Mathematical Foundations of Computer Science
Lecture Outline
November 19, 2024

Functions

Let A and B be sets. A *function* from A to B is a relation, f, from A to B such that for all $a \in A$ there is exactly one $b \in B$ such that $(a, b) \in f$. If $(a, b) \in f$, then we write $b = f(a)$. A function from A to B is also called a *mapping* from A to B and we write it as $f : A \to B$. The set A is called the *domain* of f and the set B the codomain. If $a \in A$ then the element $b = f(a)$ is called the *image* of a under f. The *range* of f, denoted by $\text{Ran}(f)$ is the set

$$Ran(f) = \{b \in B \,|\, \exists a \in A \text{ such that } b = f(a)\}$$

Two functions are *equal* if they have the same domain, have the same codomain, and map each element of the domain to the same element in the codomain.

Example. Let A and B be finite sets of size a and b, respectively. How many functions are there from A to B?

Solution. The procedure of forming a function is as follows: in Step i choose the image of the ith element in A. There are a steps and there are b ways to perform each step. Thus the total number of ways to create a function from A to B is b^a.

Let $f : A \to B$ be a function.

- f is said to be *one-to-one* or *injective*, iff for every $x, y \in A$ such that $x \neq y, f(x) \neq f(y)$.
- f is called *onto* or *surjective*, iff for every element $b \in B$ there is an element $a \in A$ with $f(a) = b$.
- f is a *one-to-one correspondence* or *bijection*, if it is both one-to-one and onto.

Example. Classify the following functions.

- $f_1(x) = x^2$ from the set of integers to the set of integers.
- $f_2(x) = x^2$ from the set of non-negative real numbers to the set of non-negative real numbers.
- $f_3(x) = x + 1$ from the set of integers to the set of integers.
- $f_4(x) = x$ from a set A to A. This function is called the identity function.

Solution.

$$\begin{aligned} \text{injective} &: f_2, f_3, f_4 \\ \text{surjective} &: f_2, f_3, f_4 \\ \text{bijective} &: f_2, f_3, f_4 \end{aligned}$$

Inverse and Composition

Let f be a one-to-one correspondence from the set A to the set B. The *inverse* function of f is the function that maps an element $b \in B$ to the unique element $a \in A$ such that $f(a) = b$. The inverse function of f is denoted by f^{-1}. Hence $f^{-1}(b) = a$ when $f(a) = b$.

Note that if f is not bijective then its inverse does not exist.

Let $f : A \to B$ and $g : B \to C$ be functions. The *composition* of the function g with f is the function $g \circ f : A \to C$, defined by

$$(g \circ f)(x) = g(f(x)), \forall x \in A$$

Example. Let g be the function from the set $\{a, b, c\}$ to itself such that $g(a) = b, g(b) = c$, and $g(c) = a$. Let f be the function from the set $\{a, b, c\}$ to the set $\{1, 2, 3\}$ such that $f(a) = 3, f(b) = 2$, and $f(c) = 1$. What is the composition of f with g and what is the composition of g with f?

Solution. The composition function $f \circ g$ is as follows: $(f \circ g)(a) = f(g(a)) = f(b) = 2$, $(f \circ g)(b) = f(g(b)) = f(c) = 1$, and $(f \circ g)(c) = f(g(c)) = f(a) = 3$.

$(g \circ f)$ is not defined as the range of f is not a subset of the domain of g.

Example. Let f and g be the functions from the set of integers to the set of integers defined by $f(x) = 2x + 3$ and $g(x) = 3x + 2$. What is the composition of f and g? What is the composition of g and f?

Solution. $(f \circ g)(x) = f(g(x)) = 2(3x+2)+3 = 6x+7$. Similarly, $(g \circ f)(x) = g(f(x)) = 3(2x + 3) + 2 = 6x + 11$. This example shows that commutative law does not apply to the composition of functions.

Example. Let $f : A \to B$ and $g : B \to C$ be two functions. Then

i. if f and g are surjective then so is $g \circ f$.

ii if f and g are injective then so is $g \circ f$.

iii if f and g are bijective then so is $g \circ f$.

Solution. Let $c \in C$. Since g is surjective there must be a $b \in B$ such that $g(b) = c$. Since f is surjective there must be a $a \in A$ such that $f(a) = b$. Thus $(g \circ f)(a) = g(f(a)) = g(b) = c$. This proves that $g \circ f$ is surjective.

