CSCI 2824 - CU Boulder, 2019 Summer

Lecture 9: Sequences and intro to set theory

17 June 2019

Lecturer: J. Marcus Hughes

Content is borrowed from Susanna Epp's Discrete Mathematics with Applications,
Rosens's Discrete Mathematics and its Applications,
Bettina and Thomas Richmond's A Discrete Transition to Advanced Mathematics, and Andrew Altomare's notes.

1 Sequences

We have talked quite a bit about sequences. I've stated a formal definition, but this is the first time we see a definition in the notes.

Definition: *sequence*
A **sequence** is a function whose domain is either all the integers between two given integers or all the integers greater than or equal to a given integer.

We talked about sequences that were defined by a recurrence relation, e.g. $a_0 = 0$, $a_1 = 1$, and $\forall n \geq 2$, $a_n = 2a_{n-1} - a_{n-2} + 2$. We discovered and proved that $a_n = n^2$ is a simpler closed form expression to give that formula.

Definition: *recurrence relation*
A **recurrence relation** for a sequence $a_0, a_1, a_2, \ldots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$ where i is an integer with $k - i \geq 0$.

We also have used the following facts without explicit proof. Try to prove them yourself:

Exercise
Prove for sequences $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2}, \ldots$ and $c \in \mathbb{R}$ that:

- $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$
- $c \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c a_k$
- $\left(\prod_{k=m}^{n} a_k\right) \times \left(\prod_{k=m}^{n} b_k\right) = \prod_{k=m}^{n} (a_k \times b_k)$

We have realized that we can find closed expressions by looking at iterations and identifying patterns that we can prove. Is there another way? Yes!

2 Second-order linear homogeneous recurrence relations with constant coefficients

Remember we talked about the Fibonacci sequence: 1, 1, 2, 3, 5, 8, 13, ...? We said that we could represent this using a recurrence relation with $F_0 = 1, F_1 = 1, F_k = F_{k-1} + F_{k-2} \forall k \geq 2$. I ran out of time in class to give the story behind this, so I will now. In 1202, Leonardo of Pisa, known often as Fibonacci, proposed a problem about rabbit mating. A single pair of rabbits (male and female) are acquired at the beginning of the year. In our scenario, rabbits are not fertile during their first month of life but then always give birth to one new pair of male and female rabbits at the end of each month. In our wonderful land of rabbits, none of them die. So, how many lives are there after a year? At first, there is one pair of rabbits so $F_0 = 1$. Then, a month passes and they become fertile but $F_1 = 1$ since they haven't produced. Then, they give birth to a new pair of rabbits so there are $F_2 = 2$. We can state that the number of rabbits alive after month k is the sum of the number of rabbits born at the end of month k and the number of rabbits alive at the end of month $k-1$. That looks like the recurrence relation $F_k = F_{k-1} + F_{k-2}$. Fantastic work Fibonacci!

But, that's hard to compute. If we can to calculate F_{100} we have to compute all the previous terms: $F_{99}, F_{98}, F_{97}, \ldots, F_2$! Is there a better way? Yes. First, let's define the category of recurrence relations that the Fibonacci sequence satisfies:

Definition: *second-order linear homogeneous recurrence relation with constant coefficients*
A **second-order linear homogeneous recurrence relation with constant coefficients** is a recurrence relation of the form:

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for every integer $k \geq m$ where m is some fixed integer and A and B are fixed real numbers with $B \neq 0$.

Then, the recurrence relation for the Fibonacci sequence has $A = B = 1$ and $m = 2$ since F_0 and F_1 give the initial conditions.

Let's do an exercise!

Exercise
Which of the following are second-order linear homogeneous recurrence relations with constant coefficients?

