Math 109, Fall 2017
Homework 8 Solutions

A. Proceed by induction on n. When n = 1, we need to show there are 2 functions \( f : \{1\} \rightarrow \{0, 1\} \). In this case, a function just corresponds to mapping 1 to 0 or 1. There are therefore two functions \( f_0 \) and \( f_1 \) defined by \( f_0(1) = 0 \) and \( f_1(1) = 1 \). For the inductive hypothesis, assume that for some \( n \geq 1 \), there are \( 2^n \) functions \( f : \{1, \ldots, n\} \rightarrow \{0, 1\} \). We will show that there are \( 2^{n+1} \) functions from \( \{1, \ldots, n+1\} \) to \( \{0, 1\} \).

Let \( f : \{1, \ldots, n\} \rightarrow \{0, 1\} \) be any function. We can “extend” \( f \) to a function on \( \{1, \ldots, n+1\} \) by deciding what \( f(n+1) \) should be: either 0 or 1. This leads to two functions \( f_0 : \{1, \ldots, n+1\} \rightarrow \{0, 1\} \) and \( f_1 : \{1, \ldots, n+1\} \rightarrow \{0, 1\} \) defined by

\[
f_0(x) = \begin{cases} f(x) & \text{if } 1 \leq x \leq n \\ 0 & \text{if } x = n+1 \end{cases} \quad \text{and} \quad f_1(x) = \begin{cases} f(x) & \text{if } 1 \leq x \leq n \\ 1 & \text{if } x = n+1 \end{cases}.
\]

Thus, for each of the \( 2^n \) functions \( f : \{1, \ldots, n\} \rightarrow \{0, 1\} \), we can define two functions \( \{1, \ldots, n+1\} \rightarrow \{0, 1\} \). To know that we really get \( 2^{n+1} \) functions this way, we need to make sure they’re all different (it is possible two different functions \( \{1, \ldots, n\} \rightarrow \{0, 1\} \) could “extend” to the same function, so we wouldn’t have defined \( 2^{n+1} \) different functions. We need to show this is not the case.) Notice that if \( f, g : \{1, \ldots, n\} \rightarrow \{0, 1\} \) are two distinct functions, i.e. \( f \neq g \), then \( f_0 \neq g_0 \) and \( f_1 \neq g_1 \). This is because, since \( f \neq g \), there is some \( x \in \{1, \ldots, n\} \) such that \( f(x) \neq g(x) \). Then \( f_i(x) \neq g_i(x) \) for \( i = 0, 1 \). It is also clear that \( f_0 \neq f_1 \), since \( f_0(n+1) \neq f_1(n+1) \). Thus, we have constructed \( 2^{n+1} \) functions from \( \{1, \ldots, n+1\} \rightarrow \{0, 1\} \): this means there are at least \( 2^{n+1} \) such functions. We now need to show that these are actually all of them (if you are confused about this, think of this: just because we can write down 10 real numbers, it doesn't follow that there's only 10 real numbers!)

Let \( F : \{1, \ldots, n+1\} \rightarrow \{0, 1\} \). We need to show that \( F = f_0 \) or \( F = f_1 \) for some function \( f : \{1, \ldots, n\} \rightarrow \{0, 1\} \). Define \( f = F \mid_{\{1, \ldots, n\}} \), that is, let \( f \) be the function \( \{1, \ldots, n\} \rightarrow \{0, 1\} \) defined by \( f(x) = F(x) \) for all \( 1 \leq x \leq n \). If \( F(n+1) = 0 \), it is then easy to verify that \( F = f_0 \). If \( F(n+1) = 1 \), \( F = f_1 \). Thus, every function \( F : \{1, \ldots, n+1\} \rightarrow \{0, 1\} \) is obtained by our construction above, and so the \( 2^{n+1} \) functions we defined above are all of them, as desired.

It follows by induction that there are \( 2^n \) functions \( f : \{1, \ldots, n\} \rightarrow \{0, 1\} \) for every \( n \geq 1 \).

B. This is proved in the book, see Theorem 14.1.4. The book does not provide many details for the direction of “equipotent to a proper subset implies infinite” (certainly, we would expect more details in a proof, especially on an exam). For us, a full proof would look more like this:

Suppose that \( X \) is equipotent to a proper subset of itself, call it \( Y \). Suppose for contradiction that \( X \) is finite. Then, since \( Y \) is a proper subset of \( X \), \( |Y| \leq |X| - 1 \), because there is at least one element that is in \( X \) and not in \( Y \). Since \( X \) is equipotent to \( Y \), this means by definition that there exists a bijection \( f : X \rightarrow Y \). However, by Prop.10.1.3, if there exists a bijection between two finite sets, they have the same cardinality. Hence \( |X| = |Y| \). This contradicts that \( |Y| \leq |X| - 1 \), so \( |X| \) must have been infinite, as desired.

C. Recall that \( d = \gcd(a, b) \) if and only if (1) \( d | a \) and \( d | b \) and (2) for all \( c \in \mathbb{Z} \), \( c|a \land c|b \implies c \leq d \). Let \( d' = \gcd(a', b') \). By definition, \( d'|a' \) and \( d'|b' \). Let \( k, \ell \in \mathbb{Z} \) be such that \( d' = kd' \) and \( b' = \ell d' \).

Then \( a = kdd' \) and \( b = \ell dd' \). Thus, \( dd'|a \land dd'|b \). Hence, by definition of \( d = \gcd(a, b) \), \( dd' \leq d \).
Since $d \geq 1$ (1 divides every integer, so by (2) $d \geq 1$), we can divide by $d$ to get $d' \leq 1$. $d' \geq 1$ for the same reason that $d \geq 1$, so we have that $d' = 1$. 