

Counting Derangements, Non Bijective Functions and the Birthday Problem¹

Cezary Kaliszyk
Institut für Informatik I4
Technische Universität München
Boltzmannstraße 3
85748 Garching, Germany

Summary. The article provides counting derangements of finite sets and counting non bijective functions. We provide a recursive formula for the number of derangements of a finite set, together with an explicit formula involving the number e . We count the number of non-one-to-one functions between two finite sets and perform a computation to give explicitly a formalization of the birthday problem. The article is an extension of [10].

MML identifier: CARDFIN2, version: 7.11.07 4.146.1112

The notation and terminology used here have been introduced in the following papers: [13], [16], [9], [1], [4], [7], [5], [6], [14], [2], [8], [3], [11], [12], [17], [18], and [15].

1. PRELIMINARIES

In this paper x denotes a set.

One can verify that every finite 0-sequence of $\mathbb{Z}$ is integer-valued.

Let n be a natural number. Observe that $n!$ is natural.

Let n be a natural number. One can check that $n!$ is positive.

Let c be a real number. One can verify that $\exp c$ is positive.

Let us observe that e is positive.

The following two propositions are true:

¹This work has been partially supported by the KBN grant N519 385136.

- (1) $\text{id}_\emptyset$ has no fixpoint.
- (2) For every real number c such that $c < 0$ holds $\exp c < 1$.

2. ROUNDING

Let n be a real number. The functor $\text{round } n$ yielding an integer is defined by:

(Def. 1) $\text{round } n = \lfloor n + \frac{1}{2} \rfloor$.

One can prove the following two propositions:

- (3) For every integer a holds $\text{round } a = a$.
- (4) For every integer a and for every real number b such that $|a - b| < \frac{1}{2}$ holds $a = \text{round } b$.

3. COUNTING DERANGEMENTS

Next we state two propositions:

- (5) Let n be a natural number and a, b be real numbers. Suppose $a < b$. Then there exists a real number c such that $c \in]a, b[$ and $\exp a = (\sum_{\alpha=0}^{\kappa} (\text{Taylor}(\text{the function } \exp, \Omega_{\mathbb{R}}, b, a))(\alpha))_{\kappa \in \mathbb{N}}(n) + \frac{\exp c \cdot (a-b)^{n+1}}{(n+1)!}$.
- (6) For every positive natural number n and for every real number c such that $c < 0$ holds $|-n! \cdot \frac{\exp c \cdot (-1)^{n+1}}{(n+1)!}| < \frac{1}{2}$.

Let s be a set. The functor $\text{derangements } s$ is defined as follows:

(Def. 2) $\text{derangements } s = \{f; f \text{ ranges over permutations of } s: f \text{ has no fixpoint}\}$.

Let s be a finite set. Observe that $\text{derangements } s$ is finite.

Next we state several propositions:

- (7) Let s be a finite set. Then $\text{derangements } s = \{h : s \rightarrow s: h \text{ is one-to-one} \wedge \bigwedge_x (x \in s \Rightarrow h(x) \neq x)\}$.
- (8) For every non empty finite set s there exists a real number c such that $c \in]-1, 0[$ and $\overline{\overline{\text{derangements } s}} - \frac{\overline{\overline{s!}}}{e} = -\overline{\overline{s!}} \cdot \frac{\exp c \cdot (-1)^{\overline{\overline{s}}+1}}{(\overline{\overline{s}}+1)!}$.
- (9) For every non empty finite set s holds $|\overline{\overline{\text{derangements } s}} - \frac{\overline{\overline{s!}}}{e}| < \frac{1}{2}$.
- (10) For every non empty finite set s holds $\overline{\overline{\text{derangements } s}} = \text{round}(\frac{\overline{\overline{s!}}}{e})$.
- (11) $\text{derangements } \emptyset = \{\emptyset\}$.
- (12) $\text{derangements}\{x\} = \emptyset$.

The function der seq from $\mathbb{N}$ into $\mathbb{Z}$ is defined as follows:

(Def. 3) $(\text{der seq})(0) = 1$ and $(\text{der seq})(1) = 0$ and for every natural number n holds $(\text{der seq})(n+2) = (n+1) \cdot ((\text{der seq})(n) + (\text{der seq})(n+1))$.

