Test 4 — Comments

Problem 1 *Cardinalities*

(a) $S := \{\text{Aidan}, \text{Dave}\}$

Answer: S is finite. It has two elements so it is finite.

We could also show that there exists a bijection from the set to $\mathbb{N}_2$, which means it is finite by the definition.

(b) $S := \mathbb{R} - \mathbb{N}$

Answer: S is uncountable. The difference between an uncountable set and a countable set is an uncountable set (we saw this on one of the practice problems).

(c) $S := (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$

Answer: S is countably infinite. The Cartesian product between two countably infinite sets will result in a countably infinite set. We can break this down into showing that $\mathbb{N} \times \mathbb{N}$ is countably infinite (we showed this in class), and then using a similar covering path to show that $(\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$ is also countably infinite.

(d) $S := \mathbb{R} - pow(\mathbb{N})$

Answer: S is uncountable. The set S is just the $\mathbb{R}$, since the set we are removing is a set of *sets*, so does not include any real numbers (and certainly not an uncountable number of them).

(e) $S := \{G \mid G \in pow(\mathbb{N} \times \mathbb{N}) \land R = (\mathbb{N}, \mathbb{N}, G) \text{ is a bijection}\}$

Answer: S is uncountable, We can define a bijection between any R and permutations of $\mathbb{N}$ (this was on the practice problems).

(f) $S :=$ the set of all surjective functions between $\mathbb{N}$ and $\mathbb{N}$.

Answer: S is uncountable. We can define a surjective function between any R and permutations of $\mathbb{N}$. Note that this set is a superset of the set in 1e since every bijection is also a surjective function. This, it must be at least as big as that set, so it must also be uncountable.

Problem 2 *Diagonalization Proof?*

In class we saw a diagonalization proof (very close to the one Cantor developed in his 1891 paper) that the set of infinite binary strings, $\{0, 1\}^\infty$ is *uncountable* (this is identical to the proof in the practice problems)

1. We prove the set of infinite binary strings, $S = \{0, 1\}^\infty$ is uncountable by contradiction.
2. Assume towards a contradiction that there exists a surjective function $R = (\mathbb{N}, S, G \subseteq \mathbb{N} \times S)$ from $\mathbb{N}$ to S.
3. Since R is function, for each $n \in \mathbb{N}$ there is at most one $s \in S$ where $(n, s) \in G$. Let $A_n := s$ be that element and identify the characters of A_n as $a_{n,1}a_{n,2}a_{n,3}\ldots$.
4. Define $b = b_1b_2b_3\ldots$ where $b_i = \neg a_{(i,i)}$ and $\neg 0 = 1$ and $\neg 1 = 0$.

5. Since b is an infinite bitstring, we know $b \in S$. Since each bit is different from one bit in each A_n and since R is surjective we know $\forall s \in S . \exists m \in \mathbb{N} . A_m = s$ but b is not in the mapping and we have a contradiction.

For each subproblem, indicate of the alternate construction for step 4 would result in a valid or invalid proof and explain why. (Differences from the previous subproblem are underlined.)

(a) Define $b = b_1 b_2 b_3 \ldots$ where $b_i = W(a_{i,i})$ where $W(0) = 5$ and $W(1) = 0$.

Answer: Invalid. b can contain 5's so b might not be a binary string ($b \notin S$).

(b) Define $b = b_1 b_2 b_3 \ldots$ where $b_i = W(a_{\underline{i+1,i+1}})$ where $W(0) = \underline{1}$ and $W(1) = 0$.

Answer: Invalid. One issue is that no bit is taken from the first row, so it is possible that $b = A_1$. Another problem is that $b_{i,i}$ may not differ from a_i because it flips a bit from a_{i+1}. Another problem is that the b_i mismatches with index $i+1$ instead of i. (Only necessary to identify one of these—any one of the problems by itself breaks the proof.)

(c) Define $b = b_1 \underline{c_1} b_2 \underline{c_2} b_3 \underline{c_3} \ldots$ where $b_i = W(a_{\underline{i,i}})$ $\underline{\text{and } c_i = W(a_{i,2i})}$ where $W(0) = 1$ and $W(1) = 0$.

Answer: Valid. For every A_i, b_{2i} is different from $A_{i,2i}$, so we know b is not in the table, but $b \in S$ since it is an infinite bitstring.

Problem 3 *True, False, or Unresolvable*

For each subproblem, indicate the truthiness of the stated proposition and provide a brief but clear and convincing justification for your answer.

