GROUPOID CARDINALITY AND RANDOM PERMUTATIONS

JOHN C. BAEZ[1]

Abstract. If we treat the symmetric group S_n as a probability measure space where each element has measure $1/n!$, then the number of cycles in a permutation becomes a random variable. The Cycle Length Lemma describes the expected values of products of these random variables. Here we categorify the Cycle Length Lemma by showing that it follows from an equivalence between groupoids.

1. Introduction

There is a well-behaved generalization of the concept of cardinality from finite sets to finite groupoids [2]. But what is it good for? As an illustration, here we use it to give a new proof of a known fact about random permutations: the Cycle Length Lemma [4]. In this lemma one treats the number of k-cycles in a permutation of n things as a random variable, where each permutation occurs with equal probability. The lemma says that in the limit as $n \to \infty$, this random variable approaches a Poisson distribution with mean $1/k$. Furthermore, in the $n \to \infty$ limit these random variables become independent for different choices of k.

These are quick rough statements. In Section 2 we state the Cycle Length Lemma in a precise way. In Section 3 we prove a *categorified* version of the Cycle Length Lemma, which asserts an equivalence of groupoids. In Section 4 we derive the original version of the lemma from this categorified version by taking the cardinalities of these groupoids. The categorified version contains more information, so it is not just a trick for proving the original lemma (which is, after all, quite easy to show). Instead, it reveals the original lemma as a consequence of a stronger fact about groupoids.

In Section 5 we sketch how some of the ideas here generalize to other finite groups.

2. The Cycle Length Lemma

In the theory of random permutations, we treat the symmetric group S_n as a probability measure space where each element has the same measure, namely $1/n!$. Functions $f\colon S_n \to \mathbb{R}$ then become random variables, and we can study their expected values:

$$E(f) = \frac{1}{n!} \sum_{\sigma \in S_n} f(\sigma).$$

An important example is the function

$$c_k \colon S_n \to \mathbb{N}$$

that counts, for any permutation $\sigma \in S_n$, its number of cycles of length k, also called k-cycles. A well-known but striking fact about random permutations is that whenever $k \leq n$, the expected number of k-cycles is $1/k$:

$$E(c_k) = \frac{1}{k}$$

This has some nice consequences. For example, a randomly chosen permutation of any finite set has, on average, one fixed point. Also, its expected number of cycles is

$$1 + \frac{1}{2} + \cdots + \frac{1}{n},$$

which for large n becomes close to $\ln n$ plus Euler's constant γ.

Another striking fact is that whenever $j \neq k$ and $j + k \leq n$, so that it is possible for a permutation $\sigma \in S_n$ to have both a j-cycle and a k-cycle, the random variables c_j and c_k are uncorrelated in the following sense:

$$E(c_j c_k) = E(c_j)E(c_k).$$

[1]Department of Mathematics, University of California, Riverside CA, USA 92521
E-mail address: baez@math.ucr.edu.

You might at first think that having many j-cycles for some large j would tend to inhibit the presence of k-cycles for some other large value of k, but that is not true unless $j + k > n$, when it suddenly becomes *impossible* to have both a j-cycle and a k-cycle!

These two facts are special cases of the Cycle Length Lemma. To state this lemma in full generality, recall that the number of ordered p-tuples of distinct elements of an n-element set is the **falling power**

$$x^{\underline{p}} = x(x-1)(x-2)\cdots(x-p+1).$$

It follows that the function

$$c_k^{\underline{p}} \colon S_n \to \mathbb{N}$$

counts, for any permutation in S_n, its ordered p-tuples of distinct k-cycles. We can also replace the word 'distinct' here by 'disjoint', without changing the meaning, since distinct cycles must be disjoint.

The two striking facts mentioned above generalize as follows:

(1) First, whenever $pk \le n$, so that it is *possible* for a permutation in S_n to have p distinct k-cycles, then

$$E(c_k^{\underline{p}}) = \frac{1}{k^p}.$$

For readers familiar with the moments of a Poisson distribution, here is a nice equivalent way to state this equation: when $pk \le n$, the pth moment of the random variable c_k equals that of a Poisson distribution with mean $1/k$.

