Irreducible and connected permutations

Martin Klazar*

Abstract

A permutation π of $[n] = \{1, 2, \dots, n\}$ is irreducible if $\pi([m]) = [m]$ for no $m \in [n]$, $m < n$, and it is connected if for no interval $I \subset [n]$, $2 \le |I| \le n - 1$, the image $\pi(I)$ is an interval. We review the enumeration of irreducible permutations and their appearances in mathematics. We enumerate connected permutations: asymptotically there are $n!/\mathrm{e}^2$ of them, and exactly, for $n > 2$, their number equals $2(-1)^{n+1}$ minus the coefficient of x^n in the compositional inverse of $1!x + 2!x^2 + \cdots$. We show that their numbers are not P-recursive, are congruent modulo high powers of 2 to $2(-1)^{n+1}$, and are congruent modulo 3 to $-C_{n-1} + (-1)^n$ where C_n is the Catalan number.

1 Introduction and definitions

A permutation π of $[n] = \{1, 2, \dots, n\}$, $n \in \mathbf{N} = \{1, 2, \dots\}$, is *reducible* if there is an $m \in \mathbf{N}$, $m < n$, such that $\pi([m]) = [m]$. If π is not reducible, it is *irreducible*. For example, $(2, 3, 1)$ is irreducible and $(2, 1, 3)$ is reducible. The number of irreducible permutations of $[n]$ is denoted ip_n. We call π *disconnected* if there is an interval $I \subset [n]$, $2 \le |I| \le n - 1$, such that its image $\pi(I)$ also is an interval. If π is not disconnected, it is *connected*. For example, all three permutations of length 1 and 2 are connected, all six permutations of length 3 are disconnected, and the only connected permutations of length 4 are $(2, 4, 1, 3)$ and $(3, 1, 4, 2)$. The number of connected permutations of $[n]$ is denoted cop_n. Irreducible permutations are sometimes

*Department of Applied Mathematics (KAM) and Institute for Theoretical Computer Science (ITI), Charles University, Malostranské náměstí 25, 118 00 Praha, Czech Republic.
ITI is supported by the project LN00A056 of the Ministry of Education of the Czech Republic.
E-mail: `klazar@kam.mff.cuni.cz`

called differently (indecomposable permutations or connected permutations) and were enumerated by Comtet [6]. The notion of connected permutations seems new. What are the numbers cop_n of connected permutations? This was the starting point for the present article. We shall see that the numerical answer is again hidden in Comtet's book [6].

In the rest of this section we give further definitions. In Proposition 2.1 and Theorem 2.2 we remind the known enumeration of irreducible permutations, which we need for the enumeration of connected permutations. In Section 2 we also discuss the appearances of irreducible permutations in mathematics. In Proposition 3.1 we characterize connected permutations by means of the permutation containment and in Proposition 3.4 and Theorem 3.5 we enumerate them exactly. Their numbers cop_n provide a combinatorial interpretation for the coefficients of the compositional inverse of $1!x+2!x^2+\cdots$. In Proposition 4.2 we give a graph sieve needed for the proof of the asymptotic estimate $\mathrm{cop}_n = (\mathrm{e}^{-2} + O(n^{-1}))n!$ in Theorem 4.3. In Theorem 5.2 we give a general criterion for non-P-recursiveness of super-exponential sequences whose ogf's satisfy first order differential equations. It implies that $(\mathrm{cop})_{n\ge1}$ is not P-recursive. In Corollaries 6.3 and 6.5 we prove the congruences $\mathrm{cop}_n \equiv 2(-1)^{n+1} \bmod 2^{\lceil (n-1)/2\rceil - \mathrm{ord}_2(n)}$ and $\mathrm{cop}_n \equiv -\frac{1}{n}\binom{2n-2}{n-1} + (-1)^n \bmod 3$, respectively.

The set of $n!$ permutations of $[n]$ is denoted S_n. An interval $\{a, a+1, \ldots, b\}$ is denoted $[a, b]$, so $[1, n] = [n]$. For $\pi \in S_n$ the reverted permutation $\sigma = \overline{\pi} \in S_n$ is defined by $\sigma(i) = \pi(n+1-i)$. With the exception of $(1, 2)$ and $(2, 1)$, every connected permutation π has the property that both π and $\overline{\pi}$ are irreducible. However, a disconnected permutation π may be still irreducible or $\overline{\pi}$ may be irreducible or both, e.g., $\pi = (5, 4, 2, 1, 6, 3)$ is disconnected but π and $\overline{\pi}$ are irreducible. Obviously, the number of $\pi \in S_n$ such that $\overline{\pi}$ is irreducible equals ip_n.

We denote the identical permutation $(1, 2, \ldots, n)$ by ι_n. Thus $\overline{\iota}_n = (n, n-1, \ldots, 1)$. The *substitution* of $\sigma_1 \in S_{n_1}, \sigma_2 \in S_{n_2}, \ldots, \sigma_r \in S_{n_r}$ in $\sigma \in S_r$ is the permutation $\pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r) \in S_{n_1+n_2+\cdots+n_r}$ given by

$$\pi(i) = n_1 + n_2 + \cdots + n_{\sigma(j)-1} + \sigma_j(i - n_1 - n_2 - \cdots - n_{j-1})$$

where $j \in [r]$ is the least number such that $n_1 + n_2 + \cdots + n_j \ge i$, and empty sums equal 0. Atkinson and Stitt [3] call this construction the *wreath product*. The partition of $[n]$, $n = n_1 + n_2 + \cdots + n_r$, in the disjoint intervals $I_i = [n_1+n_2+\cdots+n_{i-1}+1, n_1+\cdots+n_i]$, $i = 1, 2, \ldots, r$, is called the *interval* *partition associated with* $\sigma(\sigma_1, \sigma_2, \dots, \sigma_r)$. For example, if $\sigma = (2,3,1)$, $\sigma_1 = (4,2,3,1)$, $\sigma_2 = (1)$, and $\sigma_3 = (1,5,4,2,3)$, then

$$\sigma(\sigma_1, \sigma_2, \sigma_3) = (9,7,8,6,10,1,5,4,2,3)$$

and the associated interval partition is $[1,4], [5,5]$, and $[6,10]$. It is clear that $\sigma(\iota_1, \iota_1, \dots, \iota_1) = \sigma$ for every permutation σ.

We say that two injections $f : X \to \mathbf{N}$ and $g : Y \to \mathbf{N}$, where X and Y are finite subsets of $\mathbf{N}$ of the same cardinality, are *equivalent* if, with $u : X \to Y$ and $v : g(Y) \to f(X)$ being the unique increasing bijections, for every $x \in X$ we have $f(x) = v(g(u(x)))$. For example, the f given by $f(3) = 2, f(1) = 8$, and $f(100) = 7$ is equivalent to the permutation $(3,1,2)$. Every injection from a finite set $X \subset \mathbf{N}$, $|X| = n$, to $\mathbf{N}$ is equivalent to a unique permutation $\pi \in S_n$. If $\pi \in S_n$ and $X \subset [n]$ with $|X| = m$, we say that the $\sigma \in S_m$ equivalent with the restricted mapping $\pi : X \to [n]$ is the *restriction* of π (to X). We say that a permutation σ *is contained* in another permutation π, and write $\sigma \prec \pi$, if σ is a restriction of π. For example, $(3,1,2) \prec (6,7,2,8,5,4,3,1)$ but $\iota_4 \not\prec (6,7,2,8,5,4,3,1)$. For a permutation π we set $\mathrm{Forb}(\pi) = \{\sigma : \ \pi \not\prec \sigma\}$. This is an example of a *hereditary* (or *closed*) permutation class X, which is a set of permutations such that $\sigma \prec \pi \in X$ always implies $\sigma \in X$. A set of permutations X is *closed under substitutions* if $\pi = \sigma(\sigma_1, \sigma_2, \dots, \sigma_r) \in X$ whenever all $\sigma, \sigma_1, \dots, \sigma_r$ are in X.

If $\pi \in S_n$ and $I \subset [n]$ is an interval such that $\pi(I)$ is an interval, the *contraction* of π on I produces the permutation $\sigma \in S_{n-|I|+1}$ defined as the restriction of π to $([n]\backslash I) \cup \{i\}$, where $i \in I$ is arbitrary (σ does not depend on the choice of i). If $\mathcal{I} = \{I_1, I_2, \dots, I_r\}$ are mutually disjoint subintervals of $[n]$ such that every $\pi(I_i)$ is an interval, the contraction of π on $\mathcal{I}$ is defined as the restriction of π to $([n]\backslash(I_1 \cup I_2 \cup \dots \cup I_r)) \cup \{i_1, i_2, \dots, i_r\}$, where $i_j \in I_j$ are arbitrary. Note that if $\pi = \sigma(\sigma_1, \sigma_2, \dots, \sigma_r) \in S_n$ and $\mathcal{I} = \{I_1 < I_2 < \dots < I_r\}$ is the associated interval partition of $[n]$, then σ is the contraction of π on $\mathcal{I}$ and every σ_i is the restriction of π to I_i.

