Permutations and Reciprocity

Marion Scheepers

Algebra-Cryptology-Geometry Seminar

FALL 2016
1. Signs of Permutations.

2. The Tale of Three Permutations
Acknowledgements


- Dr. Jerry Shurman’s write-up: http://people.reed.edu/~jerry/361/lectures/qrz.pdf
Signs of Permutations. The Tale of Three Permutations

Sign of a Permutation: 1

Fix a positive integer $n$. $S_n$ is the set of one-to-one functions from $\{1, \ldots, n\}$ to itself.
Under functional composition $\circ$, $(S_n, \circ)$ is a group.
Each element of $S_n$ has a representation as a composition of disjoint cycles.
Each cycle has a representation as a composition of 2-cycles.
The parity of the number $n(f)$ of two-cycles used in the representation of a permutation $f$ is fixed, and is either even, or odd.

$$\sigma : S_n \rightarrow \{-1, 1\} : f \mapsto (-1)^{n(f)}$$

is the “sign” map and is a group homomorphism.
Sign of a Permutation: 2

For \( f \in S_n \), the number of pairs \((i, k)\) with \( i < k \) but \( f(i) > f(k) \), denoted \( I(f) \), is the number of inversions of \( f \).

\[
\sigma(f) = (-1)^{I(f)}
\]
Example 1

\[ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 3 & 1 & 8 & 4 & 7 \end{pmatrix} \]

**Cycle Decomposition:**

\[ f = (1 \ 2 \ 5) \circ (3 \ 6 \ 8 \ 7 \ 4). \]

**Decomposition into 2-Cycles:**

\[
(1 \ 2 \ 5) = (1 \ 2) \circ (2 \ 5) = (1 \ 5) \circ (1 \ 2) \\
(3 \ 6 \ 8 \ 7 \ 4) = (3 \ 6) \circ (6 \ 8) \circ (8 \ 7) \circ (7 \ 4) = (3 \ 4) \circ (3 \ 7) \circ (3 \ 8) \circ (3 \ 6)
\]

**Sign of the Permutation:**

\[ \sigma(f) = (-1)^{2+4} = 1. \]

**Number of inversions in** \( f \):  
\[ I(f) = 10. \]
A deck of cards.

$m$ and $n$ are odd positive integers. Cards numbered 0 through $mn - 1$ are laid out in $m$ rows of $n$ each.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>\ldots</th>
<th>\ldots</th>
<th>j</th>
<th>\ldots</th>
<th>n-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>\ldots</td>
<td>\ldots</td>
<td>j</td>
<td>\ldots</td>
<td>n-1</td>
</tr>
<tr>
<td>1</td>
<td>n</td>
<td>n+1</td>
<td>n+2</td>
<td>\ldots</td>
<td>2n+j</td>
<td>\ldots</td>
<td>2n-1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2n</td>
<td>2n+1</td>
<td>2n+2</td>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td>3n-1</td>
<td></td>
</tr>
<tr>
<td>i</td>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td>\ldots</td>
<td></td>
</tr>
<tr>
<td>m-1</td>
<td>(m-1)n</td>
<td>(m-1)n+1</td>
<td>(m-1)n+2</td>
<td>\ldots</td>
<td>(m-1)n+j</td>
<td>\ldots</td>
<td>mn-1</td>
<td></td>
</tr>
</tbody>
</table>
An alternative listing

Next, enumerate this same array of \( mn \) cards column-wise.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>( \cdots )</th>
<th>( j )</th>
<th>( \cdots )</th>
<th>( n-1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>( \cdots )</td>
<td>( j )</td>
<td>( \cdots )</td>
<td>( n-1 )</td>
</tr>
<tr>
<td>1</td>
<td>( n )</td>
<td>( n+1 )</td>
<td>( n+2 )</td>
<td>( \cdots )</td>
<td>( n+j )</td>
<td>( \cdots )</td>
<td>( 2n-1 )</td>
</tr>
<tr>
<td>2</td>
<td>( 2n )</td>
<td>( 2n+1 )</td>
<td>( 2n+2 )</td>
<td>( \cdots )</td>
<td>( 2n+j )</td>
<td>( \cdots )</td>
<td>( 3n-1 )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>( \cdots )</td>
<td>\vdots</td>
<td>( \cdots )</td>
<td>\vdots</td>
</tr>
<tr>
<td>( i )</td>
<td>( in )</td>
<td>( in+1 )</td>
<td>( in+2 )</td>
<td>( \cdots )</td>
<td>( in+j )</td>
<td>( \cdots )</td>
<td>( ((i+1)n-1 )</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>( \cdots )</td>
<td>\vdots</td>
<td>( \cdots )</td>
<td>\vdots</td>
</tr>
<tr>
<td>( m-1 )</td>
<td>((m-1)n)</td>
<td>((m-1)n+1)</td>
<td>((m-1)n+2)</td>
<td>( \cdots )</td>
<td>((m-1)n+j)</td>
<td>( \cdots )</td>
<td>( mn-1 )</td>
</tr>
</tbody>
</table>
The Permutation $\pi_{m,n}$

These two enumerations define a permutation $\pi_{m,n}$ of 
\{0, 1, $\cdots$, $mn - 1$\}.

