CSC240 Winter 2024 Homework Assignment 6

My name and student number: Haoyun (Bill) Xi, 1009992019
The list of people with whom I discussed this homework assignment: Tianchu Li, Anna Li, Joyce Qu.

1. For $n \in \mathbb{Z}^+$, let $[n]$ denote the set $\{i \in \mathbb{Z}^+ \mid i \leq n\}$.
   For each $n \in \mathbb{Z}^+$, each function $f : [n] \to \{0,1\}$, and each non-empty subset $I \subseteq [n]$, define the *restriction* of f to I to be the function $f\big|_I : I \to \{0,1\}$ where, for each $x \in I$,

$$f\big|_I(x) = f(x).$$

   Give a well-structured informal proof using double induction that, for each $k \in \mathbb{Z}^+$, each $n \in \mathbb{Z}^+$, and each subset S of functions from $[n]$ to $\{0,1\}$, if $n \geq k$ and

$$|S| > \sum_{i=0}^{k-1} \binom{n}{i},$$

   then there exists a subset $I \subseteq [n]$ with $|I| = k$ such that $\{f\big|_I \mid f \in S\}$ is the set of all functions from I to $\{0,1\}$.

   You may use the following fact, known as Pascal's Identity, without proof.

   Lemma: $\forall k \in \mathbb{Z}^+ . \forall n \in \mathbb{Z}^+ . \left[\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}\right]$.

   Notes and symbols:
   $\{0,1\}^{[n]}$ is the set of all functions from $[n]$ to $\{0,1\}$.
   In the following proof, we will treat functions as a binary sequence. A string representation s of a function f is the n-bit binary sequence where if we count from 1 to n, s_i denotes $f(i)$. Since f is from $[n]$ to $\{0,1\}$, a binary sequence is equivalent to a function in $\{0,1\}^{[n]}$
   Under this representation, $s\big|_I$ represents the concatenation of sequence s selected only at indices of I, from increasing order. For example, $(0,1,1,0)$ represents the function that maps $2,3$ to 1, and $1,4$ to 0. $s\big|_I$ when $I = \{1,3\}$ is the sequence $(0,1)$.
   $A = \{f\big|_I \mid f \in S\}$ is the set of all functions from I to $\{0,1\}$ iff A's binary sequence representation cover all permutations of k-bit binary sequence, where $|I| = k$.
   When we later say $S \in \{0,1\}^{[n]}$ is a set of n-bit binary sequences, we're actually talking about its binary sequence representation. We will treat them as the same mathematical object.
   If S is a set of n-bit binary sequence and $I \subseteq [n]$, we use $S\big|_I$ to denote $\{s\big|_I | s \in S\}$.
   Define $P(n,k) : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \{T, F\} =$ "$\forall S \in \{0,1\}^{[n]} . \Big[(n \geq k \text{ AND } |S| > \sum_{i=0}^{k-1} \binom{n}{i})$ IMPLIES $(\exists I \subseteq [n] . \big[(|I| = k)$ AND $\{f\big|_I \mid f \in S\}$ is the set of all functions from $I \to \{0,1\}\big])\Big]$".
   Define $Q(k) : \mathbb{Z}^+ \to \{T, F\} =$ "$\forall n \in \mathbb{Z}^+ . P(n,k)$."
   We will show $\forall k \in \mathbb{Z}^+ . \forall n \in \mathbb{Z}^+ . P(n,k)$ by double induction, proving $\forall k \in \mathbb{Z}^+ . Q(k)$.

   Proof.

Let $k \in \mathbb{Z}^+$ be arbitrary. Assume $\forall i \in \mathbb{Z}^+.[(i < k) \text{ IMPLIES } Q(i)]$

Base Case: $k = 1$. (We want to show $\forall n \in \mathbb{Z}^+.P(n,1)$)

Let $n \in \mathbb{Z}^+$, $S \in \{0,1\}^{[n]}$ be arbitrary.

Assume $|S| > \sum_{i=0}^{0} \binom{n}{0} = \binom{n}{0} = 1$ and $n \geq 1$.

