NOTES FOR WEEK 1 OF MATH 430: FORMAL LOGIC

SHERWOOD HACHTMAN

§1. Opening remarks. What is a proof? How does one show that a statement cannot be proven from a given set of axioms? In this class we will describe how to encode the informal process of a mathematical argument as a purely formal process, so that such things as axioms, theorems, and proofs are regarded as strings or sequences of symbols. For example,

$$(\forall x)x > 0 \to (\exists y)y \cdot y = x$$

asserts a familiar property of real numbers. But if we ignore the implied meaning of symbols like "$>$" and "$\cdot$", we are left with a meaningless string of symbols. But this is good: a string of symbols is not too different from a string of numbers. So regarded, mathematical theorems and arguments become valid *objects* of mathematical investigation.

Our goal in this class will be to develop a *formal language*, that of first order logic, in which we can encode mathematical reasoning. We will see how to interpret formulas of the language as meaningful statements about mathematical structures (like groups or rings). And we will define a *deductive calculus* laying down a list of rules for deriving new strings (theorems) from a list of strings we start with (axioms). Some milestones include

1. Gödel's completeness theorem, which asserts that the deductive calculus we define is *complete*, in the sense that it fully captures the process of mathematical proof (as a means of reasoning about mathematical structures).
2. The compactness theorem, which asserts that a theory can be realized by a structure precisely when each of its finite parts can be realized. We will explore applications to such areas of mathematics as algebra, analysis, combinatorics, and number theory.
3. Gödel's incompleteness theorem, which states that any reasonable theory strong enough to interpret arithmetic is *incomplete*, in the sense that there are true statements which it cannot prove.

As a warm-up, we start with a toy logic, known as *sentential* (or *propositional*) logic. This is just first order logic with the quantifiers dropped.

Before we can do that, though, it will be helpful to review some basic facts about sets, some of which we need to sensibly begin our subject, and others which will become relevant down the road.

§2. Sets. We start with sets because they provide a simple language in which all known mathematics can be formulated. Our presentation is informal, but we will remark on pitfalls of our informal approach where appropriate.

2.1. Basics of sets. A **set** is simply a collection of objects. Objects belonging to a set A are called **elements** of A. We write:

$$x \in A$$

to mean "x is an element of A". Then $x \notin A$ means "x is not an element of A".

Two sets are considered equal iff they have the same elements. So the set of U.S. presidents (as of Jan. 2016) is equal to the set of male U.S. presidents. A set can be designated by writing out its elements between curly braces, e.g. $\{2, 3, 5\}$ is a set with three elements, and $\{2, 3, 5\} = \{3, 5, 2, 3\}$.

A is a **subset** of B (written $A \subseteq B$) if every element of A belongs to B. The set of white U.S. presidents is a subset of the set of U.S. presidents, and these sets are not equal. Say A is a **proper subset** of B (written $A \subsetneq B$).

NOTE 2.1. $A = B$ iff $A \subseteq B$ and $B \subseteq A$.

We can define sets using "set-builder notation". Suppose $P(x)$ is a property of objects and A is a set. Then

$$\{x \in A \mid P(x)\}$$

is the set of elements x of A so that $P(x)$ holds of x.

So if P is the set of people who have lived up to now,

$$A = \{x \in P \mid x \text{ was a U.S. president}\}$$

is a set with 43 elements. (Not 44: Because Grover Cleveland.) Whereas if L is the set of lizards who have lived up to now,

$$B = \{x \in L \mid x \text{ was a U.S. president}\}$$

is a set with 0 elements. (Notice $B \subseteq A$.)

We also sometimes write: $\{x \mid P(x)\}$ for the set of *all* objects x for which $P(x)$ holds.

Let's restrict our attention to those sets whose elements are mathematical objects. What sets are there?