Let $a, a' \in A$ such that $(g \circ f)(a) = (g \circ f)(a')$. This means that $g(f(a)) = g(f(a'))$. Since g is injective we have $f(a) = f(a')$. Then since f is injective, we have $a = a'$.

The bijectivity of $(g \circ f)$ follows from the injectivity and surjectivity of $(g \circ f)$.

The *Ramsey number* $R(k, l)$ is the smallest number n such that any graph with n vertices has clique of size k or an independent set of size l. Another way to formulate this is: in any two-coloring (say, red and blue) on edges of the complete graph on n vertices, there is a monochromatic red clique of size k or a monochromatic blue clique of size l. Diagonal Ramsey Number asks for the value of $R(k, k)$ for any integer k. Finding a diagonal Ramsey number even for $k = 6$ is very difficult. We want to find a lower bound on $R(k, k)$.

Example. If $\binom{n}{k}2^{1-\binom{k}{2}} < 1$, then $R(k, k) > n$. In particular, $R(k, k) > \lfloor 2^{\frac{k}{2}} \rfloor$, for $k \geq 3$.

Solution. Consider a complete graph G in which each edge is colored red or blue with a probability of $1/2$. Let S be a any subset of k vertices and $E(S)$ be the set of edges with both endpoints in S.

$$\Pr[\text{edges in } E(S) \text{ are monochromatic}] = 2 \cdot 2^{-\binom{k}{2}}$$

Since there are $\binom{n}{k}$ subsets of size k, the probability that some subset of size k is monochromatic is at most

$$2\binom{n}{k}2^{-\binom{k}{2}} = \binom{n}{k}2^{1-\binom{k}{2}} \tag{1}$$

Since the last expression is less than 1 (given as a condition in the problem statement), there is a 2-coloring of edges of a complete graph on n vertices in which there is no monochromatic clique of size k. Thus $R(k, k) > n$.

If $n = \lfloor 2^{k/2} \rfloor$ then

$$\binom{n}{k}2^{1-\binom{k}{2}} \leq \frac{n^k}{k!} \cdot 2^{1-\frac{k(k-1)}{2}} \leq \left(\frac{2^{k^2/2}}{k!}\right) 2^{1-\frac{k^2}{2}+\frac{k}{2}} = \frac{2^{1+\frac{k}{2}}}{k!}$$

Note that the last expression is less than 1, if $k \geq 3$.

It can be shown that $R(k, k) < 4^k$. These are the best known bounds on the size of $R(k, k)$, so a lot of progress is yet to be made. What is known is that $R(2, 2) = 2, R(3, 3) = 6$, and $R(4, 4) = 18$. The values of $R(k, k)$ are not known for $k \geq 5$.

Recall that a tournament is a directed graph with exactly one directed edge between any pair of vertices. A tournament $G = (V, E)$ is called k-dominated if for every set of k vertices $v_1, v_2, \ldots, v_k$, there exists another vertex $u \in V$ such that $(u, v_i) \in E$, for $i = 1, 2, \ldots, k$.

Example. Prove that for any positive integer k, if n is large enough then there is a k-dominated tournament on n vertices. For sufficiently large values of k, $n = k^2 2^k$ suffices.

Solution. Note that for $k = 1$, a tournament on three vertices that is a directed 3-cycle is 1-dominated. We assume $k \geq 2$ for the rest of the proof. Construct a random tournament G in which an edge between any two vertices u and v is directed towards u with probability $\frac{1}{2}$ and towards v with probability $\frac{1}{2}$. The bad event for our random process is that G is not k-dominated. We will calculate the probability of this bad event as follows. Let S be a fixed set of k vertices in G. The probability that a vertex u outside of S does not dominate set S is given by $1 - (1/2)^k$. Thus the probability that S is not dominated by any of the $n - k$ vertices outside of S is given by $(1 - 1/2^k)^{n-k}$. Since there are $\binom{n}{k}$ possibilities for set S, the probability of some set of k vertices in G not being dominated is at most

$$\binom{n}{k}\left(1 - \frac{1}{2^k}\right)^{n-k} \tag{2}$$

If the above expression is less than 1, it means that the probability of the random tournament G being k-dominated is strictly larger than 0, which means that such a tournament exists.