Since $|S|$ is a set of at least two functions (binary sequences), by the uniqueness of set elements, there must be some different $s_1, s_2 \in S$ such that $\exists c \in [n].(s_1)_c \neq (s_2)_c$. In plain words, this is because two functions are different only if they differ in at least one position.

Thus if we pick $I = \{c\}$, $s_1\big|_I$ and $s_2\big|_I$ are different single bit. Thus they cover all 1-bit binary sequence. Hence, $\{f\big|_I \mid f \in S\} = \{0,1\}^{[n]}$.

$(n \geq 1 \text{ AND } |S| > \sum_{i=0}^{1-1} \binom{n}{i}) \text{ IMPLIES } (\exists I \subseteq [n].\big[(|I| = 1) \text{ AND } \{f\big|_I \mid f \in S\} = \{0,1\}^{[n]}\big)$, by proof of construction and direct proof.

Since $n \in \mathbb{Z}^+$, $S \in \{0,1\}^{[n]}$ are arbitrary, we showed $P(n,1)$, which is $Q(1)$.

Let $k \in \mathbb{Z}^+$ and $k > 1$ be arbitrary.

We want to show $Q(k)$ by showing $\forall n \in \mathbb{Z}^+.P(n,k)$ using induction on n.

Let $n \in \mathbb{Z}^+$ be arbitrary. Assume $\forall j.[(j < n) \text{ IMPLIES } P(j,k)]$.

Case 1: $n < k$. The premise $n \geq k$ is false. $P(n,k)$ is vacuously true.

Case 2: $n = k$.

Let $S \in \{0,1\}^{[k]}$ be arbitrary and assume $|S| > \sum_{i=0}^{k-1} \binom{k}{i}$.

We know that according to our binary sequence representations, the set of all functions from $[k] \to \{0,1\}$ is equivalent to the set of all k-bit binary sequences.

Pick $I = [k] \subseteq [k]$ and $|I| = k$.

Since $|S| > \sum_{i=0}^{k-1} \binom{k}{i}$, we conclude the minimal size of S is:

$$|S| \geq \sum_{i=0}^{k-1} \binom{k}{i} + 1 = \sum_{i=0}^{k-1} \binom{k}{i} + \binom{k}{i} = \sum_{i=0}^{k} \binom{k}{i}$$

Also, reminds that the size of all binary sequence with length k is calculated by summing up the number of string with i ones and $(k-i)$ zeros, from $i = 1$ to $i = k$. Such amount with i ones is exactly $\binom{k}{i}$. Thus, $|S|$ is at least the size of all k-bit binary sequences. Since that $|S|$ is also the subset of the set of all k-bit binary sequences, we conclude $|S|$ must be exactly the set of k-bit binary sequences.

Hence, $\{f\big|_I \mid f \in S\} = S = \{0,1\}^{[k]} = \{0,1\}^I$

By direct proof and proof of construction, we showed that $P(k,k)$ is true.

In other words, $(n = k)$ IMPLIES $P(n,k)$.

Case 3: $n > k$.

Since $n - 1 < n$, by our inductive hypothesis, we have $P(n-1,k)$.

Also note that $n > k$ implies $n \geq k$. This means we have a chance later in our proof to use modus ponens to obtain important information, if $|S|$ is appropriate.

Let $S \in \{0,1\}^{[n]}$ be arbitrary and assume $|S| > \sum_{i=0}^{k-1} \binom{n}{i}$.

By Pascal's identity, $|S| > \binom{n}{0} + \sum_{i=1}^{n-1} (\binom{n-1}{i} + \binom{n-1}{i-1})$

$$= \binom{n}{0} + \sum_{i=1}^{n-1} \binom{n-1}{i} + \sum_{i=1}^{k-1} \binom{n-1}{i-1} = \sum_{i=0}^{n-1} \binom{k-1}{i} + \sum_{i=1}^{k-2} \binom{n-1}{i}$$

Let $S' = \{s \in S | s_n = 0\}, S'' = \{s \in S | s_n = 1\}$. Consider their restriction of the first $n-1$ elements $A = S'\big|_{[n-1]}$ and $B = S''\big|_{[n-1]}$. As A, B are cuts of S', S'', they might have non empty intersection. Since sets do not allow duplicates, the size of the union $A \cup B$ is the sum of the sizes of A and B subtract by the amount of duplicates $|A \cap B|$. Thus, $|A \cup B| = |A| + |B| - |A \cap B|$. Rearranging we have $|A \cap B| = |S'| + |S''| - |A \cup B| = |S| - |A \cap B|$.

