ON THE CYCLIC DENSITY OF SYMMETRIC GROUPS

ADAM MARKS

Abstract. We define the *cyclic density* of a finite group, an intrinsic measurement of cyclic subgroup entanglement, and consider limits of this value in infinite sequences of finite group classes. For symmetric groups, we develop a computational process for calculating cyclic density and generate evidence suggesting that the density converges to zero.

Introduction

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group of order n, and let k be the minimum positive integer for which $g_i^k = g_i$ for all $g_i \in G$. $k = \text{LCM}\{|\langle g_i \rangle|\}$. Begin by constructing the *full cycle table* of G, in matrix form, $F = [g_{i,j}]_{n \times k}$ where $g_{i,j} = g_i^j$. Each row is a cyclic subgroup of G, but not all rows correspond to distinct subgroups; they are generally intertwined by sharing elements.

Let $\mathscr{C}(G)$ be the family of cyclic subgroups of G, partially ordered in the natural way by inclusion: $I, J \in \mathscr{C}(G)$ are comparable if $I \subseteq J$ or $J \subseteq I$, and incomparable otherwise. Collapsing all comparable rows of F so that each member of $\mathscr{C}(G)$ corresponds to a single row, we find the *reduced cycle table* $R = [x_{i,j}]_{w \times k}$ where the rows form a maximum antichain of $\mathscr{C}(G)$. We call the number of rows of R the *cyclic width* of G, $w(G)$; it is equal to the width of the poset. Finally, we define the *cyclic density* of G to be the certain ratio

$$den(G) = \frac{w(G)}{|G|}.$$

Obviously, $0 < den(G) \leq 1$.

Basic densities

Consider the cyclic densities of some basic families of finite groups. Let C_n denote the cyclic group of order n, D_n the dihedral group of order $2n$, and C_2^n the direct product of n copies of C_2. Using the Shanks *cycle graph* visualization [Shanks 2001], Figure 1 depicts the examples C_2, C_2^2, S_3, and D_4. In the Shanks cycle graph, the cyclic width is the number of *lobes* emanating from the neutral element.

So $den(C_2) = 1/2$, $den(C_2^2) = 3/4$, $den(S_3) = 2/3$, and $den(D_4) = 5/8$. And in general,

$$den(C_n) = \frac{1}{n}, \qquad den(D_n) = \frac{n+1}{2n}, \qquad den(C_2^n) = \frac{2^n - 1}{2^n}.$$

Date: v20 August 5, 2018.

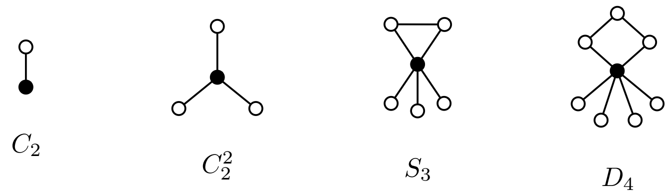


FIGURE 1. Some small cycle graphs

Thus considering *sequences* of finite groups and their corresponding sequences of cyclic densities, we have

$$den(C_n) \to 0, \qquad den(D_n) \to \frac{1}{2}, \qquad den(C_2^n) \to 1$$

in their limits as $n \to \infty$.

We can slightly improve the bounds on $den(G)$ for an arbitrary group G:

Lemma 1. *If G is a finite group of order n,*

$$\frac{1}{n} \leq den(G) \leq \frac{(\log_2 n) - 1}{\log_2 n}.$$

Proof. The cyclic group C_k has the minimum possible number of incomparable cyclic subroups, one. And the direct product C_2^k has the maximum possible number of incomparable cyclic subgroups – every element besides the neutral element has order two and generates a cyclic subgroup that is incomparable to the subgroup generated by every other element, except its inverse and the neutral element. If G is isomorphic to C_k then $k = n$. And if G is isomorphic to C_2^k then $n = 2^k$ so $k = \log_2 n$.

