beta\rangle\sim\langle\alpha,\beta\rangle$ はすぐにわかるため，$\mathbb{R}^2/\sim$ の代表系を全部列挙するかわりに$([0,n)\times\mathbb{R})/\sim$ の代表系を全部列挙することで見落しはないことがわかる．ここで $[a,b)$ は半開区間 $\{x:a\le x<b\}\subset\mathbb{R}$ を表す．また，区間 $1\le x\le n$ の $x\mapsto\alpha(x-1)+\beta$ による像の長さを考えると，$0<\alpha<1$ のときには像の長さが $n-1$ を下回り像はn 個の整数点を含めないため，$F_{\alpha,\beta}$ が単射にならない．すると，$G_{\alpha,\beta}$ も置換にならない．よって，α の範囲を$\alpha\in[1,n)$ に絞ったとしても，$G_{\alpha,\beta}$ のうち置換であるものは全て生じることになる．

このように α について絞り込んだ 組$\langle\alpha,\beta\rangle$ の「探索範囲」を

$$L=\{\langle\alpha,\beta\rangle\ ;\ \alpha\in[1,n),\ \beta\in\mathbb{R}\}$$

とおく.「探索範囲」を離散化し，最終的には有限集合としたい．各 $\langle\alpha,\beta\rangle\in L$ は 直線のグラフ $y=\alpha(x-1)+\beta$ と同一視できるが，時にこの直線が格子 $\mathbb{Z}^2$ のどれかの点$\langle i,j\rangle$ を通ることがある．このような直線を与える $\langle\alpha,\beta\rangle$ を少し特別扱いしておく: $i,j\in\mathbb{Z}$ に対し，

$$L(i,j)=\{\langle\alpha,\beta\rangle\ ;\ \alpha\in[1,n),\ \beta\in\mathbb{R},\ \alpha(i-1)+\beta=j\}$$

とする．これを利用して，$\langle\alpha,\beta\rangle$ で定義される直線については，ある領域内の整数格子点と共有点をもつものに絞って構わないことを示す.

Claim 1. 各 $\langle\alpha,\beta\rangle\in L$ に対して，$\langle\alpha,\beta'\rangle\in L(i,j)$ $(i\in[n],j+1\in[n])$ であって$(\alpha,\beta)\sim(\alpha,\beta')$ であるβ',i,j が存在する．

(証明) 直線 $y=\alpha(x-1)+\beta$ 上で$x=i\in\mathbb{Z}$ である点 $\langle i,\alpha(i-1)+\beta\rangle$ から y の負方向に出発し，最初につきあたる整数格子点の y 座標こそが$F_{\alpha,\beta}(i)$ である．そこで，

$$\varepsilon=\min_{i\in[n]}\left(\alpha(i-1)+\beta-F_{\alpha,\beta}(i)\right)$$

として，直線 $y=\alpha(x-1)+\beta$ を真下に ε だけ平行移動する(β を少しずつ減らす)過程を考える(もし $\varepsilon=0$ ならば直線は動かさず，$\varepsilon=0$ として以下の説明の通りとする)．その過程で直線は格子点をまたがないため(もし途中で格子点をまたげばε の最小性に反する)，途中での$F_{\alpha,\beta}$ の同一性が保たれる．よって，$\beta_1=\beta-\varepsilon$ とすれば $F_{\alpha,\beta}=F_{\alpha,\beta_1}$ である．さらに，ε を定義するときに最小値を達成したi の適当なひとつを i_0 とし，$j=F_{\alpha,\beta_1}(i_0)\in\mathbb{Z}$ とすれば，$\langle\alpha,\beta_1\rangle\in L(i_0,j)$ である．このとき，任意の $k\in\mathbb{Z}$ に対して$\langle\alpha,\beta_1\rangle\sim\langle\alpha,\beta_1-nk\rangle$ が成立する．また，y の負方向へ nk だけ直線を平行移動させることで$\langle\alpha,\beta_1-nk\rangle\in L(i_0,j-nk)$ を得る．特に $k=\lfloor j/n\rfloor$ とし，このときの$\beta_1-n\lfloor j/n\rfloor$ を β' とすれば，$\langle\alpha,\beta\rangle\sim\langle\alpha,\beta'\rangle$ 且つ $\langle\alpha,\beta'\rangle\in L(i_0,\mathrm{Mod}(j,n))$ であり，また $i_0\in[n],\mathrm{Mod}(j,n)+1\in[n]$ である．□

よって L の中で $\sim$ によって相互非同値な $\langle\alpha,\beta\rangle$たちを探すことは，$\bigcup_{i\in[n],j+1\in[n]} L(i,j)$ の中で相互非同値な$\langle\alpha,\beta\rangle$たちを探すことに帰着した．$\langle\alpha,\beta\rangle \in L(i,j)$ であるときに，対応する直線の方程式は $y=\alpha(x-i)+j$ となる．つまり，$\langle\alpha,\beta\rangle = \langle\alpha, j-\alpha(i-1)\rangle$ だから，$L(i,j)$ の中での探索範囲は傾き α だけに関するものとなるが，これがここまでのところ $[1,n)$ で無限集合である．これを有限集合へ追い込むことを考える．x 方向の範囲が限定された整数格子点の集合を

$$\Lambda = [n]\times\mathbb{Z}$$

と置く．Claim 1 の証明で観察したように，$F_{\alpha,\beta}(i)$ とは直線 $y=\alpha(x-1)+\beta$ 上で$x=i\in\mathbb{Z}$ である点 $\langle i,\alpha(i-1)+\beta\rangle$ から y の負方向に出発し，最初に突き当たる Λ の点の y 座標である．このため，直線を連続的に(微小に) Λ の点に触れないように動かす限りにおいては，もたらす $F_{\alpha,\beta}$ の同一性が保たれる．このことを利用し，直線 $y=\alpha(x-i)+j$ が Λ と1点のみ共有する場合の傾き αの絞り込みを行う．