For a power series $F \in \mathbf{C}[[x]]$, the coefficient at x^n is denoted $[x^n]F$. Recall that if $F \in \mathbf{C}[[x]]$ is such that $F = a_1x + a_2x^2 + \cdots$ with $a_1 \neq 0$, then there exists a unique $G \in \mathbf{C}[[x]]$ of the same form, the compositional inverse $G = F^{\langle -1 \rangle}$ of F, such that $F(G) = G(F) = x$. By Lagrange inversion formula (see ...), its coefficients satisfy

$$[x^n]F^{\langle -1 \rangle} = \frac{1}{n}[x^{n-1}]\left(\frac{x}{F(x)}\right)^n.$$

2 Irreducible permutations

The results in Proposition 2.1 and Theorem 2.2 are well known. We state and prove them for completeness because we need them later. We give Proposition 2.1 also for comparison with the less straightforward Proposition 3.4.

Irreducible permutations were introduced by Comtet [6, p. 262] (he called them indecomposable permutations) who in [5] derived the asymptotic series for the numbers ip_n (see also [6, p. 295]); it begins $\mathrm{ip}_n = n!(1-2n^{-1}-(n(n-1))^{-1}-4(n(n-1)(n-2))^{-1}+O(n^{-4}))$. The sequence starts

n	1	2	3	4	5	6	7	8	9	10
ip_n	1	1	3	13	71	461	3447	29093	273343	2829325

and Sloane [29] records it as A003319. Irreducible permutations made their way as an example in several basic texts on enumeration and combinatorics: Flajolet and Sedgewick [9, Example 13 on p. 57], Gessel and Stanley [11, p. 1030], Goulden and Jackson [12, Exercise 2.4.19], Knuth [18, Exercise 99], and Odlyzko [23, Example 7.4]. King [15] investigates their Gray codes, see also [18, Exercise 99]. It turns out that they label natural base of free quasi-symmetric functions, see Aguiar and Sottile [1], Duchamp et al. [8], and Poirier and Reutenauer [26]. Ossona de Mendez and Rosenstiehl [24] constructed a bijection between irreducible permutations of $[0, d]$ and pointed hypermaps with d darts, and a bijection between irreducible fixed-point-free involutions on $[0, 2m+1]$ and pointed maps with m edges. Not surprisingly, the decomposition in Proposition 2.1 plays an important role in enumeration of hereditary permutation classes, see Atkinson et al. [2], Atkinson and Stitt [3], and Kaiser and Klazar [13].

Besides combinatorics and algebra, irreducible permutations appear in ergodic theory and number theory. Let $\pi \in S_n$ be given and $\lambda = \{I_1 < I_2 < \ldots < I_n\}$ and $\kappa = \{J_1 < J_2 < \ldots < J_n\}$ be two partitions of the real interval $[0, 1)$ into intervals of type $[a, b)$ such that $|I_i| = |J_{\pi(i)}|$ for every $i \in [n]$; κ arises by permuting λ by π. *The interval exchange transform* $T = T(\pi, \lambda)$ is the permutation of $[0, 1)$ which sends $x \in I_i$ to $T(x) = x - |I_1| - \cdots - |I_{i-1}| + |J_1| + \cdots + |J_{\pi(i)-1}|$. Thus I_i, sent by π to $J_{\pi(i)}$, carries with itself the point x to its new place $T(x)$. Keane [14] proved that if π is irreducible and λ is irrational (this means that the lengths $|I_i|$ are linearly independent over $\mathbf{Q}$), then the orbit $O_x = \{T^k(x) : k \in \mathbf{Z}\}$ of every point x is dense in $[0,1)$. In 1979 he conjectured that for every irreducible π and almost every λ (in the sense of the probabilistic Lebesgue measure on the set of all λ's) every orbit O_x is uniformly distributed in $[0,1)$. This conjecture was proved independently by Masur [22] and Veech [31]. For further properties and applications of interval exchange transforms associated with irreducible permutations see de Oliveira and Gutierrez [7], Chaves and Noguiera [4], Kontsevich and Zorich [19], Rauzy [27], and Vuillon [32].

Interestingly, there is a link between irreducible permutations and the Prime number theorem. The PNT says that $\pi(x)$, the number of primes not exceeding x, satisfies $\pi(x) = x(1+o(1))/\log x$. In 1808, Legendre made a more precise but incorrect conjecture that $\pi(x)$ is roughly $x/(\log x - 1.08366)$. Panaitopol [25] pointed out that for every $r \in \mathbf{N}$,

$$\pi(x) = \frac{x}{\log x - 1 - \sum_{n=1}^{r-1} k_n \log^{-n} x - k_r(1+o(1)) \log^{-r} x}$$

where, in fact, $k_n = \mathrm{ip}_{n+1}$.

Proposition 2.1 *The set of permutations of the form $\pi = \iota_r(\sigma_1, \sigma_2, \ldots, \sigma_r)$, where $r \geq 1$ and all σ_i are irreducible, equals to the set of all permutations. This decomposition of π is unique.*

Proof. We prove the first claim by induction on n in $\pi \in S_n$. For $n = 1$ we have the representation $\iota_1 = \iota_1(\iota_1)$. For $n > 1$ let $m \in [n]$ be the least number such that $\pi([m]) = [m]$. The restriction σ_1 of π to $[m]$ is irreducible. If $m = n$, then $\sigma_1 = \pi$ and we have $\pi = \iota_1(\sigma_1)$. If $m < n$, we have $\pi = \iota_2(\sigma_1, \sigma)$ where σ is the restriction of π to $[m+1, n]$. We apply on σ the inductive assumption and obtain for π the stated representation.

To prove the uniqueness, we assume that

$$\pi = \iota_r(\sigma_1, \sigma_2, \ldots, \sigma_r) = \iota_s(\rho_1, \rho_2, \ldots, \rho_s) \in S_n$$

where all σ_i and ρ_i are irreducible. Let the associated interval partitions $I_1 < I_2 < \ldots < I_r$ and $J_1 < J_2 < \ldots < J_s$ of $[n]$ be distinct. Then there is a $k \geq 1$ such that $I_1 = J_1, I_2 = J_2, \ldots, I_{k-1} = J_{k-1}$, and $I_k \neq J_k$. So $I_k = [a, b]$ and $J_k = [a, c]$ with $b \neq c$. If $b < c$, $\rho_k([b-a+1]) = \sigma_k([b-a+1]) = [b-a+1]$ and ρ_k is reducible, which is a contradiction. Similarly, $b > c$ contradicts the irreducibility of σ_k. Hence we must have $r = s$, $I_1 = J_1, \ldots, I_r = J_r$, and $\sigma_1 = \rho_1, \ldots, \sigma_r = \rho_r$. The uniqueness is proved. $\square$

Theorem 2.2 *Let $I(x) = \sum_{n\geq 1} \mathrm{ip}_n x^n = x + x^2 + 3x^3 + \cdots$ be the ogf of irreducible permutations and $\varphi(x) = \sum_{n\geq 1} n! \cdot x^n = x + 2x^2 + 6x^3 + \cdots$. Then*

$$I(x) = \frac{\varphi(x)}{1+\varphi(x)} = 1 - \frac{1}{1+\varphi(x)}$$

and thus $\mathrm{ip}_n = -[x^n](1+\varphi(x))^{-1}$ for every $n \in \mathbf{N}$.

Proof. It follows from Proposition 2.1 that $1 + \varphi(x) = \sum_{r\geq 0} I(x)^r = (1 - I(x))^{-1}$. Solving this for $I(x)$ we get the stated formula. $\square$

Thus we have the recurrence $\mathrm{ip}_n = [x^n]I(x) = [x^n]\varphi(x)(1 - I(x)) = n! - \sum_{k=1}^{n-1}(n-k)! \cdot \mathrm{ip}_k$.

3 Connected permutations

The following result was our motivation to introduce connected permutations.