- $\varnothing$, the set with no elements.
- If A, B are sets, then so is
  - The union $A \cup B := \{x \mid x \in A \text{ or } x \in B\}$.
  - The intersection $A \cap B := \{x \mid x \in A \text{ and } x \in B\}$.
  - The pair $\{A, B\} := \{x \mid x = A \text{ or } x = B\}$.
  - The difference $A \setminus B := \{x \in A \mid x \notin B\}$.
- If A is a set, then so is its **power set**, $\mathcal{P}(A) = \{x \mid x \subseteq A\}$.
- If A is a set of sets, then its union $\bigcup A := \{x \mid x \in y \text{ for some } y \in A\}$ is a set. If this A comes with an indexing of its elements by some index set I, say $A = \{y_i \mid i \in I\}$, then we can write this more explicitly as

  $$\bigcup A = \bigcup_{i \in I} y_i = \{x \mid x \in y_i \text{ for some } i \in I\}.$$

- Similarly for intersections: if A is as above,

  $$\bigcap A = \bigcap_{i \in I} y_i = \{x \mid x \in y_i \text{ for all } i \in I\}.$$

  If A (hence I) is empty then this definition is problematic. So we make the convention that $\bigcap \varnothing = \varnothing$.

THEOREM 2.2 (De Morgan's Law). *$C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$, whenever A, B, C are sets.*

PROOF. We prove this to illustrate a standard way of proving two sets are equal: show each set is a subset of the other.

First, $\subseteq$. Suppose $x \in C \setminus (A \cap B)$. We need to show $x \in (C \setminus A) \cup (C \setminus B)$. That is, $x \in C \setminus A$ or $x \in C \setminus B$. If $x \in C \setminus A$, then great, we're done. So suppose $x \notin C \setminus A$; then either $x \notin C$ or $x \in A$. We know $x \in C$ since we assumed $x \in C \setminus (A \cap B)$. So $x \in A$. By the same assumption $x \notin A \cap B$ so $x \notin B$. Then $x \in C \setminus B$. This shows $C \setminus (A \cap B) \subseteq (C \setminus A) \cup (C \setminus B)$ as needed.

Conversely, suppose $x \in C \setminus A$. Then $x \in C$, and $x \notin A$; in particular, $x \notin A \cap B$, hence $x \in C \setminus (A \cap B)$. Similarly, $x \in C \setminus B$ implies $x \in C \setminus (A \cap B)$. So $x \in (C \setminus A) \cup (C \setminus B)$ implies $x \in C \setminus (A \cap B)$. That is, we have $\supseteq$, and the equality is proved. ⊣

2.2. Relations, and numbers regarded as sets. We would like familiar mathematical objects to exist as sets. For example,

- $\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- $\mathbb{Q} = \{\frac{m}{n} \mid m, n \text{ are integers with } n \neq 0\}$

are sets of numbers. But what are numbers? Let's see how to think of numbers as sets.

First, define $0 = \varnothing$. For a set n, define $n + 1 = n \cup \{n\}$.

DEFINITION 2.3. A set x is an element of $\mathbb{N}$ (a natural number) if

- $x = 0$, or
- $x = n + 1$ for some n that is already a natural number,

and the elements of $\mathbb{N}$ are only those sets obtained according to the above two rules.

Notice that with this definition, e.g. 6 is the set $\{0, 1, 2, 3, 4, 5\}$, and contains 6 elements. What's more, the usual order relation $<$ on $\mathbb{N}$ here coincides with $\in$.

It's not so important that we think of $\mathbb{N}$ this way; we just wanted to show that we can. In order to define $\mathbb{Z}$ by a similar construction, we first develop some useful technology.

DEFINITION 2.4. The **ordered pair** $\langle x, y\rangle$ is defined to be the set $\langle\{x\}, \{x, y\}\rangle$.

PROPOSITION 2.5. *$\langle a, b\rangle = \langle x, y\rangle$ iff $a = x$ and $b = y$.*

DEFINITION 2.6. The **Cartesian product** $A \times B$ is the set $\{\langle a, b\rangle \mid a \in A \text{ and } b \in B\}$.

A **binary relation** is a set of ordered pairs, $R \subseteq A \times B$. We define the **domain** of R

$$\mathrm{dom}(R) = \{x \in A \mid \langle x, y\rangle \in R \text{ for some } y \in B\},$$

and the **range** of R,

$$\mathrm{ran}(R) = \{y \in B \mid \langle x, y\rangle \in R \text{ for some } x \in A\}.$$

We recall some properties a binary relation may have.

