Winter 2021 Math 61 Notes

Kyle Chui

2021-1-27

Contents

1 Sets and Functions

1.1 Power Sets

Definition. *Power Set*
If X is a set, the *power set* of X, denoted $\mathscr{P}(X)$, is the set of subsets of X.

Example. *Power Sets*

- $\mathscr{P}(\varnothing) = \{\varnothing\}$
- $\mathscr{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$
- $\mathscr{P}(\{a, b, c\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

Definition. *Cardinality of Finite Sets*
If X has finitely many elements, then $|X|$ denotes the number of elements of X.

Theorem — *Cardinality of Power Sets*
If X is finite, then $|\mathscr{P}(X)| = 2^{|X|}$.

Proof. Let us induct on the cardinality of the set X. Suppose $|X| = 0$, so that $X = \varnothing$. Then $\mathscr{P}(X) = \{\varnothing\}$, so $|\mathscr{P}(X)| = 1 = 2^0$. Thus the statement is true when $|X| = 0$.

Suppose that the statement holds for some non-negative integer k. Let Y be a set such that $|Y| = k + 1$, and $y \in Y$. Observe that we may split $\mathscr{P}(Y)$ into two groups: the subsets containing y, and the subsets that do not contain y. A subset of Y that does not contain y is exactly $Y \setminus \{y\}$, which has k elements. By the inductive hypothesis, there exist 2^k such subsets. A subset of Y that does contain y is obtained by adding y to a subset of Y which does not contain y. Again, there are 2^k such subsets. Any subset of Y either does or does not contain y (but not both), so there are $2^k + 2^k = 2^{k+1}$ subsets of Y. Therefore $\mathscr{P}(X) = 2^{|X|}$ for all finite sets $|X|$. □

1.2 Functions

Definition. *Function*
If X, Y are sets, a function f from X to Y, written $f\colon X \to Y$ is a subset of $X \times Y$ satisfying two properties:

- For all $a \in X$, there exists $b \in Y$ such that $(a, b) \in f$
  - Everything in the domain must get mapped to something in the codomain
- For all $a \in X$ and $b, b' \in Y$, if $(a, b), (a, b') \in f$, then $b = b'$
  - Every element in the domain can map to at most one element in the codomain

Note (Function Notation). If $(a, b) \in f$, we write $f(a) = b$.

Example. *Functions*

- $f\colon \mathbb{Z} \to \mathbb{N}$ such that $f(x) = x^2$
- $g\colon \mathbb{N} \to \mathbb{N}$ such that $g(x) = x^2$

Note that f and g are different functions.

Definition. *Domain and Codomain of a Function*
If $f\colon X \to Y$, X is the domain of f and Y is the codomain of f.

Definition. *Range of a Function*
For $f\colon X \to Y$, the range of f is:

$$\operatorname{range} f = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}$$

Definition. *Surjectivity*
A function $f\colon X \to Y$ is *onto* or *surjective* if $\operatorname{range} f = Y$. In other words, a function is surjective if its range is equal to its codomain.

Example. *Surjective Functions*

- $f\colon \{a, b, c\} \to \{d, e, f\}$ defined by $f = \{(a, d), (b, e), (c, f)\}$
- $f\colon \mathbb{Z} \to \mathbb{N}$ defined by $f(x) = |x|$

Definition. *Injectivity*
A function $f\colon X \to Y$ is *one-to-one* or *injective* if, for all $x, y \in X$, $f(x) = f(y)$ implies that $x = y$. In other words, different elements in the domain map to different elements in the codomain.

Example. *Injective Functions*

- $g\colon \mathbb{N} \to \mathbb{N}$ defined by $g(x) = x^2$

Note (Properties of Functions). Observe that the both the domain and codomain of a function matter when it comes to determining whether the function satisfies certain properties. For instance, $f\colon \mathbb{Z} \to \mathbb{N}$ defined by $f(x) = x^2$ is not injective, but restricting the domain to $\mathbb{N}$ would make it injective. Similarly, a function $f\colon \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective, but restricting the codomain to $\mathbb{N}$ would make it surjective.

