For further information, contact:
cbarnes@sbc.edu

Enumeration of the Distinct Shuffles of Permutations

Camillia Smith Barnes • *Department of Mathematical Sciences* • *Sweet Briar College*

Research completed while affiliated with • *Department of Mathematics* • *Harvard University*

Algebraic Combinatorixx
Banff International Research Station
24 May 2011

Summary

A shuffle of two words is a word obtained by concatenating the two original words in either order and then sliding any letters from the second word back past letters of the first word, in such a way that the letters of each original word remain spelled out in their original relative order. Examples of shuffles of the words 1234 and 5678 are, for instance, 15236784 and 51236748.

In this paper, we enumerate the distinct shuffles of two permutations of any two lengths, where the permutations are written as words in the letters $1, 2, 3, \ldots, m$ and $1, 2, 3, \ldots, n$, respectively.

Shuffles of Words

Definition 1.1. A *word* is defined to be a finite string of elements (known as *letters*) of a given set (known as an *alphabet*); in general repetitions of letters are allowed.

Definition 1.2. We define the *length* of a word $u = a_1 \ldots a_m$ to be $\mathfrak{l}(u) = m$ and the *support* of u to be $\mathrm{supp}(u) = \{a_1, \ldots, a_m\}$.

Definition 1.3. A *subword* x of a word u is defined to be a word obtained by omitting a (possibly empty) subset of the letters of u.

Example 1.4. For the alphabet $\mathcal{A} = \{1, 2, 3, 5, 7\}$, the words $u = 25372$ and $v = 123$ have supports $\mathrm{supp}(u) = \{2, 3, 5, 7\}$ and $\mathrm{supp}(v) = \{1, 2, 3\}$, and lengths $\mathfrak{l}(u) = 5$ and $\mathfrak{l}(v) = 3$. Two subwords of u are 232 and 537.

Definition 1.5. Given two words $u = a_1 a_2 \ldots a_m$ and $v = b_1 b_2 \ldots b_n$ in some alphabet $\mathcal{A}$, we obtain a *shuffle* of u and v by concatenating u and v to get

$$c_1 c_2 \ldots c_{m+n} = a_1 a_2 \ldots a_m b_1 b_2 \ldots b_n$$

and then permuting letters in such a way to achieve

$$w = c_{\rho(1)} c_{\rho(2)} \cdots c_{\rho(m+n)},$$

for some permutation $\rho \in \mathfrak{S}_{m+n}$ on $m + n$ letters satisfying the order-preserving conditions

$$\rho^{-1}(1) < \rho^{-1}(2) < \cdots < \rho^{-1}(m) \tag{1}$$

and

$$\rho^{-1}(m+1) < \rho^{-1}(m+2) < \cdots < \rho^{-1}(m+n). \tag{2}$$

The Main Question

Question 2.1. Given words u and v, how many distinct shuffles are there of u with v?

Assuming m and n to be the lengths of u and v, respectively, note that if $\mathrm{supp}(u) \cap \mathrm{supp}(v) = \emptyset$, then there are $\binom{m+n}{m}$ distinct shuffles (all shuffles are distinct).

We resolve this question for the case where the words u and v are assumed to be permutation words. In this case, the supports are *not* necessarily disjoint.

Motivating the search to count shuffles of permutations is the beautiful result that *the distinct shuffles of the identity permutation with itself are counted by the Catalan numbers*.

The Identity Permutation

Proposition 3.1. *The number of distinct shuffles of the identity permutation on n letters with itself is the n^{th} Catalan number C_n, that is*

$$\#\mathfrak{sh}(\mathrm{id}_n, \mathrm{id}_n) = \frac{1}{n+1}\binom{2n}{n}. \tag{3}$$

Example 3.2. The $C_3 = 5$ distinct shuffles of 123 with itself are

112233 112323 121233 121323 123123

Proposition 3.3. *For $m \leq n$, the number of distinct shuffles of the identity permutation on m letters with the identity permutation on n letters is given by*

$$\#\mathfrak{sh}(\mathrm{id}_m, \mathrm{id}_n) = \frac{(n+m)! \cdot (n-m+1)}{(n+1)! \cdot m!}. \tag{4}$$

The Reverse Permutation

Definition 4.1. Let the reverse permutation word $n, n-1, \ldots, 2, 1$ be denoted by rev_n.

