My name and student number: Joseph Siu, 1010085701.

Sanchit Manchanda, Sepehr Jafari.

Question 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 F of functions from $[n]$ to $\{0,1\}$, if $n \geq k$ and

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

then there exists a subset $I \subseteq [n]$ with $|I| = k$ such that $\{f\big|_I : f \in F\}$ 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: $\forall k \in \mathbb{Z}^+ . \forall n \in \mathbb{Z}^+ . \left[\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}\right]$.

Lemma 1

For all $n \in \mathbb{Z}^+$, for all $k \in \mathbb{Z}^+$, if $n \geq k$, then

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

Proof of Lemma 1 by double induction.
For all $n \in \mathbb{Z}^+$, for all $k \in \mathbb{Z}^+$, define the predicates $P(n)$, and $Q(n,k)$ as follows:
$Q(n,k) =$ "$n \geq k$ IMPLIES $\sum_{i=0}^{k-1} \binom{n}{i} \geq 2^k - 1$";
$P(n) =$ "$\forall k \in \mathbb{Z}^+ . Q(n,k)''$.
We will prove $\forall n \in \mathbb{Z}^+ . P(n)$ by double induction.
Base Case: Consider $n = 1$.

Let $k \in \mathbb{Z}^+$ be arbitrary;

Case 1. $1 = k$.

In this case we have that $\sum_{i=0}^{1-1} \binom{1}{i} = \binom{1}{0} = 1 \geq 2^1 - 1 = 1$. Thus, $Q(1,k)$ holds.

For Case 1, we have shown $Q(1,k)$.

Case 2. $1 < k$.

In this case since $n < k$, the implication of $Q(1,k)$ is vacuously true. Thus, $Q(1,k)$ holds.

For Case 2, we have shown $Q(1,k)$.

For all cases, we have shown $Q(1,k)$.

Since $k \in \mathbb{Z}^+$ was arbitrary, we have shown $P(1)$.

Let $n \in \mathbb{Z}^+$ be arbitrary;

Assume $P(n)$;

Base Case: Since $\sum_{i=0}^{1-1}\binom{n+1}{i}=\binom{n+1}{0}=1\geq 2^1-1=1$, we have $Q(n+1,1)$.

Let $k\in\mathbb{Z}^+$ be arbitrary;

Assume $Q(n+1,k)$;

Case 1. $n+1<k+1$.

In this case, since $n+1<k+1$, the implication of $Q(n+1,k+1)$ is vacuously true. Thus, $Q(n+1,k+1)$ holds.

For Case 1, we have shown $Q(n+1,k+1)$.

Case 2. $n+1\geq k+1$.

First by Lemma we have $\sum_{i=0}^{k}\binom{n+1}{i}=\binom{n+1}{0}+\sum_{i=1}^{k}\binom{n+1}{i}=\binom{n+1}{0}+\sum_{i=1}^{k}\left(\binom{n}{i}+\binom{n}{i-1}\right)=1+\sum_{i=1}^{k}\binom{n}{i}+\sum_{i=1}^{k}\binom{n}{i-1}=\binom{n}{0}+\sum_{i=1}^{k}\binom{n}{i}+\sum_{i=1}^{k}\binom{n}{i-1}=\sum_{i=0}^{k}\binom{n}{i}+\sum_{i=0}^{k-1}\binom{n}{i}$.

Since we assumed $P(n)$, by specialization we have $\sum_{i=0}^{k}\binom{n}{i}\geq 2^{k+1}-1$ and $\sum_{i=0}^{k-1}\binom{n}{i}\geq 2^k-1$. Thus, we have $\sum_{i=0}^{k}\binom{n+1}{i}=\sum_{i=0}^{k}\binom{n}{i}+\sum_{i=0}^{k-1}\binom{n}{i}\geq 2^{k+1}-1+2^k-1\geq 2^{k+1}-1$ since $2^k\geq 1$ for all $k\in\mathbb{N}$.

For Case 2, we have shown $Q(n+1,k+1)$.

For all cases, we have shown $Q(n+1,k+1)$.

By induction, we have shown $\forall k\in\mathbb{Z}^+.Q(n+1,k)$. Thus, we have shown $P(n+1)$.

Therefore, by induction $\forall n\in\mathbb{Z}^+.P(n)$ holds.

Quod Erat Dem■

Proof of Question 1 by double induction.

