— Article —

ある型の置換の個数について II

永田 誠, 武井 由智

On the numbers of permutations of certain types II

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

[1)] *Faculty of Pharmacy, Osaka Medical and Pharmaceutical University, 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 29, 2021; Accepted December 28, 2021)

Abstract In 2019, the authors of the current paper conducted a survey research on human-generated permutations [Nagata and Takei, Bull. OUPS 2019]. In the following year, they analyzed the data from a different perspective and observed that people tend to generate certain types of permutations, then defined types NAP (nearly arithmetic progression) and pNAP (pseudo-nearly arithmetic progression) of permutations as mathematical abstractions of such tendency [Nagata and Takei, Bull. OUPS 2020]. Then, in [Nagata and Takei, Bull. OUPS 2021], the number of permutations of these types were bounded by asserting that the set of the inverse permutations of Sós type, which are defined as the translation of so-called Sós permutations [Sós, Ann. Univ. Sci. Budapest. Eötvös, Sect. Math. 1958] by a constant, include the set of the permutations of NAP type and are included in the set of the permutations of pNAP type. Especially, the authors obtained a lower bound of the number of the permutations of pNAP type as the number of the permutations of Sós type whose explicit formula is obtained from the number of Sós permutations in [Surányi, Ann. Univ. Sci. Budapest. Eötvös, Sect. Math. 1958], [Shutov, Chebyshevskii Sb. 2014], [Bockiting-Conrad, Kashina, Petersen and Tenner, Amer. Math. Monthly 2021], with the assertion by computer experiments that the set of the inverses of Sós type-permutations is indeed the same as the set of the permutations of pNAP type as long as the degree n of the permutations is not greater than 50. Thus, a remaining problem of major interest is bounding the number of pNAP permutations from above. In this paper, we address this problem. One of our results is that pNAP and the inverses of Sós permutations satisfy essentially identical recurrence relation. It gives immediately an upper bound $(n-1)n^2$ of the number of permutations of pNAP type. We note that the upper bound is of the same order in n as the lower bound, the number of the inverses of Sós type-permutations. Furthermore, using the recurrence relation, an efficient algorithm for the enumeration of pNAP permutations is given and used to enlarge the upper limit of the degrees n for which the observed property "pNAP is inverse-Sós-type" is confirmed to 1300 from 50 in our previous paper.

Key words — arithmetic progression; Sós permutation; symmetric group;

1 はじめに

今から3年前，我々は置換に関するアンケート調査を行い，その結果を本雑誌の前身である大阪薬科大学紀要に報告[1]した．その翌年，その調査で得られた1000人を超える回答のさらなる解析の結果として，ヒトはある型の置

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

換を生成しやすい傾向があることを報告[2]した．その置換の型として，NAP型やpNAP型等を挙げた．NAP型，pNAP型の定義は次節で述べる．また[2]では，NAP型の置換の個数についていくつかの考察を行い，n次のNAP型の置換すべてを，nについての多項式時間内$O(n^6)$で列挙するアルゴリズムを提示した．さらに前稿[3]で，Sós置換の逆置換の考察を通して，NAP型の置換の個数の上界とpNAP型の置換の個数の下界が得られたことを述べた．また計算機を用いた計数により50次以下の置換ではpNAP型とSinv型は一致することも報告した．Sós置換及びSinv型の定義についても次節で述べる．さて，n次のNAP型の置換は$(n-1)n$個以上あることは[2]でわかっているので，残っている問題はpNAP型の置換の個数の上界ということになる．本稿でこれについて得られた結果を報告する．今回，我々が着目したのはpNAP型の置換の「差分」である．この差分が満たす関係式は，[3]で得られたSós置換の逆置換が満たす漸化式を次数で法をとった合同式と本質的に同じであることがわかった．これよりn次のpNAP型の置換は$(n-1)n^2$個以下であることがわかり，従って，[2], [3]及び本稿で，NAP型の置換の個数とpNAP型の置換の個数のそれぞれの上界と下界の問題に対してすべて言及できたことになる．さらにその差分が満たす関係式(漸化式)がpNAP型の置換を列挙する直接的なアルゴリズムを導くことを見る．アルゴリズムは差分の関係式を用いて高々n^3個の写像を発生し，一つの写像が実際に置換であることの検査とその出力を $O(n)$ ステップで行うため全体の演算量[1]は $O(n^4)$ に収まる．これは前項 [3] で与えたpNAP型の置換の列挙アルゴリズムが $O(n^2 2^n)$ を要していたのと比較して極めて効率的であるばかりか，前項[3]で導いたpNAP型の置換の個数の下界に照して(定数ファクターを除き)ほぼ最善と言える．この効率的なアルゴリズムを用いてpNAP型の置換を計数することで，pNAP型とSinv型が一致することを，前項の次数範囲 $n \leq 50$ より大幅に広い$n \leq 1300$ に対して確認することができた．

本稿の構成は以下の通りである．次節でいくつかの用語の定義[2]と知られている結果を述べる．続く第3節で順位付け写像と順位の定義を与え，小数部分の順位の場合について得られた結果を述べる．第4節ではその応用としてpNAP型の置換の漸化式とpNAP型の置換の個数の上界についての結果を述べる．第5節では，第4節で得られた漸化式を満たす数列を計算機を用いて発生させ，それによって得られた1300次以下の置換について等の結果を述べる．尚，本稿の本文で述べた主張の証明やその詳細のついてはすべて本稿の付録に記す．

2 定義及び既知の結果

nを自然数とする．但し，置換の次数でnを用いるときは$n \geq 2$とする．ϕをオイラー関数 Euler's totient function とする．即ち，n以下の自然数でnと互いに素のものの個数を$\phi(n)$とする．n以下の自然数の集合$\{1, 2, \ldots, n\}$を$[n]$で表す．

有限集合Aに対して，$|A|$でAの要素の個数を表す．また，有理整数環，実数体をそれぞれ$\mathbb{Z}$, $\mathbb{R}$で表す．

実数αに対して，$\lfloor\alpha\rfloor$をαを超えない最大の整数とし，$\alpha - \lfloor\alpha\rfloor$を$\{\alpha\}$で表す．以下，本稿では$\lfloor\alpha\rfloor$を$\alpha$の整数部分，$\{\alpha\}$を$\alpha$の小数部分[3]と呼ぶ．また，整数$m$を$n$で割った余り[4]を$\mathrm{Mod}_n(m)$で表す．

n次対称群をS_nで表す．置換σの表記方法として$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ 或いは下段だけの$\sigma = (\sigma(1)\sigma(2)\cdots\sigma(n))$を用いる．

[1] n次のpNAP型の置換すべての列挙についての演算量である．但し，これは重複列挙の検査を行わない場合である．本稿第5節で，pNAP型の一部である基本pNAP型の置換の列挙(重複列挙の検査は不要)についての結果があり，そこでの演算量を単純にn倍したものを全体の演算量としているのだが，もし，基本pNAP型の置換の列挙を全体に拡げる際に重複列挙の検査を行うのであればその分の演算量を考慮しなくてはならないことになる．本稿では簡略化のため，そのような重複列挙の検査は考慮しないことにした．

[2] 第2節で述べた用語の定義の多くは[3, 第2節]にあるが，読者の利便性も考慮し本稿でも定義を述べる．

[3] αの正負に依らず $\lfloor\alpha\rfloor \leq \alpha, 0 \leq \{\alpha\} < 1$であることに注意する．

[4] [3]では$\mathrm{Mod}(m, n)$と記している．

本稿では$[n]$の要素に整数の順序関係や算法が適用できることを利用している．そのため，n次の置換$\sigma \in S_n$を$[n]$から$[n]$への全単射写像に限定[5]して考える．

2.1 置換の型の定義

前稿[3]でいくつかの置換の型の定義を述べた．以下に本稿で必要なものだけを述べる．

定義(NAP型) n次の置換σが NAP型(nearly arithmetic progression type)とは，$\exists\, \alpha, \beta \in \mathbb{R}$ s.t. $\forall\, i \in [n]$に対して

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

を満たすときをいう．

前々稿[2]ではα, βが整数のときのNAP型をAP型(arithmetic progression type)と称して，初めにAP型を導入してから，その後にAP型の拡張としてNAP型を導入した．さらに6次のNAP型の置換すべてを列挙確定に利用する[6]ため，次のpNAP型を導入した．

定義(pNAP型) n次の置換σがpNAP型(pseudo-nearly arithmetic progression type)とは，集合

$$K_\sigma := \{\mathrm{Mod}_n(\sigma(i) - \sigma(i+1)) \,;\, i \in [n-1]\}$$

に対して，$\exists\, m \in [n-2]$ s.t. $K_\sigma \subset \{m, m+1\}$であるときをいう(但し$n=2$のときは$m=0$とする)．

置換σがNAP型のとき，上の集合K_σは一元集合又は隣り合う2整数の二元集合[2, 付録A命題NAP-1]である．即ち，NAP型はpNAP型である．計算機による計数によれば，6次以下の置換ではNAP型であることとpNAP型であることは同値である[2, 付録A系NAP-4]が，7次以上50次以下の置換では同値ではない[3, 付録B]ことがわかっている．即ち，7次以上50次以下ではpNAP型であり且つNAP型でない置換が存在する．

定義(Sós置換・Sinv置換) nを2以上の自然数とする．$0 < \alpha < 1$を満たす任意の無理数αを固定する．n個の値

$$\{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$$

を小さい順に並べたものを

$$\{k_1\alpha\}, \{k_2\alpha\}, \ldots, \{k_n\alpha\}$$

とするとき，$\begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$は$n$次の置換である．この置換を$\alpha$に関する$n$次のSós置換[7]と呼ぶ．また，この$\alpha$に関する$n$次のSós置換の逆置換を，$\alpha$に関する$n$次のSinv置換[8](“Sós inverse” permutation)と呼ぶ．

定義(Sós型・Sinv型) n次の置換πがSós型(Sós type)[9]とは，$\exists\, \alpha, \beta \in \mathbb{R}$ s.t. n個の値

$$\{\alpha+\beta\}, \{2\alpha+\beta\}, \ldots, \{n\alpha+\beta\}$$

はすべて異なり[10]，これらを小さい順に並べると

$$\{\pi(1)\alpha+\beta\}, \{\pi(2)\alpha+\beta\}, \ldots, \{\pi(n)\alpha+\beta\}$$

の順になっているものをいう．α, βを指定したいときはこの置換πを$\pi_{\alpha,\beta}$と記す．また，$\tau \in S_n$がSinv型(Sinv type)とはn次のSós型の置換の逆置換のときをいう．つまり，$\exists\, \alpha, \beta \in \mathbb{R}$ s.t.

[5]通常，置換はn点集合から同一のn点集合への全単射のことであるが，そのn点集合を$[n]$に限定するのである．

[6][2]では次のような文脈でpNAP型が利用されている：ある置換が与えられたとき，その置換がNAP型か否かを決定するためには，NAP型の定義に於ける二つの実数α, βの存在性・非存在性を議論しなければならず，それは容易ではなさそうである．一方，pNAP型か否かはその定義から容易に決定できる．さて，単純なしらみつぶし検索により6次の置換のpNAP型の個数は60個あることがわかる．一方，NAP型の置換は単純なしらみつぶし検索は使えないのだが，とりあえず6次のNAP型の置換は60個見つかる．ここで一般にNAP型はpNAP型であるという事実を利用すれば，この60個の置換が6次のNAP型の置換すべてであることがわかる．

[7]本稿では[4, Theorem 1]の置換をSós置換と呼ぶことにする．

[8]Sinv置換は単にSós置換の逆置換のことなのであるが，Sós置換はSinv置換を定義するのに用いられているだけで，[3]と同様本稿でもSós置換は考察対象ではない．そのような状況でSinv置換のことを「Sós置換の逆置換」と称するのは不自然であろう．これがSinv置換という用語を導入した理由である．Sinv型についても同様である．

[9][7]の Sós permutations に対応するものは，本稿ではSós型と呼ぶこととし，Sós置換とは区別する．

[10]本稿では，同じ値がある場合には$\pi_{\alpha,\beta}$は定義されないとする．

$\tau = \pi_{\alpha,\beta}^{-1}$であるときをいう．

2.2 既知の結果

前稿[3]で述べた結果のうち，本稿で取り上げるべきと思われるものを三つ，定理として述べる．以下，nは2以上の自然数とする．

定理A([3, 定理4]) n次の置換について，次の(1),(2)が成り立つ．

(1) NAP型の置換はSinv型である．

(2) Sinv型の置換はpNAP型である．

定理B([7, Theorem 4], [3, 定理5]) n次のSinv型の置換の個数は$n\sum_{i=1}^{n-1}\phi(i)$である．

上の二つの定理より，n次のNAP型の置換の個数の上界とpNAP型の置換の個数の下界に$n\sum_{i=1}^{n-1}\phi(i)$ がとれる[11]ことがわかる．また，[2, 第2節]と[2, 付録A系AAP-3]から，n次のNAP型の置換の個数の下界に$(n-1)n$がとれることがわかる．

次はSinv置換が満たす漸化式[12]についての主張である．[3]では等式で与えられているが，ここではそれをnを法とした合同式で述べる．

定理C([3, 系1]) αを1未満の正の無理数とし，τ_αをαに関するn次のSinv置換とする．このとき各$\ell \in [n-1]$に対して

$$\tau_\alpha(\ell+1) - \tau_\alpha(\ell) \equiv \tau_\alpha(1) - \begin{cases} 1 & \text{if } \tau_\alpha(\ell) \geq \tau_\alpha(n) \\ 0 & \text{o.w.} \end{cases} \mod n$$

が成り立つ．

3 順位付け写像

ここで本稿でのpNAP型の置換についてのアプローチ方法を説明しておく．そのために前稿[3]を振り返っておこう．[3, 付録A]では，Sinv置換の考察に多くの頁を割いているが，そこで用いられている基本的な事実は次の二つである．一つは，無理数αに関するn次のSinv置換はn個の小数部分 $\{\alpha\}, \{2\alpha\}, \ldots, \{n\alpha\}$の順位であるという事実．もう一つは，小数部分の順序関係は整数部分の数式を用いて表すことができるという事実である．この二つの事実より，小数部分の順位，即ちSinv置換は明示的に数式で表すことができ，そしてその数式を利用した考察が可能になる．これが[3]で用いたSinv置換の考察方法である．

本稿もこれに準じる．つまり，何かしらの小数部分の順位を考え，その順位を整数部分の数式で表す．そしてその数式を利用した考察を行う．実はすべての置換は何かしらの小数部分の順位[13]と考えられる．この意味では，[3]で考察したSinv置換は，小数部分の順位としての考察した置換の一例と言えよう．本稿では，より一般的な形で小数部分の順位として表される置換を考え，その一つの応用としてpNAP型の置換を考察する．

本節は，最初に抽象的に順位付け写像と順位についての定義をし，そしてそれを小数部分の順位に限定して考えたときに成立する差分の関係式(第3.2節定理1)を述べる．その関係式のpNAP型への応用は次節で述べる．

3.1 順位付け写像の定義

定義(順位付け写像と順位) Xを有限集合，$(R, \preceq)$を全順序集合[14]とし，写像$f : X \to R$を単射とする．また$|X|$をnで表す．このとき，各$x \in X$に対して

$$\mathrm{t}_f(x) := |\{w \in X \,;\, f(w) \preceq f(x)\}|$$

で定義される写像$\mathrm{t}_f : X \to [n]$をXのfによる$(R, \preceq)$での順位付け写像，或いは単に，fによる順位付け写像と呼ぶことにする．また，$\mathrm{t}_f(x)$を$x \in X$のfによる$(R, \preceq)$での順位と呼ぶこと

[11] これはn^3のオーダーである．

[12] n次の置換σの漸化式とは，$[n]$から$[n]$への全単射σについて数列$(\sigma(i))_{i=1}^n$が満たす漸化式のことである．

[13] 第3.1節で挙げたものは(明らかな言い換えに過ぎない)自明な順位付け写像である．

[14] Rは集合, $\preceq$はR上の全順序関係．

にする．

つまり，有限集合Xのfの像$f(X)=\{f(x)\,;\,x\in X\}$の各要素を$(R,\preceq)$の順序で並べたときの$f(x)$の順位が$\mathrm{t}_f(x)$である．写像fが単射であるという条件により順位の同着はない．従って写像$\mathrm{t}_f : X\to[n]$は全単射である．特に，$x,y\in X$に対して，$f(x)\preceq f(y)$と$\mathrm{t}_f(x)\le \mathrm{t}_f(y)$は同値であることがわかる．これらについての詳細は付録Aに記す．

σをn次の置換，即ち$[n]$から$[n]$の全単射とする．写像$f:[n]\to\mathbb{R}$を$f(x):=\sigma(x)$で定義すれば，$[n]$のfによる実数の通常の順序$(\mathbb{R},\le)$での順位付け写像$\mathrm{t}_f:[n]\to[n]$とσは一致する．つまり，自明的に，すべての置換は或る順位付け写像であるとみなすことができる．$f(x):=\frac{\sigma(x)-1}{n}$としても同様である．この場合は$0\le f(x)<1$であるから(形式的には)小数部分の順位ということができよう．

