M311S24 Problem Set 1.2 *Franchi-Pereira, Philip*

Problem 5. If X and Y are finite and Y is non-empty then so is $F(X,Y)$, and $|F(X,Y)| = |Y|^{|X|}$.

Definition 1 Let $\epsilon : F(\{x\},Y) \to Y$ by $\epsilon(\{(\{x\},y)\}) = y, y \in Y$, and define an inverse $\gamma : Y \to F(\{x\},Y), \gamma(y) = \{(x,y)\}$. It is clear these two are inverses, since $(\gamma \circ \epsilon)(\{(a,b)\}) = \gamma(\epsilon(\{(a,b)\})) = \gamma(b) = \{(a,b)$ and $\epsilon \circ \gamma(b) = \epsilon(\gamma(b)) = \epsilon(\{(a,b)\}) = b$ for $a \in \{a\}$ and $b \in Y$.

Definition 2 Let $X = A \cup B$ with $A \cap B = \emptyset$, then we have the restriction map $\mathcal{C} : F(X,Y) \to F(A,Y) \times F(B,Y)$ given by $\mathcal{C}(f) = (f|_A, f|_B)$. $\mathcal{C}$ is bijective, which will be shown by defining an inverse $\mathcal{D} : F(A,Y) \times F(B,Y) \to F(X,Y)$ such that $\mathcal{D}((f|_A, f|_B) = \{(a, f|_A(a)) : a \in A\} \cup \{(b, f|_B(b)) : b \in B\}$, which will be labeled δ_f for the remainder of the proof.

First we will show that $(\mathcal{D} \circ \mathcal{C})(f) = f$ for some $f \in F(X,Y)$. Note that $(\mathcal{D} \circ \mathcal{C})(f) = \mathcal{D}(\mathcal{C}(f))) = \mathcal{D}((f|_A, f|_B)) = \delta_f$. To show that $\delta_f = f$, we will show that they are subsets of eachother. For all $x \in X, x$ is either in A or B, since they are disjoint. If $x \in A$, then $\delta_f(x) = f|_A(x) = f(x)$ and if $x \in B$, then $\delta_f(x) = f|_B(x) = f(x)$ and so $\delta_f \subseteq f$. Next, for all $x \in X, f(x) = f|_A(x) = \delta_f(x)$ if $x \in A$, and $f(x) = f|_B(x) = \delta_f(x)$ if $x \in B$. Therefore $f \subseteq \delta_f$ and so $f = \delta_f$. Note that if A and B were not disjoint, then for an element $x \in A \cap B$, $f|_A(x)$ may or may not equal $f|_B(x)$, and so $F(X,Y)$ may not be well ordered.

Next we will show that $(\mathcal{C} \circ \mathcal{D})((f|_A, f|_B)) = (f|_A, f|_B)$. Note that $(\mathcal{C} \circ \mathcal{D})((f|_A, f|_B)) = \mathcal{C}(\mathcal{D}((f|_A, f|_B))) = \mathcal{C}(\delta_f) = (\delta_f|_A, \delta_f|_B)$. To show that $(\delta_f|_A, \delta_f|_B) = (f|_A, f|_B)$, we must show that $\delta_f|_A = f|_A$ and $\delta_f|_B = f|_B$. However, by definition of δ_f, for all $a \in A, \delta_f(a) = f|_A$ and for all $b \in b, \delta_f(b) = f|_B$. Therefore $(\delta_f|_A, \delta_f|_B) = (f|_A, f|_B)$, $(\mathcal{C} \circ \mathcal{D})((f|_A, f|_B)) = (f|_A, f|_B)$, and so $\mathcal{C}$ and $\mathcal{D}$ are inverses.

Finally, we will use induction to prove that for finite sets X and Y with $Y \neq \emptyset$, then $|F(X,Y)| = |Y|^{|X|}$.

Base Case Let $|X| = 1, X = \{x\}$. Since there exists a bijection $\epsilon(F(\{x\}, Y) = Y$, $|F(\{x\}, Y| = |Y|$, and since $|Y|^{|X|} = |Y|^{|1|} = |Y|$, $|F(\{x\}, Y| = |Y|^{|X|} = |Y|$.