- R is **reflexive** if $\langle x, x\rangle \in R$ for all $x \in \mathrm{dom}(R)$.
- R is **transitive** if whenever $\langle x, y\rangle \in R$ and $\langle y, z\rangle \in R$, we have $\langle x, z\rangle \in R$.
- R is **symmetric** if $\langle x, y\rangle \in R$ implies $\langle y, x\rangle \in R$.
- R satisfies **trichotomy** on A if whenever $x, y \in A$, exactly one of $\langle x, y\rangle \in R$, $\langle y, x\rangle \in R$, or $x = y$ holds.

DEFINITION 2.7. A relation R is an **equivalence relation** if it is reflexive, transitive, and symmetric. A relation is a (strict) **linear order** if it transitive and satisfies trichotomy on A.

EXAMPLE 2.8. The relation $\{\langle m, n\rangle \in \mathbb{N} \times \mathbb{N} \mid m \text{ divides } n\}$ is reflexive and transitive, but not symmetric.

A relation $F \subseteq A \times B$ is a **function** if for all $a \in A$, there is a unique $b \in B$ so that $\langle a, b\rangle \in F$; we write $b = F(a)$. We write $F : A \to B$ to indicate that F is a function from A to B. A function should be thought of as rule that assigns each element of A to a unique element of B; in our official definition of F as a set of ordered pairs, we are essentially identifying a function with its graph. A function $F : A \times A \to A$ is called a **binary operation** on A.

Recall we defined $\mathbb{N}$ as those sets obtainable from $0 = \varnothing$ by iterating the successor operation, $n + 1 = n \cup \{n\}$. This definition allows us to define the familiar binary operations of addition and multiplication on $\mathbb{N}$ by induction (on n, simultaneously for all x):

- Addition: Base case: $x + 0 = x$. Inductive case: $x + (n + 1) = (x + n) + 1$.
- Multiplication: Base case: $x \cdot 0 = 0$. Inductive case: $x \cdot (n + 1) = x \cdot n + x$.

So we have the structure of natural number arithmetic, $(\mathbb{N}, +, \cdot)$.

If E is a relation on A that is reflexive, symmetric, and transitive, then we say E is an **equivalence relation** on A. The **E-equivalence class** of an element $x \in A$ is the set

$$[x]_E := \{y \in A \mid \langle x, y\rangle \in E\}.$$

We may now describe how to regard integers as equivalence classes of pairs. The idea is to identify a pair $\langle i, j\rangle$ of naturals with its difference $i - j$. Define a relation E on $\mathbb{N}$

$$E := \{\langle\langle i, j\rangle, \langle m, n\rangle\rangle \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) \mid i + n = m + j\}$$

Check: this is an equivalence relation. We define

$$\mathbb{Z} := \{[\langle m, n\rangle]_E \mid m, n \in \mathbb{N}\}$$

And we can define the usual arithmetical operations,

- $[\langle i, j\rangle]_E + [\langle m, n\rangle]_E := [\langle i + m, j + n\rangle]_E$,
- $[\langle i, j\rangle]_E - [\langle m, n\rangle]_E := [\langle i + n, j + m\rangle]_E$,
- $[\langle i, j\rangle]_E \cdot [\langle m, n\rangle]_E := [\langle i \cdot m + j \cdot n, i \cdot n + j \cdot m\rangle]_E$.

We stress that we are defining $+, -, \cdot$ (operations on $\mathbb{Z}$) in terms of the already defined operations $+, \cdot$ (on $\mathbb{N}$). It is easy, if tedious, to check that these operations are well-defined (i.e., do not depend on the choices of representatives) on the collection of equivalence classes. We have thus defined the structure $(\mathbb{Z}, +, -, \cdot)$ purely in terms of sets.

Since mathematical objects can be realized as "pure sets", we commonly restrict our attention to the universe of hereditary sets, or *set-theoretic universe*, denoted V. V consists of those sets all of whose elements are sets whose elements are sets... etc. This excludes such things as e.g. the collection of presidents, or of lizards, from being found in V.

All along, we've been making implicit use of a general set-building axiom, commonly known as the Axiom of Comprehension.

- Let P be a property of sets; then the collection $\{x \in V \mid P(x)\}$ is a set.

There are two problems with this axiom: One is that we haven't made precise what is meant by "property"; a large part of this class will be spent doing just that. But there is a bigger problem: It is false.