Definition. *Composition of Functions*
If $f\colon X \to Y, g\colon Y \to Z$ are functions, then $g \circ f\colon X \to Z$ is a function defined by $(g \circ f)(x) = g(f(x))$.

Theorem — *Composition of Injective/Surjective Functions is Injective/Surjective*
Let $f\colon X \to Y$, $g\colon Y \to Z$.

- If f, g are injective, so is $g \circ f$
- If f, g are surjective, so is $g \circ f$

Proof. Suppose f, g are injective functions. Let $x, x' \in X$ such that $(g \circ f)(x) = (g \circ f)(x')$. Then

$$\begin{aligned} g(f(x)) &= g(f(x')) \\ f(x) &= f(x') && \text{(Because } g \text{ is injective)} \\ x &= x' && \text{(Because } f \text{ is injective)} \end{aligned}$$

Therefore $g \circ f$ is injective. □

Proof. Suppose f, g are surjective functions. Let $z \in Z$. Because g is surjective, there exists some $y \in Y$ such that $g(y) = z$. Furthermore, because f is surjective, there exists some $x \in X$ such that $f(x) = y$. Thus, for every $z \in Z$, there exists some $x \in X$ such that $(g \circ f)(x) = g(f(x)) = g(y) = z$, so $g \circ f$ is surjective. □

Definition. *Bijectivity*
If a function is both injective and surjective, then we say that it is *bijective*.

Note (Cardinality and Bijections). If there is a bijection between two sets, they have the same number of elements.

1.3 Inverses of Functions

Definition. *Inverse of a function*
Suppose $f\colon X \to Y$, $g\colon Y \to X$ is an inverse to f (soon we'll prove that inverses are unique if they exist) if $f \circ g$ and $g \circ f$ are the identity. In other words, $(g \circ f)(x) = x$, $(f \circ g)(y) = y$ for all $x \in X$, $y \in Y$.

Theorem — *Bijective $\iff$ Inverse*
For $f\colon X \to Y$, f is a bijection if and only if f has an inverse.

Proof. Suppose f has an inverse function g. Then $f \circ g$ and $g \circ f$ are the identity. Suppose $f(a) = f(b)$. Then

$$\begin{aligned} f(a) &= f(b) \\ g(f(a)) &= g(f(b)) \\ (g \circ f)(a) &= (g \circ f)(b) \\ a &= b. \end{aligned}$$

Thus f is injective.

Suppose $b \in Y$. Since $f \circ g$ is the identity, we have that $(f \circ g)(b) = b$, so $f(g(b)) = b$. Thus f is surjective. Therefore f is a bijection.

Now suppose that f is a bijection. We define $f^{-1}(a)$ by $f^{-1}(a) = b$, where $a = f(b)$.

- Because f is surjective, we have that for all $a \in Y$, there exists some $b \in X$ such that $a = f(b)$.

- Because f is injective, any $a \in Y$ is *uniquely* mapped by some $b \in X$.

Thus f^{-1} is a function. We will now show that f^{-1} is the inverse of f. For all $x \in X$, $(f^{-1} \circ f)(x) = x$ by definition. For all $y \in Y$,

$$\begin{aligned}(f \circ f^{-1})(y) &= f(f^{-1}(y)) \\ &= f(f^{-1}(f(x))) && \text{(Because } f \text{ is surjective)} \\ &= f(x) && ((f^{-1} \circ f)(x) = x) \\ &= y.\end{aligned}$$

Therefore f^{-1} is the inverse of f. □

Theorem — *Uniqueness of Inverses*
Inverses of functions are unique, provided they exist.
Suppose $f\colon X \to Y$. If f has inverses $g, h\colon Y \to X$ such that $g \circ f = h \circ f = \mathrm{id}_X$, $f \circ g = f \circ h = \mathrm{id}_Y$, then $g = h$.