For all $k\in\mathbb{Z}^+$, for all $n\in\mathbb{Z}^+$, for all F as a subset of functions from $[n]$ to $\{0,1\}$, define the predicates $P(k)$, $Q(n,k)$, $R(n,k,F)$ as follows:

$R(n,k,F)=$

$$\text{“}\left[\left(n\geq k \text{ AND } |F|>\sum_{i=0}^{k-1}\binom{n}{i}\right)\text{ IMPLIES }\left(\exists I\subseteq[n].(|I|=k)\text{ AND }\{f\big|_I:f\in F\}=\{0,1\}^I\right)\right].\text{”}$$

$Q(n,k)=$ “$\forall F\subseteq\{0,1\}^{[n]}.R(n,k,F)$

$P(k)=$ “$\forall n\in\mathbb{Z}^+.Q(n,k)$”.

We will prove $\forall k\in\mathbb{Z}^+.P(k)$ by double induction.

Base Case:

Consider $k=1,n=1$.

Let $F\subseteq\{0,1\}^{[1]}$ be arbitrary;

Case 1. $|F|\leq 1$.

Since $|F|\leq 1=\sum_{i=0}^{1-1}\binom{1}{i}$, the implication of $R(1,1,F)$ is vacuously true.

For Case 1, we have shown R(1,1,F).

Case 2. $|F|>1$.

Since $F\subseteq\{0,1\}^{[1]}$, $|F|\geq 2$, and $\left|\{0,1\}^{[1]}\right|=2$, it follows that $F=\{0,1\}^{[1]}$. Now, let $F=\{f_1,f_2\}$ for some functions $f_1,f_2:[1]\to\{0,1\}$. By picking $I=[1]$, we have $|I|=1$, and $\{f\big|_I:f\in F\}=F=\{0,1\}^{[1]}=\{0,1\}^I$.

For Case 2, we have shown R(1,1,F).

For all cases, we have shown $R(1,1,F)$, thus we conclude $R(1,1,F)$.

Since F was arbitrary, we have shown $Q(1,1)$.

Let $n\in\mathbb{Z}^+$ be arbitrary;

Assume $Q(n,1)$;

Let $F\subseteq\{0,1\}^{[n+1]}$ be arbitrary;

Case 1. $|F|\leq\sum_{i=0}^{1-1}\binom{n+1}{i}$.

The implication of $R(n+1,1,F)$ is vacuously true.

For Case 1 we have shown $R(n+1,1,F)$.
Case 2. $|F| > \sum_{i=0}^{1-1}\binom{n+1}{i}$.
Since $|F| > \sum_{i=0}^{1-1}\binom{n+1}{i} = 1$, we have $|F| \geq 2$. This implies there exists two distinct functions, namely $\exists f \in F. \exists f' \in F - \{f\}.(\exists z \in [n+1]. f(z) \neq f'(z))$. Let $g \in F$, $g' \in F - \{g\}$, and $z \in [n+1]$ be such instances, then by constructing $I = \{z\} \subseteq [n+1]$, we have $|I| = 1$ and $\{f\big|_I : f \in F\} = \{0,1\}^I$.
For Case 2 we have that $R(n+1,1,F)$.
For all cases, we have shown $R(n+1,1,F)$, thus we conclude $R(n+1,1,F)$.
Since F was arbitrary, we have shown $Q(n+1,1)$.
By induction, we have shown $\forall n \in \mathbb{Z}^+. Q(n,1)$. Thus, we have shown $P(1)$.
Let $k \in \mathbb{Z}^+$ be arbitrary;
Assume $P(k)$;
Base Case:
Let $F \subseteq \{0,1\}^{[1]}$ be arbitrary;
Since $1 < k+1$, this shows the implication of $R(1,k+1,F)$ is vacuously true.
Since F was arbitrary, we have shown $Q(1,k+1)$.
Let $n \in \mathbb{Z}^+$ be arbitrary;
Assume $Q(n,k+1)$;
Let $F \subseteq \{0,1\}^{[n+1]}$ be arbitrary;
Case 1. $|F| \leq \sum_{i=0}^{k}\binom{n+1}{i}$.
The implication of $R(n+1,k+1,F)$ is vacuously true.
For Case 1 we have shown that $R(n+1,k+1,F)$.
Case 2. $|F| > \sum_{i=0}^{k}\binom{n+1}{i}$.
By Lemma this implies

$$
\begin{aligned}
|F| &> \sum_{i=0}^{k}\binom{n+1}{i} \\
&= \binom{n+1}{0} + \sum_{i=1}^{k}\binom{n+1}{i} \\
&= 1 + \sum_{i=1}^{k}\left(\binom{n}{i} + \binom{n}{i-1}\right) \\
&= \binom{n}{0} + \sum_{i=1}^{k}\binom{n}{i} + \sum_{i=1}^{k}\binom{n}{i-1} \\
&= \sum_{i=0}^{k}\binom{n}{i} + \sum_{i=1}^{k}\binom{n}{i-1} \\
&= \sum_{i=0}^{k}\binom{n}{i} + \sum_{i=0}^{k-1}\binom{n}{i}
\end{aligned}
$$

