Discrete Mathematics

Exercise sheet 3

17 /20 October 2016

Notation: $[n] = \{1, 2, \ldots, n\}$.

1.

(a) State how many functions there are from $[n]$ to $[m]$, where $m, n \in \mathbb{N}$.

There are m^n such functions (number of sequences of n elements $f(1), f(2), \ldots, f(n)$, each element chosen freely from $[m]$).

(b) Deduce from your answer to (a) that there are 2^n subsets of $[n]$.

A subset $S \subseteq [n]$ is uniquely defined by its *characteristic function* (or *indicator function*) $f_S : [n] \to \{0, 1\}$, defined for $x \in [n]$ by

$$f_S(x) = \begin{cases} 1 & x \in S, \\ 0 & x \notin S. \end{cases}$$

By (a) there are 2^n functions $f : [n] \to \{0, 1\}$, and hence 2^n subsets of $[n]$.

(c) Determine the number of ordered pairs (A, B), where $A \subseteq B \subseteq [n]$.

The triple of sets $(A, B \backslash A, [n] \backslash B)$ are disjoint and their union is $[n]$ (i.e. they form an ordered partition of $[n]$). There is a bijection between such ordered partitions of $[n]$ into three subsets and functions $f : [n] \to [3]$ (for example, by the correspondence $A \leftrightarrow \{x \in [n] : f(x) = 1\} = f^{-1}(\{1\})$, $B \backslash A \leftrightarrow f^{-1}(\{2\})$ and $[n] \backslash B \leftrightarrow f^{-1}(\{3\})$.

To recover (A, B) with $A \subseteq B \subseteq [n]$ from the ordered partition $(A, B \backslash A, [n] \backslash B)$ of $[n]$ into three subsets, let A be the first subset and B the union of the first two.

Hence there are 3^n ordered pairs (A, B) in which $A \subseteq B \subseteq [n]$.

(d) Determine the number of ordered triples (A, B, C), where $A \subseteq B \subseteq C \subseteq [n]$.

The quadruple of sets $(A, B \backslash A, C \backslash B, [n] \backslash C)$ are disjoint and their union is $[n]$. These are in one-to-one correspondence with functions $f : [n] \to [4]$, and in a similar way to (c) we conclude that there are 4^n ordered triples (A, B, C) with $A \subseteq B \subseteq C \subseteq [n]$.

2. A permutation of $[n]$ is a bijection $f : [n] \to [n]$.

(a) Look up/remind yourself what is meant by a *cycle* of the permutation f (e.g. section 3.2 of Matoušek & Nešetřil, *Invitation to Discrete Mathematics*, page 65 in 2nd ed).

A cycle of f consists of a finite sequence $x, f(x), f^2(x), \ldots, f^{\ell-1}(x)$, where ℓ is the least positive integer such that $f^{\ell}(x) = x$. The next term in the sequence is obtained by applying f, including the “wrap-around” at the end, $f(f^{\ell-1}(x)) = x$. (There is such an integer ℓ since $[n]$ is finite: among the $n + 1$ elements $x, f(x), f^2(x), \ldots, f^n(x)$, each belonging to $[n]$, by the pigeon-hole principle there must be $0 \le i < j \le n$ such that $f^i(x) = f^j(x)$, from which $x = f^{j-i}(x)$ by applying (composing) the inverse function f^{-1} on both sides of this equality i times, and taking ℓ to be the least positive value of $j - i$ for such pairs i, j.)

Usually a cycle of a permutation f is written $(\ x \quad f(x) \quad f^2(x) \quad \ldots \quad f^{\ell-1}(x)\ )$

Note that rather than at x we could start the cycle at $f^i(x)$ for any $0 \le i \le \ell - 1$: $(\ f^i(x) \quad f^{i+1}(x) \quad f^{i+2}(x) \quad \ldots \quad f^{\ell+i-1}(x)\ )$ is the same cycle.