Claim 2. $\langle\alpha,\beta\rangle\in L(i,j), \langle i,j\rangle\in\Lambda$ とし，直線 $y=\alpha(x-i)+j$ は Λ の $\langle i,j\rangle$ 以外の点を通らないとする．また，$G_{\alpha,\beta}$ は置換であるとする．このとき，$\langle\alpha',\beta'\rangle\in L(i,j)$ であって，$\langle\alpha',\beta'\rangle\sim\langle\alpha,\beta\rangle$ 且つ$\alpha'\in\mathbb{Q}$を満し，α' を既約分数として書いたときの分母が高々 $2(n-1)$ であるものが存在する．

(証明) その直線を，点 $\langle i,j\rangle$ を中心に少しずつ時計まわりに回転(α を減少)させたときに最初に突き当る Λ の点を $\langle i+a,j+b\rangle$ とおく．$\alpha>1$ より $b/a\geq 1$ なので a と bは同符号である．同様に少しずつ反時計まわりに回転(α を増加)させたときに最初に突き当る Λ の点を $\langle i+c,j+d\rangle$ とおく．これも $d/c\geq 1$ なので c と dは同符号である．最初の直線の傾き α は $b/a<\alpha<d/c$ の範囲にあるが，この範囲で傾きを変化させている最中に直線が ($\langle i,j\rangle$ 以外の) Λの点をまたぐことはない．つまり，$b/a<\alpha''<d/c$ である限り $\langle\alpha'', j-\alpha''(i-1)\rangle\sim\langle\alpha, j-\alpha(i-1)\rangle$ である．ここで

$$\alpha''=\frac{|b|+|d|}{|a|+|c|}$$

とおけば，$b/a<\alpha''<d/c$ が満される．$i,j,i+a,i+c\in[n]$ であるから，$|a|,|c|\leq n-1$ であり，$|a|+|c|\leq 2(n-1)$ である．

$L(i,j)$ の定義において傾き $\alpha\in[1,n)$ の制約があり，直線の傾きの変更がこの制約に違反しないか検査する．もし，$\alpha''\geq n$となるなら，$\alpha'=\alpha''-n\lfloor\alpha''/n\rfloor$ とする．既約分数で α' を書いたときの分母は α''のそれと等しい．このとき，$0\leq\alpha'<n$ で$\langle\alpha', j-\alpha'(i-1)\rangle\sim\langle\alpha'', j-\alpha''(i-1)\rangle\sim\langle\alpha, j-\alpha(i-1)\rangle$ が保たれるが，もし $\alpha'<1$ であれば $G_{\alpha,j-\alpha(i-1)}=G_{\alpha',j-\alpha'(i-1)}$ は置換たりえないため，$\alpha'\geq 1$ である．一方，$\alpha''<n$ならそのまま $\alpha'=\alpha''$ とすると$1\leq\alpha'<n$ で$\langle\alpha', j-\alpha'(i-1)\rangle\sim\langle\alpha'', j-\alpha''(i-1)\rangle\sim\langle\alpha, j-\alpha(i-1)\rangle$ が保たれる．いずれの場合も$\langle\alpha',\beta'\rangle=\langle\alpha', j-\alpha'(i-1)\rangle$ は $L(i,j)$ に属する．□

直線$y=\alpha(x-i)+j$ が Λ と2点以上で交わる場合はより簡明である．

Claim 3. $\langle\alpha,\beta\rangle\in L(i,j), \langle i,j\rangle\in\Lambda$ とし，直線 $y=\alpha(x-i)+j$ は Λ の $\langle i,j\rangle$ 以外の点 $\langle i+a,j+b\rangle$ を通るとする．また，$G_{\alpha,\beta}$ は置換であるとする．このとき，$1\leq\alpha=b/a\in\mathbb{Q}$ で，これを既約分数で書いたときの分母は高々 $n-1$である．

(証明) $\alpha\geq 1$ は，$G_{\alpha,\beta}$ が置換であることによる．$\alpha=b/a$は明らか．このとき，$i, i+a\in[n]$ から $|a|\leq n-1$ である．□

Claims 2, 3 をまとめて次を得る．

Claim 4. $\langle i,j\rangle\in\Lambda$ とする．集合

$$L_1(i,j)=\left\{\langle\alpha,\beta\rangle\ ;\ \exists\ a\in[2n-2],\ \exists\ b\in[a,2n^2-2n)\cap\mathbb{Z}\ \ \text{s.t. } \alpha=b/a,\ \beta=j-\alpha(i-1)\right\}$$

は，置換をもたらす任意の$L(i,j)/\sim$ の同値類と交わる．

(証明) $\alpha=b/a$ の分母aの範囲，および置換をもたらす同値類との交わり性については Claims 2, 3 で示してきた．分子 b の条件は $\alpha\in[1,n)$ と $a\in[2n-2]$ から得られる．$\beta=j-\alpha(i-1)$ は$\langle\alpha,\beta\rangle\in L(i,j)$ の条件である．□

Claim 1 とClaim 4 とをまとめて次を得る．

Claim 5. 集合

$$L_1=\bigcup_{i\in[n],j+1\in[n]} L_1(i,j)$$

は，置換をもたらす任意の$L/\sim$ の同値類と交わる．

次の算法は，この集合 L_1 に属する $\langle\alpha,\beta\rangle$ をすべて訪れ，重複はすれども見落しはせずに NAP の元を出力する．

```
for  (i, j) ∈ [n] × ([0, n) ∩ ℤ) {
     for  a ∈ [2n − 2] {
          for  b ∈ [a, 2n^2 − 2n) ∩ ℤ {
               G_{(b/a),j−(b/a)(i−1)} が置換かどうかをテストし，そうなら出力
          }
     }
}
```