Example 4.2. For instance, $\mathrm{rev}_4 = 4321$.

The special case of finding the number of distinct shuffles of the reverse permutation with the identity permutation illustrates the idea used to solve the general case: we determine what multiplicities can occur, then subtract the number of duplicates from the total number of shuffles with multiplicity.

The following result can be shown via a bijective proof.

Proposition 4.3.

$$\#\mathfrak{sh}(\mathrm{id}_m, \mathrm{rev}_n) = \binom{m+n}{m} - \binom{m+n-2}{m-1}. \tag{5}$$

Example 4.4. The 14 distinct shuffles of the words 123 and 321 are as follows, with their multiplicities in parentheses:

123321 (2)	132321 (1)	312321 (1)	321123 (2)
123231 (1)	132213 (2)	312213 (2)	321231 (1)
123213 (1)	132231 (2)	312231 (2)	321213 (1)
	132123 (1)	312123 (1)	

The General Case

Fact 5.1. *For any $m \leq n$ and any $\alpha \in \mathfrak{S}_m$, $\beta \in \mathfrak{S}_n$, we have $\#\mathfrak{sh}(\alpha, \beta) = \#\mathfrak{sh}(\mathrm{id}_m, (\overline{\alpha})^{-1} \circ \beta)$, where $\overline{\alpha} \in \mathfrak{S}_n$ is the natural extension of α to a permutation on n letters.*

The following proposition is key to solving the general case:

Proposition 5.2. *Given any $w \in \mathfrak{sh}(\mathrm{id}_m, \sigma)$, the multiplicity of w is a power of 2, that is $\mu_w = 2^t$ for some nonnegative integer t.*

It will now be possible to derive the main theorem (Theorem 6.1, next column) by applying the principle of Inclusion-Exclusion.

Examples of calculations using the theorem include $\#\mathfrak{sh}(\mathrm{id}_3, 321) = 14$, $\#\mathfrak{sh}(\mathrm{id}_3, 4321) = 25$, $\#\mathfrak{sh}(\mathrm{id}_2, 3421) = 11$, $\#\mathfrak{sh}(2431, 1432) = 44$, $\#\mathfrak{sh}(\mathrm{id}_6, 126354) = 374$, $\#\mathfrak{sh}(\mathrm{id}_8, 4321) = 375$, $\#\mathfrak{sh}(\mathrm{id}_8, 67812345) = 10930$, $\#\mathfrak{sh}(\mathrm{id}_8, 43215678) = 3976$, and $\#\mathfrak{sh}(\mathrm{id}_{10}, 214365) = 4746$.

Main Theorem

The following theorem provides a formula that can be programmed into a computer algebra package in order to calculate the number of distinct shuffles of two permutations. Maple 11.0 running on a 2008 laptop can quickly handle calculations up to length 13.

For example, $\#\mathfrak{sh}(\mathrm{id}_{13}, 789\ 10\ 11\ 12\ 13\ 123456) = 10104590$.

Theorem 6.1. *For any $\alpha \in \mathfrak{S}_m$ and $\beta \in \mathfrak{S}_n$ with $m \leq n$, let $\sigma = \overline{\alpha}^{-1} \circ \beta$, where $\overline{\alpha} \in \mathfrak{S}_n$ is the natural extension of α. Then*