(2) Second, as $n \to \infty$ the random variables c_k become better and better approximated by independent Poisson distributions. To state this precisely we need a bit of notation. Let $\vec{p}$ denote an n-tuple $(p_1, \ldots, p_n)$ of natural numbers, and let

$$|\vec{p}| = p_1 + 2p_2 + \cdots + np_n.$$

If $|\vec{p}| \le n$, it is possible for a permutation $\sigma \in S_n$ to have a collection of distinct cycles, with p_1 cycles of length 1, p_2 cycles of length 2, and so on up to p_n cycles of length n. If $|\vec{p}| > n$, this is impossible. In the former case, where $|\vec{p}| \le n$, we always have

$$E\left(\prod_{k=1}^n c_k^{\underline{p_k}}\right) = \prod_{k=1}^n E(c_k^{\underline{p_k}}).$$

Taken together, 1) and 2) are equivalent to the Cycle Length Lemma, which may be stated in a unified way as follows:

The Cycle Length Lemma. Suppose $p_1, \ldots, p_n \in \mathbb{N}$. Then

$$E\left(\prod_{k=1}^n c_k^{\underline{p_k}}\right) = \begin{cases} \displaystyle\prod_{k=1}^n \frac{1}{k^{p_k}} & \text{if } |\vec{p}| \le n \\ \\ 0 & \text{if } |\vec{p}| > n \end{cases}$$

This appears, for example, in Ford's comprehensive review of the statistics of cycle lengths in random permutations [4, Lem. 3.1]. He attributes it to Watterson [9, Thm. 7]. The most famous special case is when $|\vec{p}| = n$, which apparently goes back to Cauchy.

For more details on the sense in which random variables c_k approach independent Poisson distributions, see Arratia and Tavaré [1].

3. The Categorified Cycle Length Lemma

To categorify the Cycle Length Lemma, the key is to treat a permutation as an extra structure that we can put on a set, and then consider the groupoid of n-element sets equipped with this extra structure:

Definition 1. Let Perm_n be the groupoid in which

- an object is an n-element set equipped with a permutation $\sigma \colon X \to X$

and

- a morphism from $\sigma \colon X \to X$ to $\sigma' \colon X' \to X'$ is a bijection $f \colon X \to X'$ that is **permutation-preserving** in the following sense:

$$f \circ \sigma \circ f^{-1} = \sigma'.$$

We'll need the following strange fact below: if $n < 0$ then Perm_n is the empty groupoid (that is, the groupoid with no objects and no morphisms).

More importantly, we'll need a fancier groupoid where a set is equipped with a permutation together with a list of distinct cycles of specified lengths. For any $n \in \mathbb{N}$ and any n-tuple of natural numbers $\vec{p} = (p_1, \ldots, p_n)$, recall that we have defined

$$|\vec{p}| = p_1 + 2p_2 + \cdots + np_n.$$

Definition 2. Let $\mathsf{C}_{\vec{p}}$ be the groupoid of n-element sets X equipped with a permutation $\sigma \colon X \to X$ that is in turn equipped with a choice of an ordered p_1-tuple of distinct 1-cycles, an ordered p_2-tuple of distinct 2-cycles, and so on up to an ordered p_n-tuple of distinct n-cycles. A morphism in this groupoid is a bijection that is permutation-preserving and also preserves the ordered tuples of distinct cycles.

Note that if $|\vec{p}| > n$, no choice of disjoint cycles with the specified property exists, so $\mathsf{C}_{\vec{p}}$ is the empty groupoid.

Finally, we need a bit of standard notation. For any group G we write $\mathsf{B}(G)$ for its **delooping**: that is, the groupoid that has one object $\star$ and $\mathrm{Aut}(\star) = G$.

Theorem 3. (The Categorified Cycle Length Lemma.) *For any $\vec{p} = (p_1, \ldots, p_n) \in \mathbb{N}^n$ we have*

$$\mathsf{C}_{\vec{p}} \simeq \mathsf{Perm}_{n-|\vec{p}|} \times \prod_{k=1}^{n} \mathsf{B}(\mathbb{Z}/k)^{p_k}$$

Proof. Both sides are empty groupoids when $|\vec{p}| > n$, so assume $|\vec{p}| \leq n$. A groupoid is equivalent to any full subcategory of that groupoid containing at least one object from each isomorphism class. So, fix an n-element set X and a subset $Y \subseteq X$ with $n - |\vec{p}|$ elements. Partition $X - Y$ into subsets $S_{k\ell}$ where $S_{k\ell}$ has cardinality k, $1 \leq k \leq n$, and $1 \leq \ell \leq p_k$. Every object of $\mathsf{C}_{\vec{p}}$ is isomorphic to the chosen set X equipped with some permutation $\sigma \colon X \to X$ that has each subset $S_{k\ell}$ as a k-cycle. Thus $\mathsf{C}_{\vec{p}}$ is equivalent to its full subcategory containing only objects of this form.