3.2 小数部分の順位による置換

上記のように抽象的に定義された順位付け写像で，例えば，n次の置換σに対して写像$f(x)=\frac{\sigma(x)-1}{n}$を持ち出して「置換$\sigma$は小数部分の順位と考えられる」といってみたところで直ちにこれが何か益するものをもたらすとは思えない．我々は，小数部分の順位を整数部分で表して議論を進めたいのであるが，整数部分で表すことで益するためにはどうあるべきか，何をすればよいのかがわかるツールが欲しい．そしてそれはより適用範囲が広い(使用条件が緩い)ものであって欲しい．これを踏まえて次の用語を導入する．以下，$[0,1)$は0以上1未満の実数の区間を意味する．

定義(fp単射) nを自然数とする．写像$g:[n]\to\mathbb{R}$に対して，gと小数部分$\{\cdot\}$の合成写像$\{g\}:[n]\to[0,1),\ \ell\mapsto\{g(\ell)\}$が単射であるとき，$g$を$n$次のfp単射(“fractional part” injection)と呼ぶ．

定義(fp単射による置換) gがn次のfp単射であるとき，Xを$[n]$, $(R,\preceq)$を通常の実数の順序$([0,1),\le)$として，fを$\{g\}$とすれば，順位付け写像$\mathrm{t}_f=\mathrm{t}_{\{g\}}$は$n$次の置換である．この置換$\mathrm{t}_{\{g\}}$を$n$次のfp単射$g$による置換と呼ぶことにする．

次が成立する．証明は付録Aに記す．

定理1(fp単射による置換の差分の関係式) nを2以上の自然数とし，写像$g:[n]\to\mathbb{R}$をfp単射とする．また，$i,j\in\{0,1,\dots,n-1\}$に対して

$$D(i,j):=\lfloor g(i+1)-g(j+1)\rfloor-\lfloor g(i)-g(j)\rfloor$$

と書くことにする．但し，$g(0)=0$とする．このとき，n次のfp単射gによる置換$\mathrm{t}_{\{g\}}$は各$\ell\in[n-1]$に対して

$$\begin{aligned}&\mathrm{t}_{\{g\}}(\ell+1)-\mathrm{t}_{\{g\}}(\ell)\\&\quad-\left(D(\ell,0)+\sum_{k=1}^{n-1}\left(D(k,0)+D(\ell,k)\right)\right)\\&\equiv \mathrm{t}_{\{g\}}(1)-\begin{cases}1 & \text{if } \mathrm{t}_{\{g\}}(\ell)\ge \mathrm{t}_{\{g\}}(n)\\ 0 & \text{o.w.}\end{cases}\quad \bmod n\end{aligned}$$

を満たす．

もし$D(*,*)$の項がないならば，定理1の関係式は前節定理CのSinv置換の満たす漸化式と同じとなる．つまり，fp単射による置換の差分の関係式とSinv型の置換の漸化式との差異は$D(*,*)$の項だけに集約される．これが定理1の主張である．

本小節で小数部分の順位としての置換としてfp単射による置換を導入した．小数部分の順位としての置換を考えるとき，fp単射という条件は緩い条件であり，適用範囲が広いものであろう．我々はこの定理1が小数部分の順位を整数部分で表すにはどうあるべきか，何をすればよいのかを示していると考える．これによれば，fp単射による置換の差分については$D(*,*)$の項だけを考察すればよく，その考察が可能となるfp単射をもってくればよいということになる．次節でpNAP型の考察に適したfp単射を具体的に提示し，それについての結果を述べる．

4 pNAP型への応用

第2節の定義に従えば，n次の置換$\tau\in S_n$がpNAP型とは次を満たすときをいうのである：

$\exists\, d \in [n]$ s.t. 各$\ell \in [n-1]$に対して

$$\tau(\ell+1) - \tau(\ell) \equiv d + \begin{cases} 0 & \text{または} \\ 1 \end{cases} \mod n$$

このdを$\tau(1)$に限定したものを考える．

定義(基本pNAP型) τをn次のpNAP型の置換とする．各$\ell \in [n-1]$に対して

$$\tau(\ell+1) - \tau(\ell) \equiv \tau(1) + \begin{cases} 0 & \text{または} \\ 1 \end{cases} \mod n$$

であるとき，τを基本pNAP型と呼ぶことにする．

整数の定数Cを与えたとき，$\sigma \in S_n$を各$\ell \in [n]$に対して

$$\sigma'(\ell) \equiv \sigma(\ell) + C \mod n$$

となる$\sigma' \in S_n$に写すn次対称群S_nの変換$\sigma \mapsto \sigma'$を「定数Cを加える変換」と呼ぶ[15]ことにする．また(Cを指定せずに)「定数を加える変換」と言う場合は，このような定数Cが存在するという意味とする．容易にわかるように「定数を加える変換」によって，すべてのpNAP型の置換は或る基本pNAP型の置換から得ることができる．従って，n次のpNAP型の置換の個数はn次の基本pNAP型の置換の個数の高々[16]n倍である．

定義(付随するビット列) n次の基本pNAP型の置換τの「0または1の部分」をτに付随するビット列と呼ぶことにする．即ち，τに付随するビット列とは，$\ell \in [n-1]$に対して

$$\tau(\ell+1) - \tau(\ell) \equiv \tau(1) + \delta_\ell \mod n$$

となる$\delta_\ell \in \{0,1\}$の列$(\delta_k)_{k=1}^{n-1}$のことをいう．

詳細は付録Aに記すが，基本pNAP型の置換τが$\tau(1) = n$であれば，付随するビット列$(\delta_k)_{k=1}^{n-1}$は$\delta_i = \cdots = \delta_{n-1} = 1$でなくてはならないことがわかる．また，$\tau(1) = n-1$であれば，$\delta_i = \cdots = \delta_{n-1} = 0$でなくてはならないことがわかる．しかし，$\tau(1) \leq n-2$のときは$\tau(1)$に対して付随するビット列が一意に決まるとは限らない．即ち，付随するビット列は($\tau(1)$だけではなく)置換τに依存[17]する．

付随するビット列を用いれば基本pNAP型の置換τは

$$\tau(\ell) \equiv \ell\tau(1) + \sum_{k=1}^{\ell-1} \delta_k \mod n$$

と表される．

以下，本節の主張のすべての証明は付録Aに記す．

命題2(基本pNAP型のfp単射) nを2以上の自然数とする．τをn次の基本pNAP型の置換とし，$\tau(1) \leq n-2$の場合を考える．$(\delta_k)_{k=1}^{n-1}$をτに付随するビット列とする．θを$\tau(1)$より僅かに小さい無理数$(\tau(1) - \frac{1}{2n} < \theta < \tau(1))$として固定し，写像$g : [n] \to \mathbb{R}$を各$\ell \in [n]$に対して

$$g(\ell) := \frac{\ell\theta + \sum_{k=1}^{\ell-1} \delta_k}{n}$$

で定義する．このとき，gはn次のfp単射であり，fp単射gによる置換$\mathfrak{t}_{\{g\}}$はτと一致する．

このgに関して，前節定理1の$D(*,*)$の項が計算できる．次がその結果である．

定理3(基本pNAP型の置換の漸化式) nを2以上の自然数とし，τをn次の基本pNAP型の置換とする．このとき，各$\ell \in [n-1]$に対して

$$\tau(\ell+1) - \tau(\ell) \equiv \tau(1) + \begin{cases} 1 & \text{if } \mathrm{Mod}_n(\tau(\ell)) < \mathrm{Mod}_n(\tau(n)) \\ 0 & \text{o.w.} \end{cases} \mod n$$

が成立する．特に，τに付随するビット列$(\delta_k)_{k=1}^{n-1}$

[15]前稿[3, 付録A]で，n次の置換$\rho = (23\ldots n1)$を何回か左から作用させるの旨で説明しているものと同一である．
[16]重複して数えていないわけではない．
[17]本節定理3の結果からもう少し詳細なことが言える．即ち，定理3より，n次の基本pNAP型の置換τは$\tau(1)$と$\tau(n)$で決定する．従ってそれに付随するビット列も$\tau(1)$と$\tau(n)$で決定する．

は

$$\delta_\ell = \begin{cases} 1 & \text{if } \mathrm{Mod}_n(\tau(\ell)) < \mathrm{Mod}_n(\tau(n)) \\ 0 & \text{o.w.} \end{cases}$$

である．

この定理3によって，$\tau(\ell+1)$は$\tau(1)$と$\tau(\ell)$と$\tau(n)$だけで決定することがわかる．特に$\tau(2)$は$\tau(1)$と$\tau(n)$の値で決まる．そして$\tau(3)$は$\tau(2)$と$\tau(1)$と$\tau(n)$の値で決まるのだが，$\tau(2)$は$\tau(1)$と$\tau(n)$の値で決まるので，結局，$\tau(3)$も$\tau(1)$と$\tau(n)$の値で決まる．以下同様に，$\tau(4),\ldots,\tau(n-1)$も$\tau(1)$と$\tau(n)$の値で決まる．結局，n次の基本pNAP型の置換τは$\tau(1)$と$\tau(n)$の二つの値だけで一意に決まることがわかる．$\tau(1) \neq \tau(n)$であるから，n次の基本pNAP型の置換の個数は高々$(n-1)n$であることがわかる．従って，pNAP型の置換の個数の上界として次を得る．

系 4　nを2以上の自然数とする．n次のpNAP型の置換の個数は高々$(n-1)n^2$である．

定理3の漸化式は第2節の定理Cの漸化式と本質的に同じ漸化式と考えられる．実際，次が成り立つ．

系 5　基本pNAP型の置換τに1を加える変換で得られたpNAP型の置換をτ'とする．即ち，各$i \in [n]$に対して

$$\tau'(i) \equiv \tau(i) + 1 \mod n$$

とする．このとき各$\ell \in [n-1]$に対して

$$\tau'(\ell+1) - \tau'(\ell) \equiv \tau'(1) - \begin{cases} 1 & \text{if } \tau'(\ell) \geq \tau'(n) \\ 0 & \text{o.w.} \end{cases} \mod n$$

が成り立つ．

5　基本pNAP型の置換の列挙

前稿[3]においては計算機によりpNAP型の置換を列挙し，$n \leq 50$次においてはpNAP型の置換は全てSinv型であることを検証した．そこでの方法は，簡潔に述べれば，pNAP型の置換を定義する$K_\sigma = \{m, m+1\}$のmと付随するビット列$\vec{\delta} = (\delta_\ell)_{\ell=1}^{n-1}$を探索し，$(m, \vec{\delta})$からもたらされる$\sigma : [n] \to [n]$が置換になるかどうかをテストするものであった．しかしながら，2^{n-1}個存在する$\vec{\delta} \in \{0,1\}^{n-1}$を探索することは効率的ではなく，このために限られた範囲の次数$(n \leq 50)$のみに検証は留まった．これに対して，定理3は基本pNAP型の置換の具体的且つ簡潔な生成パラメータ$(\tau(1), \tau(n))$と小さい個数の上界の両方を与えるため，効率的且つ直接的な列挙が可能となる．

図1に定理3を応用した基本pNAP型の置換の列挙アルゴリズムを示す．考え方は素朴であり，それぞれの$(a,b) \in [n] \times [n]$に対して定理3の漸化式で$\tau(1) := a$, $\tau(n) := b$として準用し，列[18]$(t_{a,b}(1), t_{a,b}(2), \ldots, t_{a,b}(n))$を発生する．図1において，/* 漸化式による列の発生 */ のコメントをつけた箇所がそれである．

```
pnapsearch(n) {
  for (a ∈ [n]) {
    for (b ∈ [n]) {
      t_{a,b}(1) := a
      for (ℓ ∈ [n − 1]) {
        /* 漸化式による列の発生 */
        δ_ℓ := { 1  if Mod_n(t_{a,b}(ℓ)) < Mod_n(b)
               { 0  o.w.
        t_{a,b}(ℓ + 1) := Mod‾_n(t_{a,b}(ℓ) + t_{a,b}(1) + δ_ℓ)
      }
      t_{a,b} が(条件A1)を満たすか検査
      t_{a,b} が(条件P)を満たすか検査
      t_{a,b} が(条件N)を満たすか検査
      if ( Not(A1) 且つ P 且つ N ) {
        t_{a,b} を基本pNAP型の置換として計数
      }
    }
  }
}
```

図 1: 基本pNAP型の置換の列挙アルゴリズム

ここで$\overline{\mathrm{Mod}}_n$は

$$\overline{\mathrm{Mod}}_n(x) = \begin{cases} n & \text{if } \mathrm{Mod}_n(x) = 0 \\ \mathrm{Mod}_n(x) & \text{o.w.} \end{cases}$$

[18]ここではτではなくtを用いる．本稿ではτは置換を表す記号として用いており，一方でこの列$(t_{a,b}(1), \ldots, t_{a,b}(n))$の各項は相異なる(即ち置換)とは限らない．無用な混乱を避けるためτではなくtを使うことにした．

であり，mod nの合同を保ちながら剰余の範囲を$\{0,1,\ldots,n-1\}$から$[n]$に切り換えるための演算子である．このように，$(a,b)\in[n]\times[n]$をくまなく動かして写像$t_{a,b}:[n]\to[n]$を作れば，定理3の漸化式を満たすような置換の候補が見落しなく見つかる．但し，得られた$t_{a,b}$が実際に基本pNAP型の置換になるか，あるいは異なる$(a,b)\neq(a',b')$から同一の写像$t_{a,b}=t_{a',b'}$生じることがないのかについては別途検討を要する．

前者の問題に対応するため，次の3条件をそれぞれテストする．

(条件A1) ビット列 $\vec{\delta}$ が全て1からなる:
$$\forall\ell\in[n-1]\ \delta_\ell=1.$$
(条件P) $t_{a,b}$は置換である:
$$\forall\ell,\ell'\in[n]\ t_{a,b}(\ell)=t_{a,b}(\ell')\Rightarrow\ell=\ell'.$$
(条件N) 漸化式を定義するbと結果の$t_{a,b}(n)$が整合している:
$$b=t_{a,b}(n).$$

条件A1によって，$\vec{\delta}=(1^{n-1})$を特別扱いするのは，或るaに対して$\vec{\delta}=(1^{n-1})$で定義される置換$t_{a,b}$と$a+1$に対して$\vec{\delta}=(0^{n-1})$で定義される置換$t_{a+1,b'}$とは，「定数を加える変換」を施したときに同一の置換の集合を生じ，基本pNAP型の置換の計数結果を「定数を加える変換」によりpNAP型の置換の計数に移行するときに(確実なる)重複が起きるためである．条件Pをテストする理由は明白である．条件Nについて，定理3の漸化式は$\tau(n)$の値を用いる一方で，これに基づき実際に(素朴に)計算する場合は$\ell=1,2,\ldots,n-1$ と漸化式を利用して最後に$t(n)$ が得られるということになる．そこで，$\tau(n)$の「仮の値」として$b\in[n]$をとって，(a,b)から漸化式で$t_{a,b}$を定め，ひるがえって$b=t_{a,b}(n)$かどうかをテストするという手段をとっている．条件P 且つ 条件Nを満たす$t_{a,b}$は，条件A1をさておき，基本pNAP型の置換になることは漸化式より明らかである．

図1のアルゴリズムの演算量は，(a,b)が固定されれば，ℓに関する繰返しの演算量が$O(n)$回であり，3条件の検査も合わせて$O(n)$回でできるので，(a,b)がn^2通りあることを考えて，$O(n^3)$である．前項[3]での$O(n2^n)$と比較すると大幅に演算量が削減されている．かくして，定理3は基本pNAP型の置換を現実的な時間で列挙できる次数の範囲を大幅に広げた．$2\le n\le 1300$の範囲で$(a,b)\in[n]\times[n]$に対応する写像$t_{a,b}:[n]\to[n]$を列挙し，条件A1, P, N の成立によって(a,b)を分類計数した結果，範囲にある全てのnに対して，表1の通りとなった．

表 1: $t_{a,b}$による(a,b)の分類$(n\le 1300)$

$t_{a,b}$ が		条件N 満たす	条件N 満たさない
条件A1 満たす	条件P 満たす	$\phi(n)$	0
	条件P 満たさない	0	0
条件A1 満たさない	条件P 満たす	$\sum_{k=1}^{n-1}\phi(k)$	$\sum_{k=1}^{n-1}\phi(k)$
	条件P 満たさない	$\sum_{k=1}^{n}(k-\phi(k))$	$\sum_{k=1}^{n-1}(k-\phi(k))$

特に，Not(A1) 且つ P 且つ N を満たす $t_{a,b}$ の個数，つまり，基本pNAP型の置換であって定数を加える変換で重複を起さないものの個数は$\sum_{k=1}^{n-1}\phi(k)$である(論理的には，Not(A1) 且つ P 且つ N を満たす$t_{a,b}$をもたらす(a,b)の個数であるが，$a=t_{a,b}(1)$および条件Nから$b=t_{a,b}(n)$が課されているため，$t_{a,b}=t_{a',b'}$が異なる$(a,b)\neq(a',b')$について起こることはなく，$t_{a,b}$の個数といって良い)．これらに定数を加える変換を施したときに得られる置換がpNAP型の置換であるが，その個数高々$n\sum_{k=1}^{n-1}\phi(k)$である．定理Bにあるとおり，これはSinv型の置換の個数と等しく，定理Aの(2)でSinv型の