Subcase (1): If $\left|\left\{f\big|_{[n]} : f \in F\right\}\right| > \sum_{i=0}^{k}\binom{n}{i}$:
By Specialization of assumption $Q(n,k+1)$ this implies there exists a subset $I \subseteq [n]$ such that $|I| = k+1$ and $\{f\big|_I : f \in F\} = \{0,1\}^I$ by assumption $Q(n,k+1)$.
For subcase 2.1 we have shown that $R(n+1,k+1,F)$.

Subcase (2): If $\left|\left\{f\big|_{[n]} : f \in F\right\}\right| \leq \displaystyle\sum_{i=0}^{k}\binom{n}{i}$:

By multipling both sides we have $-\left|\left\{f\big|_{[n]} : f \in F\right\}\right| \geq -\displaystyle\sum_{i=0}^{k}\binom{n}{i}$

Add this inequality to the previous inequality at Case 2, we have $|F| - \left|\left\{f\big|_{[n]} : f \in F\right\}\right| > \sum_{i=0}^{k}\binom{n}{i} + \sum_{i=0}^{k-1}\binom{n}{i} - \sum_{i=0}^{k}\binom{n}{i} = \sum_{i=0}^{k-1}\binom{n}{i}$.

By Lemma 1 and above, since $|F| - \left|\left\{f\big|_{[n]} : f \in F\right\}\right| \geq \sum_{i=0}^{k-1}\binom{n}{i} + 1 \geq 2^k$, thus this means there are two disjoint subsets $I_1, I_2 \subseteq F$ such that $|\{f\big|_{[n]} : f \in I_1\}| = |\{f\big|_{[n]} : f \in I_2\}| = 2^k$ and $\{f\big|_{[n]} : f \in I_1\} = \{f\big|_{[n]} : f \in I_2\}$ so that the cardinality of F can decrease at least 2^k when we are restricting the domains of the functions in F to $[n]$.

Now, since $\{f\big|_{[n]} : f \in I_1\} \subseteq \{f\big|_{[n]} : f \in F\}$ and $|\{f\big|_{[n]} : f \in I_1\}| = 2^k$, this implies $|\{f\big|_{[n]} : f \in F\}| \geq 2^k \geq \sum_{i=0}^{k-1}\binom{n}{i} + 1$, hence by specialization of the assumption $P(k)$ we have $Q(n,k)$, hence $\exists I' \subseteq [n].|I'| = k$ AND $\{\left(f\big|_{[n]}\right)\Big|_{I'} : f \in F\} = \{0,1\}^{I'}$.

By constructing $I = I' \cup \{n+1\}$, since $\{f\big|_I : f \in F\} \subseteq \{0,1\}^I$ which implies $\left|\{f\big|_I : f \in F\}\right| \leq \left|\{0,1\}^I\right|$ (there exists an injection), and $\left|\{f\big|_I : f \in F\}\right| \geq 2 \cdot 2^k = 2^{k+1} = \left|\{0,1\}^I\right|$ by our disjoint I_1, I_2 (the cardinality of $\{f\big|_I : f \in F\}$ is at least $\{0,1\}^I$). Since both sets are finite, so they must have the same number of elements. Moreover, because of $\{f\big|_I : f \in F\} \subseteq \{0,1\}^I$, this also shows they are equal as sets. Hence, $|I| = k+1$ and $\{f\big|_I : f \in F\} = \{0,1\}^I$.

Since we have constructed such I, for subcase 2.2 we have shown that $R(n+1, k+1, F)$.

For Case 2, we have shown that $R(n+1, k+1, F)$.

For all cases We have shown that $R(n+1, k+1, F)$. Thus, we conclude $R(n+1, k+1, F)$.

Since F was arbitrary, we have shown $Q(n+1, k+1)$.

By induction, we have shown $\forall n \in \mathbb{Z}^+.Q(n, k+1)$. Thus, we have shown $P(k+1)$.