Thus

$$den(C_n) \leq den(G) \leq den(C_2^{\log_2 n})$$

and

$$\frac{1}{n} \leq den(G) \leq \frac{(\log_2 n) - 1}{\log_2 n}.$$

□

THE CYCLE TYPE ORDER OF SYMMETRIC GROUPS

The cycle graphs of S_4 and S_5 are relatively simple, since incomparable cyclic subgroups in $\mathscr{C}(S_n)$ for these groups are not very interleaved - they share only the neutral element of the group. The situation begins to change with S_6, as depicted in Figure 2.

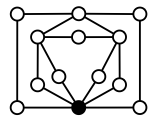


FIGURE 2. Intertwinement of cyclic subgroups $\langle(1,2,3,4,5,6)\rangle$, $\langle(1,6,3,2,5,4)\rangle$, and $\langle(1,3,2,4,6,5)\rangle$

We investigate the behavior of $den(S_n)$ as $n \to \infty$, first describing the mechanics of conjugacy class powers, in pursuit of a formula for $den(S_n)$.

Let $S = S_n$, $\mathscr{C} = \mathscr{C}(S_n)$, and let $T = T_n$ be the set of conjugacy classes of S. We think of T as the *types* of S, identifying a class $t \in T$ with its number of cycles of each length for lengths $1..n$. Using the [Sagan 2010] notation, $t = [1^{a_1}, 2^{a_2}, \ldots, n^{a_n}]$ wherein t has a_i cycles of length i. Obviously, each type can also be regarded as an integer partition of n.

Definition 1. *Let type* : $S \to T$ *map a group element to its type. If* $type(g) = t$, $g \in t$.

Definition 2. *Let* (i^k) *denote the member of* T *that composes* k *cycles of length* i, *with* $(i^1) = (i)$.

For example in S_6, both $(1,4)(2,5)(3,6)$ and $(1,2)(3,4)(5,6)$ have type (2^3) in cycle type notation or $[1^0, 2^3, 3^0, 4^0, 5^0, 6^0]$ in Sagan notation.

Definition 3. *Let* $(l_1^{a_1})(l_2^{a_2})\ldots(l_m^{a_m}) \in T$ *denote a type composed of cycle lengths* $l_1 \ldots l_m \in 1 \ldots n$ *with multiplicities* $a_1 \ldots a_m$. *Define the canonical form of a type as its unique form* $(l_1^{a_1})(l_2^{a_2})\ldots(l_m^{a_m})$ *with* $l_i < l_{i+1}$, *and* $(l_i^{a_i})$ *omitted if* $l_i = 1$ *or* $a_i = 0$.

For example in S_{14},

$$\begin{aligned} g &= (1,2)(3,4,5)(6,7,8)(10,11,12,13,14) \\ type(g) &= [1^1, 2^1, 3^2, 4^0, 5^1, 6^0, 7^0, 8^0, 9^0, 10^0, 11^0, 12^0, 13^0, 14^0] \\ &= (1^1)(2^1)(3^2)(5^1) = (2)(3^2)(5). \end{aligned}$$

Lemma 2. *If* $g, h \in S$, $k \geq 0$, *and* $type(g) = type(h)$, *then* $type(g^k) = type(h^k)$.

Proof. Since g and h have the same type, they are conjugates, and there exists $i \in S$ with $g = ihi^{-1}$. Then,

$$g^k = \underbrace{(ihi^{-1})(ihi^{-1})...(ihi^{-1})}_{k \text{ times}} = ih^k i^{-1},$$

and so g^k and h^k are conjugates and $type(g^k) = type(h^k)$. □

Definition 4. *For a type* $t \in T$ *and integer* $k \geq 0$, *let* $t^k = type(g^k)$ *for any representative* $g \in t$.