置換はpNAP型の置換なることが示されているから，次数$n \leq 1300$ではSinv型の置換の集合とpNAP型の置換の集合は等しく，要素数は$n\sum_{k=1}^{n-1}\phi(k)$であることがわかった．基本pNAP型の置換の計数という観点の他，図1のアルゴリズムの漸化式と表1での(a,b)の分類結果について観察されることを述べる．表1からすぐに読み取れることとして，「Not(A1) 且つ P 且つ N」と「Not(A1) 且つ P 且つ Not(N)」に分類される(a,b)の個数は互いに等しい．また，条件A1を満たす(a,b)は条件NもPも満たしその個数は$\phi(n)$個であるのだが，これらの理由については付録Bに記す．最後に Not(A1) 且つ Not(P) である(a,b)について言及しておく．条件Nを満たすものの個数が$\sum_{k=1}^{n}(k-\phi(k))$個，条件Nを満たさないものの個数が$\sum_{k=1}^{n-1}(k-\phi(k))$個であることが(この実験で)新たに確認された．これは置換でないものの個数についての話であるが興味深い現象である．どのような理由でこのようなことが起きているのか等は今後考察するべき話題であろう．

6 最後に

Sinv型とpNAP型は同じであろう．計算機を用いた計数の結果から，そう期待するのは自然だと思われる．さて，基本pNAP型の置換τは「初項」$\tau(1)$と「付随するビット列」$(\delta_k)_{k=1}^{n-1}$で与えられる．従って，基本pNAP型の置換の個数を数えるには，それぞれの初項に対して付随するビット列がどれだけあるかがわかればよいことになる．0と1の値しか取らないビット列は観察し易そうである．探せば何か性質が見つかるかもしれない．計算機を用いて付随するビット列を調べてみたところ，実際にいくつかの性質がみられる．しかしそれらの性質を用いてpNAP型の個数の上界を求めてみるとかなり大きな値になってしまう．Sinv型の置換の個数から随分離れてた値になってしまうのである．Sinv型とpNAP型は同じであろうと期待されるのにも関わらず，Sinv型の置換の個数とpNAP型の置換の個数の上界がかけ離れていてはやはり期待外れと言えよう．易しそうに思えた付随するビット列の観察される性質に着目して個数を評価する方法は行き詰まってしまった．

本稿第4節では，付随するビット列は基本pNAP型の置換を与えるfp単射の定義をするためだけに用いられている．つまり，付随するビット列を主たる考察対象にするのではなく，単に0と1の値しかとらない未知のパラメータとして扱っている．そのような扱い方のヒントになったのが第3.1節の終わりに述べた「置換σは$f(x)=\frac{\sigma(x)-1}{n}$の順位である」である．つまり，置換が与えられればその置換を小数部分の順位とみなす方法があるのである．小数部分の順位であれば数式を用いた議論ができる可能性がある．この方針で考察したものが今回の結果である．第3.2節の初めに，写像$f(x)=\frac{\sigma(x)-1}{n}$を持ち出して「置換は小数部分の順位と考えられる」といってみたところで直ちにこれが何か益するものをもたらすとは思えない，と述べた．実際この写像$f(x)$では役に立ちそうもない．しかしヒントとしては大いに役に立っているのである．役に立つかどうかは役に立ってから初めてわかるものなのだろうか．見方によってそのものの意義が大きく変わることを改めて知らされた次第である．

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] ヒトが生成する置換の統計的性質II： 永田誠，武井由智　大阪薬科大学紀要 Vol. 14 pp.19–48 (2020)

[3] ある型の置換の個数について： 永田誠，武井由智　大阪薬科大学紀要 Vol. 15 pp.51–70 (2021)

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

[5] Uber die Anordnung der Vielfachen einer reellen Zahl mod 1 : J. Surányi Ann. Univ. Sci. Budap. Eötvös, Sect. Math. 1, pp.107-111 (1958)

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

[7] Sós permutations : S. Bockiting-Conrad, Y. Kashina, T. K. Petersen, B. E. Tenner Amer. Math. Monthly, Vol.128, pp.407-422 (2021)

付録A

本付録Aでは，本文の第3節と第4節で述べた結果の証明を与える．本文中に述べた定義や定理等，読者の利便性等を考慮して多くの場合はこの付録Aで繰り返し述べることにする．また，本付録Aの目的は本文中の主張の証明を与えることであることを踏まえ，証明等の記述のし易さの観点から本文と若干異なる記法を用いる場合もある．(例えば，本文中のfによる順位付け写像を本付録Aでは f-ranking map と書く，$\mathfrak{t}_{\{g\}}$を$\mathfrak{T}_g$と書く等．) その場合はその旨を明確に言及する．

以下，$\mathbb{N}$は自然数全体の集合，$\mathbb{Z}$は有理整数環，$\mathbb{R}$は実数体とする．$\alpha\in\mathbb{R}$に対して，$\lfloor\alpha\rfloor$をαを超えない最大の整数とし，$\{\alpha\}=\alpha-\lfloor\alpha\rfloor$とする．故に$0\le\{\alpha\}<1$である．以下，$\{\alpha\}$を$\alpha$の小数部分と呼ぶ．自然数$n$に対して，1から$n$までの集合$\{1,2,\dots,n\}$を$[n]$で表す．即ち，$[n]:=\{1,2,\dots,n\}$である．また，$n$次の置換とは$[n]$から$[n]$の全単射を意味することとする．

A.1 順位付け写像について

用語「順位付け写像(ranking map)」を改めて定義をする．本稿ではXは有限集合の場合のみを扱うが，以下の事実1まではXは一般の集合でよい．

Rを集合，$\preceq$をRに入る全順序関係とする．即ち，$(R,\preceq)$を全順序集合とする．また，Xを集合とし，XからRへの写像$f:X\to R$が単射であるとする．fの像$f(X)$を$\mathrm{Im}f$と書くことにする．fによって誘導される写像$\mathfrak{p}_f:X\to 2^X$ を，$x\in X$に対して

$$\mathfrak{p}_f(x):=\{w\in X\ ;\ f(w)\preceq f(x)\}$$

と定義する．

事実 1. $(R,\preceq)$, X, f, $\mathfrak{p}_f$を上記のものとする．
(0) $x\in X$に対して，$x\in\mathfrak{p}_f(x)$である．
(1) $x,y\in X$が$f(x)\preceq f(y)$であるとき，$\mathfrak{p}_f(x)\subseteq\mathfrak{p}_f(y)$である．
(2) $x,y\in X$が$f(x)\preceq f(y)$ 且つ $x\neq y$であるとき，$\mathfrak{p}_f(x)\subsetneq\mathfrak{p}_f(y)$である．
従って，$\mathfrak{p}_f$は全順序集合$(\mathrm{Im}f,\preceq)$から集合の包含関係による順序集合$(2^x,\subseteq)$への順序を保つ写像である．

証明. 先ず，$f(x)\preceq f(x)$より$x\in\mathfrak{p}_f(x)$であるから(0)の主張が成立する．$f(x)\preceq f(y)$のとき，各$z\in\mathfrak{p}_f(x)$に対して，$f(z)\preceq f(x)$であるから$f(z)\preceq f(y)$であり，$z\in\mathfrak{p}_f(y)$である．即ち，$\mathfrak{p}_f(x)\subseteq\mathfrak{p}_f(y)$である．故に(1)の主張が成立する．$x,y\in X$ with $x\neq y$に対して，もし$\mathfrak{p}_f(x)=\mathfrak{p}_f(y)$ならば，$y\in\mathfrak{p}_f(x)$より$f(y)\preceq f(x)$であり，$x\in\mathfrak{p}_f(y)$より$f(x)\preceq f(y)$である．故に$f(x)=f(y)$となる．一方，$f$は単射であるから，$x\neq y$に対しては$f(x)\neq f(y)$であるので矛盾する．故に$\mathfrak{p}_f(x)\neq\mathfrak{p}_f(y)$である．(1)より(2)の主張が成立する．□

事実 2. $(R,\preceq)$, X, f, $\mathfrak{p}_f$を上記のものとする．さらに，Xを有限集合であると仮定し，nをXの要素の個数，即ち，$n=|X|$とする．写像$\mathfrak{t}_f:X\to\mathbb{N}$を，$x\in X$に対して

$$\mathfrak{t}_f(x):=|\mathfrak{p}_f|$$

で定義する．このとき，写像$\mathfrak{t}_f$は単射であり，その像$\mathrm{Im}\,\mathfrak{t}_f$は$[n]$である．

証明. $x\in X$に対して，$x\in\mathfrak{p}_f(x)$より$1\le\mathfrak{t}_f(x)$である．また，$\mathfrak{p}_f(x)\subseteq X$より$\mathfrak{t}_f(x)\le n$である．故に$\mathrm{Im}\,\mathfrak{t}_f\subseteq[n]$である．$x,y\in X$ with $x\neq y$に対して，($\preceq$は全順序なので)$f(x)\preceq f(y)$又は$f(y)\preceq f(x)$であるが，$f(x)\preceq f(y)$のとき，事実1の(2)より$\mathfrak{t}_f(x)<\mathfrak{t}_f(y)$である．即ち，$x\neq y$ならば$\mathfrak{t}_f(x)\neq\mathfrak{t}_f(y)$であり，$\mathfrak{t}_f$は単射であることがわかる．よって，$|X|=n$であるから$|\mathrm{Im}\,\mathfrak{t}_f|=n$であり，$\mathrm{Im}\,\mathfrak{t}_f=[n]$である．□

定義 3. $(R,\preceq)$を全順序集合，Xを有限集合とし，$n=|X|$とする．写像$f:X\to R$と単射とする．このとき次の well-defined な全単射写像

$$\begin{array}{rccc}\mathfrak{t}_f: & X & \to & [n] \\ & \cup & & \cup \\ & x & \mapsto & |\{w\in X\ ;\ f(w)\preceq f(x)\}|\end{array}$$

をXのfによる$(R,\preceq)$での順位付け写像(ranking map)，或いは単に，fによる順位付け写像(f-ranking map)と呼ぶことにする．

例 4. $X=[n]$の場合，f-ranking map は$[n]$から$[n]$への全単射，即ち，n次の置換である．

例 5. $X=[n]$とする．Rを長さ1の半開区間$[0,1)$とし，$\preceq$を実数の通常の順序$\leq$とする．1より小さい正の無理数αを固定して，$f(x)=\{\alpha x\}$で写像$f:[n]\to[0,1)$を定義するとこれは単射である．このときのf-ranking map は「αに関するn次のSinv置換」(cf. [3, 第4節])である．

次は本文中に言及したものである．ここで理由を記しておく．

事実 6. すべての$[n]$から$[n]$への全単射は，或るf-ranking map である．

証明. σを$[n]$から$[n]$の全単射，即ち，n次の置換とする．全順序集合$(R,\preceq)$を$R=[0,1))$(長さ1の半開区間)，$\preceq$を実数の通常の順序$\leq$とする．$X=[n]$として，写像$f:[n]\to[0,1)$を$f(x):=\frac{\sigma(x)-1}{n}$で定義する．$x,y\in[n]$に対して，$\sigma(x)\leq\sigma(y)$であることと$f(x)\leq f(y)$であることは同値である．故に$\{w\in[n]\ ;\ f(w)\leq f(x)\}=\{w\in[n]\ ;\ \sigma(w)\leq\sigma(x)\}$ である．$\sigma(w)\leq\sigma(x)$を満たす$w\in[n]$はxを含めて丁度$\sigma(x)$個あるので，$\mathfrak{t}_f(x)=\sigma(x)$であることがわかる．□

事実 7. 定義3の記法の下，$x,y\in X$に対して，次の(1)と(2)は同値である．
(1) $\mathfrak{t}_f(x)\leq\mathfrak{t}_f(y)$
(2) $f(x)\preceq f(y)$

証明. 事実1の(1)より，$f(x)\preceq f(y)$ のとき，$\mathfrak{p}_f(x)\subseteq\mathfrak{p}_f(y)$ であるから，$\mathfrak{t}_f(x)\leq\mathfrak{t}_f(y)$ である．
逆に$f(x)\preceq f(y)$でない，とすると，全順序性より$f(y)\preceq f(x)$ 且つ $f(x)\neq f(y)$である．故に(fの単射性より$x=y$ならば$f(x)=f(y)$なので) $x\neq y$である．事実1の(2)より$\mathfrak{p}_f(y)\subsetneq\mathfrak{p}_f(x)$ であるから，$\mathfrak{t}_f(y)<\mathfrak{t}_f(x)$ である．即ち，$\mathfrak{t}_f(x)\leq\mathfrak{t}_f(y)$ではない．□

A.2 fp単射による置換について

我々の主たる考察対象は置換である．それに向けてより具体的に議論を進めよう．

定義 8. nを自然数とする．写像$g:[n]\to\mathbb{R}$に対して，gと「小数部分」の写像$\{\cdot\}:\mathbb{R}\to[0,1)$の合成写像

$$\begin{array}{rccc}\{g\}: & [n] & \to & [0,1) \\ & \cup & & \cup \\ & \ell & \mapsto & \{g(\ell)\}\end{array}$$

をgのfp写像[19]と呼び，さらにgのfp写像$\{g\}$が単射であるときgはn次のfp単射であるということにする．

以下，gがn次のfp単射であるならば，($\mathfrak{t}_f$のfを$\{g\}$とした) $\mathfrak{t}_{\{g\}}$は$\{g\}$-ranking map (特に単射)であるが，これに関しては次が成り立つ．

事実 9. nの自然数とする．写像$g:[n]\to\mathbb{R}$に対して，写像$\mathfrak{T}_g:[n]\to[n]$を各$\ell\in[n]$で$\mathfrak{T}_g(\ell):=|\{k\in[n]\ ;\ \{g(k)\}\leq\{g(\ell)\}\}|$ と定義する：

$$\begin{array}{rccc}\mathfrak{T}_g: & [n] & \to & [n] \\ & \cup & & \cup \\ & \ell & \mapsto & |\{k\in[n]\ ;\ \{g(k)\}\leq\{g(\ell)\}\}|\end{array}$$

このとき，写像$\mathfrak{T}_g$が単射ならば，gはn次のfp単射である．

[19] $g(\ell)$の小数部分 fractional part を与える写像なのでfp写像と呼ぶことにした．

証明. 対偶を示す．fp写像$\{g\}$が単射でないとする．このとき，$p,q\in[n]$ with $p\neq q$で，$\{g(p)\}=\{g(q)\}$となるp,qが存在する．このp,qに対して，$\{g(p)\}$ $(=\{g(q)\})$をαと置くと，$\mathfrak{T}_g(p)=|\{k\in[n]\ ;\ \{g(k)\}\leq\alpha\}|=\mathfrak{T}_g(q)$となり，$\mathfrak{T}_g$は単射ではない．□

注意 10. 事実9の$\mathfrak{T}_g$が単射ならばこの写像$\mathfrak{T}_g$は全単射である．故に，写像$g:[n]\to\mathbb{R}$に対して，$\mathfrak{T}_g$がn次の置換であることと，gがn次のfp単射であることは同値であり，このとき，$(X=[n],R=[0,1),\mathfrak{t}_f$の$f$を$\{g\}$とした$)$ $\{g\}$-ranking map $\mathfrak{t}_{\{g\}}$ と$\mathfrak{T}_g$は同一である．本文では$\{g\}$-ranking map の記号として$\mathfrak{t}_{\{g\}}$を用いているが，これ以降，f-ranking mapは $f=\{g\}$の場合の$\mathfrak{t}_{\{g\}}$のみを考えることになる．そこで読みやすさを考慮し，本付録Aでは$\mathfrak{t}_{\{g\}}$の代わりに$\mathfrak{T}_g$を用いることにする．後述定義13も参照のこと．

次は，事実7より自明であるが，後に利用されるので記しておく．

事実 11. 事実9の記法の下，gをn次のfp単射とする．このとき，$i,j\in[n]$に対して，次の(1)と(2)は同値である．
(1) $\mathfrak{T}_g(i)\geq\mathfrak{T}_g(j)$
(2) $\{g(i)\}\geq\{g(j)\}$

証明. $X=[n]$, $R=[0,1)$, $f=\{g\}$として$\{g\}$-ranking map $\mathfrak{t}_{\{g\}}$と$\mathfrak{T}_g$は同一であるので事実7より主張が成り立つ．□

次の事実12は[3, 付録A事実5]にあるのだが，そこでの主張はa,bが非負という条件を付けたものであるので，その条件を取り除いたものをここで改めて述べておく．証明は[3, 付録A事実5]と同じである．この事実12が本文第3節初めに述べた「小数部分の順序関係は整数部分の数式を用いて表すことができるという事実」に対応する．

事実 12. $a,b\in\mathbb{R}$に対して

$$1-\lfloor a\rfloor+\lfloor b\rfloor+\lfloor a-b\rfloor=\begin{cases}1 & \text{if } \{a\}\geq\{b\}\\ 0 & \text{if } \{a\}<\{b\}\end{cases}$$