An object of this form consists of an arbitrary permutation $\sigma_Y \colon Y \to Y$ and a cyclic permutation $\sigma_{k\ell} \colon S_{k\ell} \to S_{k\ell}$ for each k, ℓ as above. Consider a second object of this form, say $\sigma'_Y \colon Y \to Y$ equipped with cyclic permutations $\sigma'_{k\ell}$. Then a morphism from the first object to the second consists of two pieces of data. First, a bijection

$$f \colon Y \to Y$$

such that

$$\sigma'_Y = f \circ \sigma_Y \circ f^{-1}.$$

Second, for each k, ℓ as above, a bijection

$$f_{k\ell} \colon S_{k\ell} \to S_{k\ell}$$

such that

$$\sigma'_{k\ell} = f_{k\ell} \circ \sigma_{k\ell} \circ f_{k\ell}^{-1}.$$

Since Y has $n - |\vec{p}|$ elements, while $\sigma_{k\ell}$ and $\sigma'_{k\ell}$ are cyclic permutations of k-element sets, it follows that $\mathsf{C}_{\vec{p}}$ is equivalent to

$$\mathsf{Perm}_{n-|\vec{p}|} \times \prod_{k=1}^{n} \mathsf{B}(\mathbb{Z}/k)^{p_k}. \qquad \square$$

The case where $|\vec{p}| = n$ is especially pretty, since then our chosen cycles completely fill up our n-element set and we have

$$\mathsf{C}_{\vec{p}} \simeq \prod_{k=1}^{n} \mathsf{B}(\mathbb{Z}/k)^{p_k}.$$

4. Groupoid Cardinality

The cardinality of finite sets has a natural extension to finite groupoids, which turns out to be the key to extracting results on random permutations from category theory. We briefly recall this concept [2]. Any finite groupoid G is equivalent to a coproduct of finitely many one-object groupoids, which are deloopings of finite groups $G_1, \ldots, G_m$:

$$\mathsf{G} \simeq \sum_{i=1}^{m} \mathsf{B}(G_i),$$

and then the **cardinality** of G is defined to be

$$|\mathsf{G}| = \sum_{i=1}^{m} \frac{1}{|G_i|}.$$

This concept of groupoid cardinality has various nice properties. For example it is additive:

$$|\mathsf{G} + \mathsf{H}| = |\mathsf{G}| + |\mathsf{H}|$$

and multiplicative:

$$|\mathsf{G} \times \mathsf{H}| = |\mathsf{G}| \times |\mathsf{H}|$$

and invariant under equivalence of groupoids:

$$\mathsf{G} \simeq \mathsf{H} \implies |\mathsf{G}| = |\mathsf{H}|.$$

None of these three properties forces us to define $|\mathsf{G}|$ as the sum of the *reciprocals* of the cardinalities $|G_i|$: any other power of these cardinalities would work just as well. What makes the reciprocal cardinalities special is that if G is a finite group acting on a set S, we have

$$|S \mathbin{/\!\!/} G| = |S|/|G|$$

where the groupoid $S \mathbin{/\!\!/} G$ is the **weak quotient** or **homotopy quotient** of S by G, also called the **action groupoid**. This is the groupoid with elements of S as objects and one morphism from s to s' for each $g \in G$ with $gs = s'$, with composition of morphisms coming from multiplication in G.

The groupoid of n-element sets equipped with permutation, Perm_n, has a nice description in terms of weak quotients:

Lemma 4. *For all $n \in \mathbb{N}$ we have an equivalence of groupoids*

$$\mathsf{Perm}_n \simeq S_n \mathbin{/\!\!/} S_n$$

where the group S_n acts on the underlying set of S_n by conjugation.

Proof. We use the fact that Perm_n is equivalent to any full subcategory of Perm_n containing at least one object from each isomorphism class. For Perm_n we can get such a subcategory by fixing an n-element set, say $X = \{1, \ldots, n\}$, and taking only objects of the form $\sigma \colon X \to X$, i.e. $\sigma \in S_n$. A morphism from $\sigma \in S_n$ to $\sigma' \in S_n$ is then a permutation $\tau \in S_n$ such that

$$\sigma' = \tau \sigma \tau^{-1}.$$

But this subcategory is precisely $S_n \mathbin{/\!\!/} S_n$. □

Corollary 5. *For all $n \in \mathbb{N}$ we have*

$$|\mathrm{Perm}(n)| = 1$$

Proof. We have $|\mathrm{Perm}(n)| = |S_n \mathbin{/\!\!/} S_n| = |S_n|/|S_n| = 1$. □

It should now be clear why we can prove results on random permutations using the groupoid Perm_n: this groupoid is equivalent to $S_n \mathbin{/\!\!/} S_n$, which has one object for each permutation $\sigma \in S_n$, with each object contributing $1/n!$ to the groupoid cardinality.