THEOREM 2.9 (Russell's Paradox). *The Axiom of Comprehension is false. In particular, the collection*

$$\{x \in V \mid x \notin x\}$$

is not a set.

PROOF. Suppose $A = \{x \in V \mid x \notin x\}$ is a set, that is, $A \in V$. We ask: Is $A \in A$? If so, then by definition of A, $A \notin A$. But if not, then $A \notin A$ and again by definition, $A \in A$. Either way leads us to a contradiction, so A cannot be a set. ⊣

It turns out that the way out is to *restrict* Comprehension to those objects that we already know are sets:

- If A is a set and P is a property of sets, then $\{x \in A \mid P(x)\}$ is also a set.

Note that then by Russell's Paradox, the universe of sets V is not itself a set: $V \notin V$.

Using only the Axiom of (Restricted) Comprehension (often known as the Axiom of Separation) apparently allows us to avoid paradoxes such as Russell's. We pointed out this issue both because of its historical importance to the development of the foundations of mathematics, and to stress the pitfalls of a naïve approach to set theory. A rigorous development could replace our appeals to unrestricted comprehension by appeals to its restricted version. We will be content with these few remarks.

2.3. Functions, sequences, and the Axiom of Choice. We defined functions as sets of ordered pairs. We let B^A denote the collection of functions $F : A \to B$:

$$B^A = \{F \in \mathcal{P}(A \times B) \mid F \text{ is a function, } F : A \to B\}.$$

We have defined ordered pairs $\langle x, y\rangle$; to define longer tuples, we make use of functions. Namely, we say a function s is an **n-tuple** if $s : n \to B$ for some set B. We denote the tuple s by $\langle s_0, s_1, \ldots, s_{n-1}\rangle$, where $s_i = s(i)$ for $i < n$. Then for sets A, A^n is the set of ordered n-tuples of elements of A.

(Note Enderton uses a different definition of ordered n-tuple and the set A^n. The advantage of Enderton's definition is that his version of A^{n+1} is (inductively) the same as $A^n \times A$. The advantage of our definition is that the length of a sequence s is uniquely determined by the set s.)

We may now extend our binary definitions to an n-ary context. A set $R \subseteq A^n$ is an **n-ary relation** on A. We say $F : A^n \to A$ is an **n-ary operation on** A. For example, F could be the function taking a 4-tuple $\langle a, b, c, d\rangle$ of integers to the determinant of the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

We similarly regard functions $f : \mathbb{N} \to A$ as **infinite sequences** of elements of A, and denote such a sequence by $\langle f(n)\rangle_{n\in\mathbb{N}}$. Then $A^{\mathbb{N}}$ is the set of all infinite sequences of elements of A; for example, $2^{\mathbb{N}}$ consists of all infinite binary sequences.

Suppose $\langle A_n\rangle_{n\in\mathbb{N}}$ is a sequence of non-empty sets of real numbers. How do we go about choosing an element $x_n \in A_n$, for each n? This would be easy if, say, each A_n was finite; then we could just let x_n be the least element of A_n in the usual order on $\mathbb{R}$. What about in general? It turns out we need a new axiom, the Axiom of Choice:

- If $\mathcal{A} = \{A_i \mid i \in I\}$ is a collection of non-empty sets indexed by a set I, then there is a **choice function** for $\mathcal{A}$: a function $F : I \to \bigcup \mathcal{A}$ so that $F(i) \in A_i$ for each $i \in I$.

There are a number of equivalent formulations of the Axiom of Choice. One is the believable statement that any I-indexed product of non-empty sets A_i,

$$\prod_{i \in I} A_i := \{f : I \to \bigcup_{i \in I} A_i \mid f(i) \in A_i\}$$

is non-empty. One particularly useful formulation is Zorn's Lemma. We say that a set C is a **chain** if it is linearly ordered by $\subseteq$; that is, for any distinct $x, y \in C$, either $x \subseteq y$ or $y \subseteq x$.