Proposition 3.1 *Let $\tau \in S_t$. The set $\mathrm{Forb}(\tau)$ is closed under substitutions if and only if τ is connected.*

Proof. If $\mathrm{Forb}(\tau)$ is not closed under substitutions, then it happens that

$$\tau \prec \pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r) \in S_n$$

although none of $\sigma, \sigma_1, \ldots, \sigma_r$ contains τ. Let $X \subset [n]$ be such that the restriction of π to X is τ and $I_1 < I_2 < \ldots < I_r$ be the interval partition of $[n]$ associated with the substitution. It is not possible that $X \subset I_i$ for some i and that $|X \cap I_i| \leq 1$ for all i because $\sigma_i \not\succ \tau$ for all i and $\sigma \not\succ \tau$. Thus $2 \leq |X \cap I_k| \leq |X| - 1$ for some k, $1 \leq k \leq r$. Let $X = \{x_1 < x_2 < \ldots < x_t\}$ and $X \cap I_k = \{x_i, x_{i+1}, \ldots, x_j\}$ where $1 \leq j - i \leq t - 2$. It follows from the definition of substitution that $\tau([i,j])$ is an interval and thus τ is disconnected.

Let τ be disconnected. Then $t \geq 3$ and $\tau([i,j])$ is an interval for some i, j with $1 \leq j - i \leq t - 2$. Let $\sigma \in S_{t-j+i}$ be the contraction of τ on $[i,j]$ and ρ be the restriction of τ to $[i,j]$. Then $\tau = \sigma(\iota_1, \ldots, \iota_1, \rho, \iota_1, \ldots, \iota_1)$ with ρ on the i-th place. But none of σ, ι_1, and ρ contains τ because all are shorter than τ. So $\mathrm{Forb}(\tau)$ is not closed under substitutions. $\square$

To enumerate connected permutations, in Proposition 3.4 we uniquely decompose by means of them any permutation. We need two simple lemmas.

Lemma 3.2 *Let $I_1 < I_2 < \ldots < I_r$ and $J_1 < J_2 < \ldots < J_s$, where $r, s \geq 2$, be two distinct interval partitions of $[n]$. Then (i) $I_1 \cup J_s = [n]$ or (ii) $J_1 \cup I_r = [n]$ or (iii) some I_i intersects at least two and at most $s-1$ intervals J_j or (iv) some J_i intersects at least two and at most $r-1$ intervals I_j.*

Proof. We may assume that $r \leq s$. Let k, $0 \leq k \leq r-1$, be such that $I_1 = J_1, I_2 = J_2, \ldots, I_k = J_k$ and $I_{k+1} \neq J_{k+1}$. Clearly, k exists and $I_{k+1} = [a, b]$ and $J_{k+1} = [a, c]$ with $b \neq c$. First, let $k = 0$ and $b < c$. Then we have (ii) or (iv) with $i = 1$. If $k = 0$ and $b < c$, we have (i) or (iii) with $i = 1$. If $k \geq 1$, we have (iii) with $i = k+1$ or (iv) with $i = k+1$. $\square$

Lemma 3.3 *If $\pi \in S_n$ and I, J are intervals in $[n]$ such that $I \neq [n]$, $J \neq [n]$, $I \cup J = [n]$, and both $\pi(I)$ and $\pi(J)$ are intervals, then π is reducible or $\overline{\pi}$ is reducible.*

Proof. It follows from the assumptions that $1 \in I$ and $n \in J$ or vice versa. Let us assume that $1 \in I$. By the same argument, $1 \in \pi(I)$ and $n \in \pi(J)$ or vice versa. In the former case π is reducible, and in the latter case $\overline{\pi}$ is reducible. $\square$

In general the decomposition $\pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r)$ with connected σ is not unique, for example $\pi = (2, 1, 4, 3, 6, 5)$ has three decompositions $\pi = \iota_1(\pi) = \iota_2((2, 1), (2, 1, 4, 3)) = \iota_2((2, 1, 4, 3), (2, 1))$. However, if ι_1, ι_2, and $\overline{\iota_2}$ are forbidden for σ, then we get a unique decomposition.

Proposition 3.4 *Consider the following four sets of permutations: (i) S_1, (ii) the reducible permutations, (iii) the permutations π such that $\overline{\pi}$ is reducible, and (iv) the permutations of the form $\pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r)$ where $r \geq 4$, σ is connected, and σ_i are arbitrary. These sets are mutually disjoint, their union is the set of all permutations, and the decomposition of π in the form (iv) is unique.*

Proof. It is clear that the sets (i), (ii), and (iii) are mutually disjoint, as well as the sets (i) and (iv). We show that every $\pi \in S_n$ of the form (iv) is irreducible. Suppose that $\pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r) \in S_n$ as in (iv) and $\pi([a]) = [a]$ for some $1 \leq a < n$. Let $I_1 < I_2 < \ldots < I_r$ be the interval partition of $[n]$ associated with the substitution and $I_1, I_2, \ldots, I_k$, $1 \leq k \leq r$, be all intervals intersected by $[a]$. It follows that $\sigma([k]) = [k]$, $\sigma([k+1, r]) = [k+1, r]$, and if

$k = r$ then $\sigma([r-1]) = [r-1]$. For any k we have a contradiction with the connectedness of σ. Thus the sets in (iv) and (ii) are disjoint, and similarly for (iv) and (iii).

To prove the second claim, we take an arbitrary $\pi \in S_n$, $n \geq 2$, such that π and $\overline{\pi}$ are irreducible and express π in the form (iv). We define a *maximal interval* I as a subinterval $I \subset [n]$ such that $1 \leq |I| \leq n-1$, $\pi(I)$ is an interval, and I is maximal to inclusion with respect to these properties. It follows that maximal intervals are pairwise disjoint. Indeed, let I and J be distinct maximal intervals with $I \cap J \neq \emptyset$. If $I \cup J \neq [n]$ then $I \cup J$ contradicts the maximality of I or of J because $\pi(I \cup J)$ is interval. If $I \cup J = [n]$, Lemma 3.3 shows that we have a contradiction with the irreducibility of π or of $\overline{\pi}$. Hence we have an interval partition $I_1 < I_2 < \ldots < I_r$ of $[n]$ into maximal intervals. We have $r \geq 2$ but $r = 2$ is impossible by Lemma 3.3. Thus $r \geq 3$. We define $\sigma \in S_r$ as the contraction of π on $\{I_1 < I_2 < \ldots < I_r\}$ and σ_i, $1 \leq i \leq r$, as the restrictions of π to I_i. Then $\pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r)$. Suppose that for some interval $I \subset [r]$, $2 \leq |I| \leq r-1$, $\sigma(I)$ is an interval. It follows that $\pi(\bigcup_{i \in I} I_i)$ is an interval, which contradicts the maximality of each of the intervals I_i, $i \in I$. So σ is connected and $r = 3$ is impossible because no permutation in S_3 is connected.

To prove the last claim, we assume that

$$\pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r) = \rho(\rho_1, \rho_2, \ldots, \rho_s) \in S_n$$

where $r, s \geq 4$ and both σ and ρ are connected. Let $I_1 < I_2 < \ldots < I_r$ and $J_1 < J_2 < \ldots < J_s$ be the associated interval partitions of $[n]$. If they are distinct, we apply Lemma 3.2. By Lemma 3.3, the cases (i) and (ii) cannot occur (we know from the proof of the first claim that π and $\overline{\pi}$ are irreducible). Suppose that the case (iii) occurs and I_i intersects the intervals $J_k, J_{k+1}, \ldots, J_l$ where $1 \leq l - k \leq s - 2$. Since ρ is connected, there are $j \in [s] \backslash [k, l]$ and $p, q \in [k, l]$ such that $\rho(p) < \rho(j) < \rho(q)$. But then $\pi(J_p) < \pi(J_j) < \pi(J_q)$ which implies $\min \pi(I_i) < \pi(J_j) < \max \pi(I_i)$, and thus $\pi(I_i)$ is not an interval. On the other hand, $\pi(I_i)$ must be an interval because I_i is one of the intervals associated with the substitution $\pi = \sigma(\sigma_1, \sigma_2, \ldots, \sigma_r)$. This contradiction shows that the case (iii) of Lemma 3.3 cannot occur. By an analogous argument, the case (iv) cannot occur as well. Thus the two interval partitions must be equal and we have $r = s$, $I_1 = J_1, \ldots, I_r = J_r$, $\sigma_1 = \rho_1, \ldots, \sigma_r = \rho_r$, and $\sigma = \rho$. The uniqueness is proved. $\square$