Proof. Let $y \in Y$. By the previous theorem we know that f is surjective, so $y = f(x)$, for some $x \in X$. Thus

$$\begin{aligned}g(y) &= g(f(x)) \\ &= x \\ &= h(f(x)) \\ &= h(y).\end{aligned}$$

Thus $g = h$ and the inverse is unique. □

1.4 Special Functions

Definition. *Sequence of elements*
A sequence in X is a function $s\colon D \to X$ where $D \subseteq \mathbb{Z}$.

Example. *Sequence*

(a) $X = \{a, b, c\}$, $D = \{1, 2, 3, 4, 5\}$. We may define $s\colon D \to X$ by:

$$\begin{aligned}1 &\mapsto a \\ 2 &\mapsto b \\ 3 &\mapsto c \\ 4 &\mapsto b \\ 5 &\mapsto a\end{aligned}$$

(b) The Fibonacci numbers are a sequence of natural numbers. They are defined by: $F_0 = 0, F_1 = 1$, and for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$.

(c) Sequence of even natural numbers: $0, 2, 4, 6, 8, \ldots$. The function $e\colon \mathbb{N} \to \mathbb{N}$ is defined by $e(n) = 2n$. Observe that the sequence of the powers of 2 is a subsequence of the even natural numbers.

Definition. *Subsequences*
A *subsequence* of $s\colon D \to X$ is a sequence obtained by restricting the domain of s. In other words, a *subsequence* is a sequence of the form $t\colon D' \to X$ where $D' \subseteq D$.

Definition. *Strings*
If X is a finite set, a *string* over X is a finite sequence of elements of X.

Example. *Strings*

(a) Let X be the English alphabet. Then c, a, t and d, o, g and m, a, t, h are all strings over X. We write strings without parentheses and commas, so c, a, t becomes *cat*.

Definition. *Special strings*
We will let X^* denote the set of strings over X. Additionally, let λ be the null string.

If α, β are strings over X, we can concatenate them to get a new string $\alpha\beta$.

Example. *Concatenation*
The string c, a, t concatenated with d, o, g becomes c, a, t, d, o, g or *catdog*.

Definition. *Substrings*
A *substring* is a string obtained by selecting some or all consecutive terms of another string. Observe that the terms must be consecutive, unlike subsequences.

2 Relations

Definition. *Relations*
A *relation* R from a set X to a set Y is a subset of $X \times Y$. We write $R(x, y)$ or xRy to denote $(x, y) \in R$. If R is a relation from X to X, we say that R is a relation on X.

Note (Relations and functions). Functions are a special type of relation.

Example. *Relations*

(a) Let X = students at UCLA, Y = Classes at UCLA in Winter '21 Quarter. Define R to be a relation between X and Y such that

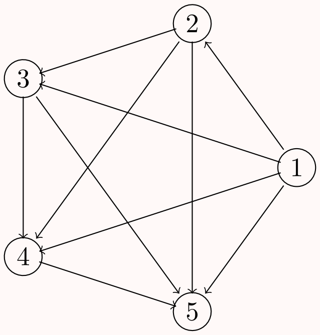
$$R = \{(x, y) \in X \times Y \mid x \text{ is a student in } y\}.$$

Is R a function? No, because a student can be taking more than one class during the Winter '21 Quarter.

(b) Let $X = \{2, 3, 4, 5\}$ and $Y = \{4, 5, 6, 7, 8\}$. Define the relation R to be: xRy if x divides y. Then

$$R = \{(2, 4), (2, 6), (2, 8), (3, 6), (4, 4), (4, 8), (5, 5)\}.$$

(c) Let $X = \{1, 2, 3, 4, 5\}$ and define a relation R on X so that xLy if $x < y$. We can visualise this by drawing an arrow $x \to y$ if $x < y$.



(d) Let $X = \{1, 2, 3, 4, 5\}$, and define a relation LE on X such that $xLEy$ if $x \leq y$. The diagram is the exact same as above, but every element is also related to itself (because $x \leq x$ for all x).

2.1 Types of Relations

(a) Reflexive: R is reflexive if for all $x \in X$, xRx (x relates to itself).

