Elem. Math. 56 (2001) 1 – 3
0013-6018/01/010001-3 $ 1.50+0.20/0

Elemente der Mathematik

On the Representation of Permutations as Products of Transpositions

Daniel Neuenschwander

Daniel Neuenschwander was born in 1963 near Neuchâtel (CH). After his doctorate (under the direction of H. Carnal) at the University of Bern in 1991, he was appointed professor of mathematics at the Biel School of Engineering and Architecture of the Bern University of Applied Sciences (the former HTL). After having got a part-time professorship for actuarial sciences at the University of Lausanne, he completed his habilitation in 1996. He teaches mathematics of insurance and finance also at the University of Bern and holds a position at the Federal section of cryptology at the Department of Defense. He has taught at the University of Dortmund and has been invited professor at the University of Nancy I. His main mathematical working-area is probability theory (especially on algebraic structures) and its applications in insurance, finance, and cryptology. Non-mathematical interests include music (organ, harpsichord, piano) and travelling.

The subject of this note is the representation of permutations of finite sets as products of a minimal number of simple transpositions.

Consider the following theorem:

Theorem 1

a) *If a permutation φ which is a product of n transpositions cannot be written as a product of fewer than n transpositions, then for any transposition occuring in this product both elements belong to the same cycle of φ.*

Einer Menge bestehend aus n Elementen ist in natürlicher Weise die Menge S_n der Permutationen der Elemente dieser Menge zugeordnet. Es ist bekannt, dass S_n eine Gruppe mit $n!$ Elementen ist. Bereits S_3 liefert ein Beispiel einer nicht-kommutativen Gruppe, und die Untergruppe $A_n \subset S_n$ vom Index 2, die sogenannte alternierende Gruppe, ist für $n > 4$ einfach, was zur Nicht-Lösbarkeit algebraischer Gleichungen vom Grad grösser als vier durch Radikale führt. Andererseits ist es einfach zu beweisen, dass jede Permutation $\pi \in S_n$ als Produkt von Zykeln darstellbar ist. Spezielle Zykeln sind die Transpositionen, d.h. die Vertauschungen zweier Elemente; es zeigt sich, dass π insbesondere als Produkt von Transpositionen darstellbar ist. Im vorliegenden Beitrag wird nun auf elementare Weise gezeigt, welches die minimale Anzahl von Transpositionen ist, die man zur Darstellung einer Permutation benötigt, und auf wieviele Arten eine solche Darstellung erfolgen kann. *jk*

b) *A permutation φ which is a cycle of length $n+1$ cannot be written as a product of fewer than n transpositions.*

Part b) of Theorem 1 is well-known, see e.g. Schwenk (1984), Lossers (1986), and the literature cited there. We show how assertions a) and b) can be proved together by induction on $n \in \mathbb{N}_0$. We will use the word "cycle" in the sense that a cycle can also be one-elemented. However, transpositions will always be genuine, i.e. two-elemented.

Proof of Theorem 1. For a cycle φ, denote by $|\varphi|$ its length. For $n = 0$, a) and b) are trivial. Assume them to be true for all $0 \le k \le n$ and consider $\varphi = \varphi'(a,b)$, where φ' is a product of n transpositions and $n+1$ is the minimum number of transpositions which is necessary to represent φ. Let c_i $(1 \le i \le m)$ denote the disjoint cycles of φ'. If both a, b belonged to the same c_{i_0}, then the permutation $c_{i_0}(a,b)$ as a product of not fewer than $|c_{i_0}|$ transpositions (induction hypothesis b)) would consist of two disjoint cycles of $|c_{i_0}|$ elements together and could therefore be represented by $|c_{i_0}| - 2$ transpositions, which is a contradiction. So a, b belong to two different c_i's, thus any of the cycles $(a,b), c_i$ $(1 \le i \le m)$ is part of one of the disjoint cycles d_i of φ, and therefore for any transposition of φ in a decomposition of φ into a minimal number of transpositions both interchanged elements belong to the same d_i, which proves a). Now assume in addition that φ is a cycle itself, i.e. w.l.o.g. $\varphi = (1, 2, \ldots, L)$, $a, b \in \mathbb{N}$, $a < b$. We show that $L = n + 2$. We have $\varphi' = \varphi''\varphi'''$, where