By induction, we have shown $\forall k \in \mathbb{Z}^+.P(k)$.

Quod Erat Dem■

Question 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
- $\sum_{i=1}^{2n} r_i \geq 0$.

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.

Lemma 2

For any $n \in \mathbb{Z}^+$. For any $r = \{r_i\}_{i=1}^{2n} \in \mathrm{OE}_n$. Let $\mathrm{CS}(r)$ denote the set of all cyclic shift of r, then for any $r' = \{r'_i\}_{i=1}^{2n} \in \mathrm{CS}(r)$, we have $\sum_{i=1}^{2n} r_i = \sum_{i=1}^{2n} r'_i$.

Proof of Lemma 2.

Let $n \in \mathbb{Z}^+$ be arbitrary;

Let $r = \{r_i\}_{i=1}^{2n} \in \mathrm{OE}_n$ be arbitrary;

Let $r' \in \mathrm{CS}(r)$ be arbitrary;

By definition of $\mathrm{CS}(r)$, we have $\exists k \in [2n]. \forall i \in [2n]. r'_i = r_{((i+k-1) \bmod 2n)+1}$.

We first show the function $f : [2n] \to [2n]$ defined by $f(i) = ((i+k-1) \bmod 2n)+1$ is a bijective function.

To this end, we show that f is injective.

Assume $f(i) = f(j)$ for some $i, j \in [2n]$.

Then, we have $((i+k-1) \bmod 2n) + 1 = ((j+k-1) \bmod 2n) + 1$;

By cancellation, we have $(i+k-1) \bmod 2n = (j+k-1) \bmod 2n$;

This implies $i+k-1 = j+k-1+2nm$ for some $m \in \mathbb{Z}$;

By cancellation, we have $i = j + 2nm$;

To obtain a contradiction, assume $m \neq 0$.

Then, we have $i = j + 2nm \geq j + 2n$ or $i = j + 2nm \leq j - 2n$.

Case 1. If $i = j+2nm \geq j+2n$, then we have $i = j+2nm \geq j+2n$. This implies $i - j \geq 2n$. However, since $i, j \in [2n]$, we notice $1 \leq i \leq 2n$ and $1 \leq j \leq 2n$, so $i - j \leq 2n - 1 < 2n$. This is a contradiction.

Case 2. If $i = j+2nm \leq j-2n$, then we have $i = j+2nm \leq j-2n$. This implies $i - j \leq -2n$. However, since $i, j \in [2n]$, we notice $1 \leq i \leq 2n$ and $1 \leq j \leq 2n$, so $i - j \geq 1 - 2n > -2n$. This is a contradiction.

For all cases contradiction occured.

Hence, by contradiction we have shown $m = 0$. This implies $i = j$.

Hence, by definition of injective, we have shown f is injective.

Now, we show that f is surjective.

Let $y \in [2n]$ be arbitrary.

Case 1. If $y = 1$, then we have $f(-k+1+2n) = (((-k+1+2n+k-1) \bmod 2n) + 1) = ((2n) \bmod 2n) + 1 = 0 + 1 = 1$.

For Case 1 all $y \in [2n]$ can be achieved by f.

Case 2. If $y \neq 1$, that is, $y > 1$.

Subcase (1): If $y \geq k$, then we have $y - k \in [2n]$, and $f(y-k) = ((y-k+k-1) \bmod 2n) + 1 = ((y-1) \bmod 2n) + 1 = y - 1 + 1 = y$. For this subcase y can be achieved by f.

Subcase (2): If $y < k$, then we have $1 - 2n \leq y - k < 0$ and so $1 \leq y-k+2n < 2n$ and $y-k+2n \in [2n]$, and $f(y-k+2n) = ((y-k+2n+k-1) \bmod 2n)+1 = ((y+2n-1) \bmod 2n)+1 = y-1+1 = y$

For this subcase y can be achieved by f.