LEMMA 2.10 (Zorn's Lemma). *Let D be a set such that for any chain $C \subseteq D$, we have $\bigcup C \in D$. Then there is a maximal element m of D: that is, for all $x \in D$, if $x \neq m$ then $m \not\subseteq x$.*

2.4. Cardinality. Recall that a function $F : A \to B$ is **injective** (or one-to-one) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$, for all $a_1, a_2 \in A$. F is **surjective** (or onto) if for every $b \in B$, there is some $a \in A$ with $F(a) = b$; that is, if $\mathrm{ran}(F) = B$. If $F : A \to B$ is both one-to-one and onto, we say it is a **bijection**, and that A and B are in **one-to-one correspondence**.

EXAMPLE 2.11.
- $\tan : (-\pi/2, \pi/2) \to \mathbb{R}$ is a bijection.
- $\exp : \mathbb{R} \to \mathbb{R}$ where $\exp(x) = e^x$ is one-to-one but not onto.
- $F : \mathbb{Z} \to \mathbb{N}$ with $F(n) = n^2$ is onto but not one-to-one.

We would like to have a way of comparing sets in terms of size. Let us say that $A \preceq B$ iff there exists an injection $F : A \to B$. We say that B **dominates** A. We write $A \sim B$ iff there is a bijection $f : A \to B$. Notice that $\sim$ is an equivalence relation on sets. We think of the equivalence classes as *cardinal numbers*, and write $\mathrm{card}(A)$ to denote the $\sim$-equivalence class of the set A, called the **cardinality** of A. If $A \preceq B$, we write $\mathrm{card}(A) \leq \mathrm{card}(B)$. Say $\mathrm{card}(A) < \mathrm{card}(B)$ if $\leq$ but not $=$ holds.

A set A is **finite** if there is a bijection $f : n \to A$ with $n \in \mathbb{N}$. A set is **infinite** if it is not finite.

PROPOSITION 2.12. *(Uses Choice.) If A is infinite, then $A \preceq \mathbb{N}$.*

PROOF. Let A be an infinite set. Let $\mathcal{F}$ be the collection of non-empty subsets of A. Then by the Axiom of Choice, there is a function $F : \mathcal{F} \to A$ so that $F(B) \in B$ for all $B \subseteq A$ that are non-empty.

We define g by induction. Let $g(0) = F(A)$. Suppose inductively that we have defined $g(i) \in A$ for all $i < n$, and that g is injective on n, that is, $g(i) \neq g(j)$ for distinct $i, j < n$. Then $A \setminus \{g(0), \ldots, g(n-1)\}$ is non-empty, since otherwise g would be a bijection of n with A, contrary to our assumption that A was infinite. Now set

$$g(n) = F(A \setminus \{g(0), g(1), \ldots, g(n-1)\}).$$

Clearly $g(n) \neq g(i)$ for all $i < n$. So by induction, we have defined $g : \mathbb{N} \to A$, and g is injective. ⊣

We say that a set A is **countable** if $A \preceq N$. The cardinality of an infinite countable set is denoted $\aleph_0$ ("aleph zero").

PROPOSITION 2.13. $\mathbb{N} \sim \mathbb{Z}$*; that is,* $\mathbb{Z}$ *is countable.*

PROOF. Let $F : \mathbb{N} \to \mathbb{Z}$ be the map

$$F(n) = \begin{cases} k & \text{if } n = 2k \text{ for some } k, \\ -k & \text{if } n = 2k+1 \text{ for some } k. \end{cases}$$

Then it is easy to check that F is a bijection. ⊣

The next theorem is the main tool for showing two sets have the same cardinality.

THEOREM 2.14. *(Uses Choice.) Given sets* A, B*, either* $A \preceq B$ *or* $B \preceq A$*.*

PROOF. Let $D = \{F \subseteq A \times B \mid F \text{ is a one-to-one function}\}$. Note that if $C \subseteq D$ is a chain, then its union is in D. So we apply Zorn's Lemma, and obtain a maximal $F \in D$.

We claim either $\text{dom}(F) = A$ or $\text{ran}(F) = B$, which proves the theorem. Otherwise, we have some $x \in A \setminus \text{dom}(F)$ and $y \in B \setminus \text{ran}(F)$. But then clearly $F \cup \langle x, y\rangle$ is a one-to-one map, that is, $F \cup \langle x, y\rangle \in D$. But this contradicts maximality of F. ⊣

THEOREM 2.15 (Cantor-Schroder-Bernstein). *Suppose there are injections* $f : A \to B$ *and* $g : B \to A$*. Then there is a bijection* $h : A \to B$*.*

Equivalently, if $A \preceq B$ *and* $B \preceq A$*, then* $A \sim B$*.*

PROOF. Deferred. ⊣

The previous results combined establish (assuming Choice) the cardinalities $\text{card}(A)$ are linearly ordered by the strict order $<$.