Assume the union has size $|A \cup B| > \displaystyle\sum_{i=0}^{k-1} \binom{n-1}{i}$.

Since $A, B \in \{0,1\}^{[n-1]}, |A \cup B| \in \{0,1\}^{[n-1]}$ too. Specialize $P(n-1,k)$ with $A \cup B$. Since $n-1 > k$ and that $A \cup B$ is sufficiently large by our assumption, by modus ponens of $P(n-1,k)$, we have a set $I' \subseteq [n-1]$ such that $|I'| = k$ and $(A \cup B)\big|_{I'} = \{0,1\}^{I'}$. Since $I' \subseteq [n-1]$ and $A \cup B = S\big|_{[n-1]}$, we have $S\big|_{I'} = (A \cup B)\big|_{I'}$. In plain words, this is because I' does not have n. Thus when we cut S with I', we will ignore every n^{th}-bit. So same cut will be obtained comparing to $A \cup B$, which is set of all functions from I' to $\{0,1\}$.

Ignoring the n^{th} digit of sequences in S first and then pick indices in I is equivalent of directly picking indices in I.
Hence if we pick $I = I'$, by substitution, $S\big|_I = \{0,1\}^I$.

Therefore, $|A \cup B| > \sum_{i=0}^{k-1} \binom{k-1}{i}$ IMPLIES $P(n,k)$.

Assume the union has size $|A \cup B| \leq \displaystyle\sum_{i=0}^{k-1} \binom{n-1}{i}$.

By our equality above, the size of intersection $|A \cap B| \geq |S| - \displaystyle\sum_{i=0}^{k-1} \binom{n-1}{i}$

$> \displaystyle\sum_{i=0}^{k-2} \binom{n-1}{i}$. As $k-1 < k$, by our strong induction hypothesis, we have $Q(k-1)$, or $\forall n \in \mathbb{Z}^+.P(n,k-1)$. Specialization gives $P(n-1,k-1)$, as $n > k > 1$ is assumed, so $n-1 \in \mathbb{Z}^+$. Also, $n > k$ implies $n-1 \geq k-1$. Since $|A \cap B| \in \{0,1\}^{[n-1]}$, by modus ponens of $P(n-1,k-1)$, we know there is a set $I' \subseteq [n-1]$ such that $|I'| = k-1$ and $(A \cap B)\big|_{I'} = \{0,1\}^{I'}$.

Pick $I = I' \cup \{n\}$. If $s \in (A \cap B)$ is a $(n-1)$-bit binary sequence, it must be in both A and B. Since A is the set restrictions of sequences with last digit being 0, and B is the set of restrictions with last digit being 1, the concatenation of s with 0, and s with 1, must both appear in S.
Since $S\big|_{I'}$ is already all permutations of $(k-1)$-bit binary sequence, when adding the n^{th} digit in, it will add the concatenation of each permutation with 0 and 1. Thus, $S\big|_I$ has all permutations of k-bit binary sequences.

By the explanation we provided in "Notes and symbols", having all permutations means the set is all functions from I to $\{0, 1\}$.

Thus by construction, $|A \cup B| \leq \sum_{i=0}^{k-1} \binom{k-1}{i}$ IMPLIES $P(n, k)$.

We see that under all cases, $(n > k)$ IMPLIES $P(n, k)$, by direct proof.

$P(n, k)$ is true when $n < k, n = k$, and $n > k$. By trichotomy, $P(n, k)$ is true.

Thus, $\forall j \in \mathbb{Z}^+.(((j < n)$ IMPLIES $P(j, k))$ IMPLIES $P(n, k))$

Since $n \in \mathbb{Z}^+$ is arbitrary, $\forall n \in \mathbb{Z}^+.[\forall j \in \mathbb{Z}^+.((j < n)$ IMPLIES $P(j, k))$ IMPLIES $P(n, k)]$.