最外側のループは $O(n^2)$ 回，a のループ $O(n)$ 回，b のループ $O(n^2)$ 回である．NAP型の置換の候補 $G_{(b/a),j-(b/a)(i-1)}$ は $O(n^5)$ 個生じ，置換かどうかのテストは $O(n)$ 時間でできるため，実行時間は$O(n^6)$ である．□

次は命題 NAP-3のMathematicaによる実装例である：nをその次数とすると

```
Union[Select[Flatten[Table[Table[Table[Table[
  Mod[Floor[(b/a) (k - 1) + j - (b/a) (i - 1)], n] + 1, {k, 1, n}],
    {b, a, 2 n^2 - 2 n}], {a, 1, 2 n - 2}], {i, 1, n}, {j, 0, n}], 3], PermutationListQ]]
```

系 NAP-2から6次の置換ではNAP型とpNAP型は一致することがわかるが，7次の置換では一致しない．

系 NAP-4　$n=2,\ldots,18$までのn次のNAP型の個数とpNAP型の個数は次の表の通りである．

NAP型とpNAP型の個数

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
NAP型	2	6	16	30	60	70	128	144	240	242	360	338	616	480	672	714	1116
pNAP型	2	6	16	30	60	84	144	198	280	352	504	598	812	960	1152	1360	1728

(証明) $n=2,\ldots,18$に対して，nのときに命題 NAP-3の実装例を利用するとすべてのNAP型が列挙できる．また，pNAP型は系 NAP-2で提示したもので計算すればよい．□

この表$(n=2,\ldots,18)$では，NAP型の個数とpNAP型の個数は共にnの倍数になっていることがわかる．pNAP型の個数をnで割った商はnに対して増加しているが，一方，NAP型の個数をnで割った商は増加とは限らない(例えば，$n=10,11$や$n=12,13$).

付録B

モーメントの計算

6次対称群S_6の720個の置換に1から720まで番号を付けて，$S_6=\{\sigma_i\ ;\ i=1,2,\ldots,720\}$ とする．例えばアンケートの設問Iの回答データのような，ある置換のデータに対してそのデータの置換σ_iの票数をv_iとする．従って$\sum_{i=1}^{720} v_i$はそのデータの個数となる．ここでNを自然数とし，S_6の部分集合で要素の個数がNであるもの全体の集合を$\mathbb{T}$とする．

$$\mathbb{T}:=\{A\ ;\ A\subset S_6,\ |A|=N\}$$

また，S_6の部分集合Aに対して

$$\chi_A(\sigma)=\begin{cases}1 & (\sigma\in A)\\ 0 & (\sigma\notin A)\end{cases}$$

をAの特性関数とする．故に $\sum_{i=1}^{720}\chi_A(\sigma_i)=|A|$である．確率変数$X_N$を，「$S_6$の部分集合$A$で$|A|=N$となるものを無作為に選ぶとき[29]の$A$の票数」とする．勿論，$X_N$の確率分布は票数のデータ$(v_i)_{i=1,\ldots,720}$の分布に依存する．

[29]すなわち，$\mathbb{T}$から一様分布に従って選ぶ．

付録B.1 期待値と分散

X_Nの期待値$E[X_N]$は

$$E[X_N]=\sum_{A\in\mathbb{T}}\frac{1}{|\mathbb{T}|}\sum_{\sigma_i\in A}v_i=\sum_{A\in\mathbb{T}}\frac{1}{|\mathbb{T}|}\sum_{i=1}^{720}\chi_A(\sigma_i)v_i=\sum_{i=1}^{720}\sum_{A\in\mathbb{T}}\frac{\chi_A(\sigma_i)}{|\mathbb{T}|}v_i=\sum_{i=1}^{720}\frac{N}{720}v_i=\frac{N}{720}\sum_{i=1}^{720}v_i$$

である．$\displaystyle\sum_{A\in\mathbb{T}}\frac{\chi_A(\sigma_i)}{|\mathbb{T}|}=\frac{N}{720}$である理由は後で述べる．以下$\mu:=E[X_N]$とする．2次モーメント$E[X_N^2]$については

$$E[X_N^2]=\sum_{A\in\mathbb{T}}\frac{1}{|\mathbb{T}|}\left(\sum_{\sigma_i\in A}v_i\right)^2=\frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\sum_{\sigma_i\in A}\sum_{\sigma_j\in A}v_iv_j=\sum_{i=1}^{720}\sum_{j=1}^{720}\frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\chi_A(\sigma_i)\chi_A(\sigma_j)v_iv_j$$

である．ここで$i\neq j$のときは，i,jの値に依らずに$\displaystyle\frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\chi_A(\sigma_i)\chi_A(\sigma_j)=\frac{N}{720}\times\frac{N-1}{719}$である．

(理由:最初に$\displaystyle\sum_{A\in\mathbb{T}}\frac{\chi_A(\sigma_i)}{|\mathbb{T}|}=\frac{N}{720}$を示す．各$A\in\mathbb{T}$に対して，$\displaystyle\sum_{k=1}^{720}\chi_A(\sigma_k)=N$であるから，$\displaystyle\sum_{k=1}^{720}\sum_{A\in\mathbb{T}}\chi_A(\sigma_k)=\sum_{A\in\mathbb{T}}\sum_{k=1}^{720}\chi_A(\sigma_k)=N|\mathbb{T}|$より$\displaystyle\sum_{k=1}^{720}\sum_{A\in\mathbb{T}}\frac{\chi_A(\sigma_k)}{|\mathbb{T}|}=N$である．$\mathbb{T}$の定義より$A$は$|A|=N$となる部分集合をもれなくわたるので，最後の等式の左辺の内側の和$\displaystyle\sum_{A\in\mathbb{T}}\frac{\chi_A(\sigma_k)}{|\mathbb{T}|}$は$k$に依存しない．よって$\displaystyle 720\times\sum_{A\in\mathbb{T}}\frac{\chi_A(\sigma_k)}{|\mathbb{T}|}=N$すなわち$\displaystyle\sum_{A\in\mathbb{T}}\frac{\chi_A(\sigma_k)}{|\mathbb{T}|}=\frac{N}{720}$である．同様に各$A\in\mathbb{T}$に対して，$\displaystyle\left(\sum_{k=1}^{720}\chi_A(\sigma_k)\right)^2=N^2$であるから

$$\sum_{p=1}^{720}\sum_{q=1}^{720}\chi_A(\sigma_p)\chi_A(\sigma_q)=\sum_{p=1}^{720}\sum_{\substack{q=1\\q\neq p}}^{720}\chi_A(\sigma_p)\chi_A(\sigma_q)+\sum_{p=1}^{720}\chi_A(\sigma_p)^2$$

