# Exam 1 Review Sheet

## Predicates, Sets, Quantified formulae

Logical operators and their meanings:

| operator | meaning | `true` when... |
|----------|---------|----------------|
| $p \wedge q$ | $p$ and $q$ | both $p$ and $q$ are true |
| $p \vee q$ | $p$ or $q$ | one of $p$ or $q$ is true |
| $p \implies q$ | $p$ implies $q$ | always unless `T` implies `F` |
| $p \iff q$ | $p$ iff $q$, $p$ equals $q$ | $p$ and $q$ are the same |
| $\neg p$ | not $p$ | $p$ is false |

Relevant logical operator facts:

- DeMorgan's Laws: $\neg(p \wedge q) = (\neg p) \vee (\neg q)$, and $\neg(p \vee q) = (\neg p) \wedge (\neg q)$

- $(p \iff q) = (p \implies q) \wedge (q \implies p)$

- $p \implies q = \neg p \vee q$

A **proposition** is either `true` or `false`.

A **predicate** is a function that produces propositions, and depends on one or more variables over a domain.

**Quantifiers** and their meanings:

| quantifier | `true` when... |
|------------|----------------|
| $(\forall x)(P(x))$ | $P(x)$ is true for all $x$ in the domain |
| $(\exists x)(P(x))$ | $P(x)$ is true for some $x$ in the domain |

Quantifiers bind variables to turn what would originally be a predicate into a proposition (or a predicate in one fewer variable).

A **set** is something that formalizes the notion of items which result in a predicate returning true. We say that for a set defined $S = \{x | P_S(x)\}$, the elements in $S$ are all $x$ for which $P_S(x)$ is true.

Set notation and its meaning:

| notation | meaning |
|----------|---------|
| $x \in S$ | $x$ is in set $S$ |
| $x \notin S$ | $x$ is not in set $S$ |
| $S \subseteq A$ | $S$ is a **subset** of $A$ |
| $S \subset A$ | $S$ is a **proper subset** of $A$ |
| $A \cup B$ | **union** of $A$ and $B$ |
| $A \cap B$ | **intersection** of $A$ and $B$ |
| $A \backslash B$ | **set difference** of $A$ and $B$ |
| $\overline{A}$ | **complement** of $A$ |
| $\emptyset$ | the **empty set** |
| $E$ | the **universe** set |
| $A \times B$ | the **set product** of $A$ and $B$ |
| $\mathcal{P}(A)$ | the **power set** of $A$ |

Definitions for set notation:

| thing | what it means |
|-------|---------------|
| $A$ subset $B$ | all elements of $A$ are in $B$ |
| $A$ proper subset $B$ | subset but $A \neq B$ |
| $A$ union $B$ | all elements that are in $A$ and $B$ |
| $A$ intersection $B$ | elements that are in both $A$ and $B$ |
| set diff of $A$ and $B$ | elements in $A$ that are not in $B$ |
| $A$ complement | elements in $E$ that are not in $A$ |
| empty set $\emptyset$ | set with no elements in it |
| universe set $E$ | set with every element in the domain |
| product $A \times B$ | ordered pairs $(x, y) : x \in A, y \in B$ |
| power set $\mathcal{P}(A)$ | set of all subsets of $A$ |

The **cardinality** of a set is its size (number of elements) for finite sets, and... *basically* its size (but not quite) for infinite sets.

The cardinality of the power set of set $A$, $|\mathcal{P}(A)| = 2^{|A|}$.

## Products, Relations, Functions (injective and surjective), Induction and Recursion, Alphabets and Strings

Products: see above (set product/Cartesian product, presumably).

A **function** $f : A \to B$ is a mapping from $A$ to $B$ that is in essence a subset of the set product of $A$ and $B$ (in other words, $f \subset A \times B$) in that it is a bunch of ordered pairs specifying which element of $A$ goes to which element of $B$. For general functions, we used the analogy of the gradebook as a function from students to grades.

Important function properties:

- For all elements $a \in A$, there is an element $b \in B$ that gets mapped to by $f$ (in other words, $\forall a \in A \exists b \in B : f(a) = b$)

- $A$ is the domain of $f$ and $B$ is the target or codomain of $f$

- Every element in the domain has only one image/element that it is mapped to – if $a$ has two images under $f$, then they must be equal to each other (the image is unique)

Ways to describe an input to $f$ and its output:

- $f$ sends $x$ to $y$

- $(x, y) \in f$

- $f(x) = y$

- $f : x \mapsto y$

The **range** of a function is the set of values in its codomain that it actually maps elements in its domain to.