Theorem 3.5 *Let* $C(x) = \sum_{n\geq 1} \mathrm{cop}_n x^n = x + 2x^2 + 2x^4 + \cdots$ *be the ogf of connected permutations and* $\varphi(x) = \sum_{n\geq 1} n! \cdot x^n = x + 2x^2 + 6x^3 + \cdots$*. Then*

$$C(x) = 2\left(x + x^2 - \frac{x^2}{1+x}\right) - \varphi(x)^{\langle -1\rangle}$$

and thus $\mathrm{cop}_1 = 1$*,* $\mathrm{cop}_2 = 2$ *and* $\mathrm{cop}_n = -[x^n]\varphi(x)^{\langle -1\rangle} + (-1)^{n+1} \cdot 2$ *for every* $n > 2$*.*

Proof. By Proposition 2.1 and Theorem 2.2, the ogf of the numbers of reducible permutations π equals

$$\sum_{r\geq 2} I(x)^r = \frac{I(x)^2}{1 - I(x)} = \frac{\varphi(x)^2}{1 + \varphi(x)}$$

and the same formula holds for reducible $\overline{\pi}$. By Proposition 3.4,

$$\varphi(x) = x + \frac{2\varphi(x)^2}{1 + \varphi(x)} + (C(x) - x - 2x^2) \circ \varphi(x)$$

where on the right the first x counts the set (i), the second summand counts the sets (ii) and (iii), and the last composition counts the set (iv). Substituting for x the power series $\varphi(x)^{\langle -1\rangle}$ and solving the result for $C(x)$, we get the stated formula. $\square$

The coefficients of $\varphi(x)^{\langle -1\rangle}$, and more generally of $(\varphi(x)^{\langle -1\rangle})^k$, were considered by Comtet [6, p. 174] (who gave for them no combinatorial interpretation); this is the only reference we know of. We denote the number $[x^n]\varphi(x)^{\langle -1\rangle}$ by Com_n and call it the *Comtet number*. Thus, for $n \neq 2$, $\mathrm{cop}_n = -\mathrm{Com}_n + (-1)^{n+1} \cdot 2$. The sequences $(\mathrm{Com}_n)_{n\geq 1}$ and $(\mathrm{cop}_n)_{n\geq 1}$ start as follows.

n	1	2	3	4	5	6	7	8	9	10
Com_n	1	−2	2	−4	−4	−48	−336	−2928	−28144	−298528
cop_n	1	2	0	2	6	46	338	2926	28146	298526

The sequence $(\mathrm{Com}_n)_{n\geq 1}$ (normalized by omitting the minus signs) is in [29] listed as A059372.

4 A forest sieve and the asymptotics of numbers of connected permutations

By the results of Comtet, $\mathrm{ip}_n = (1 - O(n^{-1})) \cdot n!$ and therefore for big n almost every $\pi \in S_n$ is irreducible. For connected permutations the situation is different. We prove that $\mathrm{cop}_n = (\mathrm{e}^{-2} + O(n^{-1})) \cdot n!$. We need two auxiliary results which are of independent interest.

For a graph $G = (V, E)$, a subset $X \subset V$ is *independent* if it spans no edge. In the opposite case (at least one edge of G has both endpoints in X) we say that X is *dependent*. Note that every dependent X satisfies $|X| \geq 2$ and that all X with $0 \leq |X| \leq 1$ are independent. For a graph $G = (V, E)$ and a vertex $v \in V$ we set

$$\alpha^{\pm}(G) = \sum_{\substack{X \subset V \\ X \text{ independent}}} (-1)^{|X|} \quad \text{and} \quad \alpha^{\pm}(G, v) = \sum_{\substack{v \notin X \subset V \\ X \text{ independent}}} (-1)^{|X|}.$$

If G is disconnected with components $G_1, \ldots, G_k$ then we have the *product formula* $\alpha^{\pm}(G) = \prod_{i=1}^{k} \alpha^{\pm}(G_i)$. A *forest* is a graph with no cycle.

Lemma 4.1 *If F is a forest then $\alpha^{\pm}(F) = -1, 0$ or 1.*

Proof. By the product formula, we may assume that F is a tree. We proceed by induction on $|V(F)|$. For $|V(F)| \leq 2$ the statement holds: $\alpha^{\pm}(K_1) = 0$ and $\alpha^{\pm}(K_2) = -1$. Let $|V(F)| \geq 3$, u be a leaf of F, v the neighbor of u, and $u_1, \ldots, u_k$, $k \geq 1$, be the neighbors of v distinct from u. Let $F' = F - u$ and F_i be the component of $F - v$ containing u_i. To obtain $\alpha^{\pm}(F)$, we split F in $(\{u\}, \emptyset) = K_1$ and F' and use the product formula. But since u and F' are connected by the edge $\{u, v\}$, we must subtract the choices of the independent sets X_1 in $(\{u\}, \emptyset)$ and X_2 in F' such that $u \in X_1$ and $v \in X_2$. The contribution of the only X_1 is -1 and the contribution of the X_2's is $-\prod_{i=1}^{k} \alpha^{\pm}(F_i, u_i)$. Thus

$$\alpha^{\pm}(F) = \alpha^{\pm}(K_1)\alpha^{\pm}(F') - (-1) \cdot \left(-\prod_{i=1}^{k} \alpha^{\pm}(F_i, u_i) \right) = -\prod_{i=1}^{k} \alpha^{\pm}(F_i, u_i).$$

If $F_i = K_1$ then $\alpha^{\pm}(F_i, u_i) = 1$. If F_i has more than one vertex then, denoting the components of $F_i - u_i$ by $G_1, \ldots, G_l$, we have $\alpha^{\pm}(F_i, u_i) = \prod_{j=1}^{l} \alpha^{\pm}(G_j)$ and $\alpha^{\pm}(F_i, u_i) \in \{-1, 0, 1\}$ by the inductive assumption. Thus also $\alpha^{\pm}(F) \in \{-1, 0, 1\}$. $\square$

It is not hard to count that P_n, the path on n vertices, has $\binom{n+1-k}{k}$ independent sets of size k. On the other hand, the recurrence from the previous proof specializes for P_n to $\alpha^{\pm}(P_n) = -\alpha^{\pm}(P_{n-3})$, where $\alpha^{\pm}(P_1) = 0$, $\alpha^{\pm}(P_2) = -1$, and $\alpha^{\pm}(P_3) = -1$. We obtain combinatorial proof of the binomial identity

$$(\alpha^{\pm}(P_n) =) \sum_{k=0}^{(n+1)/2} (-1)^k \binom{n+1-k}{k} = \left\{ \begin{array}{lll} 0 & \ldots & n = 3m+1 \\ (-1)^m & \ldots & n = 3m, 3m-1. \end{array} \right.$$

See Klazar [16] for counting independent and maximal independent sets in rooted plane trees.

If $A_1, A_2, \ldots, A_n$ are some events in a probability space and $X \subset [n]$ is a set, we denote

$$A_X = \bigwedge_{i \in X} A_i.$$

The following inequality belongs to the area of graph sieves, see Lovász [21, Problem 2.12] and Galambos and Simonelli [10, I.3].

Proposition 4.2 *For every forest $F = ([n], E)$ and events $A_1, A_2, \ldots, A_n$ in a probability space,*

$$\left| \sum_{\substack{X \subset [n] \\ X \text{ dependent}}} (-1)^{|X|} \Pr[A_X] \right| \le \sum_{e \in E} \Pr[A_e].$$

Proof. By Rényi's 0-1 principle ([10, Theorem I.1] and [21, Problem 2.6]), it suffices to prove the inequality only when every $\Pr[A_i]$ is 0 or 1. Without loss of generality we assume that every $\Pr[A_i]$ is 1. Then we have to prove, denoting the sum of $(-1)^{|X|}$ over all dependent $X \subset [n]$ by S, that $|S| \le |E|$. Since the sum of $(-1)^{|X|}$ over all subsets $X \subset [n]$ is zero, we have

$$0 = \alpha^{\pm}(F) + S$$

and it suffices to prove $|\alpha^{\pm}(F)| \le |E|$. This is by Lemma 4.1 obviously true if F has at least one edge. If F has no edge, it is also true because then $\alpha^{\pm}(F) = 0$ and $|E| = 0$. $\square$

If $F = kK_2$ consists of k disjoint edges, $B_1, \ldots, B_k$ are k mutually exclusive events (with $\Pr[B_i] \le 1/k$) and we associate with the endpoints of the i-th edge of F two copies of B_i, then the inequality holds as an equality.