PROPOSITION 2.16. *Suppose there is a surjection* $f : A \to B$*. Show there is an injection* $g : B \to A$*.*

PROOF. Exercise. (This uses the Axiom of Choice.) ⊣

PROPOSITION 2.17. $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$*; that is,* $\mathbb{N} \times \mathbb{N}$ *is countable.*

PROOF. Clearly $\mathbb{N} \preceq \mathbb{N} \times \mathbb{N}$. Define $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by setting $g(\langle m, n\rangle) = 2^m \cdot 3^n$. Clearly g is one-to-one. By Cantor-Schroder-Bernstein, we have that $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. ⊣

EXERCISE 2.18. $\mathbb{Q}$ is countable.

THEOREM 2.19. *Suppose* $\langle A_n\rangle_{n\in\mathbb{N}}$ *is a countable sequence of countable sets. Then* $A = \bigcup_{n\in\mathbb{N}} A_n$ *is countable.*

PROOF. Let, for each n, F_n be an injection $F_n : A_n \to \mathbb{N}$. (This uses the Axiom of Choice, applied to the collection $\{\mathcal{F}_n \mid n \in \mathbb{N}\}$ where $\mathcal{F}_n = \{F : A_n \to \mathbb{N} \mid F \text{ is injective}\}$. Each $\mathcal{F}_n$ is non-empty by assumption, so choice applies.) Then define a function $F : A \to \mathbb{N} \times \mathbb{N}$ by

$$F(a) = \langle m, F_m(a)\rangle \text{ iff } m \text{ is least so that } a \in A_m.$$

If $F(a) = F(b) = \langle m, n\rangle$, then we have a, b both in A_m, and $F_m(a) = F_m(b)$; since F_m is injective, we have $a = b$. So F is an injection witnessing $A \preceq \mathbb{N}\times\mathbb{N}$, and since $\mathbb{N}\times\mathbb{N} \sim \mathbb{N}$, this proves the theorem. ⊣

So far we have only identified the cardinalities of countable sets. We say a set is **uncountable** if it is infinite and not countable.

THEOREM 2.20 (Cantor). *The set* $2^{\mathbb{N}}$ *is uncountable.*

PROOF. Note that $2^{\mathbb{N}}$ consists of just infinite binary sequences. Let G be a function $G : \mathbb{N} \to 2^{\mathbb{N}}$. We show that there must exist some infinite binary sequence which does not belong to the range of G. Namely, we define a function $f : \mathbb{N} \to 2$ so that f disagrees with the sequence $G(n)$ at its n-th coordinate. That is, define, for $n \in \mathbb{N}$,

$$f(n) = 1 - G(n)(n).$$

(Recall each $G(n)$ is a function $G(n) : \mathbb{N} \to 2$.) Clearly this defines $f \in 2^{\mathbb{N}}$, and $f \notin \mathrm{ran}(G)$, since $f(n) \neq G(n)(n)$ for all n. We have shown G is not surjective. Since G was arbitrary, we have shown there can exist no surjection $G : \mathbb{N} \to 2^{\mathbb{N}}$; in particular, there is no bijection $G : \mathbb{N} \to 2^{\mathbb{N}}$. ⊣

The method used here is is one of the logician's stock-in-trade, known as *diagonalization*. So-called because if we think of the function G as a list of countably many binary sequences, say, setting $b_{ij} = G(i)(j)$, then we have an array

$$\begin{array}{ccccccc} b_{00} & b_{01} & b_{02} & \dots & b_{0j} & \dots \\ b_{10} & b_{11} & b_{12} & \dots & b_{1j} & \dots \\ b_{20} & b_{21} & b_{22} & \dots & b_{2j} & \dots \\ & & \vdots & & & & . \\ b_{i0} & b_{i1} & b_{i2} & \dots & b_{ij} & \dots \\ & & \vdots & & & \end{array}$$

We can always generate a new sequence by going along the diagonal and "toggling", that is, the sequence $\langle a_i \rangle_{i \in \mathbb{N}} = \langle 1 - b_{ii} \rangle_{i \in \mathbb{N}}$ cannot appear in this list.