$$\varphi'' = (1, 2, \ldots, a, \varphi(b), \varphi^2(b), \ldots, L)$$

and

$$\varphi''' = (\varphi(a), \varphi^2(a), \ldots, \varphi^{-1}(b), b).$$

We have $|\varphi''| = L - (b - a)$ and $|\varphi'''| = b - a$, hence (by counting transpositions in a minimal transposition decomposition and using induction hypotheses a) and b))

$$n + 1 = |\varphi''| + |\varphi'''| - 1 = L - (b - a) + b - a - 1,$$

hence $L = n + 2$. □

In this context, a natural question is also in how many ways a cycle of length n can be represented as a product of $n - 1$ transpositions. Let N_n be this number.

Theorem 2 $\quad N_n = n^{n-2} \quad (n \in \mathbb{N})$.

This property has been proved by Lossers (1986), using the formula for the number of point-labeled trees of n points. See also the literature cited in Lossers (1986) for other references to this theorem. Here, let us present a self-contained proof based on Theorem 1a) and Abel's identity:

$$\sum_{k=0}^{m} \binom{m}{k} (x + k)^{k-1} (y + m - k)^{m-k} = x^{-1}(x + y + m)^m. \tag{1}$$

Proof of Theorem 2. For $n = 1$ the assertion is trivial. We assume it to be true for $k \le n$ and prove it for $n+1$. The cycle

$$\psi = (1, 2, \ldots, n+1) = (a_1, b_1)(a_2, b_2) \cdots (a_n, b_n)$$

($a_k < b_k$ $(1 \le k \le n)$) can be represented as follows:

$$\psi = \psi'(a_n, b_n)$$

with

$$\begin{aligned}
\psi' &= \psi''\psi'', \\
\psi'' &= (1, 2, \ldots, a_n, \psi(b_n), \psi^2(b_n), \ldots, n+1), \\
\psi''' &= (\psi(a_n), \psi^2(a_n), \ldots, \psi^{-1}(b_n), b_n).
\end{aligned}$$

Writing $k := b_n - a_n$, the triple $(\psi'', \psi''', (a_n, b_n))$ is uniquely determined by the pair (k, a_n). For a given k, there exist $n+1-k$ possibilities to choose a_n. As (in consideration of Theorem 1a)) for all (a_k, b_k) $(1 \le k \le n-1)$, the elements a_k, b_k belong to the same cycle of ψ', there are (for fixed k, a_n) $\binom{n-1}{k-1} N_k N_{n+1-k}$ possibilities for ψ', thus by the induction hypothesis and (1) (with $x := y := 1, m := n-1$) we calculate

$$\begin{aligned}
N_{n+1} &= \sum_{k=1}^{n} (n+1-k) \binom{n-1}{k-1} N_k N_{n+1-k} \\
&= \sum_{k=1}^{n} (n+1-k) \binom{n-1}{k-1} k^{k-2} (n+1-k)^{n+1-k-2} \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} (k+1)^{k-1} (n-k)^{n-1-k} \\
&= (n+1)^{n-1}.
\end{aligned}$$

□

References

[1] Schwenk, A.J., Problem E 3058. *Amer. Math. Monthly* (1984), 516.

[2] Lossers, O.P., Solution to Problem E 3058. *Amer. Math. Monthly* (1986), 820–821.

Daniel Neuenschwander
Université de Lausanne
Institut des Sciences Actuarielles
CH-1015 Lausanne

Universität Bern
Institut für mathematische Statistik und Versicherungslehre
Sidlerstrasse 5
CH-3012 Bern

Sektion Kryptologie
Departement VBS
CH-3003 Bern

e-mail: neuens@bluewindow.ch