であり$\chi_A(\sigma_p)^2=\chi_A(\sigma_p)$より$\displaystyle\sum_{p=1}^{720}\chi_A(\sigma_p)^2=\sum_{p=1}^{720}\chi_A(\sigma_p)=N$なので$\displaystyle\sum_{p=1}^{720}\sum_{\substack{q=1\\q\neq p}}^{720}\chi_A(\sigma_p)\chi_A(\sigma_q)=N^2-N=N(N-1)$である．同様に

$$|\mathbb{T}|N(N-1)=\sum_{A\in\mathbb{T}}\sum_{p=1}^{720}\sum_{\substack{q=1\\q\neq p}}^{720}\chi_A(\sigma_p)\chi_A(\sigma_q)=\sum_{p=1}^{720}\sum_{\substack{q=1\\q\neq p}}^{720}\left(\sum_{A\in\mathbb{T}}\chi_A(\sigma_p)\chi_A(\sigma_q)\right)$$

であり，$\mathbb{T}$の定義より$\displaystyle\sum_{A\in\mathbb{T}}\chi_A(\sigma_p)\chi_A(\sigma_q)$は$p,q$には無関係である．よって$|\mathbb{T}|N(N-1)=720\times719\sum_{A\in\mathbb{T}}\chi_A(\sigma_p)\chi_A(\sigma_q)$より$\displaystyle\frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\chi_A(\sigma_p)\chi_A(\sigma_q)=\frac{N(N-1)}{720\times719}$である．)

従って，

$$\begin{aligned}E[X_N^2]&=\sum_{i=1}^{720}\sum_{j=1}^{720}\frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\chi_A(\sigma_i)\chi_A(\sigma_j)v_iv_j=\sum_{i=1}^{720}\sum_{\substack{j=1\\j\neq i}}^{720}\frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\chi_A(\sigma_i)\chi_A(\sigma_j)v_iv_j+\sum_{i=1}^{720}\frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\chi_A(\sigma_i)v_i^2\\&=\sum_{i=1}^{720}\sum_{\substack{j=1\\j\neq i}}^{720}\frac{N(N-1)}{720\times719}v_iv_j+\sum_{i=1}^{720}\frac{N}{720}v_i^2=\sum_{i=1}^{720}\sum_{j=1}^{720}\frac{N(N-1)}{720\times719}v_iv_j+\sum_{i=1}^{720}\frac{N}{720}\left(1-\frac{N-1}{719}\right)v_i^2\\&=\frac{N(N-1)}{720\times719}\left(\sum_{i=1}^{720}v_i\right)^2+\frac{N}{720}\left(1-\frac{N-1}{719}\right)\sum_{i=1}^{720}v_i^2\end{aligned}$$

となる．故に分散$V[X_N] = E[X_N^2] - E[X_N]^2$は

$$V[X_N] = \frac{N(N-1)}{720 \times 719}\left(\sum_{i=1}^{720} v_i\right)^2 + \frac{N}{720}\left(1 - \frac{N-1}{719}\right)\sum_{i=1}^{720} v_i^2 - \left(\frac{N}{720}\sum_{i=1}^{720} v_i\right)^2$$
$$= \frac{N}{720}\left(\left(\frac{N-1}{719} - \frac{N}{720}\right)\left(\sum_{i=1}^{720} v_i\right)^2 + \left(1 - \frac{N-1}{719}\right)\sum_{i=1}^{720} v_i^2\right)$$

である．

ちなみに3次モーメント$E[X_N^3]$も求めると，

$$E[X_N^3] = \frac{\binom{N}{3}}{\binom{720}{3}}\left(\sum_{i=1}^{720} v_i\right)^3 + 3\left(\frac{\binom{N}{2}}{\binom{720}{2}} - \frac{\binom{N}{3}}{\binom{720}{3}}\right)\left(\sum_{i=1}^{720} v_i^2\right)\left(\sum_{j=1}^{720} v_j\right) + \left(\frac{\binom{N}{1}}{\binom{720}{1}} - 3\frac{\binom{N}{2}}{\binom{720}{2}} + 2\frac{\binom{N}{3}}{\binom{720}{3}}\right)\sum_{i=1}^{720} v_i^3$$

であることがわかる．この3次モーメントは上と同様の方針で導出されるので計算過程は省略する．

この3次モーメントを利用して，確率変数X_Nの確率分布が正規分布であるとは一般には言えないことを述べておく．もしX_Nが正規分布に従っているならば，平均μと分散$\psi := V[X_N]$を用いて，3次モーメント$E[X_N^3]$は$\mu^3 + 3\mu\psi$に等しくなければならない．しかし，例えば，$|A| = |AAP_\cap|$のケースでは，設問Iのデータの3次モーメントは40643.1であり，一方その$\mu^3 + 3\mu\psi$の値は36451.1である．つまり等しくない．同様に，$D^{\mathrm{I}\times\mathrm{III}}$のデータの3次モーメントは21832.3であり，一方その$\mu^3 + 3\mu\psi$の値は21791.9である．このケースでは両者の値は近いが等しくはない．いずれのケースもX_Nは正規分布に従ってはいないことになる．