が成り立つ．

証明. $0\leq\{a\},\{b\}<1$より$-1<\{a\}-\{b\}<1$である．もし，$\{a\}\geq\{b\}$ならば$0\leq\{a\}-\{b\}<1$であり，もし，$\{a\}<\{b\}$ならば$0<\{b\}-\{a\}<1$，即ち，$0<1-(\{b\}-\{a\})<1$である．$a-b=(\lfloor a\rfloor+\{a\})-(\lfloor b\rfloor+\{b\})=\lfloor a\rfloor-\lfloor b\rfloor+(\{a\}-\{b\})=\lfloor a\rfloor-\lfloor b\rfloor-1+(1-(\{b\}-\{a\}))$ である．一般に，実数$\alpha\in\mathbb{R}$に対して，整数$m\in\mathbb{Z}$が$0\leq\alpha-m<1$を満たすならば([3, 付録A事実1]より) $\lfloor\alpha\rfloor=m$であり，$\{\alpha\}=\alpha-m$である．故に$a,b\in\mathbb{R}$に対して

$$\lfloor a-b\rfloor=\begin{cases}\lfloor a\rfloor-\lfloor b\rfloor & \text{if } \{a\}\geq\{b\}\\ \lfloor a\rfloor-\lfloor b\rfloor-1 & \text{if } \{a\}<\{b\}\end{cases}$$

であるので，主張が成立する．□

以下，条件Aに対して，

$$\mathbb{1}[A]=\begin{cases}1 & \text{if } A \text{ is true}\\ 0 & \text{if } A \text{ is false}\end{cases}$$

という記号を用いる．
事実9と注意10を踏まえて，次を用語を定義する．

定義 13. gをn次のfp単射であるとする．$\{g\}$-ranking map $\mathfrak{t}_{\{g\}}$を$\mathfrak{T}_g$と記し，これをgによるfp置換と呼ぶこととする．

本文第3節の定理1は，次の命題14の主張[20]から直ちに得られる．

命題 14. nを2以上の自然数とし，写像$g:[n]\to\mathbb{R}$がfp単射であるとする．また，$g(0)=0$として，写像$D:\{0,1,\ldots,n-1\}^2\to\mathbb{Z}$を$i,j\in\{0,1,\ldots,n-1\}$に対して，

$$D(i,j):=\lfloor g(i+1)-g(j+1)\rfloor-\lfloor g(i)-g(j)\rfloor$$

[20]命題14の写像$g:[n]\to\mathbb{R}$が「fp単射」という条件を「各$k=2,3,\ldots,n$ で $g(1)-g(k)\notin\mathbb{Z}$」に置き換えても($\mathfrak{T}_g$を事実9の意味として)主張の等式は成立する．

で定義する．このとき，gによるfp置換$\mathfrak{T}_g$について次が成り立つ．各$\ell \in [n-1]$に対して

$$\mathfrak{T}_g(1)+\mathfrak{T}_g(\ell)-\mathfrak{T}_g(\ell+1)+n\left(\lfloor g(1)\rfloor+\lfloor g(\ell)\rfloor-\lfloor g(\ell+1)\rfloor\right) \\ +D(\ell,0)+\sum_{k=1}^{n-1}\left(D(k,0)+D(\ell,k)\right)=\mathbb{1}[\mathfrak{T}_g(\ell)\geq\mathfrak{T}_g(n)] \quad (1)$$

証明. $\ell \in [n]$に対して，fp単射gによるfp置換$\mathfrak{T}_g$は事実12より

$$\mathfrak{T}_g(\ell)=|\{k\in[n]\,;\,\{g(k)\}\leq\{g(\ell)\}\}|=\sum_{k=1}^{n}\mathbb{1}[\{g(\ell)\}\geq\{g(k)\}]=n(1-\lfloor g(\ell)\rfloor)+\sum_{k=1}^{n}\left(\lfloor g(k)\rfloor+\lfloor g(\ell)-g(k)\rfloor\right)$$

である．$\ell \leq n-1$のときは

$$\mathfrak{T}_g(\ell+1)=n(1-\lfloor g(\ell+1)\rfloor)+\sum_{k=1}^{n}\left(\lfloor g(k)\rfloor+\lfloor g(\ell+1)-g(k)\rfloor\right)$$

であるから，

$$\mathfrak{T}_g(\ell+1)-\mathfrak{T}_g(\ell)=n\left(\lfloor g(\ell)\rfloor-\lfloor g(\ell+1)\rfloor\right)+\sum_{k=1}^{n}\left(\lfloor g(\ell+1)-g(k)\rfloor-\lfloor g(\ell)-g(k)\rfloor\right) \quad (2)$$

である．写像$g:[n]\to\mathbb{R}$の定義域を拡張した写像$\tilde{g}:\{-n,-(n-1),\ldots,-1,0,1,2,\ldots,n\}\to\mathbb{R}$を

$$\tilde{g}(0):=g(0)=0,\quad \ell\in[n]\text{ に対して }\tilde{g}(\ell):=g(\ell),\quad \tilde{g}(-\ell):=-g(\ell)$$

で定義する．さらに，各$i,j\in[n]$に対して，写像$h:[n]\times[n]\to\mathbb{Z}$を

$$h(i,j):=\lfloor g(i)-g(j)\rfloor-\lfloor\tilde{g}(i-j)\rfloor$$

で定義する．$\lfloor g(i)-g(j)\rfloor=h(i,j)+\lfloor\tilde{g}(i-j)\rfloor$であるから

$$\sum_{k=1}^{n}\left(\lfloor g(\ell+1)-g(k)\rfloor-\lfloor g(\ell)-g(k)\rfloor\right)=\sum_{k=1}^{n}\left(h(\ell+1,k)+\lfloor\tilde{g}(\ell+1-k)\rfloor\right)-\left(h(\ell,k)+\lfloor\tilde{g}(\ell-k)\rfloor\right) \\ =\sum_{k=1}^{n}\left(\lfloor\tilde{g}(\ell+1-k)\rfloor-\lfloor\tilde{g}(\ell-k)\rfloor\right)+\sum_{k=1}^{n}\left(h(\ell+1,k)-h(\ell,k)\right) \quad (3)$$

さて，$\lfloor\tilde{g}(\ell-n)\rfloor=\lfloor g(\ell)-g(n)\rfloor-h(\ell,n)$であるから，$\ell\in[n-1]$のときは$\tilde{g}(\ell)=g(\ell)$なので

$$\sum_{k=1}^{n}\left(\lfloor\tilde{g}(\ell+1-k)\rfloor-\lfloor\tilde{g}(\ell-k)\rfloor\right)=\left(\lfloor\tilde{g}(\ell+1-1)\rfloor+\lfloor\tilde{g}(\ell+1-2)\rfloor+\cdots+\lfloor\tilde{g}(\ell+1-n)\rfloor\right) \\ -\left(\lfloor\tilde{g}(\ell-1)\rfloor+\lfloor\tilde{g}(\ell-2)\rfloor+\cdots+\lfloor\tilde{g}(\ell-n)\rfloor\right) \\ =\lfloor\tilde{g}(\ell)\rfloor-\lfloor\tilde{g}(\ell-n)\rfloor=\lfloor g(\ell)\rfloor-\lfloor g(\ell)-g(n)\rfloor+h(\ell,n)$$

故に

$$\text{式}(3)=\lfloor g(\ell)\rfloor-\lfloor g(\ell)-g(n)\rfloor+h(\ell,n)+\sum_{k=1}^{n}\left(h(\ell+1,k)-h(\ell,k)\right) \\ =\lfloor g(\ell)\rfloor-\lfloor g(\ell)-g(n)\rfloor+\sum_{k=1}^{n}h(\ell+1,k)-\sum_{k=1}^{n-1}h(\ell,k)$$

式(2)より

$$\mathfrak{T}_g(\ell+1)-\mathfrak{T}_g(\ell)=n\left(\lfloor g(\ell)\rfloor-\lfloor g(\ell+1)\rfloor\right)+\lfloor g(\ell)\rfloor-\lfloor g(\ell)-g(n)\rfloor+\sum_{k=1}^{n}h(\ell+1,k)-\sum_{k=1}^{n-1}h(\ell,k)$$

即ち，

$$-\lfloor g(\ell)\rfloor+\lfloor g(\ell)-g(n)\rfloor=-\mathfrak{T}_g(\ell+1)+\mathfrak{T}_g(\ell)+n\left(\lfloor g(\ell)\rfloor-\lfloor g(\ell+1)\rfloor\right)+\sum_{k=1}^{n}h(\ell+1,k)-\sum_{k=1}^{n-1}h(\ell,k)\tag{4}$$

さて，gがfp単射のとき，各$k=2,3,\dots,n$で$g(1)-g(k)\notin\mathbb{Z}$が成り立つことに注意する．なぜならば，もし$\exists\, m\in\mathbb{Z}$ s.t. $g(1)+m=g(k)$とすると，$\{g(1)\}=\{g(1)+m\}=\{g(k)\}$となり，$g$がfp単射でないからである．([3, 付録A事実2]より) 一般に$\alpha\in\mathbb{R}\setminus\mathbb{Z}$のとき，$\lfloor\alpha\rfloor+\lfloor-\alpha\rfloor=-1$であるから

$$\lfloor g(1)-g(k)\rfloor=\begin{cases}0 & \text{if } k=1\\ -\lfloor g(k)-g(1)\rfloor-1 & \text{if } k=2,\dots,n\end{cases}$$

である．$k=2,\dots,n$に対して$\lfloor g(k)-g(1)\rfloor=h(k,1)+\lfloor\tilde{g}(k-1)\rfloor=h(k,1)+\lfloor g(k-1)\rfloor$に注意すると

$$\begin{aligned}\mathfrak{T}_g(1)&=n\left(1-\lfloor g(1)\rfloor\right)+\sum_{k=1}^{n}\left(\lfloor g(k)\rfloor+\lfloor g(1)-g(k)\rfloor\right)=n\left(1-\lfloor g(1)\rfloor\right)+\sum_{k=1}^{n}\lfloor g(k)\rfloor-\sum_{k=2}^{n}\left(\lfloor g(k)-g(1)\rfloor+1\right)\\&=n\left(1-\lfloor g(1)\rfloor\right)+\sum_{k=1}^{n}\lfloor g(k)\rfloor-(n-1)-\sum_{k=2}^{n}\lfloor g(k)-g(1)\rfloor\\&=n\left(1-\lfloor g(1)\rfloor\right)+\sum_{k=1}^{n}\lfloor g(k)\rfloor-(n-1)-\sum_{k=2}^{n}\left(h(k,1)+\lfloor g(k-1)\rfloor\right)\\&=n\left(1-\lfloor g(1)\rfloor\right)+\lfloor g(n)\rfloor-(n-1)-\sum_{k=2}^{n}h(k,1)=-n\lfloor g(1)\rfloor+\lfloor g(n)\rfloor+1-\sum_{k=2}^{n}h(k,1)\end{aligned}$$

即ち，

$$1+\lfloor g(n)\rfloor=\mathfrak{T}_g(1)+n\lfloor g(1)\rfloor+\sum_{k=2}^{n}h(k,1)\tag{5}$$

式(4)と式(5)を加えて

$$\begin{aligned}1-\lfloor g(\ell)\rfloor+\lfloor g(n)\rfloor+\lfloor g(\ell)-g(n)\rfloor=&\\&-\mathfrak{T}_g(\ell+1)+\mathfrak{T}_g(\ell)+n\left(\lfloor g(\ell)\rfloor-\lfloor g(\ell+1)\rfloor\right)+\sum_{k=1}^{n}h(\ell+1,k)-\sum_{k=1}^{n-1}h(\ell,k)\\&+\mathfrak{T}_g(1)+n\lfloor g(1)\rfloor+\sum_{k=2}^{n}h(k,1)\end{aligned}$$

事実12より

$$1-\lfloor g(\ell)\rfloor+\lfloor g(n)\rfloor+\lfloor g(\ell)-g(n)\rfloor=\begin{cases}1 & \text{if } \{g(\ell)\}\geq\{g(n)\}\\ 0 & \text{if } \{g(\ell)\}<\{g(n)\}\end{cases}$$

であるから，

$$\begin{aligned}\mathfrak{T}_g(1)+\mathfrak{T}_g(\ell)-\mathfrak{T}_g(\ell+1)+n\left(\lfloor g(1)\rfloor+\lfloor g(\ell)\rfloor-\lfloor g(\ell+1)\rfloor\right)+\sum_{k=2}^{n}h(k,1)+\sum_{k=1}^{n}h(\ell+1,k)-\sum_{k=1}^{n-1}h(\ell,k)&\\=\begin{cases}1 & \text{if } \{g(\ell)\}\geq\{g(n)\}\\ 0 & \text{if } \{g(\ell)\}<\{g(n)\}\end{cases}&\end{aligned}\tag{6}$$

さて，$g(0)=0$であり，$k=2,\dots,n$で$\tilde{g}(k-1)=g(k-1)$なので，

$$\sum_{k=2}^{n} h(k,1) = \sum_{k=2}^{n} (\lfloor g(k)-g(1)\rfloor - \lfloor \tilde{g}(k-1)\rfloor)$$
$$= \sum_{k=2}^{n} (\lfloor g(k)-g(1)\rfloor - \lfloor g(k-1)-g(0)\rfloor) = \sum_{k=1}^{n-1} (\lfloor g(k+1)-g(1)\rfloor - \lfloor g(k)-g(0)\rfloor) = \sum_{k=1}^{n-1} D(k,0) \quad (7)$$

また

$$\sum_{k=1}^{n} h(\ell+1,k) - \sum_{k=1}^{n-1} h(\ell,k) = \sum_{k=0}^{n-1} h(\ell+1,k+1) - \sum_{k=1}^{n-1} h(\ell,k) = h(\ell+1,1) + \sum_{k=1}^{n-1} (h(\ell+1,k+1) - h(\ell,k))$$
$$= h(\ell+1,1) + \sum_{k=1}^{n-1} ((\lfloor g(\ell+1)-g(k+1)\rfloor - \lfloor \tilde{g}(\ell-k)\rfloor) - (\lfloor g(\ell)-g(k)\rfloor - \lfloor \tilde{g}(\ell-k)\rfloor))$$
$$= h(\ell+1,1) + \sum_{k=1}^{n-1} (\lfloor g(\ell+1)-g(k+1)\rfloor - \lfloor g(\ell)-g(k)\rfloor) = \lfloor g(\ell+1)-g(1)\rfloor - \lfloor \tilde{g}(\ell)\rfloor + \sum_{k=1}^{n-1} D(\ell,k)$$
$$= \lfloor g(\ell+1)-g(1)\rfloor - \lfloor g(\ell)-g(0)\rfloor + \sum_{k=1}^{n-1} D(\ell,k) = D(\ell,0) + \sum_{k=1}^{n-1} D(\ell,k) \quad (8)$$

事実11，式(6), 式(7), 式(8)より式(1)を得る．□

A.3 基本pNAP型について

基本pNAP型の置換で初項[21]を指定したものを考える．

定義 15. $m\in\mathbb{Z}$, $n\in\mathbb{N}$ に対して$\mathrm{Mod}_n(m)$でmをnで割った余りを表す．即ち $q,r\in\mathbb{Z}$ with $0\le r\le n-1$を用いて$m=qn+r$と書けるとき，$\mathrm{Mod}_n(m)=r$である．

事実 16. 各$a\in\mathbb{Z}$, $n\in\mathbb{N}$ に対して，次が成り立つ．

$$\mathrm{Mod}_n(a-1)+1 = \begin{cases} n & \text{if } \mathrm{Mod}_n(a)=0 \\ \mathrm{Mod}_n(a) & \text{o.w.} \end{cases}$$

証明. $a=mn+r$, $m,r\in\mathbb{Z}$, $r=\mathrm{Mod}_n(a)$とすると$0\le r\le n-1$である．$r=0$のとき，$a-1=mn-1=(m-1)n+n-1$より$\mathrm{Mod}_n(a-1)=n-1$であるから，$\mathrm{Mod}_n(a-1)+1=n$である．$1\le r\le n-1$のとき，$a-1=mn+r-1$より$\mathrm{Mod}_n(a-1)=r-1$であり，$\mathrm{Mod}_n(a-1)+1=r$である．□

次は初項を指定した基本pNAP型の名称の定義である．

定義 17. aを非負整数とし，$\delta_1,\dots,\delta_{n-1}$を0又は1の整数とする．$n$次の置換$\tau$が，各$\ell\in[n]$で[22]

$$\tau(\ell) = \mathrm{Mod}_n\left(\left(\ell a + \sum_{k=1}^{\ell-1}\delta_k\right) - 1\right) + 1$$

であるとき，τを$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型と呼ぶことにする．また，この数列$(\delta_k)_{k=1}^{n-1}$を$\tau$に付随するビット列と呼ぶことにする．$\tau$に付随するビット列$(\delta_k)_{k=1}^{n-1}$を省略しても混乱しないときは，単に a-基本pNAP型と呼ぶことにする．