(b) Symmetric: R is symmetric if for all $x, y \in X$, $xRy \implies yRx$.

(c) Antisymmetric: R is antisymmetric if for all $x, y \in X$, xRy and yRx implies $x = y$.

(d) Transitive: R is transitive if for all $x, y, z \in X$, xRy and yRz implies xRz.

Example. *Types of relations*

(a) The relation $<$ over the reals is transitive, (vacuously) antisymmetric, not symmetric, and not reflexive.

(b) The relation $\leq$ over the reals is transitive, antisymmetric, not symmetric, and not reflexive.

(c) Let $X =$ people, and xNy if x and y have the same name. Then N is reflexive, symmetric, and transitive.

(d) Let $X =$ people, and xTy if x is taller than y. Then T is transitive, because if x is taller than y, and y is taller than z, then x is taller than z.

Definition. *Inverse of a relation*
If R is a relation from X to Y, then R^{-1} is the relation from Y to X defined by:

$$R^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in R\}.$$

Definition. *Composition of relations*
If $R \subseteq X \times Y$, and $S \subseteq Y \times Z$, then $S \circ R \subseteq X \times Z$ such that

$$S \circ R = \{(x, z) \in X \times Z \mid \text{there exists } y \in Y \text{ such that } (x, y) \in R \text{ and } (y, z) \in S\}.$$

2.2 Equivalence Relations

Definition. *Equivalence relation*
A relation R on aset X is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Note. An equivalence relation gives us a notion of two different elements in a set being “the same”.

- Reflexive: Everything is “the same” as itself
- Symmetric: If x is “the same” as y, then y is “the same” as x
- Transitive: If x is “the same” as y, and y is “the same” as z, then x is “the same” as z

Example. *Equivalence Relations*

(a) The relation E on the integers where xEy if $x - y$ is even.

- Reflexive: For all $x \in \mathbb{Z}$, $x - x = 0$, which is even, so xEx
- Symmetric: For all $x, y \in \mathbb{Z}$, if $x - y$ is even, so is $-(x - y) = y - x$. Thus if xEy, then yEx
- Transitive: For all $x, y, z \in \mathbb{Z}$, if $x - y$ is even and $y - z$ is even, then their sum, $x - z$, is also even. Thus if xEy and yEz, then xEz.

Observe that this relation relates two integers if they have the same parity.

(b) Let Y be any finite set, and $a, b \in Y^*$ (the set of all strings constructed using Y). Consider the relation L over Y^* such that aLb if a and b have the same length.

(c) Let X be the set of all animals, with animals $x, y \in X$. Consider the relation S over X such that xSy if x and y are of the same species.

(d) Let $x, y \in \mathbb{R}$. Consider the relation C over $\mathbb{R}$ such that xCy if $x - y$ is an integer.

Definition. *Equivalence Classes*
If R is an equivalence relation on a set X, then for $x \in X$, the *equivalence class* of X is the set (with respect to R), denoted by $[x] = [x]_R = \{y \in X \mid xRy\}$.

Example. *Equivalence Classes*

(a) Let E be a relation on $\mathbb{Z}$, where xEy if $x - y$ is even. The equivalence classes for E are $[0]$ (the evens) and $[1]$ (the odds). So, the set of equivalence classes $= \{[0], [1]\}$.

(b) Let $x, y \in \mathbb{R}$, with the relation C over $\mathbb{R}$ defined by xCy if $x - y$ is an integer. The set of equivalence classes $= \{[x] \mid x \in [0, 1)\}$.

If R is an equivalence relation on a set X, then:

- For all $x \in X$, if $x \in [y]$ and $x \in [z]$, then $[y] = [z]$.

  Proof. Suppose $x \in [y]$ and $x \in [z]$. Let $w \in [y]$. Because $w \in [y]$, we know that yRw. We also know that yRx because $x \in [y]$. By symmetry of R, we have wRy, and by transitivity, we have wRx. But $x \in [z]$, so zRx, and by symmetry we have xRw. By transitivity, zRw so $w \in [z]$. Thus $[y] \subseteq [z]$.