付録B.2　モーメント母関数

上の記法を用いるとき，X_Nのk次モーメント$E[X_N^k]$に対して

$$\prod_{i=1}^{720}\left(1 + e^{v_i t}y\right) = \sum_{N=0}^{720}\left(\sum_{k=0}^{\infty}\frac{E[X_N^k]}{k!}t^k\right)\binom{720}{N}y^N$$

が成立する．

(証明) 確率変数X_Nは「S_6からN個の置換を非復元無作為抽出で選んだときの，あるデータに関する票数の和」である．従って「$\mathbb{T}$からあるひとつの集合Aを選んでX_Nの値が$\sum_{i\in A} v_i$となる」のは確率$1/|\mathbb{T}|$で起きる．すなわち「$\mathbb{T}$からあるひとつの集合Aを選んで$\exp(X_N t)$の値が，$\exp(\sum_{i\in A} v_i t)$となる」のは確率$1/|\mathbb{T}|$である．故に

$$E[\exp(X_N t)] = \sum_{A\in\mathbb{T}}\frac{1}{|\mathbb{T}|}\exp(\sum_{i\in A} v_i t) = \frac{1}{|\mathbb{T}|}\sum_{A\in\mathbb{T}}\prod_{i\in A} e^{v_i t}$$

である．$|\mathbb{T}| = \binom{720}{N}$であるから$\binom{720}{N}E[\exp(X_N t)] = \sum_{A\in\mathbb{T}}\prod_{i\in A} e^{v_i t}$である．一方で$|A| = N$であるから，$\sum_{A\in\mathbb{T}}\prod_{i\in A} e^{v_i t}$は主張の式の左辺$\prod_{i=1}^{720}\left(1 + e^{v_i t}y\right)$の$y^N$の係数である．故に

$$\prod_{i=1}^{720}\left(1 + e^{v_i t}y\right) = \sum_{N=0}^{720}\binom{720}{N}E[\exp(X_N t)]y^N = \sum_{N=0}^{720}\left(\sum_{k=0}^{\infty}\frac{E[X_N^k]}{k!}t^k\right)\binom{720}{N}y^N$$

である．□

付録C

AP族と同サイズのS_6の部分集合を無作為に選んだときにAP族が得た票数以上となる確率

$S \subset S_6$ は，AP, NAP, AAP のどれかであるとする．第3.1節では，$R = S$, S_{inv}, $S_{\cap}$, $S_{\cup}$ のそれぞれにつき，AP族 R と同一サイズの S_6 の部分集合 A を無作為に選んだとき，各設問 I, II, III, IV およびこれらの id 除外版 の得票分布のもとで，Aの得票数が Rの得票数以上となる確率の近似値を報告した．また，第4.1.1節 では，同様に$D^{\mathrm{I,III}}$ について下線部の確率近似値を報告した．ここでは，数え上げによるこれらの確率の厳密な値について記述する．

付録Bの記号に従うと，$N = |R|$ としたときに A を $\mathbb{T} = \{A \subset S_6 : |A| = N\}$ から選ぶ場合の数

$$\mathcal{D} := |\mathbb{T}| = \binom{720}{N} = \binom{720}{|R|}$$

を分母とし，Aの得票数が R の得票数以上となる場合の数

$$\mathcal{N} := \left| \left\{ A \in \mathbb{T} \,;\, \sum_{i \in A} v_i \geq \sum_{i \in R} v_i \right\} \right|$$

を分子とした分数が下線部の確率で，第3.1節，第4.1.1節 では簡潔に「偏差値以上となる確率」と呼んだものである．この分子は，付録Bで述べた通り，各 v_i は設問に依存していることに注意する．

付録C.1　偏差値以上となる確率の分母を構成する場合の数

これは，AP 族 R のサイズにのみ依存し，次の値をとる: ただし，$|R| = |R_{\mathrm{inv}}|$ であるため，R_{inv} については R で代表させて記述を省略する．さらに，$R = AP$ のときは$AP = AP_{\mathrm{inv}} = AP_{\cap} = AP_{\cup}$ であるため，$R = AP$ で代表させて他3つに関する記述を省略する．

$\mathcal{D}(AP) = \binom{720}{|AP|} = \binom{720}{12} = 369512391263542662276094 20 \in [3 \times 10^{25}, (3+1) \times 10^{25})$
$\mathcal{D}(NAP) = \binom{720}{|NAP|} = \binom{720}{60} = 263903967952226779757272075097692816277612768625875894563025341753362548185515595864127888 \in [2 \times 10^{88}, (2+1) \times 10^{88})$
$\mathcal{D}(AAP) = \binom{720}{|AAP|} = \binom{720}{48} = 230239609588577421745204839923166883041780153186247245018649938925983977655 0 \in [2 \times 10^{75}, (2+1) \times 10^{75})$
$\mathcal{D}(NAP_{\cap}) = \binom{720}{|NAP_{\cap}|} = \binom{720}{22} = 467524309903018460404470082728097266866400 \in [4 \times 10^{41}, (4+1) \times 10^{41})$
$\mathcal{D}(AAP_{\cap}) = \binom{720}{|AAP_{\cap}|} = \binom{720}{20} = 441439262569373653600787202575885831376 \in [4 \times 10^{38}, (4+1) \times 10^{38})$
$\mathcal{D}(NAP_{\cup}) = \binom{720}{|NAP_{\cup}|} = \binom{720}{98} = 109222874601073605876793594250910949150853731026863047517423653772196340112822909850116786034689074570871860258877735322 0000 \in [1 \times 10^{123}, (1+1) \times 10^{123})$
$\mathcal{D}(AAP_{\cup}) = \binom{720}{|AAP_{\cup}|} = \binom{720}{76} = 125692768584100093216218728509096541623524416953206449519495113420133830417496303832002833364934814564020 \in [1 \times 10^{104}, (1+1) \times 10^{104})$