[21] n次の置換τ, 即ち，全単射$\tau:[n]\to[n]$に対して，$\tau(1)$を初項と呼んでいる．

[22] 以下，$\mathrm{Mod}_n(a-1)+1$の類いが頻繁に現れる．本文第5節のように，事実16からこれを$\overline{\mathrm{Mod}}_n(a)$と短く表した方が簡明になる場合もあるが，実際に余りの計算をするとなると馴染みのあるMod_nを用いた方が直感的でわかりやすいであろう．計算することが多い本付録Aでは，冗長な記法になることを承知の上でMod_nをそのまま用いることにした．

a-pNAP型のn次の置換τの初項は$\tau(1)=\mathrm{Mod}_n(a-1)+1$ であるから，aがnの倍数のときは$\tau(1)=n$であり，aがnの倍数でないときは$\tau(1)$はaをnで割った余りである．また，$\mathrm{Mod}_n(\left(\ell(a+n)+\sum_{k=1}^{\ell-1}\delta_k\right)-1)=\mathrm{Mod}_n(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1+an)=\mathrm{Mod}_n(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1)$ であるから，a-pNAP型のaは0以上$n-1$以下の整数を考えれば十分である．

aが$0\le a\le n-1$のとき[23]，$(a,(\delta_k)_{k=1}^{n})$-pNAP型のn次の置換τに対して，

$$\tau(1)=\mathrm{Mod}_n(a-1)+1,\quad \tau(n)=\mathrm{Mod}_n(\left(\sum_{k=1}^{n-1}\delta_k\right)-1)+1$$

である．つまり，a-pNAP型は初項$\tau(1)$を$\mathrm{Mod}_n(a-1)+1$と指定した基本pNAP型[24]のことである．もし，$\sum_{k=1}^{n-1}\delta_k=0$, 即ち，$\delta_1=\cdots=\delta_{n-1}=0$であるとき，$\tau(n)=n-1+1=n$である．一方，$\sum_{k=1}^{n-1}\delta_k\ge 1$ならば，$\tau(n)=\sum_{k=1}^{n-1}\delta_k$である．

事実 18. aを$0\le a\le n-1$なる整数とし，n次の置換τを$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型とする．このとき，$a=0$の場合は$\tau(1)=n$, それ以外の場合は$\tau(1)=a$である．また($a=0$でもそれ以外でも)各$\ell\in[n-1]$に対して，

$$\tau(\ell+1)-\tau(\ell)=\begin{cases}a+\delta_\ell & \text{if } \tau(\ell)+a+\delta_\ell\le n\\ a+\delta_\ell-n & \text{o.w.}\end{cases}$$

である．特にτはpNAP型である．

証明. $a=0$のとき，$\tau(1)=\mathrm{Mod}_n(0-1)+1=n$である．このとき，$\tau(2)=\mathrm{Mod}_n(\delta_1-1)+1$ であるが，τは置換であるから$\tau(2)\ne\tau(1)=n$である．従って$\delta_1\ne 0$, 即ち，$\delta_1=1$でなくてはならない．このとき$\tau(2)=1$であるから，$\tau(2)-\tau(1)=1-n=a+\delta_1-n$であり，$\tau(1)+a+\delta_1=n+0+1>n$である．また，$\ell\ge 2$のとき，$\tau(\ell)\ne\tau(1)=n$より$1\le\tau(\ell)\le n-1$である．$\tau(\ell)+a+\delta_\ell\le n-1+0+1\le n$であり，また，$\delta_1=1$より$1\le\sum_{k=1}^{\ell-1}\delta_k\le n-1$であるから，$\tau(\ell)=\mathrm{Mod}_n(\left(\sum_{k=1}^{\ell-1}\delta_k\right)-1)+1=\sum_{k=1}^{\ell-1}\delta_k$であり，$\tau(\ell+1)-\tau(\ell)=\delta_\ell$である．従って$a=0$のとき，主張が成立する．

$1\le a\le n-1$のとき，$\tau(1)=\mathrm{Mod}_n(a-1)+1=a$である．さて，一般に$m,b\in\mathbb{Z}_{\ge 0}$とし，$m=qn+r$, $q,r\in\mathbb{Z}$, $r=\mathrm{Mod}_n(m)$とするとき，$m+b=qn+r+b=(q+1)n+r+b-n$ より，$r+b\le n-1$ならば$\mathrm{Mod}_n(m+b)=\mathrm{Mod}_n(m)+b$であり，$r+b\ge n$ならば$\mathrm{Mod}_n(m+b)=\mathrm{Mod}_n(m)+b-n$である．従って，各$\ell\in[n-1]$に対して，($b=a+\delta_\ell$として)

$$\begin{aligned}\tau(\ell+1)-\tau(\ell)&=\mathrm{Mod}_n(\left((\ell+1)a+\sum_{k=1}^{\ell}\delta_k\right)-1)+1-\left(\mathrm{Mod}_n(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1)+1\right)\\&=\mathrm{Mod}_n(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1+a+\delta_\ell)-\mathrm{Mod}_n(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1)\\&=\begin{cases}a+\delta_\ell & \text{if } \mathrm{Mod}_n(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1)+a+\delta_\ell\le n-1\\ a+\delta_\ell-n & \text{o.w.}\end{cases}\end{aligned}$$

よって主張の式が成立する．また，δ_ℓは0か1なのでこの式からτはpNAP型であることがわかる．□

事実 19. n次の置換が0-pNAP型ならば$(0,(1)_{k=1}^{n-1})$-pNAP型である．即ち，$a=0$のときの$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型の置換に付随するビット列は$\delta_1=\cdots=\delta_{n-1}=1$の場合だけである．特に，$n$次の置換$\tau$が0-pNAP型ならば$\tau(1)=n$, 各$\ell\in[n-1]$で$\tau(\ell+1)=\ell$である．

証明. $a=0$のとき，事実18より$\tau(1)=n$である．このとき，$\delta_1=1$である．なぜならば(事実18の証明で既に述べたが) もし$\delta_1=0$ならば，事実18より$\tau(2)=n=\tau(1)$となり，τは置換ではない．よって$\delta_1=1$であり，このとき(事実18の証明で述べたが)$\tau(2)=1$であることがわかる．同様に各$\ell=2,\ldots,n-1$ に対して，$\delta_1,\ldots,\delta_{\ell-1}=1$であり，$\tau(\ell)=\ell-1$であると仮定する．もし$\delta_\ell=0$ならば，$\tau(\ell)+a+\delta_\ell\le n$であるから，

[23]以下，$0\le a\le n-1$を$1\le a\le n$としても構わないかもしれないのだが，そうしなかった理由は，$0\le a\le n-1$のとき「$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型の置換に対して，$(n-1-a,(1-\delta_k)_{k=1}^{n-1})$-pNAP型の置換が存在する」という性質があるからである．例えば，$0\le a\le n-1$とすることで，事実19と事実20がこのような対称的なpNAP型の置換の存在性を示唆することになると思われる．

[24]頭に“a-”がついているので(a-基本pNAP型と書かずに) a-pNAP型と書いても混乱しないであろう．

事実18より$\tau(\ell)=\tau(\ell+1)$となるが，これはτが置換であることに反する．故に$\delta_\ell=1$であり，事実18より$\tau(\ell+1)=\tau(\ell)+1=\ell$となる．□

事実 20. n次の置換が$(n-1)$-pNAP型ならば$(n-1,(0)_{k=1}^{n-1})$-pNAP型である．即ち，$a=n-1$のときの$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型の置換に付随するビット列は$\delta_1=\cdots=\delta_{n-1}=0$の場合だけである．特に，$n$次の置換$\tau$が$(n-1)$-pNAP型ならば各$\ell\in[n-1]$で$\tau(\ell)=n-\ell$で，$\tau(n)=n$である．

証明. $n=2$のとき，$\tau(1)=1$であるから $\tau(2)=2$であり，よって$\delta_1=1$である．$n\geq 3$とする．$a=n-1$のとき，a-pNAP型の定義より，$\tau(1)=n-1$である．$\tau(1)+n-1>n$であるから，事実18より$\tau(2)=\tau(1)+n-1+\delta_1-n=n-2+\delta_1$ であるが，もし$\delta_1=1$ならば$\tau(2)=n-1=\tau(1)$となりτは置換であることに反する．故に$\delta_1=0$である．同様に各$\ell=2,\ldots,n-1$ に対して，$\delta_1,\ldots,\delta_{\ell-1}=0$であり，$\tau(\ell)=n-\ell$であると仮定する．もし$\delta_\ell=1$ならば，$\tau(\ell)+a+\delta_\ell=n-\ell+n-1+1=n+(n-\ell)>n$であるから，事実18より$\tau(\ell+1)=\tau(\ell)+n-1+\delta_\ell-n=\tau(\ell)$となるが，これは$\tau$が置換であることに反する．故に$\delta_\ell=0$である．$\tau(\ell)=n-\ell>1$のとき，即ち，$\ell<n-1$のとき，$\tau(\ell)+a+\delta_\ell=n-\ell+n-1=n+(n-1-\ell)>n$であるから事実18より$\tau(\ell+1)=\tau(\ell)-1=n-(\ell+1)$である．$\tau(\ell)=n-\ell=1$ 即ち，$\ell=n-1$のとき，$\tau(\ell)+a+\delta_\ell=\tau(n-1)+(n-1)=1+(n-1)=n$であるから事実18より$\tau(n)=\tau(n-1)+a=n$である．□

事実 21. $0\leq a\leq n-1$とし，n次の置換τを$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型とする．このとき，次の(1)〜(4)が成立する．

(1) 付随するビット列が$\delta_1=\cdots=\delta_{n-1}=0$ならば，$\tau(n)=n$ 且つ aとnは互いに素[25]である．このとき，各$\ell\in[n]$で$\tau(\ell)\equiv\ell a \mod n$である．

(2) 付随するビット列が$\delta_1=\cdots=\delta_{n-1}=1$ならば，$\tau(n)=n-1$ 且つ $(a+1)$とnは互いに素である．このとき，各$\ell\in[n]$で$\tau(\ell)\equiv\ell(a+1)-1 \mod n$である．

(3) $\tau(n)=n$ならば，付随するビット列は$\delta_1=\cdots=\delta_{n-1}=0$である．

(4) $\tau(n)=n-1$ならば，付随するビット列は$\delta_1=\cdots=\delta_{n-1}=1$である．

証明. (1) $\delta_1=\cdots=\delta_{n-1}=0$より，$\tau(n)=\mathrm{Mod}_n((\sum_{k=1}^{n-1}\delta_k)-1)+1=\mathrm{Mod}_n(-1)+1=n-1+1=n$である．このとき，$\tau(\ell)\equiv\ell a \mod n$となるが，$\tau$は置換なので，$\ell a \mod n$ は各$\ell\in[n]$で相異なる．(特に$a\neq 0$である．) つまり，正の整数k with $\ell+k\leq n$で，各$\ell\in[n]$に対して，$\tau(\ell+k)-\tau(\ell)\equiv(\ell+k)a-\ell a\equiv ka\neq 0 \mod n$である．即ち，$ka\equiv 0 \mod n$ となる整数kは$1\leq k\leq n-1$では存在しない．一方，もし，aとnの最大公約数(a,n) (これをbとする) が1より大きいとすると，$a=ba'$, $n=bn'$ $(a',n'\in\mathbb{Z}_{\geq 0}, n'<n)$と書くとき，$n'a=n'ba'=na'\equiv 0 \mod n$ であるので，これは矛盾する．故に $(a,n)=1$, 即ち，aとnは互いに素である．

(2) $\tau(n)=\mathrm{Mod}_n((\sum_{k=1}^{n-1}\delta_k)-1)+1=\mathrm{Mod}_n((n-1)-1)+1=n-1$である．このとき，$\tau(\ell)\equiv\ell a+\ell-1\equiv\ell(a+1)-1 \mod n$であるが，$\tau$が置換であるので，$\ell(a+1) \mod n$は各$\ell\in[n]$で相異なる．(1)と同様の議論により，$(a+1)$と$n$は互いに素であることがわかる．

(3) $\tau(n)=n$ならば$\tau(n)=\mathrm{Mod}_n((\sum_{k=1}^{n-1}\delta_k)-1)+1$より$\mathrm{Mod}_n((\sum_{k=1}^{n-1}\delta_k)-1)=n-1$である．$0\leq\sum_{k=1}^{n-1}\delta_k\leq n-1$より$\sum_{k=1}^{n-1}\delta_k=0$であり，$0\leq\delta_\ell\leq 1$であるから$\delta_1=\cdots=\delta_{n-1}=0$でなければならない．

(4) $\tau(n)=n-1$ならば$\tau(n)=\mathrm{Mod}_n((\sum_{k=1}^{n-1}\delta_k)-1)+1$より$\sum_{k=1}^{n-1}\delta_k=n-1$であり，$0\leq\delta_\ell\leq 1$であるから$\delta_1=\cdots=\delta_{n-1}=1$でなければならない．□

注意 22. aとnが互いに素であっても，$\tau(n)=n$ではないa-pNAP型は存在する．例えば，$n=8$, $a=5$ で$(\delta_k)_{k=1}^{n-1}=(0,1,1,0,1,1,0)$ のとき$\mathrm{Mod}_8(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1)+1$は $\ell=1,\ldots,8$の順に$(5,2,8,6,3,1,7,4)$ である．即ち，置換$\tau=(52863174)$は$(5,(0,1,1,0,1,1,0))$-pNAP型，つまり$(a=5$と$n=8$は互いに素であり$)$ τは5-pNAP型で$\tau(8)=4$である．

注意 23. aとnは互いに素とする．$a'=a-1$のとき，nと$(a'+1)$が互いに素の場合の事実21の(2)の$(a',(1)_{k=1}^{n-1})$-pNAP型の置換をτとし，このτに(本文第4節の意味で)「定数1を加える変換」をした置換は，事実21の(1)の$(a,(0)_{k=1}^{n-1})$-pNAP型の置換である．例えば，$n=8$, $a=5$, $a'=4$として，$(4,(1)_{k=1}^{n-1})$-pNAP型の置換(41638527)に定数1を加える変換をした置換は，$(5,(0)_{k=1}^{n-1})$-pNAP型の置換(52741638)である．

$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型の$n$次の置換について，事実19, 事実20より$a=0$と$n-1$のときは，付属するビット列$(\delta_k)_{k=1}^{n-1}$はそれぞれの場合で一意であり，置換は確定する．従って，$a=0$と$a=n-1$の場合を除いた$a\in[n-2]$の場合を考察すればよいことになる．

次は一度しか引用されないのが，似たような議論は複数出てくるので補題とした．

補題 24. $a\in[n-2]$とし，τを$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型の$n$次の置換とする．もし$i\in[n-1]$で$\tau(i)=n$ならば，$\delta_i=1$である．

[25] $a=0$のとき，aとnは互いに素ではない．

証明. $1 \leq a+\delta_i$であるから$\tau(i)=n$より$\tau(i)+a+\delta_i > n$である．事実18より$\tau(i+1)=\tau(i)+a+\delta_i-n=a+\delta_i$であるが，$\tau(1)=a$であり，$\tau$は置換であるから$(\tau(i+1)\neq\tau(1)$より$)$ δ_iは0ではない．故に$\delta_i=1$である．□

注意 25. $\tau(i)=n$となるiが$i=n$のときは，事実21で既出である．

以下の補題はa-pNAP型であることは仮定していないことに注意する．

補題 26. nを2以上の自然数，aを$a\in[n-1]$なる整数とし，a'を$a'<a$を満たす正の無理数とする．ここで$\epsilon := a-a'$とし，$0<\epsilon<\frac{1}{2n}$であると仮定する．$(\delta_k)_{k=1}^{n-1}$を各kに対してδ_kは0又は1となる数列とする．このとき，各$i\in[n]$に対して次の(0),(1),(2)が成立する．

(0) $ia+\sum_{k=1}^{i-1}\delta_k$は正の整数である．特に$\{\frac{ia+\sum_{k=1}^{i-1}\delta_k}{n}\}=\frac{r}{n}$ となる整数rは$r=0$或いは$r\in[n-1]$を満たす．また，$ia'+\sum_{k=1}^{i-1}\delta_k$は正の無理数である．特に$\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}$と$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}$は正の無理数である．

(1) $\{\frac{ia+\sum_{k=1}^{i-1}\delta_k}{n}\}=0$のとき，$1-\epsilon\leq\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}\leq 1-\frac{\epsilon}{n}$である．特に$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}<1$である．

(2) $\{\frac{ia+\sum_{k=1}^{i-1}\delta_k}{n}\}=\frac{r}{n}$ となる整数rが$r\in[n-1]$のとき，$\frac{r}{n}-\epsilon\leq\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}\leq\frac{r}{n}-\frac{\epsilon}{n}$である．特に$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}<\frac{r}{n}$である．

証明. $a=a'+\epsilon$であるから$ia+\sum_{k=1}^{i-1}\delta_k=(ia'+\sum_{k=1}^{i-1}\delta_k)+i\epsilon$ である．以下，$\frac{\epsilon}{n}\leq\frac{i\epsilon}{n}\leq\epsilon$に注意する．(0)は自明である．

(1) $\{\frac{ia+\sum_{k=1}^{i-1}\delta_k}{n}\}=0$ならば，$ia+\sum_{k=1}^{i-1}\delta_k=qn$なる正の整数$q$が存在する．このとき，$ia'+\sum_{k=1}^{i-1}\delta_k=qn-i\epsilon=(q-1)n+n-i\epsilon$であるから，$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}=\{\frac{n-i\epsilon}{n}\}=\{1-\frac{i\epsilon}{n}\}=1-\frac{i\epsilon}{n}$ である．故に主張が成立する．