By the principle of strong induction, $\forall n \in \mathbb{Z}^+.P(n, k)$.

This is equivalent to $Q(k)$.

As $k \in \mathbb{Z}^+$ is arbitrary, $\forall k \in \mathbb{Z}^+.[\forall i \in \mathbb{Z}^+.((i < k)$ IMPLIES $Q(i))$ IMPLIES $Q(k)]$, direct proof.

By the principle of strong induction, again, we have $\forall k \in \mathbb{Z}^+.Q(k)$.

By the definition of Q, this means $\forall k \in \mathbb{Z}^+.\forall n \in \mathbb{Z}^+.P(n, k)$.

2. A *cyclic shift* of a sequence $\{s_i\}_{i=1}^n$ is a sequence $\{s'_i\}_{i=1}^n$ such that, for some $k \in [n]$ and for all $1 \leq i \leq n$, the i'th term of this sequence is $s'_i = s_{((i+k-1) \bmod n)+1}$.
For example, the sequence 3,4,5,1,2 is a cyclic shift of the sequence 1,2,3,4,5, where $k = 2$.

The *prefix sums* of a sequence $\{s_i\}_{i=1}^n$ of numbers are the numbers $\sum_{i=1}^m s_i$ for $1 \leq m \leq n$. For example, the prefix sums of the sequence 1,2,3,4,5 are the numbers 1,3,6,10, and 15.

For all $n \in \mathbb{Z}^+$, let OE_n denote the set of finite sequence $\{r_i\}_{i=1}^{2n}$ of integers such that

- $r_i > 0$ if i is odd,
- $r_i < 0$ if i is even, and
- $\sum\limits_{i=1}^{2n} r_i \geq 0$.

Using the well-ordering principle, give a well-structured informal proof that, for all $n \in \mathbb{Z}^+$ and all sequences $r \in \mathrm{OE}_n$, there is a cyclic shift of r all of whose prefix sums are non-negative.

Proof.

Let $P(n) : \mathbb{Z}^+ \to \{T, F\} =$ "$\forall r \in OE_n$, there is a cyclic shift of r all of whose prefix sums are non-negative".

To obtain a contradiction, assume $\forall n.P(n)$. is not true.

Let $C = \{e \in \mathbb{Z}^+ | P(e) \text{ is false}\}$ be the set of counterexamples of P. By our assumption, $C \neq \emptyset$. Since $C \subseteq \mathbb{Z}^+ \subseteq \mathbb{N}$, by the well-ordering principle, let e be the smallest element of C. Furthermore, we let $r \in OE_e$ be an arbitrary counterexample where all of its cyclic shift, the prefix sums sequence must contain at least one negative number.

Let S be set of all indexes where the prefix sums of r with no shift (cyclic shift by $k = 0$) that are negative. Finite set of integers are well-ordered, and in addition r is a counterexample, S must be non-empty. Thus, S has a minimum. We call the index where the prefix sum attains its minimum j (the first occurrence if multiple), and we have $P_j = \sum\limits_{i=1}^{j} r_j < 0$.

Formally, if P is the prefix sums of r, $S = \{x \in P | x < 0\}$. P_j is the first occurrence of $\min(S)$.

Furthermore, since P_j is a minimum of P, for all $b \in [2e], P_j \leq P_b$
Consider the cyclic shift of r with a shift of j, call it r'. In other word, r' is obtained by shifting the most negative prefix sum of r to the last index.
From the definition of cyclic shift, if $i \leq 2e - j, i + j - 1 \leq 2e - 1$. Thus, $(i + j - 1) \mod n$ is itself. So $r'_i = r_{((i+j-1) \mod n+1)} = r_{(i+j-1+1)} = r_{i+j}$.