Two cycles

$$(\ x_1 \quad x_2 \quad x_3 \quad \ldots \quad x_\ell\ ) \quad \text{and} \quad (\ y_1 \quad y_2 \quad y_3 \quad \ldots \quad y_m\ )$$

are the same permutation if and only if $\ell = m$ and there is $0 \le d < \ell$ such that

$$y_i = \begin{cases} x_{i+d} & i + d \le \ell \\ x_{i+d-\ell} & i + d > \ell \end{cases}$$

(this just says that you can cyclically permute the elements y_i to obtain the elements x_i). For example, $(\ 1 \quad 2 \quad 3\ )$, $(\ 2 \quad 3 \quad 1\ )$ and $(\ 3 \quad 1 \quad 2\ )$ are the same cycle, while $(\ 3 \quad 2 \quad 1\ )$, $(\ 1 \quad 3 \quad 2\ )$ and $(\ 2 \quad 1 \quad 3\ )$ are different to these.

(b) How many permutations of $[n]$ have a single cycle?

A sequence of length n is cyclically equivalent to n distinct cycles (including itself). There are $n!$ sequences of length n with elements in $[n]$. Hence there are $n!/n = (n-1)!$ permutations of $[n]$ consisting of a single cycle.

(c) For a permutation $f : [n] \to [n]$, define the k-fold composition of f recursively by $f^1 = f$ and $f^k = f^{k-1} \circ f$. Let R be the relation on $[n]$ defined by $(x, y) \in R$ if and only if there exists an integer $k \ge 1$ such that $f^k(x) = y$.

Prove that the relation R is reflexive, symmetric and transitive.

$(x, x) \in R$: $f^\ell(x) = x$, where ℓ is the length of the cycle containing x.

$(x, y) \in R$ implies $(y, x) \in R$: if $f^k(x) = y$ then x, y belong to the same cycle, say of length ℓ, and we may assume $0 \le k < \ell$. Then $f^\ell(y) = y = f^k(x)$, from which $f^{\ell-k}(y) = x$.

$(x, y) \in R$ and $(y, z) \in R$ imply $(x, z) \in R$: by hypothesis there are positive integers k, j such that $f^k(x) = y$ and $f^j(y) = z$. By substitution, $z = f^j(f^k(x)) = f^{j+k}(x)$, so that $(x, z) \in R$.

3. Let $\binom{n}{k}$ denote the number of subsets of k elements from $[n]$. (For $n \ge 0$ we have $\binom{n}{0} = 1 = \binom{n}{n}$.)

Prove the following identities by using this combinatorial definition of $\binom{n}{k}$:

(a) $\binom{n}{n-k} = \binom{n}{k}$ for $0 \le k \le n$.

There is a one-to-one correspondence between subsets $S \subseteq [n]$ of size k and their complements $[n] \setminus S$, which are subsets of size $n - k$.

(b) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ for $1 \le k \le n - 1$.

Subsets $S \subseteq [n]$ of size k may be partitioned into two classes: subsets of $[n-1]$ of size k and sets $\{n\} \cup T$ where $T \subseteq [n-1]$ has size $k - 1$.

(c)

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

By 1(b) the number of subsets of $[n]$ is 2^n, and these can be partitioned according to their size $0 \leq k \leq n$ and by definition there are $\binom{n}{k}$ subsets of size k.

(d)

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

NB The identity holds for $n \geq 1$ (when $n = 0$ the sum is 1).

Taking all the negative terms to the other side of this equality, the assertion is that the number of subsets of $[n]$ having even size is equal to the number of subsets having odd size. If n is odd this is immediate by the bijection between subsets and their complements (these have opposite parity, since n is odd).

For an argument that works for both odd and even n, partition sets as in part (b) into those that contain n as an element and those that do not. The map $S \mapsto S \cup \{n\}$ is a bijection between those not containing n and those containing n, with the property that it changes the parity of the set (from odd to even, or even to odd). This pairing of an odd-sized subset with an even-sized subset establishes that the number of odd-sized subsets is equal to the number of even-sized subsets.

[Alternatively, define a bijection on the set of all subsets of $[n]$ by the map $S \mapsto S \triangle \{n\}$ (symmetric difference with $\{n\}$, i.e., remove the element n if it belongs to S, add n to S otherwise).]