In general it does not hold if F is not a forest. Consider the graph kK_3. Since $\alpha^{\pm}(K_3) = -2$, the product formula gives $\alpha^{\pm}(kK_3) = (-2)^k$. For $F = 4K_3$ and all $\Pr[A_i] = 1$, the left hand side of the inequality equals $|\alpha^{\pm}(4K_3)| = 16$ and the right hand side is $|E(4K_3)| = 12$. The inequality holds for every class of graphs $\mathcal{G}$ that is closed on induced subgraphs and such that $|\alpha^{\pm}(G)| \le |E(G)|$ for every $G \in \mathcal{G}$.

Theorem 4.3 *For $n \to \infty$,*

$$\mathrm{cop}_n = (\mathrm{e}^{-2} + O(n^{-1})) \cdot n! = (0.13533\ldots + O(n^{-1})) \cdot n!$$

where $\mathrm{e} = 2.71828\ldots$ *is Euler number.*

Proof. We take a random permutation $\pi \in S_n$ from the uniform distribution and calculate the probability that π is (dis)connected. Let A_I be, for an interval $I \subset [n]$, the event that $\pi(I)$ is an interval, and E_k, $2 \le k \le n-1$, be the event $\bigvee_{|I|=k} A_I$, that is, the event that for some interval $I \subset [n]$, $|I| = k$, $\pi(I)$ is an interval. For $|I| = k$ we have

$$\Pr[A_I] = (n-k+1) \cdot \binom{n}{k}^{-1}$$

because there are $n-k+1$ image intervals $\pi(I)$ in $[n]$ and for two fixed k-sets $X, Y \subset [n]$ we have $\Pr[\pi(X) = Y] = 1/\binom{n}{k}$ (the events that $\pi(X)$ is a fixed k-set are equiprobable and mutually exclusive). Thus

$$\Pr[E_k] \le \sum_{|I|=k} \Pr[A_I] = (n-k+1)^2 \cdot \binom{n}{k}^{-1}.$$

For $k = 2$ this gives nothing but for the remaining k we get

$$\Pr[E_3 \vee E_4 \vee \ldots \vee E_{n-1}] \le \sum_{k=3}^{n-1} \Pr[E_k] \le \sum_{k=3}^{n-1} \frac{(n-k+1)^2}{\binom{n}{k}} = O(n^{-1}).$$

It follows that

$$\Pr[\pi \text{ is disconnected}] = \Pr[E_2] + O(n^{-1}).$$

For $i \in [n-1]$ we set $B_i = A_{\{i,i+1\}}$. By the inclusion-exclusion principle,

$$\Pr[E_2] = \Pr[B_1 \vee B_2 \vee \ldots \vee B_{n-1}] = -\sum_{\emptyset \ne X \subset [n-1]} (-1)^{|X|} \Pr[B_X]$$

where $B_X = \bigwedge_{i\in X} B_i$. Let P be the path with the vertex set $[n-1]$ and the edges $\{i, i+1\}$, $i \in [n-2]$. We split the last sum in the sum over X independent on P and the sum over X dependent on P. By Proposition 4.2 and the above calculations,

$$\Bigg| \sum_{\substack{X\subset[n-1]\\ X \text{ dependent}}} (-1)^{|X|}\Pr[B_X]\Bigg| \le \sum_{i=1}^{n-2} \Pr[B_i \wedge B_{i+1}] \le \sum_{|I|=3} \Pr[A_I] = O(n^{-1}).$$

Thus

$$\Pr[\pi \text{ is disconnected}] = \sum_{\substack{\emptyset\neq X\subset[n-1]\\ X \text{ independent}}} (-1)^{|X|+1}\Pr[B_X] + O(n^{-1}).$$

Suppose that $X \subset [n-1]$ consists of $k \ge 1$ elements, no two of them consecutive. $\Pr[B_X]$ is the probability that each $\pi(\{i, i+1\})$, $i \in X$, is an interval. We have $\binom{n-k}{k}k!2^k$ possible restrictions of π to $\bigcup_{i\in X}\{i, i+1\}$ because the $\pi(\{i, i+1\})$'s are k mutually disjoint 2-element intervals $J_1, \ldots, J_k$ in $[n]$ and, as we already know, there are $\binom{n-k}{k}$ of them, there are $k!$ assignments of the J_j's to the intervals $\{i, i+1\}$, $i \in X$, and there are two ways for $\pi(\{i, i+1\}) = J_j$. The probability of a fixed restriction of π to a given $A \subset [n]$ is $1/(n(n-1)\ldots(n-|A|+1))$. Thus

$$\Pr[B_X] = \binom{n-k}{k} \frac{k!2^k}{n(n-1)\ldots(n-2k+1)}$$

and

$$\Pr[\pi \text{ is disconnected}] = \sum_{k=1}^{n/2} \binom{n-k}{k}^2 \frac{(-1)^{k+1}k!2^k}{n(n-1)\ldots(n-2k+1)} + O(n^{-1}).$$

Rearranging the summand, we rewrite the last sum as

$$-\sum_{k=1}^{n/2} \frac{(-2)^k}{k!} \cdot \prod_{i=0}^{k-1}\left(1 - \frac{k}{n-i}\right) = -\sum_{k=1}^{n/2} \frac{(-2)^k}{k!} \cdot P(k, n).$$

For all $k \le n/2$, $0 \le P(k, n) < 1$ and for $0 < k \le n^{1/4}$, by standard estimates, uniformly $P(k, n) = 1 - k^2/n + O(n^{-1})$. Hence the last sum equals

$$\sum_{k=1}^{n^{1/4}} \frac{(-2)^k(1 + O(n^{-1}))}{k!} - \frac{1}{n}\sum_{k=1}^{n^{1/4}} \frac{k^2(-2)^k}{k!} + \sum_{n^{1/4}<k\le n/2} \frac{(-2)^k}{k!} \cdot P(k, n)$$

$$= \sum_{k=1}^{\infty} \frac{(-2)^k}{k!} + O(n^{-1}) + O(\textstyle\sum_{k>n^{1/4}} 2^k/k!)$$
$$= \mathrm{e}^{-2} - 1 + O(n^{-1})$$

and $\Pr[\pi \text{ is disconnected}] = 1 - \mathrm{e}^{-2} + O(n^{-1})$. Finally,

$$\Pr[\pi \text{ is connected}] = 1 - (1 - \mathrm{e}^{-2} + O(n^{-1})) = \mathrm{e}^{-2} + O(n^{-1})$$

and $\mathrm{cop}_n = (\mathrm{e}^{-2} + O(n^{-1})) \cdot n!$. $\square$

Theorems 3.5 and 4.3 give the asymptotics of Com_n.

Corollary 4.4 *For $n \to \infty$,*

$$\mathrm{Com}_n = [x^n] \left(\sum_{n=1}^{\infty} n! x^n \right)^{\langle -1 \rangle} = (-\mathrm{e}^{-2} + O(n^{-1})) \cdot n!.$$

To obtain asymptotics of some combinatorially defined numbers, one usually applies to their generating function analytic and algebraic methods. In the derivation of Corollary 4.4 we proceeded the other way around — we obtained asymptotics of the coefficients of a power series by using their combinatorial representation.

5 Non-P-recursiveness

A sequence of numbers $(a_n)_{n\geq 0}$ is called P-recursive if it satisfies a linear recurrence with polynomial coefficients. A power series is called D-finite if it satisfies a linear differential equation with polynomial coefficients. A sequence $(a_n)_{n\geq 0}$ is P-recursive if and only if its ogf $A(x) = \sum_{n\geq 0} a_n x^n$ is D-finite. More information on D-finiteness and P-recursiveness can be found in Stanley [30, Chapter 6]. If $a_n = n!$ then $a_n - n a_{n-1} = 0$ for $n \in \mathbf{N}$, $a_0 = 1$, and thus $(n!)_{n\geq 0}$ is P-recursive. We show that on the other hand neither $(\mathrm{ip}_n)_{n\geq 0}$ nor $(\mathrm{cop}_n)_{n\geq 0}$ is P-recursive. By Theorem 3.5, instead of the latter sequence we can work with $(\mathrm{Com}_n)_{n\geq 0}$.