(a) There exists a surjective function from the natural numbers to the reals $R = (\mathbb{N}, \mathbb{R}, G)$.

Answer: **False**. Since $|\mathbb{N}| < |\mathbb{R}|$ there cannot be a surjective function between $\mathbb{N}$ and $\mathbb{R}$.

(b) There exists a G for which $R = (\mathbb{N}, pow(\mathbb{N}), G \subseteq \mathbb{N} \times pow(\mathbb{N}))$ is total (≥ 1 out) and injective (≤ 1 in).

Answer: **True**. Since $|pow(\mathbb{N})| > |\mathbb{N}|$ there must be a surjective function from $pow(\mathbb{N})$ to $\mathbb{N}$. In the other direction, there must be a total injective relation (we can just reverse the arrows to find one).

(c) $|pow(pow(\mathbb{R}))| > |pow(\mathbb{R})|$.

Answer: **True**. Cantor's Theorem proved that for any set A, $|pow(A)| > |A|$, here $A = pow(\mathbb{R})$.

Problem 4 *Subsets of* $\mathbb{N}$

Define S_n as the set of all n-element subsets of $\mathbb{N}$:

$$S_n := \{s | s \in pow(\mathbb{N}) \wedge |s| = n\}$$

(a) $P := \forall n \in \mathbb{N} \, . \, S_n$ is Countable.

Comments: The subtlety to notice here is that for $n = 0$, S_n is a finite set (with one element). We hope many of you realized this in attempting the proof. For $n \geq 1$, S_n is countably infinite (so we did award partial credit for this answer).

(b) Prove the proposition P (as you completed it in part a).

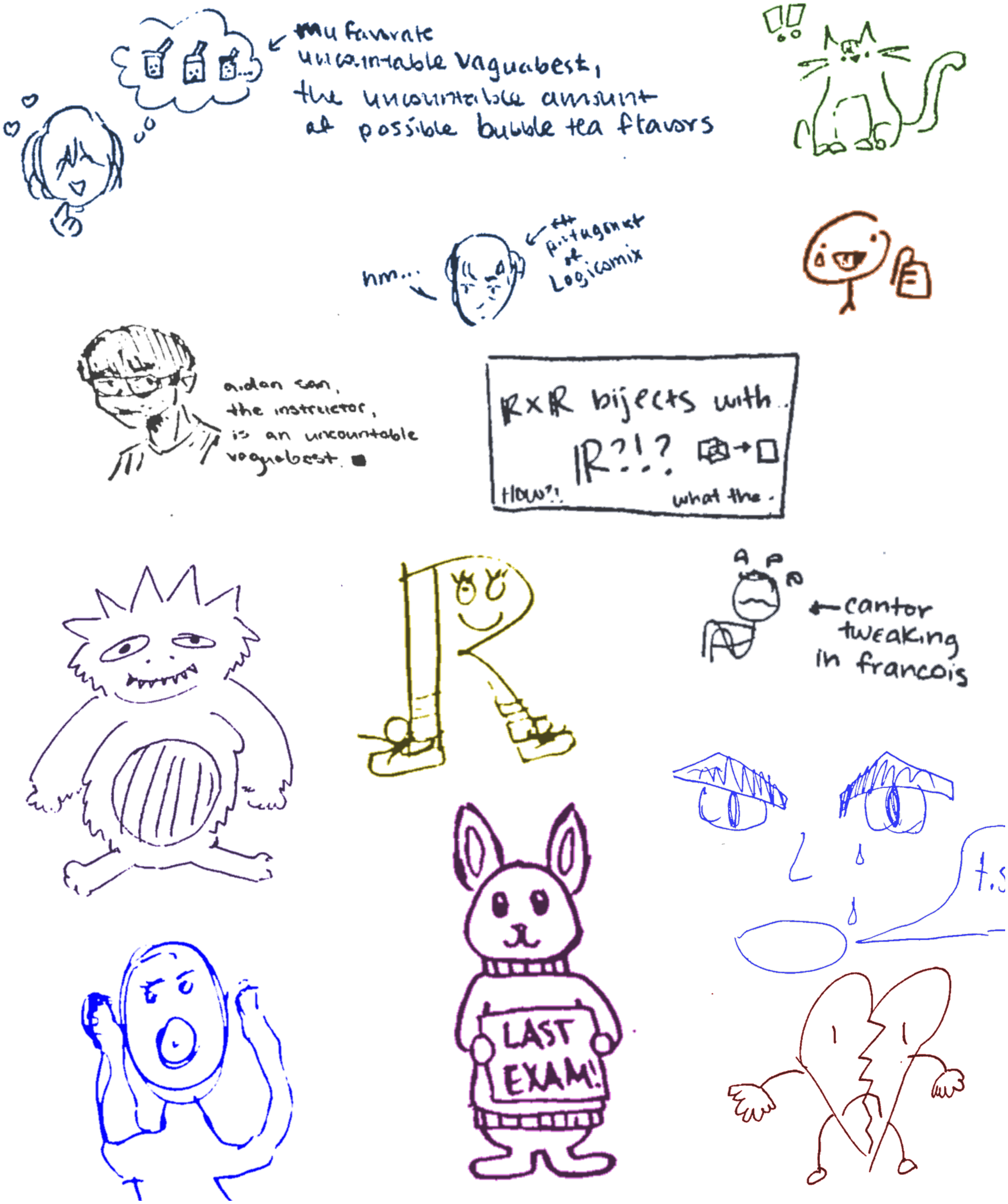
Induction Proof. We prove the proposition, $P := \forall n \in \mathbb{N} \, . \, S_n$ is countable, using the principle of induction on the natural numbers:

1. Our inductive predicate is $P(n) ::= S_n$ is countable.
2. **Base Case:** $P(0)$.

   The set S_0 consists of all subsets of $\mathbb{N}$ with exactly 0 elements. There is only one such subset: the empty set: $S_0 = \{\emptyset\}$. This has cardinality 1, so it is finite and countable.
3. **Inductive Step:** $\forall m \in \mathbb{N}. P(m) \implies P(m+1)$. To prove the implication, we need to show the conclusion is true when $P(m)$ is true.
4. By $P(m)$, since S_m is countable, there exists a surjective function:
$$R_m = (\mathbb{N}, S_m, G_m)$$
5. We construct a surjective function from $\mathbb{N} \times \mathbb{N}$ onto S_{m+1}
$$R_{m+1} = (\mathbb{N} \times \mathbb{N}, S_{m+1}, G_{m+1})$$
$$G_{m+1} = \{((n_1, n_2), G_m(n_1) \cup \{n_2\}) \mid (n_1, n_2) \in \mathbb{N} \times \mathbb{N}\}$$
6. Since $\mathbb{N} \times \mathbb{N}$ is countable and we have a surjective function onto S_{m+1}, it follows that S_{m+1} is countable.
7. We have shown $P(m) \Rightarrow P(m+1)$, completing the inductive step.
8. Thus, by the principle of induction on the natural numbers, S_n is countable for all $n \in \mathbb{N}$. ■

Well-Ordering Principle Proof. Here, we show another proof of the theorem, this time using the well-ordering principle.

1. Define the predicate, $P(n) ::= S_n$ is countable.
2. Define the set of counter-examples:
$$C ::= \{n \in \mathbb{N} \mid \neg P(n)\}$$
3. Assume, towards a contradiction, that the set of counterexamples is non-empty.
4. By the well-ordering principle, C has a minimum element. Let $m \in C$ be the minimal counterexample.
5. We know $m > 0$, since $S_0 = \{\emptyset\}$ has exactly one element, so S_0 is countable. Thus, $0 \notin C$.
6. Since m is the minimum of C and we know $m > 0$ from the previos step, we know $m - 1 \notin C$, so $P(m-1)$ holds.
7. Thus, S_{m-1} is countable and there exists a surjective function:
$$R_m = (\mathbb{N}, S_{m-1}, G_{m-1})$$
8. We construct a surjective function from $\mathbb{N} \times \mathbb{N}$ onto S_m
$$R_m = (\mathbb{N} \times \mathbb{N}, S_m, G_m = \{((n_1, n_2), G_m(n_1) \cup \{n_2\}) \ \mid \ (n_1, n_2) \in \mathbb{N} \times \mathbb{N}\})$$
9. Since $\mathbb{N} \times \mathbb{N}$ is countable, we know S_m is countable because of the surjective function we constructed in the previous step.
10. But this contradicts $m \in C$. Therefore, our assumption that C is non-empty must be false.
11. Thus, since C is empty, $P(n)$ holds for all $n \in \mathbb{N}$.



Some of our favorite uncountable vaguabeasts.

Have a great summer! Hope to see you in DMT2 or Law & AI in the Fall.