By Lemma 2, t^k is well-defined, having the same value regardless of which representative from the conjugacy class is chosen. In other words, $[type(g)]^k = type(g^k)$ for all $g \in S$. So the diagram,

$$\begin{array}{ccc} S & \xrightarrow{type} & T \\ {\scriptstyle p_k}\downarrow & & \downarrow{\scriptstyle q_k} \\ S & \xrightarrow[type]{} & T \end{array}$$

commutes, where $k \geq 0$, $p_k : S \to S$ is the power map on group elements, $p_k(g) = g^k$, and $q_k : T \to T$ is the power map on types, $q_k(t) = t^k$.

Continuing the example from Figure 2, we have, $(6)^2 = (3^2)$ since $(1, 2, 3, 4, 5, 6)^2 = (1, 3, 5)(2, 4, 6)$.

Lemma 3. $(t^m)^n = t^{mn}$.

Proof. $type \circ q_m \circ q_n = p_m \circ p_n \circ type = p_{mn} \circ type$. □

Let (a, b) denote the greatest common divisor of a and b.

Lemma 4. *For a type with singular cycle length $i \in 1 \ldots n$ and positive integer k,*

$$\left(i\right)^k = \left(\frac{i}{(i,k)}^{(i,k)}\right).$$

Proof. Let $(x) = (x_1, \ldots, x_i)$ be a cycle of length i, and consider the effect of composing (x) with itself k times. We consider the following cases.

1) If $i|k$, then $(i, k) = i$, and (x) is neutralized, becoming i fixed points:

$$(x_1, \ldots..., x_i)^k = (x_1) \ldots (x_i),$$

thus, $(x_i) = (1^i) = \left(\frac{i}{(i,k)}^{(i,k)}\right)$.

2) Alternatively, if $k|i$, then $(i, k) = k$, and $i = jk$ for some positive integer j. Then,

$$\begin{aligned}(x_1, \ldots, x_i)^k &= (x_{1,1}, \ldots, x_{1,k}, x_{2,1}, \ldots, x_{2,k}, \ldots, x_{j,1}, \ldots, x_{j,k})^k \\ &= (x_{1,1}, x_{2,1}, \ldots, x_{j,1})(x_{1,2}, x_{2,2}, \ldots, x_{j,2}) \ldots (x_{1,k}, \ldots, x_{j,k}).\end{aligned}$$

That is, (x) is split into k cycles of length i/k, and so $(i)^k = (\frac{i}{k}^k) = \left(\frac{i}{(i,k)}^{(i,k)}\right)$.

3) If $i \nmid k$ and $k \nmid i$, consider the two subcases:

3a) If $(i, k) = 1$, i and k are relatively prime and $(x)^k$ remains a single cycle of length i, so $(i)^k = (i^1) = \left(\frac{i}{(i,k)}^{(i,k)}\right)$.

3b) If $(i, k) > 1$, say $(i, k) = j$ and let $i = aj$ and $k = bj$ for positive positive integers a and b. Writing (x) as a matrix with a rows of length j,

$$\begin{bmatrix} x_{1,1} & x_{1,2} & \dots & x_{1,j} \\ x_{2,1} & x_{2,2} & \dots & x_{2,j} \\ \vdots & \vdots & \ddots & \vdots \\ x_{a,1} & x_{a,2} & \dots & x_{a,j} \end{bmatrix},$$

we see that on $k = bj$ iterations we step down b mod a rows, each column becoming a separate cycle of length a. Since there are j cycles, we have $(i)^k = (a^j) = \left(\frac{i}{(i,k)}^{(i,k)}\right)$. □

We say that (i) is *absorbed*, *preserved*, or *split* when raised to a power.

Corollary 1. *For a type with singular cycle length $i \in 1 \dots n$, multiplicity m, and a positive integer k,*

$$\left(i^m\right)^k = \left(\frac{i}{(i,k)}^{(i,k)m}\right).$$

Proof. Apply Lemma 4 to each cycle. □

Now that we can compute powers of types in T, we define the type poset.

Definition 5. *Let $\leq$ operate on T, such that for $a, b \in T$, $b \leq a$ if and only if there exists $k > 0$ with $b = a^k$.*

In order to prove that $\leq$ is a partial order on T, we shall need one further concept regarding the mechanics of powers in T, the cycle type *fingerprint*.