Inductive Proposition Let A and Y be finite sets, with $Y \neq \emptyset$ and $|A| = n$. Assume $|A| = n$ implies $|F(A, Y)| = |Y|^{|A|} = |Y|^n$, Then for some set X with $|X| = n + 1$, $|F(X, Y)| = |Y|^{|X|} = |Y|^{n+1}$.

Proof Let A and Y be finite sets, with $Y \neq \emptyset$ and $|A| = n$. Let $A = X - \{x\}$, and $B = \{x\}$. It is clear that $A \cap B = \emptyset$, and that $X = A \cup B$. Then by Definition 2 there exists a map $\mathcal{C} : F(X, Y) \to F(A, Y) \times F(B, Y)$ and its inverse $\mathcal{D}$. Since $\mathcal{C}$ has an inverse $\mathcal{D}$, it is a bijection and therefore $|F(X, Y)| = |F(A, Y) \times F(B, Y)|$. By Corollary 2.2.17 in the class notes, $|F(A, Y) \times F(B, Y)| = |F(A, Y)| \cdot |F(B, Y)| = |F(X, Y)|$.
Since $|B| = 1, |F(B, Y)| = |Y|$, and by the inductive hypothesis $|A| = n, |F(A, Y)| = |Y|^n$, then $|F(X, Y)| = |Y|^n \cdot |Y|^1 = |Y|^{|n+1|}$. Therefore, $|F(X, Y)| = |Y|^{|n+1|} = |Y|^{|X|}$.

Problem 6. An Alternate Proof of $|\mathcal{P}(X)| = 2^{|X|}$.

For a positive integer n we denote the set $\{0, 1, 2, ...n - 1\}$ by $\mathbb{Z}_n$. Thus $\mathbb{Z}_2 = \{0, 1\}$ We have a map $\Sigma : F(X, \mathbb{Z}_2) \to \mathcal{P}(X), f \mapsto f^{-1}(1)$. Given $A \subseteq X$ we define $\chi_A \in F(X, \mathbb{Z}_2)$ by $\chi_A(x) = 1$ for $x \in A$ and $\chi_A(x) = 0$ for $x \notin A$. Last, define the map $\Xi : (\mathcal{P}(X) \to F(X, \mathbb{Z}_2)$ by $\Xi(A) = \mathcal{X}_A$.

First we will show that Ξ and Σ are inverses. Consider first $(\Sigma \circ \Xi)(A), A \subseteq X$. $(\Sigma \circ \Xi)(A) = \Sigma(\Xi(A)) = \Sigma(\chi_A) = \chi_A^{-1}(1)$. To show that $\chi_A^{-1}(1) = A$, we will show that $\chi_A^{-1}(1) \subseteq A$ and then $A \subseteq \chi_A^{-1}(1)$. First, for all $x \in \chi_A^{-1}(1), \chi_A(x) = 1$, and so $x \in A$, therefore $\chi_A^{-1}(1) \subseteq A$. Next, for all $a \in A, \chi_A(a) = 1$, and so $a \in \chi_A^{-1}(1)$. Therefore, $A \subseteq \chi_A^{-1}(1)$ and so $A = \chi_A^{-1}(1)$ and $(\Sigma \circ \Xi)(A) = A$.

Next, consider $(\Xi \circ \Sigma)(f) = \Xi(\Sigma(f)) = \Xi(f^{-1}(1)) = \chi_{f^{-1}(1)}$. First we show that $f \subseteq \chi_{f^{-1}}(1)$. For all $x \in X$, if $(x, 1) \in f, x \in f^{-1}(1)$, and so $(x, 1) \in \chi_{f^{-1}(1)}$. In the case instead where $(x, 0) \in f$ the $x \notin f^{-1}(1)$ and so $(x, 0) \notin \chi_{f^{-1}(1)}$. Therefore $f \subseteq \chi_{f^{-1}(1)}$. To show that $\chi_{f^{-1}(1)} \subseteq f$, note that for all $x \in X$, if $\chi_{f^{-1}(1)}(x) = 1$, then $x \in f^{-1}(1)$ and therefore $(x, 0) \in f$. If $\chi_{f^{-1}(1)}(x) = 0$, then $x \notin f^{-1}(1)$ and so $(x, 0) \in f$. Therefore $f \subseteq \chi_{f^{-1}(1)}$, so $f = \chi_{f^{-1}(1)}, (\Xi \circ \Sigma)(f) = f$, and so Ξ and Σ are inverses.