(2) $\{\frac{ia+\sum_{k=1}^{i-1}\delta_k}{n}\}=\frac{r}{n}$のとき，$ia+\sum_{k=1}^{i-1}\delta_k=qn+r$なる正の整数$q$が存在する．このとき，$ia'+\sum_{k=1}^{i-1}\delta_k=qn+r-i\epsilon$であり，$i\epsilon<n\times\frac{1}{2n}=\frac{1}{2}$であるから，$(r-i\epsilon>1-\frac{1}{2}=\frac{1}{2}$であり$)$ $\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}=\{\frac{r-i\epsilon}{n}\}=\frac{r}{n}-\frac{i\epsilon}{n}$である．故に主張が成立する．□

次の主張は本文第4節の命題2に対応する[26]ものである．

補題 27. nを2以上の自然数，aを$a\in[n-1]$となる整数とし，τをn次の$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型とする．$a'$を$0<a-a'<\frac{1}{2n}$を満たす無理数として固定する．このとき，各$\ell\in[n]$に対して次が成立する．

$$\tau(\ell)=|\{j\in[n]\ ;\ \{\frac{ja'+\sum_{k=1}^{j-1}\delta_k}{n}\}\leq\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}\}|$$

証明. $\epsilon := a-a'$とする．$\tau(\ell)=n$とそれ以外で場合わけをする．

$\tau(\ell)=n$の場合：a-pNAP型の定義の$\tau(\ell)=\mathrm{Mod}_n(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-1)+1$ より$\mathrm{Mod}_n(\ell a+\sum_{k=1}^{\ell-1}\delta_k)=0$なので$\{\frac{\ell a+\sum_{k=1}^{\ell-1}\delta_k}{n}\}=0$ である．故に補題26の(1)より$1-\epsilon\leq\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}<1$である．$i\neq\ell$の各$i\in[n]$では$\tau(i)\neq n$であるから，$i$に依存した整数$q,r$ with $1\leq r\leq n-1$ で$ia+\sum_{k=1}^{i-1}\delta_k=qn+r$ となるものが存在する．補題26の(2)より$\frac{r}{n}-\epsilon\leq\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}<\frac{r}{n}$ であるから，特に$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}$は$1-\epsilon$より小さい．故に$|\{j\in[n]\ ;\ \{\frac{ja'+\sum_{k=1}^{j-1}\delta_k}{n}\}\leq\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}\}|=n$であり，主張が成立する．

$\tau(\ell)=r$ with $r\in[n-1]$の場合：$\mathrm{Mod}_n(\ell a+\sum_{k=1}^{\ell-1}\delta_k)=r$である．故に補題26の(2)より$\frac{r}{n}-\epsilon\leq\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}<\frac{r}{n}$である．

以下，各$i\in[n]$に対して，$r_i := \tau(i)$とおく．$r_i=n$のときは$\mathrm{Mod}_n(ia+\sum_{k=1}^{i-1}\delta_k)=0$であり，$r_i\neq n$のときは$\mathrm{Mod}_n(ia+\sum_{k=1}^{i-1}\delta_k)=r_i$である．(さらに，$i=\ell$のときは$\tau(\ell)=r$である．)

さて，$r_i<r$なるiに対して，$r_i+1\leq r$であり，また補題26の(2)より$\frac{r_i}{n}-\epsilon\leq\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}<\frac{r_i}{n}$ であり，さらに$(\frac{r}{n}-\epsilon)-\frac{r_i}{n}=\frac{r-r_i}{n}-\epsilon>\frac{1}{n}-\epsilon>0$ であるから，$\frac{r_i}{n}$は$\frac{r}{n}-\epsilon$より小さい．故に，$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}$は$\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}$より小さい．

[26] $1\leq a\leq n-2$として，補題27のa,a'をそれぞれ命題2で$\tau(1),\theta$とすればよい．

逆に，$r < r_i$なるiに対して，先ず，$r_i = n$の場合を考える．補題26の(1)より$1-\epsilon \le \{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\} < 1$であり，$1-\frac{r}{n} = \frac{n-r}{n} \ge \frac{1}{n} > \epsilon$より$1-\epsilon > \frac{r}{n}$であるから，$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}$は$\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}$より大きい．

次に，$r_i \neq n$の場合を考える．$r_i \ge r+1$であるから$(\frac{r_i}{n}-\epsilon)-\frac{r}{n} = \frac{r_i-r}{n}-\epsilon > \frac{1}{n}-\epsilon > 0$より$\frac{r_i}{n}-\epsilon$は$\frac{r}{n}$より大きい．補題26の(2)より$\frac{r_i}{n}-\epsilon \le \{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\} < \frac{r_i}{n}$であるから，$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}$は$\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}$より大きい．

以上をまとめると，$i \neq \ell$で$r_i < r$となるiに対しては$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}$は$\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}$より小さく，$r_i > r$となる$i$に対しては$\{\frac{ia'+\sum_{k=1}^{i-1}\delta_k}{n}\}$は$\{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}$より大きい．$\tau$は置換であるから，$r_1, r_2, \ldots, r_n$は1から$n$の並び替えであり，重複はない．故に，$r_1, \ldots, r_n$のなかで，$r\ (= r_\ell = \tau(\ell))$以下のものは($r_\ell$を含めて)丁度$r$個ある．従って，$|\{j \in [n]\ ;\ \{\frac{ja'+\sum_{k=1}^{j-1}\delta_k}{n}\} \le \{\frac{\ell a'+\sum_{k=1}^{\ell-1}\delta_k}{n}\}\}| = r = \tau(\ell)$であり，主張が成立する．□

次の主張が本文の定理3に対応するものである．これよりn次のa-pNAP型の置換τはaと$\tau(n)$で決定することがわかる．

定理 28. nを2以上の自然数とし，aを$0 \le a \le n-1$を満たす整数とする．n次の置換τが$(a, (\delta_k)_{k=1}^{n-1})$-pNAP型ならば，各$\ell \in [n-1]$に対して

$$\tau(\ell+1) - \tau(\ell) \equiv a + \mathbb{1}[\mathrm{Mod}_n(\tau(\ell)) < \mathrm{Mod}_n(\tau(n))] \qquad \mod n \tag{9}$$

が成り立つ．特に

$$\delta_\ell = \mathbb{1}[\mathrm{Mod}_n(\tau(\ell)) < \mathrm{Mod}_n(\tau(n))]$$

である．

証明. 先ず，$n \ge 3$の場合を考える．$a = 0$と$a = n-1$の場合は後で考えることにし，先に$a \in [n-2]$の場合を考える．

補題27の記法の下$(\epsilon := a - a' \text{ with } 0 < \epsilon < \frac{1}{2n})$で，写像$g : [n] \to \mathbb{R}$を，$\ell \in [n]$に対して

$$g(\ell) := \frac{\ell a' + \sum_{k=1}^{\ell-1}\delta_k}{n}$$

と定義し，以下，$g(0) = 0$とする．さて，$i, j \in [n] \text{ with } i \neq j$に対して，$a'$が無理数なので

$$g(i) - g(j) = \frac{ia' + \sum_{k=1}^{i-1}\delta_k}{n} - \frac{ja' + \sum_{k=1}^{j-1}\delta_k}{n} = \frac{(i-j)a' + \left(\sum_{k=1}^{i-1}\delta_k\right) - \left(\sum_{k=1}^{j-1}\delta_k\right)}{n}$$

は0ではない．即ち，写像$g : [n] \to \mathbb{R}$は単射である．

さらに，この$g : [n] \to \mathbb{R}$に対して事実9の写像$\mathfrak{T}_g : [n] \to [n]$を考える．補題27より$(a, (\delta_k)_{k=1}^{n-1})$-pNAP型の置換$\tau$と$\mathfrak{T}_g$は等しい．即ち，$\mathfrak{T}_g$は置換(特に$[n]$から$[n]$への単射)であるから，事実9より$g$は$n$次のfp単射であり，$\mathfrak{T}_g\ (= \tau)$は$g$によるfp置換(定義13)である．

a-pNAP型の定義(定義17)より各$\ell \in [n]$に対して，$\exists\, m_\ell \in \mathbb{Z}$ s.t.

$$\tau(\ell) - 1 = \left(\ell a + \sum_{k=1}^{\ell-1}\delta_k\right) - 1 - m_\ell n \tag{10}$$

であるから，$\epsilon := a - a' \text{ with } 0 < \epsilon < \frac{1}{2n}$より

$$\tau(\ell) + m_\ell n = \left(\ell a' + \sum_{k=1}^{\ell-1}\delta_k\right) + \ell\epsilon = ng(\ell) + \ell\epsilon$$

即ち，各$\ell \in [n]$に対して

$$g(\ell) = \frac{\tau(\ell) - \ell\epsilon}{n} + m_\ell$$

である．よって$i, j \in [n]$に対しては

$$g(i) - g(j) = \left(\frac{\tau(i) - i\epsilon}{n} + m_i\right) - \left(\frac{\tau(j) - j\epsilon}{n} + m_j\right) = \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} + m_i - m_j \tag{11}$$

$g(0)=0$なので，繰り返しになるが

$$g(i)-g(0)=\frac{\tau(i)-i\epsilon}{n}+m_i \tag{12}$$

である．式(10)より

$$\tau(\ell+1)-\tau(\ell)=\left(\left((\ell+1)a+\sum_{k=1}^{\ell}\delta_k\right)-m_{\ell+1}n\right)-\left(\left(\ell a+\sum_{k=1}^{\ell-1}\delta_k\right)-m_\ell n\right)=a+\delta_\ell-(m_{\ell+1}-m_\ell)n$$

であるから，$\ell\in[n-1]$に対しては

$$\begin{aligned}g(\ell+1)=\frac{\tau(\ell+1)-(\ell+1)\epsilon}{n}+m_{\ell+1}&=\frac{\tau(\ell)+a+\delta_\ell-(m_{\ell+1}-m_\ell)n-(\ell+1)\epsilon}{n}+m_{\ell+1}\\&=\frac{\tau(\ell)+(a'+\epsilon)+\delta_\ell-(\ell+1)\epsilon}{n}+m_\ell=\frac{\tau(\ell)+a'+\delta_\ell-\ell\epsilon}{n}+m_\ell\end{aligned}$$

故に$i,j\in[n-1]$に対して

$$\begin{aligned}g(i+1)-g(j+1)&=\left(\frac{\tau(i)+a'+\delta_i-i\epsilon}{n}+m_i\right)-\left(\frac{\tau(j)+a'+\delta_j-j\epsilon}{n}+m_j\right)\\&=\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}+\frac{\delta_i-\delta_j}{n}+m_i-m_j\end{aligned} \tag{13}$$

また，$g(1)=\frac{a'}{n}$であるから

$$g(i+1)-g(1)=\left(\frac{\tau(i)+a'+\delta_i-i\epsilon}{n}+m_i\right)-\frac{a'}{n}=\frac{\tau(i)-i\epsilon}{n}+\frac{\delta_i}{n}+m_i \tag{14}$$

一般に，実数αと整数mに対して，$\alpha+m=\lfloor\alpha\rfloor+m+\{\alpha\}$, $\lfloor\alpha\rfloor+m\in\mathbb{Z}$, $0\le\{\alpha\}<1$であるから([3, 付録A 事実2]より) $\lfloor\alpha+m\rfloor=\lfloor\alpha\rfloor+m$である．

故に式(11), (13)より$m_i-m_j\in\mathbb{Z}$であるから命題14の$D(i,j)$は

$$D(i,j):=\lfloor g(i+1)-g(j+1)\rfloor-\lfloor g(i)-g(j)\rfloor=\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}+\frac{\delta_i-\delta_j}{n}\rfloor-\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}\rfloor \tag{15}$$

となる．$D(i,i)=0$に注意しておく．また，式(12), (14)より

$$D(i,0)=\lfloor g(i+1)-g(1)\rfloor-\lfloor g(i)-g(0)\rfloor=\lfloor\frac{\tau(i)-i\epsilon}{n}+\frac{\delta_i}{n}\rfloor-\lfloor\frac{\tau(i)-i\epsilon}{n}\rfloor$$

である．

$\sum_{k=1}^{n-1}D(k,0)$の計算：

$i\in[n-1]$とする．$1\le\tau(i)\le n-1$のとき，$1\le\tau(i)+\delta_i\le n$である．故に$0<i\epsilon\le i\cdot\frac{1}{2n}\le\frac{1}{2}$より$0<\tau(i)+\delta_i-i\epsilon<n$なので$\lfloor\frac{\tau(i)-i\epsilon}{n}+\frac{\delta_i}{n}\rfloor=\lfloor\frac{\tau(i)+\delta_i-i\epsilon}{n}\rfloor=0$であり，同様に$0<\tau(i)-i\epsilon\le n-1$より$\lfloor\frac{\tau(i)-i\epsilon}{n}\rfloor=0$である．故に$D(i,0)=0$である．

$\tau(i)=n$のとき，$i\in[n-1]$であるから，補題24より$\delta_i=1$であり，$n<n+1-i\epsilon<n+1$より

$$D(i,0)=\lfloor\frac{n-i\epsilon}{n}+\frac{1}{n}\rfloor-\lfloor\frac{n-i\epsilon}{n}\rfloor=1-0=1$$

である．従って，$i\in[n-1]$に対しては

$$D(i,0)=\begin{cases}1 & \text{if } \tau(i)=n\\ 0 & \text{if } \tau(i)\neq n\end{cases} \tag{16}$$

である．$\tau(i)=n$となる$i\in[n-1]$の個数は(τは置換なので)

$$\begin{cases}\tau(n)=n\text{のとき，}\tau(i)=n\text{となる}i\in[n-1]\text{は存在しない．}\\ \tau(n)\neq n\text{のとき，}\tau(i)=n\text{となる}i\in[n-1]\text{は1つだけ存在する．}\end{cases}$$

従って，式(16)から

$$\sum_{k=1}^{n-1}D(k,0)=|\{k\in[n-1]\ ;\ \tau(k)=n\}|=\begin{cases}0 & \text{if }\ \tau(n)=n\\ 1 & \text{if }\ \tau(n)\neq n\end{cases}\tag{17}$$

ちなみに，$\tau(n)=n$となる$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型の置換は，事実21の(1)と(3)より決定している．

$\sum_{k=1}^{n-1}D(\ell,k)$の計算：
$D(\ell,\ell)=0$に注意しておく．さて，$i,j\in[n-1]$ with $i\neq j$に対して，$D(i,j)$の値を調べよう．$\delta_1,\ldots,\delta_{n-1}$の値は0又は1であるから，

$$\delta_i-\delta_j=\begin{cases}1 & \text{if }\ (\delta_i,\delta_j)=(1,0)\\ -1 & \text{if }\ (\delta_i,\delta_j)=(0,1)\\ 0 & \text{o.w.}\end{cases}$$

τは置換であるから$|\tau(i)-\tau(j)|\geq 1$であり，また，$-(n-1)=1-n\leq\tau(i)-\tau(j)\leq n-1$である．
以下，次の(ア)~(オ)で場合わけをする．
(ア)　$\tau(i)-\tau(j)=-(n-1)$の場合．これは$(\tau(i),\tau(j))=(1,n)$のときだけである．
(イ)　$\tau(i)-\tau(j)=n-1$の場合．これは$(\tau(i),\tau(j))=(n,1)$のときだけである．
(ウ)　$\tau(i)-\tau(j)=-1$の場合．
(エ)　$\tau(i)-\tau(j)=1$の場合．
(オ)　$2\leq|\tau(i)-\tau(j)|\leq n-2$の場合．
最初に(オ)の場合を考える．$|(i-j)\epsilon|\leq|i-j|\cdot\frac{1}{2n}\leq\frac{1}{2}$であるから，

$$\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}\rfloor\rfloor=\begin{cases}-1 & \text{if }\ -(n-2)\leq\tau(i)-\tau(j)\leq-2\\ 0 & \text{if }\ 2\leq\tau(i)-\tau(j)\leq n-2\end{cases}$$

$-(n-2)\leq\tau(i)-\tau(j)\leq-2$のとき，$-1\leq\delta_i-\delta_j\leq 1$であるから，$-(n-1)\leq\tau(i)-\tau(j)-1\leq\tau(i)-\tau(j)+(\delta_i-\delta_j)\leq\tau(i)-\tau(j)+1\leq-1$ である．故に$-n<\tau(i)-\tau(j)+\delta_i-\delta_j-(i-j)\epsilon<0$ であり，

$$\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}+\frac{\delta_i-\delta_j}{n}\rfloor=-1$$

である．同様に，$2\leq\tau(i)-\tau(j)\leq n-2$のとき，$1\leq\tau(i)-\tau(j)-1\leq\tau(i)-\tau(j)+(\delta_i-\delta_j)\leq\tau(i)-\tau(j)+1\leq n-1$である．故に$0<\tau(i)-\tau(j)+\delta_i-\delta_j-(i-j)\epsilon<n$であり，

$$\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}+\frac{\delta_i-\delta_j}{n}\rfloor=0$$

である．従って式(15)より

$$D(i,j)=\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}+\frac{\delta_i-\delta_j}{n}\rfloor-\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}\rfloor=0$$