1. $a_k = 3a_{k-1} + 2a_{k-2}$
2. $b_k = b_{k-1} + b_{k-2} + b_{k-3}$
3. $c_k = \frac{1}{2}c_{k-1}0\frac{3}{7}c_{k-2}$
4. $d_k = d_{k-1}^2 + d_{k-1}d_{k-2}$

5. $e_k = 2e_{k-2}$

6. $f_k = 2f_{k-1} + 1$

7. $g_k = g_{k-1} + g_{k-2}$

8. $h_k = -h_{k-1} + (k-1)h_{k-2}$

Okay. So the Fibonacci sequence is an example, but why does that help us? Because we can figure out how to solve these recurrence relations generally. Consider some generic second-order linear homogeneous recurrence relation with constant coefficients defined as

$$a_k = Aa_{k-1} + Ba_{k=2}$$

for every integer $k \geq 2$ and A and B some fixed real numbers. Suppose that there's a number t with $t \neq 0$ where $1, t, t^2, t^3, \ldots$ satisfies the relation. Then, for the kth term (where $k \geq 2$) we have

$$t^k = At^{k-1} + Bt^{k-2}$$

. Even cooler when $k = 2$ we have

$$t^2 = At + B$$

. Who knows how to solve for t? What if we go the other direction? Suppose we have some t that satisfies $t^2 - At - B = 0$. Does the sequence $1, t, t^2, t^3, \ldots, t^n, \ldots$ work for the original relation? Well let's just multiply by t^{k-2}:

$$\begin{aligned} t^2 - At - B &= 0 \\ t^{k-2}t^2 - t^{k-2}At - t^{k-2}B &= 0 \\ t^k - At^{k-1} - Bt^{k-2} &= 0 \\ t^k &= At^{k-1} + Bt^{k-2} \end{aligned}$$

So, yes!

Theorem 2.1. *Let A and B be real numbers. A recurrence relation of the form*

$$a_k = Aa_{k-1} + Ba_{k-1}$$

for every integer $k \geq 2$ is satisfied by the sequence $1, t, t^2, t^3, \ldots, t^n, \ldots$ where t is a nonzero real number, if, and only if, t satisfies the equation

$$t^2 - At - B = 0$$

.

We give this equation a special name.

Definition: *characteristic equation of the relation*
Given a second-order linear homogeneous recurrence relation with constant coefficients

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for every integer $k \geq 2$ the **characteristic equation of the relation** is

$$t^2 - At - B = 0$$

.

We can use this equation to prove an explicit formula. I'll let you all have a stab at it first.

Exercise
Suppose a sequence $a_0, a_1, a_2, \ldots$ satisfies a recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for some real numbers A and B with $B \neq 0$ and every integer $k \geq 2$. If the characteristic equation

$$t^2 - At - B = 0$$

ahs two distinct roots r and s then $a_0, a_1, a_2, \ldots$ is given by the explicit formula

$$a_n = Cr^n + Ds^n$$

where C and D are determined by the values a_0 and a_1, i.e. they are solutions to the simultaneous equations $a_0 = C + D$ and $a_1 = Cr + Ds$.

We did all this work so that we can now show an explicit formula for the Fibonacci sequence!

Exercise
What's the explicit formula for the Fibonacci sequence?

3 Introduction to Set Theory

We have been indirectly talking about sets without really defining them. That's because it's actually a bit tricky, and they're very important to the foundations of mathematics.

Definition: *Set: first attempt*
A "set" is a collection of objects.

Then, $\{cat, dog, dog\}$ is a set and $\{cat, dog\}$ is a set, but are they the same? By our first definition, they are different. That makes it a bit difficult. We want our idea of set to be the simplest thing possible. Thus, let's restrict so we only talk about distinct objects.

Definition: *Set: second attempt*
A “set" is a collection of distinct objects.

Consider the set of everything that is not a flamingo. Well this set itself is not a flamingo so it’s inside itself. That’s kind of weird, right? We’ll call sets that don’t contain themselves “normal" and weird sets that contain themselves “abnormal." Think about the set of all normal sets. Is it normal or abnormal? If it’s normal, then it should be a member of itself. But then, it’s by definition abnormal. That’s a contradiction. But, if it’s abnormal, then it’s by definition a member of itself but it contained only normal sets to begin with... oh no! We have a paradox!

Figure 1: Isn’t this flamingo picture from here adorable?