Finally, since Ξ and Σ are inverses, then Σ is bijective, and so $|\mathcal{P}(X)| = |F(X, \mathbb{Z}_2)|$. By the proof demonstrated in Problem 5, $|F(X, \mathbb{Z}_2)| = |\mathbb{Z}_2|^{|X|}$. Since $\mathbb{Z}_2$ is known to only have the elements $\{0, 1\}$, $|\mathbb{Z}_2| = 2$, and so $|F(X, \mathbb{Z}_2)| = 2^{|X|}$. Therefore, $|\mathcal{P}(X)| = |F(X, \mathbb{Z}_2)| = 2^{|X|}$.

Problem 7. $\#(Gl(n, \mathbb{Z}_p)) = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{n-1}) = p^{n^2}(1 - \frac{1}{p^n})(1 - \frac{1}{p^{n-1}})(1 - \frac{1}{p})$.

Since the size of the group $Gl(n, \mathbb{Z}_p)$ of invertible $n \times n$ matrices is the number of the possible ordered basis of $\mathbb{Z}_p^n$, we will show that the number of orderings of a span of k vectors in $\mathbb{Z}_p^n = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{k-1})$. We will induce on k, limiting the induction such that $k \leq n$, since if the span contains more than n vectors they are by definition no longer independent.

Base Case $k = 1$
Each vector has n components, each with p possible values. The choice of v_k could be any of the p^n possible vectors, except for the 0 vector. So there are $p^n - 1$ choices for v_0. The number of orderings of the span are therefore $p^n - p^{k-1} = p^n - p^{1-1} = p^n - 1$.

Base Case $k = 2$
There are p^n possible choices for v_2, but it cannot be a scalar multiple of $span(v_1)$. Since there is only one vector in the $span(v_1)$, then there are p scalar mutlipes of existing vectors in the span that v_2 cannot be chosen, in order to maintain independence. There are then $(p^n - p)$ choices for v_2, and therefore $(p^n - p)(p^n - 1)$ possible orderings of the span.

Inductive Proposition.
Assume the number of orderings of a $span(v_1, v_2, ..., v_k) = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{k-1})$. Then for any number $a \in \mathbb{N}, a \leq n, a = k + 1$, the number of orderings of vectors in $span(v_1, v_2, ..., v_a) = (p^n - 1)(p^n - p)(p^n - p^2)...(p^n - p^{a-1})$.

Again, the choice of the next vector v_a could be one of any p^n vectors. However, we cannot pick any scalar multiple of a vector already in $span(v_1, v_2, ..., v_{a-1})$. There are $a-1$ vectors in the span, and so there are p^{a-1} vectors that cannot be chosen, which makes the number of choices for $v_a = (p^n - p^{a-1} = p^n - p^k$, since $a = k+1, k = a-1$. By the inductive hypothesis, the total number of orderings of the previous {a-1} vectors, $span(v_1, v_2, ..., v_k)$ is assumed to be $(p^n-1)(p^n-p)(p^n-p^2)...(p^n-p^{k-1})$. Therefore the orderings of the span, including v_a are

$$\begin{aligned}(p^n - p^k) \times (p^n-1)(p^n-p)(p^n-p^2)...(p^n-p^{k-1}) &= \\ (p^n-p)(p^n-p^2)...(p^n-p^{k-1})(p^n-p^k) &= \\ (p^n-p)(p^n-p^2)...(p^n-p^{a-2})(p^n-p^{a-1}).\end{aligned}$$

which proves the inductive proposition.

Finally, since the size of $Gl(n, \mathbb{Z}_p))$ is equal to the number of orderings of basis in $\mathbb{Z}_p^n$, there are n vectors in the span and so $\#(Gl(n, \mathbb{Z}_p)) = (p^n-1)(p^n-p)(p^n-p^2)...(p^n-p^{n-1})$.