付録C.2　偏差値以上となる確率の分子を構成する場合の数

これは，設問と AP 族 R の両方に依存する．

$\mathcal{N}(\mathrm{I}\,; AP) = 343249837310661987280 \in [3 \times 10^{20}, (3+1) \times 10^{20})$
$\mathcal{N}(\mathrm{I}\,; NAP) = 195080640909891661618725263268519767300712013592941406272497031390331633251172570640 \in [1 \times 10^{82}, (1+1) \times 10^{82})$
$\mathcal{N}(\mathrm{I}\,; AAP) = 203962458593567175438740357676292052637350799327805211661100401232654 5 \in [2 \times 10^{69}, (2+1) \times 10^{69})$
$\mathcal{N}(\mathrm{I}\,; NAP_{\cap}) = 38794414249140510978589136226971721 \in [3 \times 10^{34}, (3+1) \times 10^{34})$
$\mathcal{N}(\mathrm{I}\,; AAP_{\cap}) = 153456556636667895304335275118 06 \in [1 \times 10^{31}, (1+1) \times 10^{31})$
$\mathcal{N}(\mathrm{I}\,; NAP_{\cup}) = 111747848961422285627462647216788308297467191064920977229612943154204623893326700727$

$645285593364047290205281886267140 40 \in [1 \times 10^{118}, (1+1) \times 10^{118})$
$\mathcal{N}(\ \mathrm{I}\ ; AAP_{\cup}) = 8624932116366922643461203172117992522661086782233761211473105700138751414502972066752266723952496386 \in [8 \times 10^{98}, (8+1) \times 10^{98})$

$\mathcal{N}(\ \mathrm{II}\ ; AP) = 15493956311090109935 \in [1 \times 10^{19}, (1+1) \times 10^{19})$
$\mathcal{N}(\ \mathrm{II}\ ; NAP) = 1854345363156357013589440430271665471736777348607646932399398967743572121076349679739 \in [1 \times 10^{84}, (1+1) \times 10^{84})$
$\mathcal{N}(\ \mathrm{II}\ ; AAP) = 4806679933643638306654504796756146046520953828109940677759723675931295 51 \in [4 \times 10^{71}, (4+1) \times 10^{71})$
$\mathcal{N}(\ \mathrm{II}\ ; NAP_{\cap}) = 436674415961782268038021948928686656 5 \in [4 \times 10^{36}, (4+1) \times 10^{36})$
$\mathcal{N}(\ \mathrm{II}\ ; AAP_{\cap}) = 140484993274393704408290446310636 8 \in [1 \times 10^{33}, (1+1) \times 10^{33})$
$\mathcal{N}(\ \mathrm{II}\ ; NAP_{\cup}) = 19729475509513416488236121999822072684299408633409104691526560761645014983868368342499974147261697724162416871121627913 90 \in [1 \times 10^{120}, (1+1) \times 10^{120})$
$\mathcal{N}(\ \mathrm{II}\ ; AAP_{\cup}) = 492176187675897600129317301814152929349638105337803232418650599937690956945781900268986148018824434414 \in [4 \times 10^{101}, (4+1) \times 10^{101})$

$\mathcal{N}(\ \mathrm{III}\ ; AP) = 5592822256698965 \in [5 \times 10^{15}, (5+1) \times 10^{15})$
$\mathcal{N}(\ \mathrm{III}\ ; NAP) = 11816414394027085036175787079963595148343588280836983406691844489612636685116527 18 \in [1 \times 10^{81}, (1+1) \times 10^{81})$
$\mathcal{N}(\ \mathrm{III}\ ; AAP) = 3243008090450017125101754848261228013932844673854063630684704889562 \in [3 \times 10^{66}, (3+1) \times 10^{66})$
$\mathcal{N}(\ \mathrm{III}\ ; NAP_{\cap}) = 2306741735119925335356696198877 8 \in [2 \times 10^{31}, (2+1) \times 10^{31})$
$\mathcal{N}(\ \mathrm{III}\ ; AAP_{\cap}) = 1909619992539893966038062534 8 \in [1 \times 10^{28}, (1+1) \times 10^{28})$
$\mathcal{N}(\ \mathrm{III}\ ; NAP_{\cup}) = 436874180547655987943701266024349421339215248423328343222583593755993405683803045385152136495827375099449597171830376 \in [4 \times 10^{116}, (4+1) \times 10^{116})$
$\mathcal{N}(\ \mathrm{III}\ ; AAP_{\cup}) = 221535414053349816677463078659648111641019939705113646448590678661486836612956079285135940319954 \in [2 \times 10^{95}, (2+1) \times 10^{95})$

$\mathcal{N}(\ \mathrm{IV}\ ; AP) = 18726865996705857820564 \in [1 \times 10^{22}, (1+1) \times 10^{22})$
$\mathcal{N}(\ \mathrm{IV}\ ; NAP) = 1051973831745176860677856398173627079472874278582907213535243622366831232618369253116407 \in [1 \times 10^{86}, (1+1) \times 10^{86})$
$\mathcal{N}(\ \mathrm{IV}\ ; AAP) = 2340495547740957657029560818683142474674458850043776768411334226515777726 \in [2 \times 10^{72}, (2+1) \times 10^{72})$
$\mathcal{N}(\ \mathrm{IV}\ ; NAP_{\cap}) = 2121889725495849518598613370506989404 2 \in [2 \times 10^{37}, (2+1) \times 10^{37})$
$\mathcal{N}(\ \mathrm{IV}\ ; AAP_{\cap}) = 2135168288495091487903044486729017 2 \in [2 \times 10^{34}, (2+1) \times 10^{34})$
$\mathcal{N}(\ \mathrm{IV}\ ; NAP_{\cup}) = 1380869918510351353388067485251032479583088049227700553435453596696690513998170479381282963421112199440921046885842323443 0 \in [1 \times 10^{121}, (1+1) \times 10^{121})$
$\mathcal{N}(\ \mathrm{IV}\ ; AAP_{\cup}) = 1632863602771908374319367117295807044267113375733667137144996384412573000258953198926556442575962516 57 \in [1 \times 10^{101}, (1+1) \times 10^{101})$