Let P be the list of initial primes, taken into a matrix at stride n. That is, $P = [p_{i,j}]$ is the $n \times n$ matrix filled with the first n^2 prime numbers, filled top to bottom, left to right.

Let $a = [1^{a_1}, \dots, n^{a_n}] \in T$, and let M_a be the $n \times n$ matrix of bits, a cell $m_{i,j} = 1$ if and only if $i \leq a_j$, and $m_{i,j} = 0$ otherwise. We use M_a as a mask and assign a unique numeric identifier to a by multiplying all of the unmasked primes in P. Specifically,

Definition 6. *Let $f : T \to \mathbb{N}$,*

$$f(a) = \prod_{\substack{i,j \in 1 \dots n \\ m_{i,j}=1}} p_{i,j}.$$

$f(a)$ is the fingerprint *of a.*

Lemma 5. *If $a \leq b$ in T, $f(a) \leq f(b)$.*

Proof. Since $a \leq b$, there exists $k > 0$ with $a = b^k$. Since under the power map of k, each cycle in b is preserved, split, or absorbed into smaller cycles, positive cells move only to the left going from M_b to M_a, masking larger primes in P and unmasking smaller ones. And since the number of positive cells remains constant at n, the product $f(a)$ must be no greater than the product $f(b)$. □

Lemma 6. *f is injective.*

Proof. Since each cell in the fingerprint matrix corresponds to a unique prime, the product of every possible subset of cells is unique. □

Theorem 1. *$(T, \leq)$ is a partially ordered set.*

Proof. Let $a, b, c \in T$.

(Reflexivity) $a^1 = a$, hence $a \leq a$.

(Transitivity) Suppose $a \leq b$ and $b \leq c$. Then there exist $m, n > 0$ with $a = b^m$ and $b = c^n$. Then $a = b^m = (c^n)^m = c^{mn}$ by Lemma 3, so $a \leq c$.

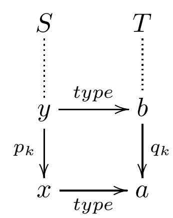
(Antisymmetry) Suppose $a \leq b$ and $b \leq a$. Then $f(a) \leq f(b)$ and $f(b) \leq f(a)$ by Lemma 5. Hence $f(a) = f(b)$ and by Lemma 6, $a = b$. □

The Cyclic Density of Symmetric Groups

Using the type order, we can calculate the cyclic width of S without resorting to constructing its full cycle table.

Lemma 7. *If $a < b$ in T and $x \in S$ with type$(x) = a$, then there exists $y \in S$ with $\langle x \rangle \subset \langle y \rangle$ and type$(y) = b$.*

Proof. Since $a < b$, there exists $k > 1$ with $a = b^k$. Let $Z = \{z^k : z \in b\}$, which is nonempty since S is symmetric. Let $z \in Z$. Since z^k and x have the same type (and S is symmetric), they are conjugate, so there exists $w \in S$ such that $x = wz^k w^{-1}$. Then letting $y = wzw^{-1}$, we have $y^k = (wzw^{-1})^k = wz^k w^{-1} = x$, so $\langle x \rangle \subseteq \langle y \rangle$. And since $k > 1$, the containment is proper, $\langle x \rangle \subset \langle y \rangle$.



□

Lemma 8. *Let $x \in S$. $\langle x \rangle$ is maximal in $\mathscr{C}$ if and only if type(x) is maximal in T.*

Proof. Suppose $\langle x \rangle$ is maximal in $\mathscr{C}$ and suppose *type*(x) is not maximal in T. Then there exists $t \in T$ with *type*$(x) < t$, and by Lemma 7, there exists $y \in S$ with $\langle x \rangle \subset \langle y \rangle$, a contradiction since $\langle x \rangle$ is maximal in $\mathscr{C}$.