Consider the card placed in position $(i,j)$ where $i$ is the row number, $j$ the column number with enumeration starting at 0.

The original number is $i \cdot n + j$.

In the new enumeration, this same position card is enumerated, and 
the new number is $i + j \cdot m$

Thus:  
$$\pi_{m,n}(i \cdot n + j) = i + j \cdot m \quad \text{for all } i \text{ and } j$$
The Sign of Permutation $\pi_{m,n}$

To find the sign of $\pi_{m,n}$, count the number of inversions.

**Lemma**

$$\sigma(\pi_{m,n}) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}}.$$ 

**Proof Idea:**

Consider $(i, j)$ and $(i', j')$ in $\{0, 1, \cdots, m-1\} \times \{0, 1, \cdots, n-1\}$ where $i < i'$ but $j > j'$.

We have:

$$\pi_{m,n}(i \cdot n + j) = i + j \cdot m$$ and $$\pi_{m,n}(i' \cdot n + j') = i' + j' \cdot m$$

and

$$i \cdot n + j < i' \cdot n + j', \text{ while } i' + j' \cdot m < i + j \cdot m.$$
If $\gcd(m, n) = 1$ then

$$F : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n : k \mapsto (k \mod m, k \mod n)$$

is a ring isomorphism. $F^{-1}$ is calculated using the Chinese Remainder Theorem.
The Permutation $\mu$

Define the permutation $\mu$ of $\{0, 1, \cdots, m-1\} \times \{0, 1, \cdots, n-1\}$ by:

$$\mu(x, y) = (nx + y \mod m, y)$$

1. On a column indexed “y” $\mu$ is the composition of:
   a) $x \mapsto n \cdot x \mod m$ on $\mathbb{Z}_m$, say $\gamma$
   and
   b) $x \mapsto x + y \mod m$ on $\mathbb{Z}_m$, say $\delta$

2. $\mu$ is the composition of $n$ such permutations, the $k^{th}$ acting on column $y$ only, and the identity on all other columns.
The Permutation $\mu$

\[
\left[ \frac{n}{m} \right] := \sigma(\mu) = (\sigma(\gamma))^n \times (\sigma(\delta))^n.
\]

$\delta$ has $gcd(n, m)$ cycles of length $\frac{m}{gcd(n,m)}$ each.

As $m$ is odd, these numbers are odd, and $\sigma(\delta) = 1$.

As $n$ is odd, $\sigma(\gamma)^n = \sigma(\gamma)$.

\[
\left[ \frac{n}{m} \right] := \sigma(\mu) = \sigma(\gamma).
\]
The Permutation $\nu$

Define the permutation $\nu$ of $\{0, 1, \cdots, m-1\} \times \{0, 1, \cdots, n-1\}$ by:

$$\nu(x, y) = (x, x + my \mod n)$$

1. On a row indexed “x” $\nu$ is the composition of:
   a) $y \mapsto m \cdot y \mod n$ on $\mathbb{Z}_n$, say $\alpha$
   and
   b) $y \mapsto x + y \mod n$ on $\mathbb{Z}_n$, say $\beta$

2. $\nu$ is the composition of $m$ such permutations, the $k^{th}$ acting on row $x$ only, and the identity on all other rows.
The Permutation $\nu$

\[
\left[ \frac{m}{n} \right] := \sigma(\nu) = \sigma(\alpha).
\]

as before
Synthesis

\[ \nu = F \circ \pi_{m,n} \circ F^{-1} \circ \mu \]

Thus

\[ \nu \circ \mu^{-1} = F \circ \pi_{m,n} \circ F^{-1} \]

and so

\[ \sigma(\nu)\sigma(\mu^{-1}) = \sigma(F)\sigma(\pi_{m,n})\sigma(F^{-1}) \]

This reduces to

**Theorem (Zolotarev’s Reciprocity Theorem)**

*For m and n odd relatively prime integers,*

\[ \left[ \frac{m}{n} \right] \left[ \frac{n}{m} \right] = (-1)^{m-1/2} \cdot n^{-1/2} \]
The homomorphism $\frac{\cdot}{m}$.

Each prime number has a primitive root.

**Lemma**

*If m is an odd prime number and g is a primitive root of m, then*

$$\left[ \frac{g^k}{m} \right] = (-1)^{\text{gcd}(k,m-1)}.$$

---

Marion Scheepers

Permutations and Reciprocity
Legends Function

Lemma (Zolotarev)

For an odd prime number $p$, the kernel of the group homomorphism
\[
\left\{ \frac{\cdot}{p} \right\} : \mathbb{Z}_p \setminus \{0\} \to \{-1, 1\}
\]
is the set of quadratic residues of $p$.

Corollary

$\left\{ \frac{\cdot}{p} \right\}$ coincides with the Legendre function $\left( \frac{\cdot}{p} \right)$.

Corollary (Quadratic Reciprocity)

For odd prime numbers $p$ and $q$, $\left\{ \frac{q}{p} \right\}[\left\{ \frac{p}{q} \right\}] = (-1)^{(p-1)(q-1)/4}$. 
THANKS!