である．即ち，(オ)の場合は$D(i,j)=0$である．
次に(ア)の場合を考える．$-n<-n+1-(i-j)\epsilon<-n+2$より

$$\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}\rfloor=\lfloor\frac{1-n-(i-j)\epsilon}{n}\rfloor=-1$$

であり，

$$\lfloor\frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n}+\frac{\delta_i-\delta_j}{n}\rfloor=\lfloor\frac{1-n-(i-j)\epsilon}{n}+\frac{\delta_i-\delta_j}{n}\rfloor$$

$$= \begin{cases} \lfloor \dfrac{1-n-(i-j)\epsilon}{n} + \dfrac{1}{n} \rfloor = -1 & \text{if } (\delta_i, \delta_j) = (1,0) \\ \lfloor \dfrac{1-n-(i-j)\epsilon}{n} + \dfrac{-1}{n} \rfloor = \lfloor -1 + \dfrac{-(i-j)\epsilon}{n} \rfloor = -2 & \text{if } (\delta_i, \delta_j) = (0,1) \text{ 且つ } i > j \\ \lfloor \dfrac{1-n-(i-j)\epsilon}{n} + \dfrac{-1}{n} \rfloor = \lfloor -1 + \dfrac{-(i-j)\epsilon}{n} \rfloor = -1 & \text{if } (\delta_i, \delta_j) = (0,1) \text{ 且つ } i < j \\ \lfloor \dfrac{1-n-(i-j)\epsilon}{n} + \dfrac{0}{n} \rfloor = -1 & \text{o.w.} \end{cases}$$

で[27]ある．従って式(15)より

$$D(i,j) = \lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor - \lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} \rfloor = \begin{cases} -1 & \text{if } (\delta_i, \delta_j) = (0,1) \text{ 且つ } i > j \\ 0 & \text{o.w.} \end{cases}$$

となるが，$(\delta_i, \delta_j) = (0,1)$ 且つ $i > j$はあり得ない．なぜならば，もしそうだとすると$(i, j \in [n-1]$に注意して$)$ $(\tau(i), \tau(j)) = (1, n)$なので，事実18より$\tau(i+1) \equiv \tau(i) + a + \delta_i \equiv a+1 \mod n$であり，$\tau(j+1) \equiv \tau(j) + a + \delta_j \equiv a+1 \mod n$なので$\tau(i+1) \equiv \tau(j+1) \mod n$となるが，これは$\tau$が$n$次の置換であることに矛盾する．よって，$(\delta_i, \delta_j) = (0,1)$ 且つ $i > j$の場合はない．以上により，(ア)の場合は$D(i,j) = 0$である．

次に(イ)の場合を考える．$n-2 < n-1-(i-j)\epsilon < n$より

$$\lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} \rfloor = \lfloor \frac{n-1-(i-j)\epsilon}{n} \rfloor = 0$$

であり，

$$\lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor = \lfloor \frac{n-1-(i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor$$

$$= \begin{cases} \lfloor \dfrac{n-1-(i-j)\epsilon}{n} + \dfrac{1}{n} \rfloor = \lfloor 1 + \dfrac{-(i-j)\epsilon}{n} \rfloor = 0 & \text{if } (\delta_i, \delta_j) = (1,0) \text{ 且つ } i > j \\ \lfloor \dfrac{n-1-(i-j)\epsilon}{n} + \dfrac{1}{n} \rfloor = \lfloor 1 + \dfrac{-(i-j)\epsilon}{n} \rfloor = 1 & \text{if } (\delta_i, \delta_j) = (1,0) \text{ 且つ } i < j \\ \lfloor \dfrac{n-1-(i-j)\epsilon}{n} + \dfrac{-1}{n} \rfloor = 0 & \text{if } (\delta_i, \delta_j) = (0,1) \\ \lfloor \dfrac{n-1-(i-j)\epsilon}{n} + \dfrac{0}{n} \rfloor = 0 & \text{o.w.} \end{cases}$$

である．式(15)より

$$D(i,j) = \lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor - \lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} \rfloor = \begin{cases} 1 & \text{if } (\delta_i, \delta_j) = (1,0) \text{ 且つ } i < j \\ 0 & \text{o.w.} \end{cases}$$

となるが，この場合も$(\delta_i, \delta_j) = (1,0)$ 且つ $i < j$はあり得ない．なぜならば，もしそうだとすると$(\tau(i), \tau(j)) = (n, 1)$なので，事実18より$\tau(i+1) \equiv \tau(i) + a + \delta_i \equiv n + a + 1 \equiv a+1 \mod n$であり，$\tau(j+1) \equiv \tau(j) + a + \delta_j \equiv 1 + a \mod n$なので$\tau(i+1) \equiv \tau(j+1) \mod n$となるが，これは$\tau$が$n$次の置換であることに矛盾する．以上により，(イ)の場合も$D(i,j) = 0$である．

(ウ)の場合を考える．$\tau(i) - \tau(j) = -1$であるから，$-2 < -1-(i-j)\epsilon < 0$より

$$\lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} \rfloor = \lfloor \frac{-1-(i-j)\epsilon}{n} \rfloor = -1$$

であり，

$$\lfloor \frac{\tau(i) - \tau(j) - (i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor = \lfloor \frac{-1-(i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor$$

[27] $n \geq 3$であることに注意する．

$$= \begin{cases} \lfloor \dfrac{-1-(i-j)\epsilon}{n} + \dfrac{1}{n} \rfloor = \lfloor \dfrac{-(i-j)\epsilon}{n} \rfloor = -1 & \text{if } (\delta_i, \delta_j) = (1,0) \text{ 且つ } i > j \\ \lfloor \dfrac{-1-(i-j)\epsilon}{n} + \dfrac{1}{n} \rfloor = \lfloor \dfrac{-(i-j)\epsilon}{n} \rfloor = 0 & \text{if } (\delta_i, \delta_j) = (1,0) \text{ 且つ } i < j \\ \lfloor \dfrac{-1-(i-j)\epsilon}{n} + \dfrac{-1}{n} \rfloor = -1 & \text{if } (\delta_i, \delta_j) = (0,1) \\ \lfloor \dfrac{-1-(i-j)\epsilon}{n} + \dfrac{0}{n} \rfloor = -1 & \text{o.w.} \end{cases}$$

である．式(15)より

$$D(i,j) = \lfloor \frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor - \lfloor \frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n} \rfloor = \begin{cases} 1 & \text{if } (\delta_i, \delta_j) = (1,0) \text{ 且つ } i < j \\ 0 & \text{o.w.} \end{cases}$$

となるが，この場合も$(\delta_i, \delta_j) = (1,0)$ 且つ $i < j$ はあり得ない．なぜならば，もしそうだとすると$\tau(i) - \tau(j) = -1$ 即ち，$\tau(j) = \tau(i) + 1$であるが，事実18より$\tau(i+1) \equiv \tau(i) + a + \delta_i \equiv \tau(i) + a + 1 \mod n$であり，$\tau(j+1) \equiv \tau(j) + a + \delta_j \equiv \tau(i) + 1 + a \mod n$なので$\tau(i+1) \equiv \tau(j+1) \mod n$となるが，これは$\tau$が$n$次の置換であることに矛盾する．以上により，(ウ)の場合も$D(i,j) = 0$である．

最後に(エ)の場合を考える．$\tau(i) - \tau(j) = 1$であるから，$0 < 1 - (i-j)\epsilon < 2$より

$$\lfloor \frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n} \rfloor = \lfloor \frac{1-(i-j)\epsilon}{n} \rfloor = 0$$

であり，

$$\lfloor \frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor = \lfloor \frac{1-(i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor$$

$$= \begin{cases} \lfloor \dfrac{1-(i-j)\epsilon}{n} + \dfrac{-1}{n} \rfloor = \lfloor \dfrac{-(i-j)\epsilon}{n} \rfloor = -1 & \text{if } (\delta_i, \delta_j) = (0,1) \text{ 且つ } i > j \\ \lfloor \dfrac{1-(i-j)\epsilon}{n} + \dfrac{-1}{n} \rfloor = \lfloor \dfrac{-(i-j)\epsilon}{n} \rfloor = 0 & \text{if } (\delta_i, \delta_j) = (0,1) \text{ 且つ } i < j \\ \lfloor \dfrac{1-(i-j)\epsilon}{n} + \dfrac{1}{n} \rfloor = 0 & \text{if } (\delta_i, \delta_j) = (1,0) \\ \lfloor \dfrac{1-(i-j)\epsilon}{n} + \dfrac{0}{n} \rfloor = 0 & \text{o.w.} \end{cases}$$

である．式(15)より

$$D(i,j) = \lfloor \frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n} + \frac{\delta_i - \delta_j}{n} \rfloor - \lfloor \frac{\tau(i)-\tau(j)-(i-j)\epsilon}{n} \rfloor = \begin{cases} -1 & \text{if } (\delta_i, \delta_j) = (0,1) \text{ 且つ } i > j \\ 0 & \text{o.w.} \end{cases}$$

となるが，この場合も$(\delta_i, \delta_j) = (0,1)$ 且つ $i > j$ はあり得ない．なぜならば，もしそうだとすると$\tau(i) - \tau(j) = 1$ 即ち，$\tau(j) = \tau(i) - 1$であるが，事実18より$\tau(i+1) \equiv \tau(i) + a + \delta_i \equiv \tau(i) + a \mod n$であり，$\tau(j+1) \equiv \tau(j) + a + \delta_j \equiv \tau(i) - 1 + a + 1 = \tau(i) + a \mod n$なので$\tau(i+1) \equiv \tau(j+1) \mod n$となるが，これは$\tau$が$n$次の置換であることに矛盾する．以上により，(エ)の場合も$D(i,j) = 0$である．

以上より，(ア)〜(オ)のすべての場合で$D(i,j) = 0$であるから，

$$\sum_{k=1}^{n-1} D(\ell, k) = 0$$

であることがわかる．式(17)及び(iをℓに置き換えた)式(16)より

$$D(\ell, 0) + \sum_{k=1}^{n-1} D(k, 0) + \sum_{k=1}^{n-1} D(\ell, k) = \mathbb{1}[\tau(\ell) = n] + \mathbb{1}[\tau(n) \neq n]$$

従って，$\mathfrak{T}_g = \tau$であるから，命題14より

$$\tau(1) + \tau(\ell) - \tau(\ell+1) + n\left(\lfloor g(1) \rfloor + \lfloor g(\ell) \rfloor - \lfloor g(\ell+1) \rfloor\right) + \mathbb{1}[\tau(\ell) = n] + \mathbb{1}[\tau(n) \neq n] = \mathbb{1}[\tau(\ell) \geq \tau(n)] \qquad (18)$$

であることがわかる．

さて，

$$\mathbb{1}[\tau(\ell)=n]+\mathbb{1}[\tau(n)\neq n]-\mathbb{1}[\tau(\ell)\geq\tau(n)]$$

を計算しよう．$\ell\in[n-1]$のとき，(τは置換なので)$\tau(\ell)=n$と$\tau(n)=n$は両立しない．即ち，$\tau(\ell)=n$ならば$\tau(n)\neq n$であり，$\tau(n)=n$ならば$\tau(\ell)\neq n$である等に注意すると

$$\mathbb{1}[\tau(\ell)=n]+\mathbb{1}[\tau(n)\neq n]=\begin{cases}2 & \text{if } \tau(\ell)=n \text{ 且つ } \tau(n)\neq n\\ 1 & \text{if } \tau(\ell)=n \text{ 且つ } \tau(n)=n\\ 1 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)\neq n\\ 0 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)=n\end{cases}=\begin{cases}2 & \text{if } \tau(\ell)=n \text{ 且つ } \tau(n)\neq n\\ 1 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)\neq n\\ 0 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)=n\end{cases}$$

$$=\begin{cases}2 & \text{if } \tau(\ell)=n\\ 1 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)\neq n\\ 0 & \text{if } \tau(n)=n\end{cases}$$

であることがわかる．ここで$\tau(\ell)=n$のときは$\tau(\ell)>\tau(n)$であり，$\tau(n)=n$のときは$\tau(\ell)<\tau(n)$であるから，

$$\mathbb{1}[\tau(\ell)=n]+\mathbb{1}[\tau(n)\neq n]-\mathbb{1}[\tau(\ell)\geq\tau(n)]=\begin{cases}2 & \text{if } \tau(\ell)=n\\ 1 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)\neq n\\ 0 & \text{if } \tau(n)=n\end{cases}$$

$$-\begin{cases}1 & \text{if } \tau(\ell)\geq\tau(n)\\ 0 & \text{if } \tau(\ell)<\tau(n)\end{cases}$$

$$=\begin{cases}1 & \text{if } \tau(\ell)=n\\ 0 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)\neq n \text{ 且つ } \tau(\ell)\geq\tau(n)\\ 1 & \text{if } \tau(\ell)\neq n \text{ 且つ } \tau(n)\neq n \text{ 且つ } \tau(\ell)<\tau(n)\\ 0 & \text{if } \tau(n)=n\end{cases}=\begin{cases}1 & \text{if } \tau(\ell)=n\\ 0 & \text{if } n>\tau(\ell)\geq\tau(n)\\ 1 & \text{if } \tau(\ell)<\tau(n)<n\\ 0 & \text{if } \tau(n)=n\end{cases}$$

$\ell\in[n-1]$に注意すると，「$\mathrm{Mod}_n(\tau(\ell))\geq\mathrm{Mod}_n(\tau(n))$」と同値な条件は，「$\tau(n)=n$」或いは「$\tau(n)\leq\tau(\ell)<n$」である．同様に，「$\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))$」と同値な条件は，「$\tau(\ell)=n$」或いは「$\tau(\ell)<\tau(n)<n$」である．従って

$$\mathbb{1}[\tau(\ell)=n]+\mathbb{1}[\tau(n)\neq n]-\mathbb{1}[\tau(\ell)\geq\tau(n)]=\mathbb{1}[\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))]$$

よって式(18)より

$$\tau(1)+\tau(\ell)-\tau(\ell+1)+n\left(\lfloor g(1)\rfloor+\lfloor g(\ell)\rfloor-\lfloor g(\ell+1)\rfloor\right)=-\mathbb{1}[\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))]$$

$\tau(1)=a$であるから，以上により，式(9)が得られる．このとき，事実18より$\delta_\ell=\mathbb{1}[\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))]$であることがわかる．

$a=0$のときは，事実19より，$(\delta_k)_{k=1}^{n-1}=(1)_{k=1}^{n-1}$であり，且つ，$\tau(n)=n-1$であるが，このとき$(\mathrm{Mod}_n(\tau(i))$の最大値は$n-1$だから)$\ell\in[n-1]$に対して$\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))$が成立するので，$a=0$のときも$\delta_\ell=\mathbb{1}[\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))]=1$が成立し，式(9)も成立することがわかる．

$a=n-1$のときは，事実20より$(\delta_k)_{k=1}^{n-1}=(0)_{k=1}^{n-1}$であり，且つ，$\tau(n)=n$であるが，このとき$\ell\in[n-1]$に対して$\mathrm{Mod}_n(\tau(\ell))>\mathrm{Mod}_n(\tau(n))$が成立するので，$a=n-1$のときも$\delta_\ell=\mathbb{1}[\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))]=0$が成立し，式(9)も成立することがわかる．

最後に$n=2$の場合を考える．置換は$\tau=(12)$又は$\tau=(21)$の二つしかない．$\tau=(12)$のとき，このτは$(1,(0)_{k=1}^{1})$-pNAP型で式(9)を満たし，定理の主張が成立することがわかる．同様に$\tau=(21)$のとき，このτは$(0,(1)_{k=1}^{1})$-pNAP型で式(9)を満たし，定理の主張が成立することがわかる．□

定理28より，n次の置換τが$(a,(\delta_k)_{k=1}^{n-1})$-pNAP型のとき，$\tau$は，($a$と)$\tau(n)$の値で決定する．$\tau(1)=\mathrm{Mod}_n(a-1)+1$であり，このとき$\tau(n)$は($\tau(1)$以外の)高々$(n-1)$個の値しか取り得ない．また，事実19と事実20より$a=0$と$a=n-1$のときはa-pNAP型の置換はそれぞれ一つだけである．よって，n次のa-pNAP型の総数は高々$1+1+(n-2)(n-1)=n^2-3n+4$個である．pNAP型はa-pNAP型の置換を「定数を加える変換」をしたも

ので尽きる[28]ので，結局の次の主張が成立する．これは本文の系4を僅かに精密化したものである．

系 29. n次のpNAP型の置換は高々(n^3-3n^2+4n)個である．

式(9)のτを「1を加える変換」をした置換をτ'とする(つまり，$\tau'(\ell)\equiv\tau(\ell)+1 \mod n$)．このとき，「$\tau(\ell)\neq n$ 且つ $\tau(n)\neq n$」の場合$(\Leftrightarrow \tau'(\ell)\neq 1$ 且つ $\tau'(n)\neq 1)$は$\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))$ と$\tau(\ell)<\tau(n)$ は同値である．さらにこのとき，$\tau(\ell)<\tau(n)$と$\tau'(\ell)<\tau'(n)$は同値である．$\tau(\ell)=n$の場合は$\tau'(\ell)=1$であるから，$\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))$と$\tau'(\ell)<\tau'(n)$の両方ともが成り立つ．$\tau(n)=n$の場合は$\tau'(n)=1$であるから，$\mathrm{Mod}_n(\tau(\ell))<\mathrm{Mod}_n(\tau(n))$と$\tau'(\ell)<\tau'(n)$の両方ともが成り立たない．即ち，式(9)を$\tau'$で書けば

$$\tau'(\ell+1)-\tau'(\ell)\equiv a+\mathbb{1}[\tau'(\ell)<\tau'(n)] \mod n$$

となる．

$$-1+\mathbb{1}[\tau'(\ell)<\tau'(n)]=-(1-\mathbb{1}[\tau'(\ell)<\tau'(n)])=-\mathbb{1}[\tau'(\ell)\geq\tau'(n)]$$