An **injective** function (also called one-to-one) is one for which each element in the range is mapped to by only one element in the domain. In the line-drawing analogy from class, we might

think of it as prohibiting elements in the codomain from having more than one line drawn to them from the domain. We used the parking lot analogy for this in class.

A **surjective function** is one for which every output is mapped to by an input. (Probably not on the exam, as we didn't go over them in class.)

The **inverse** $f^{-1}$ of a function $f$ essentially switches the ordering of the ordered pairs from $f$. It maps from the range of $f$ to the domain of $f$. (Note that it can't necessarily map from the codomain to the domain as it's possible that not every element of the codomain was used by $f$.) We call $f^{-1}$ the *partial inverse function.*

A **partial function** is a function $f : S \rightarrow A$ where $S \subseteq A$. In other words, it is a function whose domain is a subset of its codomain. If some element $x$ is in the codomain but not the domain of $f$, we say that $f(x)$ is *undefined.*

A **relation** is basically a generalized function that doesn't have the restriction that one input cannot map to multiple outputs. (Probably not on the exam, as we didn't go over them in class.)

A **total** function is one for which the domain is the same set as the codomain.

An **alphabet** is any *finite* set, typically denoted (e.g.) $\Sigma = \{$a, b, c$\}$.

A **letter** is an element of an alphabet, e.g. a or b.

A **string** is any *finite* sequence of letters. An example from the above alphabet might be ababba.

The **length** of a string is the number of letters in the string, denoted $|s|$ for string $s$.

The **empty string**, denoted $\lambda$, is the string without any letters in it. We say that $|\lambda| = 0$.

The concatenation of strings $x$ and $y$, denoted $x \circ y$ or $x \cdot y$, is $xy$ ($x$ written next to $y$). Ex. for $x =$ abca, $y =$ bac, $x \circ y =$ abcabac and $|x \circ y| = |x| + |y| = 4 + 3 = 7$.

A **language** is any set of strings (over the given alphabet). A language is always *infinite* (consider concatenating $n$ letters, starting from $n = 0$ which gives $\lambda$ and continuing. There is an injection from each of these $n$-letter strings to the natural numbers $\mathbb{N}$).

**Induction** is one method of proving things, but will not be explored too much. *We won't ever have to write an inductive proof for something* – it's enough to just know the reasoning behind it. It boils down to a base case and an inductive hypothesis.

Ex. Consider a ladder with (countably) infinite rungs, and we want to show that we can climb to any rung. Induction allows us to say that if we can climb to the first rung (base case), and if we're at any rung, we can climb to the next rung

on the ladder (inductive hypothesis), we can climb to any of the rungs on the ladder.

Anyone reading this should already be familiar with **recursion** from coding such functions in their previous CS classes, but it doesn't really matter anyway because we didn't explicitly go over it in class. Induction uses a kind of recursion which is probably as much as you need to know for the exam (if anything).

### Cardinalities, the natural numbers $\mathbb{N}$, Countable and Uncountable sets, Counting $\bigcup_{k=1}^{\infty} \mathbb{N}^k$

More precise definition of **cardinality**: We say that $|A|$ is the cardinality of a set $A$. Given two sets $A$ and $B$, if $|A| \leq |B|$, there exists some injective function from $A$ to $B$. With our parking lot idea, $A$ is the set of cars and $B$ is the set of parking spots. If $|A| = |B|$, then there are injections from $A$ to $B$ and from $B$ to $A$. If $|A| < |B|$ then there is an injection from $A$ to $B$ but *not* from $B$ to $A$.

A set $A$ has **infinite cardinality** if there is some proper subset $S \subset A$ of $A$ with the same cardinality $|S| = |A|$ (there are injections between the two sets $S$ and $A$).

The set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ of **natural numbers** is infinite.

A set $A$ is **finite** if its cardinality $|A|$ is strictly less than $\aleph_0 = |\mathbb{N}|$.

A set is **countable** if its cardinality is not greater than $\aleph_0$. Otherwise, it is **uncountable**. In other words, a set is countable if it is either finite or has cardinality $\aleph_0$ (is countably infinite).

The **Gödel injection** is one of our "failed attempts to construct an uncountable set." It essentially allows us to write any $k$-tuple of natural numbers as another natural number in $\mathbb{N}$. It is defined as $\mathcal{G} : \bigcup_{k=1}^{\infty} \mathbb{N}^k \rightarrow \mathbb{N}$.