$$\begin{aligned}\#\mathfrak{sh}(\alpha, \beta) &= \#\mathfrak{sh}(\mathrm{id}_m, \sigma)\\ &= \sum_{k=0}^{\lfloor \frac{m}{2} \rfloor} \sum_{\mathbf{a} \in \mathbf{A}_m(k)} (-1)^{h(\mathbf{a})} \prod_{r=0}^{k} \det \mathfrak{F}_m^\sigma(a_{2r}, a_{2r+1}) \prod_{s=1}^{k} \det \Lambda^\sigma(a_{2s-1}, a_{2s}),\end{aligned} \tag{6}$$

where

$$\mathbf{A}_m(k) = \{\{0 = a_0 < a_1 < \cdots < a_{2k} < a_{2k+1} = m+1\} \mid a_i \in \mathbb{N}\}$$

and

$$h(\mathbf{a}) = m - \sum_{t=1}^{k} (a_{2t} - a_{2t-1}),$$

and where we define the matrices

$$\mathfrak{F}_m^\sigma(c, d) = \left[\hat{\mathfrak{f}}_m^\sigma(i, j+1)\right]_{c \leq i, j \leq d-1},$$

with

$$\hat{\mathfrak{f}}_m^\sigma(i, j) = \begin{cases} 0, & i > j \\ 1, & i = j \\ 0, & 0 < i < j < m+1 \text{ and } \sigma^{-1}(i) > \sigma^{-1}(j) \\ \binom{j-i-1+\sigma^{-1}(j)-\sigma^{-1}(i)-1}{j-i-1}, & 0 < i < j < m+1 \text{ and } \sigma^{-1}(i) < \sigma^{-1}(j) \\ \binom{j-1+\sigma^{-1}(j)-1}{j-1}, & i = 0 \text{ and } j < m+1 \\ \binom{m-i+n-\sigma^{-1}(i)}{m-i}, & j = m+1 \text{ and } i > 0 \\ \binom{m+n}{m}, & i = 0 \text{ and } j = m+1, \end{cases}$$

and the matrices

$$\Lambda^\sigma(e, f) = [\omega^\sigma(i, j)]_{e \leq i, j \leq f-1},$$

with

$$\omega^\sigma(i, j) = \begin{cases} 0, & i - j > 1 \text{ or } \sigma^{-1}(i+1) \neq \sigma^{-1}(i) + 1 \\ -1, & i - j = 1 \text{ and } \sigma^{-1}(i+1) = \sigma^{-1}(i) + 1 \\ C_{j-i}, & i \leq j \text{ and } \sigma^{-1}(i+1) = \sigma^{-1}(i) + 1 \end{cases}$$

and where

$$C_{j-i} = \frac{1}{j-i+1}\binom{2(j-i)}{j-i}, \text{ the } (j-i)^{th} \text{ Catalan number.}$$

Acknowledgments

I would like to thank my advisor, Richard Stanley, for his invaluable guidance and for suggesting such an enjoyable problem. I am also grateful to Lauren Williams and Thomas Lam for their willingness to help me improve various drafts of this paper. Moreover, I am very thankful for the generous support provided me by the National Science Foundation Graduate Research Fellowship and the AT&T Labs Fellowship Program.

Selected References

W.F. Doran IV, *Shuffling lattices*, J. Combinatorial Theory Ser. A **66** (2002), 1–26.

R. Ehrenborg, *On posets and Hopf algebras*, Adv. Math. **119** (1996), 1–25.

C. Greene, *Posets of shuffles*, J. Combinatorial Theory Ser. A **47** (1988), 191–206.

P. Hersh, *Two generalizations of posets of shuffles*, J. Combinatorial Theory Ser. A **97** (2002), 1–26.

C. Reutenauer, *Free Lie Algebras*, Clarendon Press, 1993.

R. Simion & R.P. Stanley, *Flag-symmetry of the poset of shuffles and a local action of the symmetric group*, Discrete Math. **204** (1999), 369–396.

C. Smith, *Enumeration of the distinct shuffles of permutations*, Harvard University Ph.D. dissertation, 2009.

R.P. Stanley, *Generalized riffle shuffles and quasisymmetric functions*, Ann. Comb. **5** (3–4) (2001), 479–491.