Let c be an integer and let F be a finite 0-sequence of $\mathbb{Z}$. Observe that cF is finite, integer-valued, and transfinite sequence-like.

Let c be a complex number and let F be an empty function. One can check that cF is empty.

Next we state three propositions:

- (13) For every finite 0-sequence F of $\mathbb{Z}$ and for every integer c holds $c \cdot \sum F = \sum((cF) \upharpoonright (\text{len } F -' 1)) + c \cdot F(\text{len } F -' 1)$.
- (14) Let X, N be finite 0-sequences of $\mathbb{Z}$. Suppose $\text{len } N = \text{len } X + 1$. Let c be an integer. If $N \upharpoonright \text{len } X = cX$, then $\sum N = c \cdot \sum X + N(\text{len } X)$.
- (15) For every finite set s holds $(\text{der seq})(\overline{s}) = \overline{\overline{\text{derangements } s}}$.

4. COUNTING NOT-ONE-TO-ONE FUNCTIONS AND THE BIRTHDAY PROBLEM

Let s, t be sets. The functor $\text{not-one-to-one}(s, t)$ yields a subset of t^s and is defined by:

(Def. 4) $\text{not-one-to-one}(s, t) = \{f : s \rightarrow t : f \text{ is not one-to-one}\}$.

Let s, t be finite sets. Observe that $\text{not-one-to-one}(s, t)$ is finite.

The scheme *FraenkelDiff* deals with sets $\mathcal{A}, \mathcal{B}$ and a unary predicate $\mathcal{P}$, and states that:

$$\{f : \mathcal{A} \rightarrow \mathcal{B} : \text{not } \mathcal{P}[f]\} = \mathcal{B}^{\mathcal{A}} \setminus \{f : \mathcal{A} \rightarrow \mathcal{B} : \mathcal{P}[f]\}$$

provided the following requirement is met:

- If $\mathcal{B} = \emptyset$, then $\mathcal{A} = \emptyset$.

We now state three propositions:

- (16) For all finite sets s, t such that $\overline{s} \leq \overline{t}$ holds $\overline{\overline{\text{not-one-to-one}(s, t)}} = \overline{\overline{t}}^{\overline{s}} - \frac{\overline{t}!}{(\overline{t} -' \overline{s})!}$.
- (17) For every finite set s and for every non empty finite set t such that $\overline{s} = 23$ and $\overline{t} = 365$ holds $2 \cdot \overline{\overline{\text{not-one-to-one}(s, t)}} > \overline{t}^{\overline{s}}$.
- (18) For all non empty finite sets s, t such that $\overline{s} = 23$ and $\overline{t} = 365$ holds $P(\text{not-one-to-one}(s, t)) > \frac{1}{2}$.

REFERENCES

- [1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(2):377–382, 1990.
- [2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
- [3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(1):91–96, 1990.
- [4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(3):507–513, 1990.
- [5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [7] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(1):165–167, 1990.

- [8] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(5):887–890, 1990.
- [9] Yatsuka Nakamura and Hisashi Ito. Basic properties and concept of selected subsequence of zero based finite sequences. *Formalized Mathematics*, 16(3):283–288, 2008, doi:10.2478/v10037-008-0034-y.
- [10] Karol Pąk. Cardinal numbers and finite sets. *Formalized Mathematics*, 13(3):399–406, 2005.
- [11] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(2):213–216, 1991.
- [12] Konrad Raczkowski and Paweł Sadowski. Topological properties of subsets in real numbers. *Formalized Mathematics*, 1(4):777–780, 1990.
- [13] Piotr Rudnicki and Andrzej Trybulec. Abian’s fixed point theorem. *Formalized Mathematics*, 6(3):335–338, 1997.
- [14] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [15] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.
- [16] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(4):825–829, 2001.
- [17] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.
- [18] Yuguang Yang and Yasunari Shidama. Trigonometric functions and existence of circle ratio. *Formalized Mathematics*, 7(2):255–263, 1998.

Received November 27, 2009