であるから，$\tau'(1)\equiv\tau(1)+1\equiv a+1 \mod n$より

$$\tau'(\ell+1)-\tau'(\ell)\equiv\tau'(1)-\mathbb{1}[\tau'(\ell)\geq\tau'(n)] \mod n$$

である．即ち，本文の系5が言える．特に次が言える．

注意 30. 定理28の式(9)と[3, 系1の漸化式]のnで法をとった合同式は，定数を加える変換の違いを無視すれば，同一のものである．

付録B

本付録Bでは，本文第5節で述べた定理3の漸化式に関するいくつかの性質についての詳細を記す．以下，第5節で用いた記号や記法をそのまま用いる．

命題 31. nを3以上の自然数とする．本文第5節の記法の下，「Not(A1) 且つ P 且つ N」なる(a,b)と「Not(A1) 且つ P 且つ Not(N)」なる(a,b)に一対一対応がある．特に，「Not(A1) 且つ P 且つ N」なる(a,b)の個数と「Not(A1) 且つ P 且つ Not(N)」なる(a,b)の個数は等しい．

証明. 条件Nを満たすならば$(a,b)=(t_{a,b}(1),t_{a,b}(n))$ であるから，異なる$(a,b),(a',b')$が同一の写像$t_{a,b}=t_{a',b'}$になることはない．一方で，条件Nを満たしていない(a,b)についてはその限りではない．実際のところ，Not(A1) 且つ P 且つ N を満たす(a,b)に対して，「bをひとつ増した」$(a,\overline{\mathrm{Mod}}_n(b+1))$は同一の写像$t_{a,b}=t_{a,\overline{\mathrm{Mod}}_n(b+1)}$を生じることを見よう．以下，$b'=\overline{\mathrm{Mod}}_n(b+1)$とする．先ず，$b=t_{a,b}(n)$が$n-1$未満の場合を考える．このときは$b'=b+1$である．基本pNAP型の置換$t_{a,b}$に付随するビット列を$\vec{\delta}=(\delta_\ell)$とすると，$\delta_\ell$ $(\ell<n)$は$\mathrm{Mod}_n(b)=b$ より

$$\delta_\ell=\mathbb{1}[\mathrm{Mod}_n(t_{a,b}(\ell))<b]$$

で定まるわけであるが，$t_{a,b}$は置換であり$t_{a,b}(n)=b$ であるから，$\ell<n$ に対して$t_{a,b}(\ell)=b$ となることがない．従って，δ_ℓ $(\ell<n)$を定める式を

$$\delta_\ell=\mathbb{1}[\mathrm{Mod}_n(t_{a,b}(\ell))\leq b]$$

としても変化がないということになる．「$\leq b$」は「$<b+1$」と書き替えても同じである．そして，$b<n-1$から$b+1=\mathrm{Mod}_n(b+1)$ である．従って，$(a,b+1)$に対して$a=t_{a,b+1}(1)=t_{a,b}(1)$から出発して漸化式で

$$\delta'_\ell=\mathbb{1}[\mathrm{Mod}_n(t_{a,b+1}(\ell))<\mathrm{Mod}_n(b+1)]$$

[28]かぶりはある．例えば注意23の8次の置換(52741638)は基本pNAP型であり，且つ(基本pNAP型の)(41638527)に定数1を加える変換から得られる置換である．尚，pNAP型はa-pNAP型の置換を定数を加える変換したもので尽きる理由は，定数を加える変換は定数を加える変換の逆変換でもあり，pNAP型ならば定数を加える変換で基本pNAP型に変換できるからである．

で$\vec{\delta'}$ と写像$t_{a,b+1}$ を定めたとして，結果の写像は同じ$t_{a,b}$となる．勿論，$t_{a,b+1}(n) = b \neq b+1$なので条件Nは満たさない．次に$b = n$の場合を考える．$\mathrm{Mod}_n(b) = 0$だから，$t_{a,b}$に付随するビット列は

$$\delta_\ell = \mathbb{1}[\mathrm{Mod}_n(t_{a,b}(\ell)) < 0]$$

で定まっていることになる．よって，$\vec{\delta} = \vec{0}$ である．このとき，$b' = \overline{\mathrm{Mod}}_n(b+1) = 1$であり，$t_{a,b'}$に付随するビット列$\vec{\delta'}$は

$$\delta'_\ell = \mathbb{1}[\mathrm{Mod}_n(t_{a,b'}(\ell)) < 1]$$

であるから，$t_{a,b'}(\ell) \neq n$である限り$\delta'_\ell = 0$ である．よって，$t_{a,b'}(\ell) = n$である最小のℓをℓ_0とするとき，$t_{a,b'}(\ell) = t_{a,b}(\ell)$ が$\ell \leq \ell_0$ について成立するが，$t_{a,b}(\ell) = n$ は，条件Nから$\ell < n$では成立しない．よって，この場合も，$\delta' = \vec{0}$ となって，$t_{a,b} = t_{a,b'}$ である．最後に，$b = n-1$の場合であるが，$t_{a,b}$が「Not(A1) 且つ P 且つ N」を満たすという前提ではこの状況は発生しない．実際，$t_{a,b}$ が「P 且つ N」を満たすと，付録A事実21の(4)より，$t_{a,b}$に付随するビット列は$\vec{\delta} = (1^{n-1})$に限られ，Not(A1)は満たさない．

固定した各$a \in [n]$に対して

$$\mathcal{B}_0 = \{b \in [n] : t_{a,b}\text{は Not(A1) 且つ P 且つ Nを満たす}\}$$
$$\mathcal{B}_1 = \{b \in [n] : t_{a,b}\text{は Not(A1) 且つ P 且つ Not(N)を満たす}\}$$

と仮におくと，ここまでで

$$\begin{array}{rccc} \psi_+ : & \mathcal{B}_0 & \to & \mathcal{B}_1 \\ & \cup & & \cup \\ & b & \mapsto & b' = \overline{\mathrm{Mod}}_n(b+1) \end{array}$$

なる写像が存在し，しかも$t_{a,b} = t_{a,b'}$であることがわかった．仮にこの写像で$b_1, b_2 \in \mathcal{B}_0$ に対して$b'_1 = b'_2$ になったとすると$t_{a,b_1} = t_{a,b'_1} = t_{a,b'_2} = t_{a,b_2}$で条件Nより$b_1 = b_2$となる．つまり，この写像 ψ_+ は単射である．これが実は全単射であることを示したい．

$b_3 \in \mathcal{B}_1$を任意に一つとったとする．このとき，図1のアルゴリズムでt_{a,b_3}を定めれば

$$t_{a,b_3}(\ell+1) - t_{a,b_3}(\ell) \equiv a + \mathbb{1}[t_{a,b_3}(\ell) < \mathrm{Mod}_n(b_3)] \mod n \quad (\ell < n)$$

が成立する．一方，t_{a,b_3}は基本pNAP型の置換であるから，定理3によって$b_0 := t_{a,b_3}(n)$に対して

$$t_{a,b_3}(\ell+1) - t_{a,b_3}(\ell) \equiv a + \mathbb{1}[t_{a,b_3}(\ell) < \mathrm{Mod}_n(b_0)] \mod n \quad (\ell < n)$$

もまた，成立する．2つの合同式を整理すると

$$\mathbb{1}[t_{a,b_3}(\ell) < \mathrm{Mod}_n(b_3)] \equiv \mathbb{1}[t_{a,b_3}(\ell) < \mathrm{Mod}_n(b_0)] \mod n \quad (\ell < n)$$

を得るが，インジケータ変数は0か1の値をとるため，これは等式

$$\mathbb{1}[t_{a,b_3}(\ell) < \mathrm{Mod}_n(b_0)] = \mathbb{1}[t_{a,b_3}(\ell) < \mathrm{Mod}_n(b_3)] \tag{19}$$

である．図1のアルゴリズムでt_{a,b_0}を定めたとすると，$t_{a,b_0}(1) = a = t_{a,b_3}(1)$, $t_{a,b_0}(2) = \overline{\mathrm{Mod}}_n(a + t_{a,b_0}(1) + \mathbb{1}[t_{a,b_0}(1) < \mathrm{Mod}_n(b_0)]) = \overline{\mathrm{Mod}}_n(a + t_{a,b_3}(1) + \mathbb{1}[t_{a,b_3}(1) < \mathrm{Mod}_n(b_3)]) = t_{a,b_3}(2)$, ... が$\ell = n-1$まで順次成立し，結局$t_{a,b_0} = t_{a,b_3}$が成立する．そして特に$b_0 = t_{a,b_3}(n) = t_{a,b_0}(n)$であり，$(a, b_0)$は条件Nを満足している．この対応$b_3 \mapsto b_0$ は$\mathcal{B}_1$から$\mathcal{B}_0$への写像を与えているが，これをψ_-と命名しよう．t_{a,b_0}による$[n-1]$の像が$[n] \setminus \{b_0\}$ ($t_{a,b_0} = t_{a,b_3}$が置換で$t_{a,b_0}(n) = b_0$に注意) であることから，前述のインジケータ等式(19)より

$$\forall x \in [n] \setminus \{b_0\} \quad \mathbb{1}[x < \mathrm{Mod}_n(b_0)] = \mathbb{1}[x < \mathrm{Mod}_n(b_3)] \tag{20}$$

が成立する．b_3は Not(N), b_0は N を満たすとしているから$b_3 \neq b_0$, 従って$\mathrm{Mod}_n(b_3) \neq \mathrm{Mod}_n(b_0)$ である．仮に$\mathrm{Mod}_n(b_0) - \mathrm{Mod}_n(b_3) \geq 2$ であると，$\mathrm{Mod}_n(b_0) > y > \mathrm{Mod}_n(b_3)$ なる$y \in [n]$ が存在する．$y < \mathrm{Mod}_n(b_0) \leq b_0$より$y \neq b_0$であるから，この$y$を式(20)の$x$に代入すると左辺が 1, 右辺が 0 で矛盾する．また，$\mathrm{Mod}_n(b_3) - \mathrm{Mod}_n(b_0) \geq 2$のとき，$\mathrm{Mod}_n(b_3) > y > \mathrm{Mod}_n(b_0)$ なる$y \in [n]$ をとると，$n > y > \mathrm{Mod}_n(b_0)$ であり，さらに$b_0 = n$ではない．なぜなら，もし$b_0 = n$であれば，インジケータ等式(20)は$x \in [n-1]$で成立し，その左辺はすべて 0 である．故に$x \in [n-1]$のすべてで$x \geq \mathrm{Mod}_n(b_3)$でなくてはならないが，このような$b_3$は$\mathrm{Mod}_n(b_3) = 0$か$\mathrm{Mod}_n(b_3) = 1$ である．いずれの場合も$\mathrm{Mod}_n(b_3) - \mathrm{Mod}_n(b_1) \geq 2$ にはならない．即ち，$b_0 \neq n$であり，$\mathrm{Mod}_n(b_0) = b_0$である．やはり$y \in [n] \setminus \{b_0\}$であるから等式(20)に代入すると左辺は 0, 右辺が 1 で矛盾であ

る．$\mathrm{Mod}_n(b_3) \neq \mathrm{Mod}_n(b_0)$より，残る場合は$\mathrm{Mod}_n(b_3) = \mathrm{Mod}_n(b_0) - 1$と$\mathrm{Mod}_n(b_3) = \mathrm{Mod}_n(b_0) + 1$とである．前者の場合，インジケータ等式(20)は

$$\forall x \in [n] \setminus \{b_0\} \quad \mathbb{1}[x < \mathrm{Mod}_n(b_0)] = \mathbb{1}[x < \mathrm{Mod}_n(b_0) - 1]$$

であり，もし$\mathrm{Mod}_n(b_0) - 1 \geq 1$であれば，この$\mathrm{Mod}_n(b_0) - 1 \in [n] \setminus \{b_0\}$を$x$として，$1 = \mathbb{1}[x < \mathrm{Mod}_n(b_0)] \neq \mathbb{1}[x < \mathrm{Mod}_n(b_0) - 1] = 0$と矛盾するため，$\mathrm{Mod}_n(b_0) - 1 < 1$となり，$\mathrm{Mod}_n(b_0) = 0$, あるいは$\mathrm{Mod}_n(b_0) = 1$である．$\mathrm{Mod}_n(b_3) = \mathrm{Mod}_n(b_0) - 1 \geq 0$より$\mathrm{Mod}_n(b_0) = 0$は否定される．すると，$\mathrm{Mod}_n(b_0) = 1$, つまり，$b_0 = 1$ということになる．しかしこのとき，$t_{a,b_0}$を定める漸化式は

$$t_{a,b_0}(\ell + 1) = \overline{\mathrm{Mod}}_n(t_{a,b_0}(\ell) + a + \mathbb{1}[t_{a,b_0}(\ell) < 1]) \quad (\ell < n)$$

となり，この$\mathbb{1}[t_{a,b_0}(\ell) < 1]$は$\ell < n$で常にゼロ，つまり，付随するビット列が$\vec{0}$であることにより$t_{a,b_0}$はその定義より$t_{a,b_0}(\ell) \equiv \ell a \mod n$が$\ell \in [n]$について成り立つ．すると，$\mathrm{Mod}_n(t_{a,b_0}(n)) = 0$だが，これは$1 = b_0 = t_{a,b_0}(n)$と相反する．これで，$\mathrm{Mod}_n(b_3) = \mathrm{Mod}_n(b_0) - 1$の可能性が排除され，$\mathrm{Mod}_n(b_3) = \mathrm{Mod}_n(b_0) + 1$の場合だけが残った．$\mathrm{Mod}_n(b_3) = 0$は$\mathrm{Mod}_n(b_0) \geq 0$よりありえない．よって

$$b_3 = \overline{\mathrm{Mod}}_n(b_0 + 1) \quad (b_3 \in \mathcal{B}_1)$$

つまり，

$$b_3 = \psi_+(\psi_-(b_3)) \quad (b_3 \in \mathcal{B}_1)$$

となって，単射$\psi_+; \mathcal{B}_0 \to \mathcal{B}_1$は全射であることがわかった．

以上より，「Not(A1) 且つ P 且つ N」なる(a, b)と「Not(A1) 且つ P 且つ Not(N)」なる(a, b)の一対一対応があることがわかる．□

命題 32. nを3以上の自然数とする．本文第5節の記法の下，条件A1を満たす(a, b)は条件NもPも満たす．さらにそのような(a, b)は全部で$\phi(n)$個である．

証明. $t_{a,b}$を条件A1を満たす写像とする．$\vec{\delta} = (1^{n-1})$であるから，mod nでみると初項a公差$a + 1$の等差数列なること，即ち，$t_{a,b}(\ell) \equiv a + (\ell - 1)(a + 1) \mod n$が成立する．$d = \gcd(a + 1, n)$とすると，$t_{a,b}(\ell + n/d) \equiv a + (\ell + n/d - 1)(a + 1) \equiv t_{a,b}(\ell) \mod n$と，$t_{a,b}$は周期$n/d$をもつ．特に，$t_{a,b}(n) \equiv a + (n - 1)(a + 1) \equiv -1 \mod n$から$t_{a,b}(n) = n - 1$であるが，もし$d > 1$ならば，上記の周期性より$t_{a,b}(n - n/d) = n - 1$も成り立つ．一方で，$\vec{\delta} = (1^{n-1})$である以上，

$$\delta_\ell = \begin{cases} 1 & \text{if } \mathrm{Mod}_n(t_{a,b}(\ell)) < \mathrm{Mod}_n(b) \\ 0 & \text{o.w.} \end{cases}$$

この場合分けは全ての$\ell < n$について1行目が成立しなければならない．$d > 1$であると，$\ell = n - n/d$のとき$n - 1 < \mathrm{Mod}_n(b)$が成立しなければならないが，これは$\mathrm{Mod}_n$の定義より不可能である．よって，$d = 1$が要請されるが，このときは$t_{a,b}$は置換になる．$t_{a,b}(n) \equiv a + (n - 1)(a + 1) \equiv -1 \mod n$より$t_{a,b}(n) = n - 1$であるから，集合$[n - 1]$の$t_{a,b}$による像は$[n] \setminus \{n - 1\}$であり，その$\mathrm{Mod}_n$による像は$\{0, 1, \ldots, n - 2\}$である．従って，前述の場合分けを$\ell < n$についてすべて1行目の場合にするには，$\mathrm{Mod}_n(b) = n - 1$とするしかなく，$b = n - 1$である．よって，条件A1を満たす$(a, b)$はすべて条件NもPも満足し，$\gcd(a + 1, n) = 1$と$b = n - 1$の要請から，そのような$(a, b)$は$\phi(n)$個だけ存在する．□