This is why we never mix flamingos and sets! And it’s also why we introduce a much more rigorous idea of a set. In fact, Zermelo-Fraenkel set theory (ZFC) derives everything from a set of axioms:

- **Axiom of extensionality**. Two sets are equal and are the same set if they have the same elements. $\forall x \forall y\, [\forall z (z \in x \leftrightarrow z \in y) \to x = y]$
- **Axiom of regularity or Axiom of foundation**. Every non-empty set x contains a member y such that x and y are disjoint sets. $\forall x\, (x \neq \emptyset \to \exists y \in x (y \cap x = \emptyset))$
- **Axiom schema of specification**. For any formula ϕ in ZFC with all free variables $x, z, w_1, \ldots, w_n$. Then, $\forall z \forall w_1 \forall w_2 \ldots \forall w_n \exists y \forall x\, [x \in y \leftrightarrow (x \in z \wedge \phi)]$. It lets you construct sets. This helps avoid Russell’s paradox. This also tells us that empy sets exist. Let ϕ be a property no set has such as $(u \in u) \wedge \neg(u \in u)$. Then, $\emptyset = \{u \in w | \phi(u)\}$
- **Axiom of pairing**. For sets x and y there’s a set that contains x and y as elements. $\forall x \forall y \exists z (x \in z \wedge y \in z)$.
- **Axiom of union**: The union of any sets exists. For sets $\mathcal{F}$ there is a set A that contains every element that is a member of some member of $\mathcal{F}$: $\forall \mathcal{F} \exists A \forall Y \forall x\, [(x \in Y \wedge Y \in \mathcal{F}) \to x \in A]$.

- **Axiom schema of replacement**: The image of a set under any function is also inside a set. We can let ϕ be a formula with free variables $x, y, Aw_1, \ldots, W_n$. Then,

$$\forall A \forall w_1 \forall w_2 \ldots \forall w_n \left[\forall x(x \in A \to \exists! y \phi) \to \exists B \forall x(x \in A \to \exists y(y \in B \land \phi)) \right]$$

- **Axiom of infinity**. There exists a set having infinitely many members. More formally, let $S(w)$ abbreviate $w \cup \{w\}$ where w is some set. Then, there exists a set X such that the empty set $\emptyset$ is a member of X, and, whenever a set y is a member of X, then $S(y)$ is also a member of X.

$$\exists X \left[\emptyset \in X \land \forall y(y \in X \to S(y) \in X) \right]$$

- **Axiom of power set**. For a set X, there is a set Y that contains every subset of X. $\forall x \exists y \forall z \left[z \subset x \to z \in y \right]$.

- **Well-ordering theorem**: For any set X there is a binary relation R which well-orders X. Thus, R is a linear order on X such that every nonempty subset of X has a member which is minimal under R. $\forall X \exists R (R$ well orders $X)$. A well ordering is a binary relation R on some set X that holds the following:

  - It's antisymmetric. If $a \leq b$ and $b \leq a$ then $a = b$.
  - It's transitive. If $a \leq b$ and $b \leq c$ then $a \leq c$.
  - It's connex. $a \leq b$ or $b \leq a$.
  - Every non-empty subset of S has a least element in the ordering.

  Given the before axioms, this can be proven to be equivalent to something called the axiom of choice (where the C in ZFC comes from). For a set X whose members are all non-empty,the axiom of choice says that there exists a function f from X to the union of the members of X such that for all $Y \in X$ one has $f(Y) \in Y$. This really only matters for infinite sets and can lead to bizarre things like the Banach-Tarski Paradox.

You don't really have to memorize all these unless you're a hard core math nerd or pursuing a math degree maybe. It's nice to know that everything in math can be derived from a few simple statements. There are alternative versions of set theory. There are also competitors to set theory called type theory and category theory that give the foundation of math.

Thus, we'll settle on the following definition:

> **Definition:** *set*
> A set is a well-defined collection of distinct mathematical objects, where well-defined means we can answer whether an element is in the set unequivocally (a sly way of saying we need to meet the above axioms).

We can define a set wither by listing all its elements, e.g. $\{1, 2, 3, 4\}$. Or by defining it symobically using set-builder notation. $\{x \in \mathbb{N} | x < 6\}$ This last example is the set of all x such that $x \in \mathbb{N}$ and $x < 6$.

3.1 Set operations

3.1.1 Elements

Let A be the set $\{\text{Alabama}, \text{Alaska}, \text{Arizona}, \text{Arkansas}\}$. We can talk about the contents of a set with $\in$. We can say that Arizona $\in A$ but that Colorado $\notin A$.