If $i > 2e - j, i + j - 1 > 2e - 1 \geq 2e$. By the definition of mod operation, $(i + j - 1) \mod n$ $= (i + j - 1) - 2e = i + j - 2e - 1$. Thus, $r'_i = r_{i+j-2e-1+1} = r_{i+j-2e}$.
To conclude, we have $r'_i = \begin{cases} r_{i+j} & 0 < i \leq 2e - j \\ r_{i+j-2e} & 2e \geq i > 2e - j \end{cases}$.
Recall that all cyclic shift of r, including r', must have its prefix sums somewhere negative.

Let the first occurrence of negative number in the prefix sums of r' is at index c.
We know c exists because if S' is the set of indices where the prefix sums of r' is negative, by def of r and r', it must be non-empty. Since indices are subset of the natural numbers, by the principle of well ordering, S' must have a smallest index too.

Let P' be the prefix sums of r', where $P'_m = \sum_{i=1}^{m} r'_i$ for $1 \leq m \leq 2e$

Assume $1 \leq c \leq 2e - j$.

$P'_c = \sum_{i=1}^{c} r'_i = \sum_{i=1}^{c} r_{i+j}$ (since $i \leq c \leq 2e - j$) $= \sum_{i=j+1}^{c+j} r_i = \sum_{i=1}^{c+j} r_i - \sum_{i=1}^{j} r_i = P_{c+j} - P_j$

By our definition of P_j, since $(c + j) \in [2e]$, we have $P_j \leq P_{c+j}$, which is $P_{c+j} - P_j \geq 0$.
Thus, $P'_c \geq 0$ is not negative.

Hence, $1 \leq c \leq 2e - j$ IMPLIES P'_c is not negative.

Assume $2e - j < c \leq 2e$

$P'_c = \sum_{i=1}^{c} r'_i = \sum_{i=1}^{2e-j} r'_i + \sum_{i=2e-j+1}^{c} r'_i = \sum_{i=1}^{2e-j} r_{i+j} + \sum_{i=2e-j+1}^{c} r_{i+j-2e}$ (since $i \geq 2e - j + 1 > 2e - j$)

$= \sum_{i'=j+1}^{2e} r_{i'} + \sum_{i'=1}^{c+j-2e} r_{i'}$ (by changing the first i' to $i + j$ and second i' to $i + j - 2e$)

(from now on we change i' back to i, by dummy variable substitution)

$= \sum_{i=1}^{2e} r_i - \sum_{i=1}^{j} r_i + \sum_{i=1}^{c+j-2e} r_i$ (since sum from "1 to $2e$" is sum from "1 to j" + "$(j + 1)$ to $2e$")

(Since $2e - j < c \leq 2e$, we have $2e - j + j - 2e < c + j - 2e \leq 2e + j - 2e$, so $0 < c + j - 2e \leq j < 2e$ is a legally defined index of P)
$P'_c = P_{2e} - P_j + P_{c+j-2e}$ is legally defined and $c + j - 2c \in [2e]$.
Since P_{2e} is the total sum of r, and also $r \in OE_e$. By definition, $P_{2e} \geq 0$.
Also by definition of P_j and $c + j - 2c \in [2e]$, we have $P_j \leq P_{c+j-2c}$.
So, $P_{c+j-2c} - P_j \geq 0$. We also have $P_{2e} + P_{c+j-2c} - P_j \geq 0$ as $P_{2e} \geq 0$.
Therefore, $P'_c \geq 0$.

Hence, $2e - j < c \leq 2e$ IMPLIES P'_c is not negative.
We have exhausted all cases and conclude that P'_c cannot be negative. This contradicts to c is

the smallest element of S' (S' is the set of indices where the prefix sums of r' is negative). Hence, we must conclude S' is empty.

However, since r' is the cyclic shift of r with a shift of number j, it must have some indices where prefix sums are negative. Thus, the fact that S' is empty is a contradiction.

Therefore, $r \in OE_e$ is not a counterexample. Since $r \in OE_e$ is initialized under the assumption that $P(e)$ is false, we must conclude such assumption is wrong and $P(e)$ does hold.

The fact that $P(e)$ is true contradicts to the assumption where e is the smallest element of C.

By the proof of well-ordering, C must be empty. In other words, we have $\forall n \in \mathbb{Z}^+ . P(n)$.