Now let us use these ideas to derive the original Cycle Length Lemma from the categorified version.

Theorem 6. (The Cycle Length Lemma.) *Suppose $p_1, \ldots, p_n \in \mathbb{N}$. Then*

$$E\left(\prod_{k=1}^{n} C_k^{p_k}\right) = \begin{cases} \displaystyle\prod_{k=1}^{n} \frac{1}{k^{p_k}} & \text{if } |\vec{p}| \leq n \\ \\ 0 & \text{if } |\vec{p}| > n \end{cases}$$

Proof. We know that

$$\mathsf{C}_{\vec{p}} \simeq \mathsf{Perm}(n - |\vec{p}|) \times \prod_{k=1}^{n} \mathsf{B}(\mathbb{Z}/k)^{p_k}$$

So, to prove the Cycle Length Lemma it suffices to show three things:

$$|\mathsf{C}_{\vec{p}}| = E\left(\prod_{k=1}^{n} c_k^{p_k}\right)$$

$$\mathsf{Perm}(n - |\vec{p}|) = \begin{cases} 1 & \text{if } |\vec{p}| \leq n \\ \\ 0 & \text{if } |\vec{p}| > n \end{cases}$$

and

$$|\mathsf{B}(\mathbb{Z}/k)| = 1/k$$

The last of these is immediate from the definition of groupoid cardinality. The second follows from the Corollary above, together with the fact that $\mathsf{Perm}(n - |\vec{p}|)$ is the empty groupoid when $|\vec{p}| > n$. Thus we are left needing to show that

$$|\mathsf{C}_{\vec{p}}| = E\left(\prod_{k=1}^{n} c_k^{p_k}\right).$$

We prove this by computing the cardinality of a groupoid equivalent to $\mathsf{C}_{\vec{p}}$. We claim this groupoid is of the form $Q_{\vec{p}} /\!\!/ S_n$ where $Q_{\vec{p}}$ is some set on which S_n acts. As a result we have

$$|\mathsf{C}_{\vec{p}}| = |Q_{\vec{p}} /\!\!/ S_n| = |Q_{\vec{p}}|/n!$$

and to finish the proof we need to show

$$E\left(\prod_{k=1}^{n} c_k^{p_k}\right) = |Q_{\vec{p}}|/n!\,.$$

What is the set $Q_{\vec{p}}$, and how does S_n act on it? An element of $Q_{\vec{p}}$ is a permutation $\sigma \in S_n$ equipped with an ordered p_1-tuple of distinct 1-cycles, an ordered p_2-tuple of distinct 2-cycles, and so on up to an ordered p_n-tuple of distinct n-cycles. Any element $\tau \in S_n$ acts on $Q_{\vec{p}}$ in a natural way, by conjugating the permutation $\sigma \in S_n$ to obtain a new permutation, and mapping the chosen cycles of σ to the corresponding cycles of this new conjugated permutation $\tau\sigma\tau^{-1}$.

Recalling the definition of the groupoid $\mathsf{C}_{\vec{p}}$, it is clear that any element of $Q_{\vec{p}}$ gives an object of $\mathsf{C}_{\vec{p}}$, and any object is isomorphic to one of this form. Furthermore any permutation $\tau \in S_n$ gives a morphism between such objects, all morphisms between such objects are of this form, and composition of these morphisms is just multiplication in S_n. It follows that

$$\mathsf{C}_{\vec{p}} \simeq Q_{\vec{p}} /\!\!/ S_n.$$

To finish the proof, note that

$$E\left(\prod_{k=1}^{n} c_k^{p_k}\right)$$

is $1/n!$ times the number of ways of choosing a permutation $\sigma \in S_n$ and equipping it with an ordered p_1-tuple of distinct 1-cycles, an ordered p_2-tuple of distinct 2-cycles, and so on. This is the same as $|Q_{\vec{p}}|/n!$. □

5. Conclusion

We have opted to treat an example rather than develop a general theory, but many of the ideas here go beyond the symmetric group. Any finite group G acts on itself by conjugation and gives a groupoid $G /\!\!/ G$ of cardinality 1. Any functor $F\colon G /\!\!/ G \to \mathsf{FinSet}$ describes a conjugation-equivariant structure we can put on elements of G, with $F(g)$ being the set of structures we can put on the element $g \in G$. Taking the ordinary cardinality of these sets, we obtain a function $|F|\colon G \to \mathbb{N}$. Its expected value with respect to the normalized Haar measure on G is, by definition,

$$E(|F|) = \frac{1}{|G|} \sum_{g \in G} |F(g)|.$$

However, $E(|F|)$ also equals the cardinality of a certain groupoid for which an object is an element $g \in G$ equipped with a structure $x \in F(g)$. This groupoid is the familiar **category of elements** of F, denoted $\int F$, for which:

(1) an object is a pair (g, x) where $g \in G$ and $x \in F(g)$;
(2) a morphism from (g, x) to (g', x') is an element $h \in G$ such that $g' = hgh^{-1}$ and $x' = F(h)(x)$;
(3) composition of morphisms is multiplication of group elements.