Since for all subcases of Case 2 y can be achieved by f, this shows for Case

2 all $y \in [2n]$ can be achieved by f.
For all cases, y can be achieved by f.
Since y was arbitrary, we have shown f is surjective by definition.
Since f is both injective and surjective, we have shown f is bijective.
Hence $\sum_{i=1}^{2n} r_i = \sum_{i=1}^{2n} r_{f(i)} = \sum_{i=1}^{2n} r'_i$ since addition is commutative and f is bijective.
Since $r' \in \mathrm{CS}(r)$ was arbitrary, we have shown $\forall r' \in \mathrm{CS}(r). \sum_{i=1}^{2n} r_i = \sum_{i=1}^{2n} r'_i$.
Since $r \in \mathrm{OE}_n$ was arbitrary, we have shown $\forall r \in \mathrm{OE}_n.\forall r' \in \mathrm{CS}(r). \sum_{i=1}^{2n} r_i = \sum_{i=1}^{2n} r'_i$.
Since $n \in \mathbb{Z}^+$ was arbitrary, we have shown $\forall n \in \mathbb{Z}^+.\forall r \in \mathrm{OE}_n.\forall r' \in \mathrm{CS}(r). \sum_{i=1}^{2n} r_i = \sum_{i=1}^{2n} r'_i$.

Quod Erat Dem■

Proof of Question 2 by Well Ordering.
For $n \in \mathbb{Z}^+$, let $P(n)$ denote the statement "$\forall r \in \mathrm{OE}_n.\exists r' \in \mathrm{CS}(r).\forall m \in \mathbb{Z}^+.1 \leq m \leq 2n. \sum_{i=1}^{m} r'_i \geq 0$". We will show $\forall n \in \mathbb{Z}^+.P(n)$ by well ordering.

To obtain a contradiction assume $\exists n \in \mathbb{Z}^+.\mathrm{NOT}(P(n))$, that is, there exists $n \in \mathbb{Z}^+$, and exists a sequence $r \in \mathrm{OE}_n$ such that there is no cyclic shift of r all of whose prefix sums are non-negative.
Namely, for all sequences $r = \{r_i\}_{i=1}^{2n}$, let $\mathrm{CS}(r)$ denote the set of all cyclic shift of r, then $\exists n \in \mathbb{Z}^+.\mathrm{NOT}(P(n)) =$

$$\exists n \in \mathbb{Z}^+.\exists r = \{r_i\}_{i=1}^{2n} \in \mathrm{OE}_n.\forall \{r'_i\}_{i=1}^{2n} \in \mathrm{CS}(r).\exists m \in \mathbb{Z}^+.1 \leq m \leq 2n \text{ AND } \sum_{i=1}^{m} r'_i < 0.$$

Let $C = \{2n \in \mathbb{Z}^+ \mid \exists r = \{r_i\}_{i=1}^{2n} \in \mathrm{OE}_n.\forall \{r'_i\}_{i=1}^{2n} \in \mathrm{CS}(r).\exists m \in \mathbb{Z}^+.1 \leq m \leq 2n \text{ AND } \sum_{i=1}^{m} r'_i < 0\}$. Then, $C \neq \varnothing$ by our assumption.
Since $\mathbb{N}$ has a well ordering and $\mathbb{Z}^+ \subseteq \mathbb{N}$, this implies $\mathbb{Z}^+$ has a well ordering, so there exists a smallest element $2n_0 \in C$.
Let $2n_0 \in C$ be such smallest element.
To obtain a contradiction, assume $n_0 = 1$;
Then, for all sequences $r \in \mathrm{OE}_n$, consider $r \in \mathrm{CS}(r)$;
By specialization in the condition of C, let $m \in \mathbb{Z}^+$ be such that $1 \leq m \leq 2n_0 = 2$ AND $\sum_{i=1}^{m} r_i < 0$. Then, we show there is no such m exists using 2 cases:
Case 1. $m = 1$.
Since $r_1 > 0$ by definition of $r \in \mathrm{OE}_n$, we have $\sum_{i=1}^{1} r_i = r_1 > 0$, hence contradiction.
Case 2. $m = 2$.
Since $\sum_{i=1}^{2} r_i = \sum_{i=1}^{2n_0} r_i \geq 0$ by definition of $r \in \mathrm{OE}_n$, and we have $\sum_{i=1}^{m} r_i = \sum_{i=1}^{2} r_i < 0$, hence contradiction.
Since for all cases we have reached a contradiction, we conclude this is a contradiction.
Since $n_0 = 1$ is a contradiction, we have shown that $n_0 \neq 1$. That is, $n_0 \geq 2$.
Let $r_0 = \{r_i\}_{i=1}^{2n_0} \in \mathrm{OE}_{n_0}$ be such that for all $\{r'_i\}_{i=1}^{2n_0} \in \mathrm{CS}(r_0)$, there exists $m \in \mathbb{Z}^+$ such that $1 \leq m \leq 2n_0$ and $\sum_{i=1}^{m} r'_i < 0$.
Let $\{r'_i\}_{i=1}^{2n_0} \in \mathrm{CS}(r_0)$ be arbitrary such that $r'_i > 0$ for $i \in [2n_0]$ and i is odd. Then by specialization of the condition of C, we have $\exists m \in \mathbb{Z}^+.1 \leq m \leq 2n_0$ AND $\sum_{i=1}^{m} r'_i < 0$.
Define $C' = \{m \in \mathbb{Z}^+ \mid 1 \leq m \leq 2n_0 \text{ AND } \sum_{i=1}^{m} r'_i < 0\}$.
Then, $C' \neq \varnothing$ by our assumption.
Let $m_0 \in C'$ be such that m_0 is the smallest element of C'.
To obtain a contradiction, assume m_0 is odd;
Then, by our assumption, we have $r_{m_0} > 0$.