Proposition 5.1 *The power series $I(x) = \sum_{n\geq 1} \mathrm{ip}_n x^n = x + x^2 + 4x^3 + \cdots$ and $\psi(x) = \varphi(x)^{\langle -1 \rangle} = \sum_{n\geq 1} \mathrm{Com}_n x^n = x - 2x^2 + 2x^3 - \cdots$ satisfy the differential equations*

$$I' = -x^{-2} I^2 + (x^{-2} + x^{-1}) I - x^{-1} \quad \textit{and} \quad \psi' = \frac{\psi^2}{x - (1+x)\psi}.$$

Proof. It follows from the recurrence for $n!$ that $\varphi(x) = \sum_{n\geq 1} n!x^n$ satisfies $x + x\varphi + x^2\varphi' = \varphi$. Thus $\varphi' = ((1-x)\varphi - x)/x^2$. Combining this with $\varphi = I/(1-I)$ (Theorem 2.2), we obtain the differential equation for $I(x)$. Similarly, $\psi' = 1/\varphi'(\psi) = \psi^2/((1-\psi)x-\psi)$ which is the differential equation for $\psi(x)$. $\square$

In Klazar [17] we used the following method to show that $(a_n)_{n\geq 0}$ is not P-recursive. Suppose that the ogf $A(x)$ is nonanalytic and satisfies a first order differential equation $A' = R(x, A)$ where R is some expression. Differentiating it and replacing A' by $R(x, A)$, we express the derivatives of A as $A^{(k)} = R_k(x, A)$; $R_0(x, A) = A$ and $R_1(x, A) = R(x, A)$. Substituting $R_k(x, A)$ in the equation of D-finiteness

$$b_0A + b_1A' + b_2A'' + \cdots + b_sA^{(s)} = 0,$$

where $s \geq 1$, $b_i \in \mathbf{C}(x)$ and $b_s \neq 0$, we get a non-differential equation $\sum_{k=0}^{s} b_kR_k(x, A) = 0$. If R is such that the expressions $R_0, R_1, R_2, \ldots$ are (i) analytic or even algebraic and (ii) linearly independent over $\mathbf{C}(x)$, we have a nontrivial analytic equation for A. This implies, see [17] for more details, that A is analytic, which is a contradiction. So A cannot be D-finite and the sequence of its coefficients cannot be P-recursive.

To state the result of [17] precisely, we remind the reader that a power series $R(x, y) \in \mathbf{C}[[x, y]]$ is analytic if it absolutely converges in a neighborhood of the origin and that $R(x, y) \in \mathbf{C}((x, y))$ is an analytic Laurent series if, for some $k \in \mathbf{N}$, $(xy)^kR(x, y) \in \mathbf{C}[[x, y]]$ is analytic. Theorem 1 of [17] says that if $A \in \mathbf{C}[[x]]$ is nonanalytic, $R(x, y) \in \mathbf{C}((x, y))$ is analytic, $A' = R(x, A)$, and R contains at least one monomial ax^iy^j, $a \neq 0$, with $j < 0$, then A is not D-finite. This result applies directly neither to $I(x)$ nor $\psi(x)$ (see Proposition 5.1) because in the case of $I(x)$ the last condition on R is not satisfied and in the case of $\psi(x)$ the right hand side R even cannot be expanded as a Laurent series.

However, the substitution $x - (1 + x)\psi(x) = \theta(x)$ turns the second differential equation of Proposition 5.1 to

$$\theta' = -\frac{x^2}{1+x} \cdot \frac{1}{\theta} + \frac{1+2x}{1+x}.$$

Now all conditions are satisfied ($\varphi(x)$ is clearly nonanalytic which implies that $\psi(x)$ and $\theta(x)$ are nonanalytic) and thus $\theta(x)$ is not D-finite by Theorem 1 of

[17]. The dependence of $\psi(x)$ and $C(x) = \sum_{n\geq 1} \mathrm{cop}_n x^n$ on $\theta(x)$ and the fact that D-finite power series form a $\mathbf{C}(x)$-algebra ([30, Theorem 6.4.9]) show that $\psi(x)$ and $C(x)$ are not D-finite too. We conclude that the sequences $(\mathrm{Com}_n)_{n\geq 0}$ and $(\mathrm{cop}_n)_{n\geq 0}$ are not P-recursive.

We use this opportunity to complement Theorem 1 of [17] in which $R \in \mathbf{C}((x, y))$ by the following theorem which treats the case $R \in \mathbf{C}(x, y)$. Neither of the theorems subsumes the other because not every rational function in x and y can be represented by an element of $\mathbf{C}((x, y))$ (as we have seen) and, of course, not every Laurent series sums up to a rational function. However, the next theorem seems to be more useful because in both examples in [17] and both examples here the right hand side $R(x, y)$ is, in fact, a rational function.

Theorem 5.2 *Let $P, Q \in \mathbf{C}[x, y]$ be two nonzero coprime polynomials and $A \in \mathbf{C}[[x]]$ be a nonanalytic power series which satisfies the differential equation*

$$A' = \frac{P(x, A)}{Q(x, A)}.$$

If $\deg_y Q = 0$ and $\deg_y P \leq 1$ then A is, trivially, D-finite. In all remaining cases A is not D-finite.

Proof. The first claim is clear. If $\deg_y Q = 0$ and $r = \deg_y P \geq 2$ then $A' = a_0 + a_1 A + \cdots + a_r A^r$ where $a_i \in \mathbf{C}(x)$, $r \geq 2$, and $a_r \neq 0$. Differentiation by x gives

$$A^{(k)} = R_k(x, A) = a_{0,k} + a_{1,k}A + \cdots + a_{kr-k+1,k}A^{kr-k+1}$$

where $a_{i,j} \in \mathbf{C}(x)$ and

$$a_{kr-k+1,k} = r(2r-1)(3r-2)\ldots((k-1)r-k+2)a_r^k \neq 0.$$

Thus $R_k(x, y) \in \mathbf{C}(x)[y]$ have y-degrees $kr - k + 1$, $k = 0, 1, 2, \ldots$, which is for $r \geq 2$ a strictly increasing sequence. Therefore $R_0, R_1, R_2, \ldots$ are linearly independent over $\mathbf{C}(x)$ and, by the above discussion, A is not D-finite.

In the remaining case $\deg_y Q \geq 1$. Differentiation of $A' = R(x, A) = P(x, A)/Q(x, A)$ by x gives $A^{(k)} = R_k(x, A)$ where $R_k(x, y) \in \mathbf{C}(x, y)$. For example,

$$\begin{aligned} R_2 &= \frac{(P_x + P_y R_1)Q - P(Q_x + Q_y R_1)}{Q^2} \\ &= \frac{P_x Q - P Q_x}{Q^2} + \frac{P(P_y Q - P Q_y)}{Q^3}. \end{aligned}$$

Let α, $Q(x, \alpha) = 0$, be a pole of $R_1(x, y)$ of order $\mathrm{ord}_\alpha(R_1) = \mathrm{ord}_\alpha(P/Q) = -\mathrm{ord}_\alpha(Q) = l \geq 1$. We have $\mathrm{ord}_\alpha((P_xQ - PQ_x)Q^{-2}) \leq 2l$ and $\mathrm{ord}_\alpha(P(P_yQ - PQ_y)Q^{-3}) = 3l + \mathrm{ord}_\alpha(P_yQ - PQ_y) = 2l + 1$ since $\mathrm{ord}_\alpha(P) = 0$, $\mathrm{ord}_\alpha(P_yQ) \leq -l$, and $\mathrm{ord}_\alpha(PQ_y) = -l + 1$. So $\mathrm{ord}_\alpha(R_2) = 2l + 1$. In general, the same argument shows that $\mathrm{ord}_\alpha(R_{k+1}) = 2 \cdot \mathrm{ord}_\alpha(R_k) + 1$. Hence $\mathrm{ord}_\alpha(R_k) = 2^{k-1}l + 2^{k-1} - 1$, $k = 1, 2, \ldots$. This is a strictly increasing sequence and we conclude again, since $R_0, R_1, R_2, \ldots$ are linearly independent over $\mathbf{C}(x)$, that A is not D-finite. $\square$

Proposition 5.1 and Theorem 5.2 give the following corollary.

Corollary 5.3 *The sequences* $(\mathrm{ip}_n)_{n\geq 1}$, $(\mathrm{Com}_n)_{n\geq 1}$, *and* $(\mathrm{cop}_n)_{n\geq 1}$ *are not P-recursive.*

6 Congruences

By the Lagrange inversion formula (recalled at the end of Section 1),

$$\mathrm{Com}_n = \frac{1}{n}[x^{n-1}] \left(\sum_{k\geq 0} (-1)^k (2!x + 3!x^2 + \cdots)^k \right)^n .$$

We use this representation to derive modular properties of the numbers Com_n. For a prime p, let $\mathrm{ord}_p(n)$ denote the largest $m \in \mathbf{N}_0$ such that p^m divides n. It is a remarkable fact that the Comtet numbers are divisible by high powers of 2:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathrm{ord}_2(\mathrm{Com}_n)$	0	1	1	2	2	4	4	4	4	5	5	15	13	12	12

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
8	8	9	9	10	10	12	12	14	14	15	15	17	17	22

In Theorem 6.2 we give a lower bound on $\mathrm{ord}_2(\mathrm{Com}_n)$ which is tight for infinitely many n and we completely characterize the values of n for which the equality is attained.