$\mathcal{N}(\ \mathrm{I(id除外)}\ ; AP) = 35383255839570163478882 \in [3 \times 10^{22}, (3+1) \times 10^{22})$
$\mathcal{N}(\ \mathrm{I(id除外)}\ ; NAP) = 3515891093613768208815726431207775146188686543597796867948959147663464444190086316096 \in [3 \times 10^{83}, (3+1) \times 10^{83})$
$\mathcal{N}(\ \mathrm{I(id除外)}\ ; AAP) = 4726118385533318523827916290428359418170461832135788529045073749179769 4 \in [4 \times 10^{70}, (4+1) \times 10^{70})$
$\mathcal{N}(\ \mathrm{I(id除外)}\ ; NAP_{\cap}) = 2498812050133567408763432058034148437 \in [2 \times 10^{36}, (2+1) \times 10^{36})$
$\mathcal{N}(\ \mathrm{I(id除外)}\ ; AAP_{\cap}) = 1163786890913286930114536864532878 \in [1 \times 10^{33}, (1+1) \times 10^{33})$
$\mathcal{N}(\ \mathrm{I(id除外)}\ ; NAP_{\cup}) = 1085058316762158181211441254566441120020196379918122340391020792818464389487514862809274218275109312068677252106371675 04 \in [1 \times 10^{119}, (1+1) \times 10^{119})$
$\mathcal{N}(\ \mathrm{I(id除外)}\ ; AAP_{\cup}) = 1120714207447893238853589776763635493034115594328543975540064518799504066982563111382618726210586278 2 \in [1 \times 10^{100}, (1+1) \times 10^{100})$

$\mathcal{N}(\ \mathrm{II(id除外)}\ ; AP) = 1861572004035825312323 \in [1 \times 10^{21}, (1+1) \times 10^{21})$
$\mathcal{N}(\ \mathrm{II(id除外)}\ ; NAP) = 2881988441080420407691488689374016462149650000060637258715494306375847091088 5077103384 \in [2 \times 10^{85}, (2+1) \times 10^{85})$
$\mathcal{N}(\ \mathrm{II(id除外)}\ ; AAP) = 9246452315210681521334956389080506981303156686584347047847255653540481526$

$\in [9\times 10^{72},(9+1)\times 10^{72})$
$\mathcal{N}(\ \mathrm{II}(\mathrm{id除外})\ ;NAP_{\cap})=221526808543861597332829682385283435237\in[2\times 10^{38},(2+1)\times 10^{38})$
$\mathcal{N}(\ \mathrm{II}(\mathrm{id除外})\ ;AAP_{\cap})=828141028823477417254225796092090 16\in[8\times 10^{34},(8+1)\times 10^{34})$
$\mathcal{N}(\ \mathrm{II}(\mathrm{id除外})\ ;NAP_{\cup})=165544084335957059380950414694172996937792733974412326137652704393773502572$
$243990235919529962078230561576654259767448242 93\in[1\times 10^{121},(1+1)\times 10^{121})$
$\mathcal{N}(\ \mathrm{II}(\mathrm{id除外})\ ;AAP_{\cup})=521507323112910537163907862729194631691624653412741895327708385175696739400 3$
$167771721230683942468147047\in[5\times 10^{102},(5+1)\times 10^{102})$

$\mathcal{N}(\ \mathrm{III}(\mathrm{id除外})\ ;AP)=1270699922392028417\in[1\times 10^{18},(1+1)\times 10^{18})$
$\mathcal{N}(\ \mathrm{III}(\mathrm{id除外})\ ;NAP)=223254243228826078977496091722238709180580459216515426949805278058431634345 9$
$7622978\in[2\times 10^{82},(2+1)\times 10^{82})$
$\mathcal{N}(\ \mathrm{III}(\mathrm{id除外})\ ;AAP)=87459100515932884010440362201216893493228453120173644144526917473870\in[8\times$
$10^{67},(8+1)\times 10^{67})$
$\mathcal{N}(\ \mathrm{III}(\mathrm{id除外})\ ;NAP_{\cap})=203264233619886881407473058946505 7\in[2\times 10^{33},(2+1)\times 10^{33})$
$\mathcal{N}(\ \mathrm{III}(\mathrm{id除外})\ ;AAP_{\cap})=196168800607733355893042119069 8\in[1\times 10^{30},(1+1)\times 10^{30})$
$\mathcal{N}(\ \mathrm{III}(\mathrm{id除外})\ ;NAP_{\cup})=440931443696936438548516210200760911076705215507370462336194381848726884068$
$44014998805170500087028376672470920662634 53\in[4\times 10^{117},(4+1)\times 10^{117})$
$\mathcal{N}(\ \mathrm{III}(\mathrm{id除外})\ ;AAP_{\cup})=333766517961186020897124908889632478700083198597001267824689212747354618170$
$9561370950070741112971\in[3\times 10^{96},(3+1)\times 10^{96})$

$\mathcal{N}(\ \mathrm{IV}(\mathrm{id除外})\ ;AP)=1467508736524577425121808\in[1\times 10^{24},(1+1)\times 10^{24})$
$\mathcal{N}(\ \mathrm{IV}(\mathrm{id除外})\ ;NAP)=1430696586261278654062725170846011112797990089988440958016375939224037060289$
$029482373800\in[1\times 10^{87},(1+1)\times 10^{87})$
$\mathcal{N}(\ \mathrm{IV}(\mathrm{id除外})\ ;AAP)=414724956979767496504365289346789340626805938779761900643647689858016050 76$
$\in[4\times 10^{73},(4+1)\times 10^{73})$
$\mathcal{N}(\ \mathrm{IV}(\mathrm{id除外})\ ;NAP_{\cap})=943426177294391280053180941603728183070\in[9\times 10^{38},(9+1)\times 10^{38})$
$\mathcal{N}(\ \mathrm{IV}(\mathrm{id除外})\ ;AAP_{\cap})=105123463038335810343306759785486605 1\in[1\times 10^{36},(1+1)\times 10^{36})$
$\mathcal{N}(\ \mathrm{IV}(\mathrm{id除外})\ ;NAP_{\cup})=110442025356615370580393006031155154370407147707128217695918653464969288216$
$462646759561884570507333343105896606459657200423\in[1\times 10^{122},(1+1)\times 10^{122})$
$\mathcal{N}(\ \mathrm{IV}(\mathrm{id除外})\ ;AAP_{\cup})=177662090068752855865743407241592435231667146361149165500790261646037900601$
$26122950236196124821966599 29\in[1\times 10^{102},(1+1)\times 10^{102})$