Conversely, suppose *type*(x) is maximal in T, and suppose $\langle x \rangle$ is not maximal in $\mathscr{C}$, so there exists $y \neq x$, $\langle x \rangle \subseteq \langle y \rangle$. Then there exists $k > 1$ such that $x = y^k$, so *type*$(x) =$ *type*$(y^k) =$ *type*$(y)^k$. Then *type*$(x) <$ *type*(y), a contradiction since *type*(x) is maximal. □

Definition 7. *For a type $t \in T$, let $||t||$ be the order of group elements with type t.*

If $t = [1^{t_1}, \ldots, n^{t_n}]$, then $||t|| = LCM\{i : t_i > 0\}$. Let φ be the totient function.

Lemma 9. *Let z be a maximal type in T. Let w_z be the number of maximal members of $\mathscr{C}$ generated by elements of type z. Then*

$$w_z = \frac{|z|}{\varphi(||z||)}.$$

Proof. Let $z = \{x_1, \ldots, x_q\}$, and consider $\{\langle x_1 \rangle, \ldots, \langle x_q \rangle\}$. By Lemma 8, each $\langle x_i \rangle$ is maximal in $\mathscr{C}$, so $w_z = |\{\langle x_1 \rangle, \ldots, \langle x_q \rangle\}|$. Hence the value of w_z depends on which $\langle x_i \rangle$ are distinct.

Let $r = \varphi(||z||)$ and let $\{k_1, \ldots, k_r\}$ be the totatives of $||z||$. For each x_i, $\langle x_i^{k_1} \rangle = \ldots = \langle x_i^{k_r} \rangle$, since $k_j \nmid |x_i| = ||z||$. Hence $w_z \leq \frac{|z|}{\varphi(||z||)}$.

Furthermore, if $\langle x_i \rangle = \langle x_j \rangle$, $i \neq j$, then $x_j = x_i^k$ for some $k > 1$ and since $\langle x_j \rangle$ is maximal, k is a totative of $|x_i| = ||z||$. Thus $w_z \geq \frac{|z|}{\varphi(||z||)}$.

□

Lemma 10. *Let $W = \{\langle x_1 \rangle, \ldots, \langle x_w \rangle\}$ be the maximal members of $\mathscr{C}$. Then $w(S) = w$.*

Proof. Since each $\langle x_i \rangle$ is maximal in $\mathscr{C}$, each pair $\langle x_i \rangle, \langle x_j \rangle$ is incomparable, hence W is an antichain. And since W contains *all* maximal members of $\mathscr{C}$, there is no antichain in $\mathscr{C}$ of greater length. □

Theorem 2. *Let $z_1, \ldots, z_d$ be the maximal types in T. Then*

$$w(S) = \sum_{i \in 1 \ldots d} \frac{|z_i|}{\varphi(||z_i||)}$$

Proof. Let

$$W = \{\underbrace{\langle x_{1,1} \rangle, \ldots, \langle x_{1,w_1} \rangle}_{\text{type } z_1}, \underbrace{\langle x_{2,1} \rangle, \ldots, \langle x_{2,w_2} \rangle}_{\text{type } z_2}, \ldots, \underbrace{\langle x_{d,1} \rangle, \ldots, \langle x_{d,w_d} \rangle}_{\text{type } z_d}\}$$

be the maximal members of $\mathscr{C}$, grouped by type, with the grouping for type z_i having w_i items. By Lemma 9, for each i,

$$w_i = \frac{|z_i|}{\varphi(||z_i||)},$$

and by Lemma 10, their sum is $w(S)$. □

The cardinality of a type $t = [1^{t_1}, \ldots, n^{t_n}]$ is given by

$$|t| = \frac{n!}{1^{t_1} t_1! 2^{t_2} t_2! \cdots n^{t_n} t_n!}$$

[Sagan 2010], and finally then our computation of the cyclic density of S_n is completed:

Corollary 2.

$$den(S_n) = \frac{w(S_n)}{n!}.$$

The first eighty members of the sequence $\{den(S_n)\}$ are shown in Figure 3 and Table 1, computed using this type-order counting method. This algorithm is exponential in both time and space complexity. In future work, we hope to improve the algorithm by leveraging T_n in the calculation of T_{n+1}, and to prove that $den(S_n) \to 0$.