  By a similar argument, we have that $[z] \subseteq [y]$, so $[y] = [z]$. □

- For any $x \in X$, x is in some equivalence class, $x \in [x]$ by reflexivity.
  So, for every $x \in X$, x is in exactly one equivalence class. If x is in another equivalence class $[y]$, then by the above $[x] = [y]$.

Definition. *Partition*
For X a set, a *partition* $\mathcal{S}$ of X is a set of nonempty subsets of X such that every element of X is an element of exactly one of the subsets. In other words, for all $A, B \in \mathcal{S}$

- $A, B \subseteq X$
- $A, B \neq \varnothing$
- If $A \cap B \neq \varnothing$ then $A = B$
- For all $x \in X$, there exists exactly one $A \in \mathcal{S}$ such that $x \in A$

Note. We showed that if R is an equivalence relation on X then $\{[x]_R \mid x \in X\}$ is a partition of X.

Theorem — *Equivalence Relations and Partitions*
For X a set, there is a bijection $F\colon$ Set of equivalence relations on $X \to$ Set of partitions of X, defined by

$$F(E) = \{[x]_E \mid x \in X\},$$

the inverse function F^{-1} sends a partition $\mathcal{S}$ to the equivalence relation $F^{-1}(\mathcal{S})$ defined by $xF^{-1}(\mathcal{S})y$ if and only if x and y are in the same element of $\mathcal{S}$ (in the same equivalence class of E).

Note. For the theorem above, we need to verify:

- $F^{-1}(\mathcal{S})$ is an equivalence relation,
- $F \circ F^{-1}(\mathcal{S}) = \mathcal{S}$ for all partitions $\mathcal{S}$,
- $F^{-1} \circ F(R) = R$ for all equivalence relations R.

Example. *Equivalence relations* $\iff$ *partitions*
Let

$$\begin{aligned} X &= \{1, 2, 3, 4, 5\} \\ R &= \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,5), (5,1), (1,3), (3,1), (3,5), (5,3), (2,4), (4,2)\}. \end{aligned}$$

What is the corresponding partition, i.e. what is $F(R)$?
The corresponding partition to the aforementioned relation R is $\{\{1,3,5\}, \{2,4\}\}$.

Let $\mathcal{S} = \{\{1,2,3\}, \{4,5\}\}$ what is the corresponding equivalence relation? i.e. what is $F^{-1}(\mathcal{S})$?
The corresponding equivalence relation for S is

$$\{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (4,5), (5,4)\}.$$

3 Counting

Question. If $|X| = n$, and $|Y| = m$, how many functions are there from X to Y?
Every element in the domain must get mapped to something in the codomain, but it does not matter *which* element in the codomain. Furthermore, the function maps each element in the domain to *exactly one* element in the codomain. Observe that for each $x \in X$, there are m "choices" for where x gets mapped. Thus there are $\underbrace{m \cdot m \cdots m}_{n \text{ times}} = m^n$ total functions.

Theorem — *Multiplication principle*
If a set can be enumerated/constructed in t steps (where each step is independent of the other steps) and each step has n_i choices/outcomes, then the set has $n_1 n_2 \cdots n_t$ elements.

Example. I am going to get a pizza from Vito's or D'more's:

Vito's:	D'more's:
2 crusts	1 crust
6 toppings	2 sauces
2 cheeses	3 toppings

The total number of pizzas I could order is: $2 \cdot 6 \cdot 2 + 1 \cdot 2 \cdot 3 = 30$.

Theorem — *Addition principle*
If X and Y are disjoint finite sets, then $|X \cup Y| = |X| + |Y|$.

Example. How many strings of length 5 in $\{0, 1\}$ start with 10 or end with 01?

By the multiplication principle, we know there are 2^3 strings that start with 10. By similar reasoning, there are 2^3 strings that end with 01. Furthermore, there are 2 strings that satisfy both of these properties. Thus the total number of strings satisfying the statement above is $2^3 + 2^3 - 2 = 16$.