Recall some properties of $\mathrm{ord}_p(\cdot)$: $\mathrm{ord}_p(ab) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b)$, $\mathrm{ord}_p(a + b) \geq \min(\mathrm{ord}_p(a), \mathrm{ord}_p(a))$, and $\mathrm{ord}_p(a+b) = \min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))$ whenever $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(b)$.

Lemma 6.1 *For every $m \in \mathbf{N}$,*

$$\mathrm{ord}_2((m+1)!) \geq \left\lceil \frac{m}{2} \right\rceil$$

where the equality holds iff $m = 1$ or 2. Also, $\mathrm{ord}_3(m!) \leq m-1$ for every $m \in \mathbf{N}$.

Proof. This follows from the more general formula

$$\mathrm{ord}_p(m!) = \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \cdots$$

which is well-known. In particular, $\mathrm{ord}_2(m!) = m - d(m)$ for every $m \in \mathbf{N}$, where $d(m)$ is the number of unit digits in the binary expansion of m, and the stated results on ord_2 follow. As for ord_3, $\mathrm{ord}_3(1) = 0$ and for $m \geq 2$, $\mathrm{ord}_3(m!) \leq m(1/3 + 1/3^2 + \cdots) = m/2 \leq m-1$. $\square$

Theorem 6.2 *Let $n \in \mathbf{N}$ and $m = \lfloor n/2 \rfloor$. Then*

$$\mathrm{ord}_2(\mathrm{Com}_n) \geq \left\lceil \frac{n-1}{2} \right\rceil$$

and the equality holds if and only if $\binom{3m}{m}$ is odd. In other words, the equality holds if and only if the binary expansion of m has no two consecutive unit digits.

Proof. Let the numbers b_k, $k \geq 0$, be defined by

$$\sum_{k \geq 0} b_k x^k = \sum_{k \geq 0} (-1)^k (2!x + 3!x^2 + \cdots)^k.$$

Thus $b_0 = 1$ and for $k \in \mathbf{N}$,

$$b_k = \sum_{\substack{c_1, c_2, \ldots, c_s \geq 1 \\ c_1 + c_2 + \cdots + c_s = k}} (-1)^s \cdot (c_1+1)! \cdot (c_2+1)! \cdot \ldots \cdot (c_s+1)!.$$

By the above formula for Com_n,

$$n \cdot \mathrm{Com}_n = \sum_{\substack{k_1, k_2, \ldots, k_n \geq 0 \\ k_1 + k_2 + \cdots + k_n = n-1}} b_{k_1} b_{k_2} \ldots b_{k_n}.$$

By Lemma 6.1, $\mathrm{ord}_2((c+1)!) \geq c/2$ for every $c \in \mathbf{N}$. Hence, for every $k \geq 0$ and $n \in \mathbf{N}$,

$$\mathrm{ord}_2(b_k) \geq \frac{k}{2} \quad \text{and} \quad \mathrm{ord}_2(n \cdot \mathrm{Com}_n) \geq \frac{n-1}{2}.$$

In particular, for odd n we have $\mathrm{ord}_2(\mathrm{Com}_n) = \mathrm{ord}_2(n \cdot \mathrm{Com}_n) \geq (n-1)/2$.

We claim that, more precisely,

$$\mathrm{ord}_2(b_k) \begin{cases} = k/2 & \dots \text{ for even } k \\ = (k+1)/2 & \dots \text{ for } k \equiv 1 \bmod 4 \\ > (k+1)/2 & \dots \text{ for } k \equiv 3 \bmod 4. \end{cases}$$

For the proof we look more closely at the sum for b_k. Let k be even. Then the sum has exactly one summand with ord_2 equal to $k/2$, namely that with $c_1 = c_2 = \ldots = c_{k/2} = 2$ (by Lemma 6.1, $\mathrm{ord}_2((c+1)!) = c/2$ only if $c = 2$), and the other summands have ord_2 bigger than $k/2$. Hence $\mathrm{ord}_2(b_k) = k/2$. Let k be odd. Then each summand has an odd number of odd c_i's. The summands t with three and more odd c_i's satisfy $\mathrm{ord}_2(t) \geq (k+3)/2$ (each odd c_i contributes $1/2$ to $k/2$). The same is true if t has only one odd c_i but that c_i is not 1 (by Lemma 6.1, $\mathrm{ord}_2((c+1)!) \geq (c+3)/2$ for odd $c > 1$), or if some even c_i is not 2 (Lemma 6.1). The remaining summands t, in which $c_i = 2$ with multiplicity $(k-1)/2$ and once $c_i = 1$, satisfy $\mathrm{ord}_2(t) = (k+1)/2$. We see that, for odd k, $\mathrm{ord}_2(b_k) = (k+1)/2$ iff the number of the remaining summands is odd. This number equals $(k-1)/2 + 1 = (k+1)/2$. So $\mathrm{ord}_2(b_k) = (k+1)/2$ iff k is of the form $4l+1$.

Let $n = 2m+1$ be odd. If s is a summand of the above sum for $n \cdot \mathrm{Com}_n$, then $\mathrm{ord}_2(s) = (n-1)/2$ iff all k_i in s are even; other summands t have $\mathrm{ord}_2(t) > (n-1)/2$. It follows that $\mathrm{ord}_2(\mathrm{Com}_n) = (n-1)/2$ iff the number of the former summands s is odd. This number equals

$$[x^{n-1}] \left(\sum_{r \geq 0} x^{2r} \right)^n = [x^{n-1}] \frac{1}{(1-x^2)^n} = [x^{n-1}] \sum_{r \geq 0} \binom{n+r-1}{r} x^{2r} = \binom{3m}{m}.$$

Let $n = 2m$ be even. We know that $\mathrm{ord}_2(b_k) = k/2$ for even k and $\mathrm{ord}_2(b_k) \geq (k+1)/2$ for odd k. In the sum for $n \cdot \mathrm{Com}_n$, every composition $k_1 + k_2 + \cdots + k_n = n-1$ of $n-1$ has an odd number of odd parts. For any t-tuple $l_1, l_2, \ldots, l_t$, where t and all l_i are odd and $l_1 + \cdots + l_t \leq n-1$, we let $S(l_1, l_2, \ldots, l_t)$ denote the sum of those $b_{k_1} b_{k_2} \ldots b_{k_n}$ with $k_1 + k_2 + \cdots + k_n = n-1$ in which $k_i = l_i$, $1 \leq i \leq t$, and k_i is even for $i > t$. It follows that

$$n \cdot \mathrm{Com}_n = \sum \binom{n}{t} S(l_1, l_2, \ldots, l_t)$$

where we sum over all mentioned t-tuples $l_1, l_2, \ldots, l_t$. By the properties of ord_2 and of the numbers b_k, $\mathrm{ord}_2(S(l_1, l_2, \ldots, l_t)) \geq (n+t-1)/2$. Also, for odd t we have $\mathrm{ord}_2(\binom{n}{t}) = \mathrm{ord}_2(\frac{n}{t}\binom{n-1}{t-1}) = \mathrm{ord}_2(n) - \mathrm{ord}_2(t) + \mathrm{ord}_2(\binom{n-1}{t-1}) \geq \mathrm{ord}_2(n)$, and $\mathrm{ord}_2(\binom{n}{1}) = \mathrm{ord}_2(n)$. It follows that $\mathrm{ord}_2(\mathrm{Com}_n) = n/2$ iff

$$\mathrm{ord}_2\left(\sum_{l \leq n,\, l \text{ odd}} S(l)\right) = n/2.$$

In the last sum still many summands have ord_2 bigger than $n/2$: if $l \equiv 3 \mod 4$ then $\mathrm{ord}(S(l)) > n/2$. On the other hand, if $l \equiv 1 \mod 4$ then each summand $b_l b_{k_2} \ldots b_{k_n}$ in $S(l)$ has $\mathrm{ord}_2(b_l b_{k_2} \ldots b_{k_n}) = n/2$. We conclude that $\mathrm{ord}_2(\mathrm{Com}_n) = n/2$ iff the number $c(n)$ of compositions of $n-1$ into n parts, where the first part is $\equiv 1 \mod 4$ and the remaining $n-1$ parts are even (zero parts are allowed), is odd. We have

$$\begin{aligned} c(n) &= [x^{n-1}]\frac{x}{1-x^4} \cdot \frac{1}{(1-x^2)^{n-1}} = [x^{n-1}]\frac{x}{1+x^2} \cdot \frac{1}{(1-x^2)^n} \\ &\equiv [x^{n-1}]\frac{x}{1-x^2} \cdot \frac{1}{(1-x^2)^n} = [x^{n-1}]\frac{x}{(1-x^2)^{n+1}} \mod 2 \\ &= \binom{3m-1}{m-1} \equiv \frac{3m}{m}\binom{3m-1}{m-1} \mod 2 \\ &= \binom{3m}{m}. \end{aligned}$$

It was noted by Kummer [20], see also Singmaster [28], that $\mathrm{ord}_p(\binom{a+b}{a})$ equals to the number of carries required when adding a and b represented by p-ary expansions. Applying this for $p = 2$, $a = m$, and $b = 2m$, we get the stated criterion. $\square$

Corollary 6.3 *For every $n \in \mathbf{N}$, $n \geq 3$,*

$$\mathrm{cop}_n \equiv \begin{cases} 2 \mod 2^{(n-1)/2} & \text{for odd } n \\ -2 \mod 2^{n/2} & \text{for even } n. \end{cases}$$

$\square$

Let

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

be the nth Catalan number.