Case 1. $m_0 = 1$.

Since $r_1 > 0$, we have $\sum_{i=1}^{m_0} r_i = r_1 > 0$.

This is contradicting the definition of m_0 having negative prefix sum.

Case 2. $m_0 > 1$.

Since $\sum_{i=1}^{m_0} r'_i < 0$ and $r_{m_0} > 0$, we have $\sum_{i=1}^{m_0-1} r_i < 0$.

This is contradicting the definition of m_0 being the smallest such m_0.

For all cases contradiction occured.

Thus, by contradiction, m_0 must be even.

To obtain a contradiction, assume $m_0 = 2n_0$;

Then, we have $\sum_{i=1}^{2n_0} r'_i < 0$.

However, by definition of $r_0 \in \mathrm{OE}_{n_0}$, we have $\sum_{i=1}^{2n_0} r_i \geq 0$.

By Lemma 2, this is a contradiction.

We conclude $m_0 \neq 2n_0$. That is, $m_0 \leq 2n_0 - 1$.

Since $m_0 + 1 \leq 2n_0$, we have $2n_0 - m_0 \geq 1$. Hence, define a sequence $\{s_i\}_{i=1}^{2n_0-m_0}$ such that $s_i = r_{i+m_0}$ for all $i \in [2n_0 - m_0]$, here $2n_0 - m_0$ is even since both $2n_0$ and m_0 are even;

Then, since we assumed n_0 is the smallest element of C, this implies $2n_0 - m_0 \notin C$.

That is, there exists a cyclic shift of s all of whose prefix sums are non-negative.

Namely, $\exists s' = \{s'_i\}_{i=1}^{2n_0-m_0} \in \mathrm{CS}(s).\forall m \in \mathbb{Z}^+.1 \leq m \leq 2n_0 - m_0 \implies \sum_{i=1}^{m} s'_i \geq 0$.

Consider the sequence $t = \{t_i\}_{i=1}^{2n_0} = \{s'_i\}_{i=1}^{2n_0-m_0} \circ \{r'_i\}_{i=1}^{m_0}$. Since $t \in \mathrm{CS}(r_0)$ by our construction of s' and s, this implies there exists $m_1 \in \mathbb{Z}^+.1 \leq m_1 \leq 2n_0$ AND $\sum_{i=1}^{m_1} t_i < 0$.

Since by definition of $r_0 \in \mathrm{OE}_{n_0}$ and Lemma 2, we have $\sum_{i=1}^{2n_0} t_i \geq 0$.

Moreover, by our construction of s' and s, we have $\sum_{i=1}^{p} t'_i \geq 0$ for all $p \in [2n_0 - m_0]$. Also, by definition of m_0, we have $\sum_{i=m_0+1}^{q} t_i \geq 0$ for all $q \in [2n_0 - 1] - [m_0]$.

Combining these 2 inequalities, we have $\sum_{i=1}^{p'} t_i \geq 0$ for all $p' \in [2n_0 - 1]$.

Combining with $\sum_{i=1}^{2n_0} t_i \geq 0$ we have $\forall q' \in [2n_0]. \sum_{i=1}^{q'} t_i \geq 0$.

This contradicts our definition of C and constuction of r_0 where $\forall r' = \{r'_i\}_{i=1}^{2n_0} \in \mathrm{CS}(r_0).\exists m \in \mathbb{Z}^+.1 \leq m \leq 2n_0$ AND $\sum_{i=1}^{m} r'_i < 0$.

Therefore, we conclude $\forall n \in \mathbb{Z}^+.P(n)$. That is, 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.

QUOD ERAT DEM■