FIGURE 3. $den(S_n)$

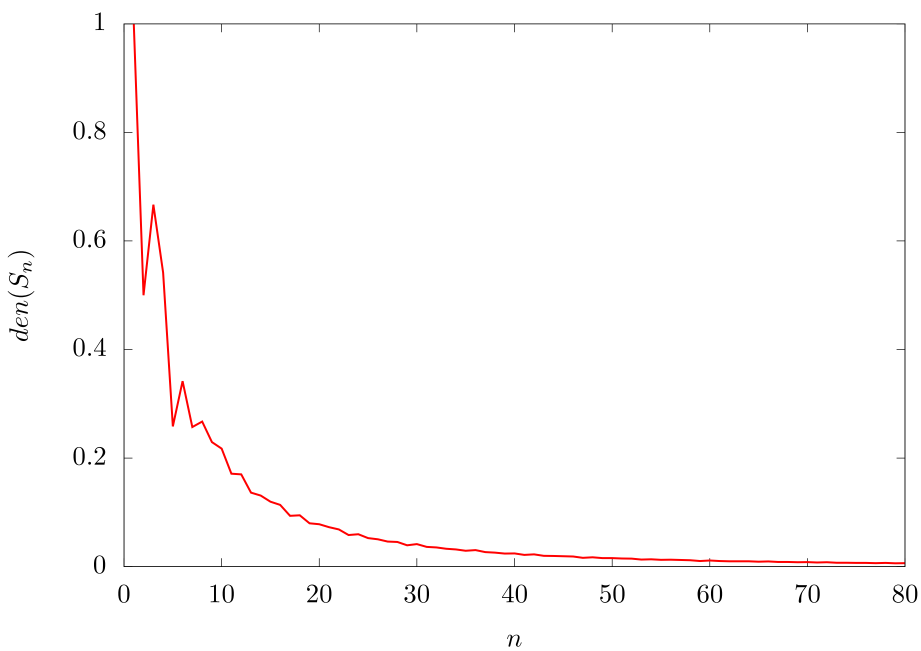


Table 1. Cyclic densities of small symmetric groups.