Proposition 6.4 *For every $n \in \mathbf{N}$,*

$$\mathrm{Com}_n \equiv C_{n-1} \bmod 3.$$

Proof. Let $n \in \mathbf{N}$. We have, for every $k \in \mathbf{N}_0$,

$$(2!x + 3!x^2 + \cdots)^k = (2x)^k + 3a_k(x)$$

with $a_k(x) \in \mathbf{Z}[[x]]$. Thus

$$\begin{aligned}\sum_{k\geq 0}(-1)^k(2!x + 3!x^2 + \cdots)^k &= \frac{1}{1+2x} + 3\sum_{k\geq 0}(-1)^k a_k(x) \\ &= \frac{1}{1+2x} + 3b(x)\end{aligned}$$

with $b(x) \in \mathbf{Z}[[x]]$. Let $m = \mathrm{ord}_3(n)$. Since $\mathrm{ord}_3(k!) \leq k-1$ for every $k \in \mathbf{N}$ (Lemma 6.1), we have

$$\mathrm{ord}_3\Big(3^k\tbinom{n}{k}\Big) \geq m+1 \text{ for } k = 1, 2, \ldots, n.$$

By the above formula for Com_n,

$$\begin{aligned}n \cdot \mathrm{Com}_n = [x^{n-1}]\left(\frac{1}{1+2x} + 3b(x)\right)^n &\equiv [x^{n-1}]\frac{1}{(1+2x)^n} \bmod 3^{m+1} \\ &= (-2)^{n-1}\binom{2n-2}{n-1}.\end{aligned}$$

Canceling in the last congruence the common factor 3^m, we get

$$\frac{n}{3^m} \cdot \mathrm{Com}_n \equiv \frac{(-2)^{n-1}}{3^m}\binom{2n-2}{n-1} \equiv \frac{1}{3^m}\binom{2n-2}{n-1} \bmod 3.$$

Since $n/3^m \not\equiv 0 \bmod 3$, we can divide by it and get

$$\mathrm{Com}_n \equiv \frac{1}{n}\binom{2n-2}{n-1} \bmod 3.$$

□

Corollary 6.5 *For every $n \in \mathbf{N}$, $n > 2$,*

$$\mathrm{cop}_n \equiv -C_{n-1} + (-1)^n \bmod 3.$$

□

References

[1] M. Aguiar and F. Sottile, Structure of the Malvenuto–Reutenauer Hopf algebra of permutations, `Archiv:math.CO/0203282`.

[2] M. D. Atkinson, M. M. Murphy and N. Ruškuc, Partially well-ordered closed sets of permutations, *J. of Order,* **19** (2002), 101–113.

[3] M. D. Atkinson and T. Stitt, Restricted permutations and the wreath product, *Discrete Math.,* **259** (2002), 19–36.

[4] J. Chaves and R. Noguiera, Spectral properties of interval exchange maps, *Monatsh. Math.,* **134** (2001), 89–102.

[5] L. Comtet, Sur les coefficients de l'inverse de la série formelle $\sum n!t^n$, *C. R. Acad. Sci., Paris, Sér. A,* **275** (1972), 569–572.

[6] L. Comtet, *Advanced Combinatorics,* D. Reidel Publ. Co., Boston, MA, 1974.

[7] C. R. de Oliveira and C. Gutierrez, Almost periodic Schrödinger operators along interval exchange transformations, preprint, 12 pages, 2002.

[8] G. Duchamp, F. Hivert and J.-Y. Thibon, Noncommutative symmetric functions VI: Free quasi-symmetric functions and related algebras, `Archiv:math.CO/0105065`.

[9] P. Flajolet and R. Sedgewick, Analytic Combinatorics — Symbolic Combinatorics, preprint, 2002, 186 pages; available at `http://pauillac.inria.fr/algo/flajolet/Publications/`

[10] J. Galambos and I. Simonelli, *Bonferroni-type Inequalities with Applications,* Springer-Verlag, 1996, Berlin.

[11] I. M. Gessel and R. P. Stanley, Algebraic enumeration. In: R. L. Graham, M. Grötschel and L. Lovász (ed.), *Handbook of Combinatorics, Volume II,* North-Holland, Amsterdam, 1995; pp. 1021–1061.

[12] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration,* John Wiley & Sons, New York, 1983.

[13] T. KAISER AND M. KLAZAR, On growth rates of hereditary permutation classes, submitted, 2002.

[14] M. KEANE, Interval exchange transformations, *Math. Z.,* **141** (1975), 25–31.

[15] A. KING, *Transposition Gray codes for indecomposable permutations*, B.Sc. honours thesis, University of Victoria, Canada, 2002; available at `http://www.cs.toronto.edu/~king`

[16] M. KLAZAR, Twelve countings with rooted plane trees, *European J. Comb.,* **18** (1997), 195–210. Addendum, *ibidem*, **18** (1997), 739–740.

[17] M. KLAZAR, Non-P-recursiveness of numbers of matchings or linear chord diagrams with many crossings, *Adv. Appl. Math.,* **30** (2003), 126–136.

[18] D. E. KNUTH, *The Art of Computer Programming*, pre-fascicle 2b, a draft of section 7.2.1.2: generating all permutations, 58 pages, available at `http://www-cs-faculty.Stanford.EDU/~knuth/`

[19] M. KONTSEVICH AND A. ZORICH, Connected components of the moduli spaces of Abelian differentials with prescribed singularities, `Archiv:math.GT/0201292`.

[20] E. E. KUMMER, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgezetzen, *J. Reine Angew. Math.,* **44** (1852), 93–146.

[21] L. LOVÁSZ, *Combinatorial Problems and Exercises,* Akadémiai Kiadó, Budapest, 1993.

[22] H. MASUR, Interval exchange transformations and measured foliations, *Ann. Math.,* **115** (1982), 169–200.

[23] A. M. ODLYZKO, Asymptotic enumeration methods. In: R. L. Graham, M. Grötschel and L. Lovász (ed.), *Handbook of Combinatorics, Volume II,* North-Holland, Amsterdam, 1995; pp. 1063–1229.

[24] P. OSSONA DE MENDEZ AND P. ROSENSTIEHL, Connected permutations and hypermaps, Tech. Report 183, CAMS, 1999.

[25] L. Panaitopol, A formula for $\pi(x)$ applied to a result of Koninck-Ivič, *Nieuw. Arch. Wiskd (5),* **1** (2000), 55–56.

[26] S. Poirier and C. Reutenauer, Algèbre de Hopf des tableaux, *Ann. Sci. Math. Québec,* **19** (1995), 79–90.

[27] G. Rauzy, Echanges d'intervalles et transformations induites, *Acta Arith.,* **34** (1979), 315–328.

[28] D. Singmaster, Notes on binomial coefficients. I. A generalization of Lucas' congruence, *J. London Math. Soc.,* **8 (2)** (1974), 545–548.

[29] N. J. A. Sloane (2000), The On-Line Encyclopedia of Integer Sequences, published electronically at `http://www.research.att.com/~njas/sequences/`.

[30] R. P. Stanley, *Enumerative Combinatorics. Volume II,* Cambridge University Press, Cambridge, UK, 1999.

[31] W. A. Veech, Gauss measures for transformations on the space of interval exchange maps, *Ann. Math.,* **115** (1982), 201–242.

[32] L. Vuillon, On the number of return words in infinite words with complexity $2n+1$, `Archiv:math.CO/0009094`.