Theorem 7. *If G is a finite group and $F\colon G /\!\!/ G \to \mathsf{FinSet}$ is a functor, then*

$$E(|F|) = \left|\int F\right|.$$

Proof. Let $\mathrm{Ob}(\int F)$ be the set of objects of $\int F$. The group G acts on $\mathrm{Ob}(\int F)$, with $h \in G$ mapping the object (g, x) to the object $(hgh^{-1}, F(h)(x))$. Using the explicit description of $\int F$ in items (1)–(3) above, there is an evident isomorphism of groupoids

$$\int F \cong \mathrm{Ob}(\int F) \mathbin{/\!\!/} G$$

that is the identity on objects and sends each morphism h from (g, x) to (g', x') to the analogous morphism in $\mathrm{Ob}(\int F) \mathbin{/\!\!/} G$. It follows that

$$\left|\int F\right| = \left|\mathrm{Ob}(\int F) \mathbin{/\!\!/} G\right| = |\mathrm{Ob}(\int F)|/|G| = \frac{1}{|G|} \sum_{g \in G} |F(g)| = E(|F|). \qquad \square$$

The expected value of $|F|$ is its integral over G with respect to normalized Haar measure, so we can write it as $\int |F|$, and then the theorem above takes an amusing though perhaps confusing form:

$$\int |F| = \left|\int F\right|.$$

The above theorem sheds new light on the proof of Theorem 6, because the S_n-set $Q_{\vec{p}}$ in that proof is none other than $\mathrm{Ob}(\int C_{\vec{p}})$ for the functor $C_{\vec{p}} \colon S_n \mathbin{/\!\!/} S_n \to \mathsf{FinSet}$ assigning to any permutation the set where an element is an ordered p_1-tuple of distinct 1-cycles, an ordered p_2-tuple of distinct 2-cycles, and so on. Thus, the groupoid $\mathsf{C}_{\vec{p}}$ is equivalent to $\int C_{\vec{p}}$. The same ideas apply to other structures that we can put on a finite set equipped with a permutation.

The above theorem may also let us derive results about random elements of other groups from equivalences of groupoids. Results on $\mathrm{GL}(n, \mathbb{F}_q)$ are promising candidates [5], since some are already proved using generating functions, which are connected to the category-theoretic techniques used here [2, 3, 6], and there are powerful analogies between finite sets and finite-dimensional vector spaces over finite fields [7, 8].

References

[1] Richard Arratia and Simon Tavaré, The cycle structure of random permutations, *The Annals of Probability* **20** (1992), 1567–1591. Available at https://doi.org/10.1214/aop/1176989707.

[2] John C. Baez and James Dolan, From finite sets to Feynman diagrams, in *Mathematics Unlimited—2001 and Beyond*, vol. 1, eds. Björn Engquist and Wilfried Schmid, Springer, Berlin, 2001, pp. 29–50. Available as arXiv:0004133.

[3] François Bergeron, Gilbert Labelle and Pierre Leroux, *Combinatorial Species and Tree-like Structures*, Cambridge U. Press, Cambridge, 1998.

[4] Kevin Ford, Cycle type of random permutations: a toolkit, *Discrete Analysis* **29** (2022). Available as arXiv:2104.12019.

[5] Jason Fulman, Random matrix theory over finite fields: a survey, *Bulletin of the American Mathematical Society* **39** (2001), 51–85. Available as arXiv:0003195.

[6] André Joyal, Une théorie combinatoire des séries formelles, *Advances in Mathematics* **42** (1981), 1–82.

[7] Tom Leinster, The probability that an operator is nilpotent, *American Mathematical Monthly* **128** (2021), 371–375. Available as arXiv:1912.12562.

[8] Oliver Lorscheid, Algebraic groups over the field with one element, *Mathematische Zeitschrift* **271** (2012), 117–138. Available as arXiv:0907.3824.

[9] G. A. Watterson, The sampling theory of selectively neutral alleles, *Advances in Applied Probability* **6** (1974), 463–488.