$\mathcal{N}(\ D^{\mathrm{I,III}}\ ;AP)=67436983300354457022\in[6\times 10^{19},(6+1)\times 10^{19})$
$\mathcal{N}(\ D^{\mathrm{I,III}}\ ;NAP)=200397625372511163270532455804074493494088139140228267521468560875690505301244045$
$944009\in[2\times 10^{86},(2+1)\times 10^{86})$
$\mathcal{N}(\ D^{\mathrm{I,III}}\ ;AAP)=31698082411639727199895857003385329862639017792144330605948276689712978 19\in$
$[3\times 10^{72},(3+1)\times 10^{72})$
$\mathcal{N}(\ D^{\mathrm{I,III}}\ ;NAP_{\cap})=45459607500373470555792818821360197 92\in[4\times 10^{36},(4+1)\times 10^{36})$
$\mathcal{N}(\ D^{\mathrm{I,III}}\ ;AAP_{\cap})=27448759280059683887199965210460 27\in[2\times 10^{33},(2+1)\times 10^{33})$
$\mathcal{N}(\ D^{\mathrm{I,III}}\ ;NAP_{\cup})=425963408270678577941968270586776569553937028467562596566256098473078244293896 3$
$490370294412360217041846001190528490594223\in[4\times 10^{120},(4+1)\times 10^{120})$
$\mathcal{N}(\ D^{\mathrm{I,III}}\ ;AAP_{\cup})=550730391721079005925483209449794286891857106100496602352470514937133406192729 9$
$81552137892145565140111\in[5\times 10^{101},(5+1)\times 10^{101})$

付録C.3　分子の数え上げについて

問題の分子

$$\mathcal{N}=\left|\left\{A\in\mathbb{T}\ ;\ \sum_{i\in A}v_i\geq\sum_{i\in R}v_i\right\}\right|$$

を数えることは，分母から分子を引き去った

$$\mathcal{D}-\mathcal{N}=\left|\left\{A\in\mathbb{T}\,;\,\sum_{i\in A}v_i<\sum_{i\in R}v_i\right\}\right|$$

を数えることに帰着する．よって，$m=\sum_{i\in R}v_i$ であるとき，

$$C_k:=\left|\left\{A\in\mathbb{T}\,;\,\sum_{i\in A}v_i=k\right\}\right|$$

を各 $k:0\le k<m$ について数えれば良い．各 C_k は次のように求めた．まず，得票分布 $\langle v_i:i\in S_6\rangle$ から，「特定票数xを得た置換の集合」

$$B_x:=\{i\in S_6:v_i=x\}$$

を $x=0,1,\ldots,m-1$ に対して計算する．S_6 を $\bigsqcup_{x=0}^{\infty}B_x$ と排他的和集合に分解して考えると(これは実際は有限和である) $A\subset S_6$ を定めることは，$A\cap B_x$ を各 $x=0,1,2,\ldots$ に対して定めることと同値である．$c_x:=|A\cap B_x|$ とするとき，$A\in\mathbb{T}$ すなわち $|A|=N$ となる条件は，

$$\sum_{x=0}^{\infty}c_x=N \tag{1}$$

であり，A が k 票を得る，つまり $\sum_{i\in A}v_i=k$ となる条件は

$$\sum_{x=0}^{\infty}xc_x=k \tag{2}$$

である．式(2) の条件から，$x>k$ において $c_x=0$ となるため，列(c_x)は長さ $k+1$ の有限列としてよい．そして式 (1), (2) の両方を満足する固定された非負整数列 $(c_0,c_1,\ldots,c_k)$ に対し，$c_x=|A\cap B_x|(x=0,1,\ldots,k)$ を満たす A の選び方は，$b_x:=|B_x|$ と書けば，$\prod_{x=0}^{k}\binom{b_x}{c_x}$ 通りある．ただし，$c_x>b_x$ となる x に対して $\binom{b_x}{c_x}=0$ とする．

式 (1),(2) の両方を満足する非負整数列の探索であるが，$c_0\ge 0$ を残して$\lambda_j:=\sum_{x=j}^{k}c_x$ $(1\le j\le k)$ と変数変換すれば，非負非増加列

$$\lambda_1\ge\lambda_2\ge\cdots\ge\lambda_k\ge 0 \tag{3}$$

であって，式 (1) を言い換えた

$$\lambda_1=N-c_0 \tag{4}$$

および式 (2) を言い換えた

$$\sum_{j=1}^{k}\lambda_j=k, \tag{5}$$

そして各 c_x が b_x 以下となる条件

$$\lambda_j-\lambda_{j+1}\le b_j\quad(1\le j\le k-1) \tag{6}$$

を満たす列 $(\lambda_1,\lambda_2,\ldots,\lambda_k)$ の探索に帰着する．式 (3) と 式 (5) の連立は列が 整数 $k>0$ の分割を与えるという条件，すなわち列が面積 k のフェラーズ図形を形成するという条件である．$0\le c_0\le N$ の各 c_0 に対し，λ_j が式 (4) と式(6)を満たすような面積 k のフェラーズ図形を計算機で探索し，それぞれにつき$\prod_{x=0}^{k}\binom{b_x}{c_x}$ を積算することで，C_k を求めた．