Fancily typeset, this is:

$$\mathcal{G} : \underbrace{\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}}_{k \text{ times}} \rightarrow \mathbb{N}$$

The way we achieve this injection is with prime factorization. Any $k$-tuple, written $\langle x_1, x_2, \ldots, x_k \rangle$, gets mapped to a natural number as follows:

$$\mathcal{G}(\langle x_1, x_2, \ldots, x_k \rangle) = p_1^{x_1+1} \cdot p_2^{x_2+1} \cdot \cdots \cdot p_k^{x_k+1},$$

where $p_i$ represents the $i$th prime number.

Examples of **computing Gödel numbers**:

- $[1] \rightarrow 2^{1+1} = 2^2 = 4$

- $[1, 0] \rightarrow 2^{1+1} \cdot 3^{0+1} = 12$

- $[1, 0, 0] \rightarrow 2^{1+1} \cdot 3^{0+1} \cdot 5^{0+1} = 60$

Examples of **inverse Gödel numbering**:

- $\mathcal{G}^{-1}(2) = [0]$ because its prime factorization is $2^1$ which corresponds to $2^{0+1}$ and therefore the sequence containing only one 0

- $\mathcal{G}^{-1}(4480) = \mathtt{undefined}$ because its prime factors do not cover consecutive primes $(2, 3, 5, \text{etc.})$ starting from 2 (without doing all the math it looks like it's missing a 3)

- $\mathcal{G}^{-1}(720) = [3, 1, 0]$ because 720's prime factorization is $2^4 \cdot 3^2 \cdot 5^1$ which corresponds to $2^{3+1} \cdot 3^{1+1} \cdot 5^{0+1}$ and therefore $[3, 1, 0]$

Other questions about Gödel numbering can be in the form of being given some tuple of variables, and being told various things about it, and using the properties of the numbering system to deduce things about the tuple's corresponding Gödel number. Look at the class notes (`4.pdf`, page 5) for more examples.

DIAGONALIZATION PROOF THAT $|\{f : \mathbb{N} \to \{0,1\}\}| > \aleph_0$, PARTIAL FUNCTIONS

Partial functions: see above, by FUNCTIONS.

The **diagonalization proof** that $\mathcal{P}(\mathbb{N})$ is uncountable follows.

Assume for the sake of contradiction that there is some injection from the natural numbers $\mathbb{N}$ to its power set $\mathcal{P}(\mathbb{N})$. Then, we can write this injection as a table like so (the actual contents of the below table are irrelevant, they are just sequences of bits):

|       | 0 | 1 | 2 | 3 | 4 | 5 | 6 | ... |
|-------|---|---|---|---|---|---|---|-----|
| $f_0$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| $f_1$ | 1 | 0 | 0 | 0 | 1 | 0 | 0 | ... |
| $f_2$ | 0 | 0 | 1 | 0 | 0 | 0 | 0 | ... |
| $f_3$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | ... |
| $f_4$ | 0 | 1 | 0 | 1 | 0 | 1 | 0 | ... |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ |

Here, each 0 or 1 represents whether the natural number in the top row is contained or not contained in $f_i$, each of which is a subset of $\mathbb{N}$. The table should list all of the infinite subsets of $\mathbb{N}$ in this way. Then, the argument against this construction proceeds as follows. Take a subset $D$ of $\mathbb{N}$, such that $n \in D \iff n \notin f_n$. In other words, $D$ is the subset of $\mathbb{N}$ created by flipping each of the elements (from 0 to 1 or 1 to 0) along the diagonal. Then, since $D$ is a subset of $\mathbb{N}$, it must have its own row in the table, which we will call number $\alpha$. So, $D = f_\alpha$.

This, however, leads to a contradiction. If $\alpha \in D$ (the $\alpha$th bit in $D$ is a 1), then $\alpha \notin f_\alpha$ by our definition of $D$ as the subset created by flipping all the bits along the diagonal. But then, by the definition of $\alpha$ as the row to which $D$ is assigned (we said that $D = f_\alpha$), $\alpha \notin D$ (the $\alpha$th bit in $D$ is a 0). This is a contradiction.

The same occurs when we try to assume $\alpha \notin D$. If $\alpha \notin D$, then it must be in $f_\alpha$ by the definition of $D$ (as it was flipped on the diagonal). But since $D = f_\alpha$ by the definition of $\alpha$, $\alpha$ must be in $D$ and therefore we have the same contradiction.

So, we have proven by contradiction that $\mathbb{P}(\mathbb{N})$ is uncountable and thus that $|\mathcal{P}(\mathbb{N})| > \aleph_0$.

$\square$

**Exam on Monday. Good luck!**