EXERCISE 2.21. For any set A, we have $\mathrm{card}(A) < \mathrm{card}(\mathcal{P}(A))$.

On the other hand,

THEOREM 2.22. *Let $\mathcal{P}_{\mathrm{fin}}(\mathbb{N})$ be the collection of finite subsets of $\mathbb{N}$. Then $\mathcal{P}_{\mathrm{fin}}(\mathbb{N})$ is countable.*

PROOF. There are two ways to see this. One is to note that there are finitely many subsets of n for each n, and every finite set of naturals is a subset of some n. So $\mathcal{P}_{\mathrm{fin}}(\mathbb{N}) = \bigcup_{n \in \mathbb{N}} \mathcal{P}_{\mathrm{fin}}(n)$, that is, a countable union of countable sets, which is therefore countable.

The other way to see this is to explicitly define an injection of $\mathcal{P}_{\mathrm{fin}}(\mathbb{N})$ into $\mathbb{N}$. Let p_n be the n-th prime, and set

$$f(A) = \prod_{n \in A} p_n$$

for each $A \in \mathcal{P}_{\mathrm{fin}}(\mathbb{N})$. Notice this is well-defined, since A is taken to be finite. And it is injective, by the Fundamental Theorem of Arithmetic. ⊣

PROOF OF CANTOR-SCHRODER-BERNSTEIN. Without loss of generality we can take A and B to be disjoint, since we can replace A by $\{0\} \times A$ and B by $\{1\} \times B$. We construct a bijection $h : A \to B$ using the functions f and g.

Let $a \in A$ and define the set

$$S_a = \{\dots f^{-1}(g^{-1}(a)), g^{-1}(a), a, f(a), g(f(a)), \dots\}.$$

Let $b \in B$ and define the set

$$S_b = \{\dots g^{-1}(f^{-1}(b)), f^{-1}(b), b, g(b), f(g(b)) \dots\}.$$

Note that, whenever $f^{-1}(x)$ or $g^{-1}(x)$ exists, it is unique, since f, g are both injective. Note also that since these inverse images needn't exist, that for $c \in A \cup B$ the set S_c might have a "left-most" element; that is, an x so that $f^{-1}(x)$ (if $x \in B$) or $g^{-1}(x)$ (for $x \in A$) doesn't exist. In this event we say S_c terminates. If the left-most element of S_c is in A, then we S_c is A-terminating; otherwise we call it B-terminating.

Observe that if $c_1, c_2 \in A \cup B$ and $c_1 \in S_{c_2}$, then $S_{c_1} = S_{c_2}$.

Define h as follows. Let $a \in A$. If S_a is A-terminating or does not terminate, then define $h(a) = f(a)$. If S_a is B-terminating, then a is in the image of g, so define $h(a) = g^{-1}(a)$.

Clearly this defines a map from A to B, we just need to check that it is a bijection. First we check that it is onto. Let $b \in B$. If S_b is A-terminating or doesn't terminate, then b is in the image of f and $S_{f^{-1}(b)} = S_b$ is A-terminating or doesn't terminate, so we defined $h(f^{-1}(b)) = f(f^{-1}(b)) = b$ as required. If S_b is B-terminating, then $S_{g(b)}$ is also B-terminating, so we defined $h(g(b)) = g^{-1}(g(b)) = b$. It follows that h is onto.

Let $a_1, a_2 \in A$ and suppose that $h(a_1) = h(a_2)$. We will show that $a_1 = a_2$. If S_{a_1} and S_{a_2} are either

1. both A-terminating or non-terminating; or
2. both B-terminating,

then $a_1 = a_2$ follows from the injectivity of f or g.

Suppose for a contradiction that S_{a_1} is A-terminating or nonterminating and S_{a_2} is B-terminating. Then by the definition of h, $f(a_1) = h(a_1) = h(a_2) = g^{-1}(a_2)$. It follows that $S_{a_1} = S_{a_2}$ which is a contradiction. $\dashv$