Theorem — *Inclusion/Exclusion principle*
If X, Y are finite sets, then

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Note. The addition principle is just a special case of the inclusion/exclusion principle where $X \cap Y = \varnothing$.

Proposition. If $X_1, X_2, \ldots, x_n$ are finite sets, then

$$|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \cdot |X_2| \cdots |X_n|.$$

Proof. Let the n_i be the cardinality of X_i. The proposition is true by the multiplication principle and definition of cartesian product. □

Example. How many injective functions are there from $\{a, b, c\}$ to $\{1, 2, 3, 4, 5\}$?

There are $5 \cdot 4 \cdot 3$ functions. When constructing f, there are five elements that a can map to, four elements that b can map to (because it cannot map to $f(a)$), and three elements that c can map to (because it cannot map to $f(a)$ or $f(b)$).

Example. If the cardinality of a set X is 50, how many symmetric relations are there on X?

Let the elements of X be $x_1, \ldots, x_{50}$. We can depict the set of all relations on X as shown:

$$\begin{bmatrix} (x_1, x_1) & \ldots & (x_1, x_{50}) \\ \vdots & \ddots & \vdots \\ (x_{50}, x_1) & \ldots & (x_{50}, x_{50}) \end{bmatrix}$$

Observe that every symmetric relation on X can be represented as a subset of the top right triangle of the matrix. There are $\frac{50(51)}{2}$ elements in that triangle (observe that the diagonals form the integers from 1 to 50), so there are $2^{\frac{50(51)}{2}}$ symmetric relations on X.

3.1 Permutations and Combinations

Example. My, my wife, my cat, and my baby are going to line up for a photo. In how many ways can this be done?

There are four "choices" for where I go, 3 choices for where the cat goes, 2 for where the baby goes, and 1 for where the wife goes. Thus there are $4! = 24$ ways to line up for a photo.

Note. This is the same as the number of bijections on the set $\{\text{me}, \text{wife}, \text{cat}, \text{baby}\}$.

Definition. *Permutation*
A *permutation* of an n-element set is an ordering of the n elements. In other words, a permutation of a set X is a bijection from X to itself.
An n element set has $n!$ permutations.

Example. Ten distinct people form a circle. How many different circles are there? (We define two circles to be the same if you can rotate one of them to get the other)

Pick one "favorite" person from the group. Then each circle has a unique representation where the favorite person remains at the top of the circle, so there are 9 remaining slots for the others to fill. There are 9! different circles.

Example. In my family of four, in how many ways can two of us line up for a photo?

There are four choices for the first person, and three choices for the second person (note that the order of the people taking the photo still matters). There are $4 \cdot 3 = 12$ ways to do this.

Definition. *r-permutation*
An *r-permutation* from an n element set is an ordering of r elements from the set. In other words, it is a function $f\colon \{1, 2, \ldots, r\} \to \{1, 2, \ldots, n\}$.
The number of r-permutations from a set with n elements is denoted

$$P(n, r) = \frac{n!}{(n-r)!} = n(n-1)\cdots(n-r+1).$$

We say $P(n, r) = 0$ if $r > n$ (or if n or r is negative).

Example. Five people are stranded on an island. They find a boat that can hold three people. In how many ways can they choose three people to escape?

Note that the order of the people being rescued *does not* matter. Say we choose the first three people out of a permutation of the five people. We overcount because the order of the first three people doesn't matter, nor does the order of the two people left on the island. Thus the total number is $\binom{5}{3} = \frac{5!}{3!(5-3)!}$ ways to choose three survivors.

Definition. *r-combination*
An *r-combination* from an n-element set is a choice of r elements from the set.
The number of r-combinations from an n-element set is denoted

$$C(n,r) = \binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!(n-r)!}.$$

We say $\binom{n}{r} = 0$ if $r > n$ (or if n or r is negative).

Note. If $|X| = n$ for some set X, then there are $\binom{n}{r}$ subsets of X with r elements.