n	$w(S_n)$	$\sim den(S_n)$
1	1	1
2	1	0.5
3	4	0.6666
4	13	0.5416
5	31	0.2583
6	246	0.3416
7	1296	0.2571
8	10774	0.2672
9	83238	0.2293
10	788820	0.2173
11	6835170	0.1712
12	81364944	0.1698
13	848378532	0.1362
14	11423650616	0.1310
15	156289508025	0.1195
16	2380629720720	0.1137
17	33284133330760	0.0935
18	605934954285120	0.0946
19	9708364832948820	0.0798
20	190330953679235040	0.0782
21	3715069138923234960	0.0727
22	77101583995105472880	0.0685
23	1506549946554254503440	0.0582
24	37085926496811294533760	0.0597
25	813989318776589220602400	0.0524
26	20286724694924822693488800	0.0503
27	503710829808452894892841200	0.0462
28	13887195057050218869166488000	0.0455
29	348272721955775727439932808800	0.0393
30	11013343418113167554927377927200	0.0415
31	299525866629875593570738065758400	0.0364
32	9322826183877867484327026191424000	0.0354
33	286763650660486041097115373721689600	0.0330
34	9371817964591207598535556216967481600	0.0317
35	301268566995597210504803720693407822080	0.0291
36	11326316038352132010680884583190572789760	0.0304
37	368881447472189915401630493345851845972480	0.0268
38	13444922248316538295622839278511900989335040	0.0257
39	491421461275132665706920117858844810311878400	0.0240
40	19857709075853485176201075522751818794029578240	0.0243
41	719055699279594212207796715169675340608369940480	0.0214
42	31611884406214794110428530253504975830662873702400	0.0224
43	1206105162663567514746833472751365795076522663925760	0.0199
44	52377614870443718611384480162093712567870225487943680	0.0197
45	2303400843384995796208525457718657670456239109987123200	0.0192
46	102313631394535209559802424760527485279978570527215513600	0.0185
47	4220859784185577604289114922955343578697260749966826112000	0.0163
48	213966495849606562024253813099938025025661094258449891737600	0.0172
49	9552008913521138192380098130788166735170057346027730331648000	0.0157
50	479666661063419920512399022748484421688812728225741115152384000	0.0157
51	23100816947839245714566716383990394137898561470289970170318848000	0.0148
52	1185638738875026721324817542909215763200399220216081803153960960000	0.0146
53	55578525410829379267534275065417768858370142242619681448575125504000	0.0130
54	3114321293813311569201949556789675050245392967947295230178818623488000	0.0134
55	159872427264540547525642910182336743973417102827576918276715753651200000	0.0125
56	9119377122303799191154944492097727892119800625825096920740616076697600000	0.0128
57	493221942197043298744535425382727610803619200955519310432300459476862976000	0.0121
58	27653295674688959597881092447622663471357639530052458448788479717132673024000	0.0117
59	1446452047820216000735291994550847225570252963429248752920656008847563595776000	0.0104
60	94668861200165803011793930744908641725380487692270747100283011675044972380160000	0.0113
61	5186700108224280630903445738626466108430127147133118396880674834791450293043200000	0.0102
62	312035350820025500282426252619721562500633723620316522033652183840781223584116736000	0.0099
63	19261366285690477779593318059665275599762807345400873574396706814641734538407290880000	0.0097
64	1234985722704918748608184514810183020767106604477143192369635345049810587251893862400000	0.0097
65	74943853302723584976140271690579504230005839074962794571965670948894221752352041533440000	0.0090
66	5213216769369230988116269349072724168330393991338481274634380003909419257234602313646080000	0.0095
67	314249064867514123059668985200848396090875728907530495730136143032028522080088104047804416000	0.0086
68	21167694898911430218656977395884662983490413526923089315334362754791165456135511127129325568000	0.0085
69	1394825770653687764513214754414684459621541144582425878016418968487712313981001126158740553728000	0.0081
70	100517294790035665535955661469674549563259116410839166649194388636593262426139148114055344160768000	0.0083
71	6420148446302318094946571129858662083507141618573344958548451210043776827493453913239484216639488000	0.0075
72	491497661462211521276690162446806857000849921622694006842368970131582899145863211422809305601540096000	0.0080
73	32235232323001996058924745207702135463690102493724140099479462022862300446677820296106187042710421504000	0.0072
74	2328697268051059033054785926285587081087638766090349959473601489001912590389261251560846213401761808384000	0.0070
75	171023529103156868592891169295392525725993923425628519031884249274819794477262876933959357510321403985920000	0.0068
76	13026767343370529518250692684337901462730263222056175244651826403068706799655674167847417843050192851435520000	0.0069
77	933327102502100403459003557072229765325014439189347729006821802398478741654507067544514582844261177133629440000	0.0064
78	76527997967861689941598350174602884008742173397787323359769090311208325726251064162203479686794080298942464000000	0.0067
79	5474091191314163573534751617507999348870885886793680702561943978892614213152647944068775448110882997148349562880000	0.0061
80	454361649078287790075667944495073000843750924912610155800436185656638484848606413964401437866760528147637715599360000	0.0063

References

[1] A. Marks. *den* software package. 2018. https://github.com/adam1/math/tree/master/symmetric_groups/den

[2] B. Sagan. *The Symmetric Group, Representations, Combinatorial Algorithms, and Symmetric Functions*. Springer-Verlag New York, Inc. 2010.

[3] D. Shanks. *Solved and Unsolved Problems in Number Theory.* American Mathematical Society. 2001.