3.2 Cardinality

There is a set that contains nothing. We call it the empty set which we write $\emptyset$. A set is finite if there is a whole number that tells the number of elements in the set (this is actually how we define numbers!). The set A is finite since it contains only 4 elements.

Definition: *cardinality*
The cardinality of a finite set S is the number of elements in the set S and is denoted $|S|$.

If a set is not finite, it is infinite. There are different sizes of infinity but we will return to that later. For now, let's build some more intuition.

3.3 Subset and superset

Sets can be contained in other or contain others. Let $A = \{1, 2, 3\}$. $B = \{1, 2, 3, 4\}$, $C = \{1\}$, and $D = \{1, 2, 9\}$.

Definition: *subset*
A set T is a subset of S if and only if every element of T is also an element of S. We write this $T \subset S$.

Definition: *superset*
A set T is a superset of S if and only if S is a subset of T. We write this $T \supset S$.

Exercise
Tell whether the following are true.

1. $A \subset B$
2. $A \supset B$
3. $A \subset C$
4. $A \supset C$
5. $A \subset D$

6. $A \supset D$

If $T \subset S$ but $T \neq S$ we say it is a proper subset.

Exercise
How many subsets does the set $\{1, 2, 3\}$ have?

3.4 Equality

Definition: *equality*
Two sets S and T are equal if every element in S is in T and every element in T is in S. We write this $S = T$. This is symbolically:

$$S = T \leftrightarrow S \subset T \text{ and } T \subset S$$

3.5 Intersection and Union

Definition: *intersection*
The intersection of sets S and T is the set of elements that are common both sets. We write this $S \cap T$.

Definition: *union*
The union of sets S and T is the set of elements that are in at least one of the sets. We write this $S \cup T$.

Note how this notation is similar to $\wedge$ and $\vee$. That's not on accident.

For example: if $A = \{1, 3, 5, 7\}$ and $B = \{3, 4, 5, 6\}$ then: $A \cap B = \{3, 5\}$ and $A \cup B = \{1, 3, 4, 5, 6, 7\}$. Two sets that don't overlap are called disjoint.

Definition: *disjoint*
Sets S and T are disjoint if $S \cap T = \emptyset$.

For a collection of sets $\{S_i | i \in I\}$ we say that they are mutually disjoint if $S_i \neq S_j$ implies $S_i \cap S_j = \emptyset$.

3.6 Complement

For numbers we get their "opposite" with a negative sign. For logical operations, we use $\neg$. What's the opposite of a set?

Definition: *complement*
If S is any subset of universal set U (a set that contains all the elements in our universe of discourse), then the complement of S in U, denote S^C or $U \setminus S$, is the set $\{x \in U | x \notin S\}$.

The set $R \setminus S = \{x \in R | x \notin S\}$ is called the complement of S in R. To emphasize that the set R may not be the universal set, we sometimes call $R \setminus S$ the relative complement of S in R.

3.7 Cartesian products

How do we make even more new sets from a set? Let's say you're picking out an outfit in the morning. You pick a shirt from some set $\{\text{orange shirt}, \text{green shirt}, \text{black tank top}\}$ (might want to do laundry since it seems you're running low on shirts). You also pick some shorts $\{\text{blue shorts}, \text{gray shorts}, \text{black shorts white shorts}\}$. We can define a new set of all possibilities like: $\{(\text{orange shirt}, \text{blue shorts}), (\text{orange shirt}, \text{gray shorts}), \ldots, (\text{black tank top}, \text{white shorts})\}$. This is called the Cartesian product.

Definition: *Cartesian product*
The Cartesian product of two nonempty sets A and B denoted $A \times B$ is the set $\{(a, b) | a \in A, b \in B\}$.

3.8 Partitions

We might want to divide a set up into categories so that every element belongs to exactly one category. For example, playing cards are divided into hearts, clubs, diamonds, and spades. We call this a partition.

Definition: *partition*
A partition of a nonempty set S is ac ollection $\mathcal{S} = \{B_i\}_{i \in I}$ of nonempty mutually disjoint subsets of S with $\cup_{i \in I} B_i = S$. The sets $B_i \in \mathcal{S}$ are called the blocks of the partition.