Math 4990 Fall 2017 (Darij Grinberg): homework set 3 with solutions

Contents

0.1. Counting triples 1
0.2. Stirling numbers of the 2nd kind, again 3
0.3. Counting 2-lacunar subsets 5
0.4. Counting shadowed subsets 8
0.5. Counting smords (Smirnov words, or Carlitz words) 9
0.6. Necklaces 2: rotational equivalence of tuples 12

0.1. Counting triples

Recall that the word "*triple*" means a 3-tuple. Tuples are always ordered by definition.

Exercise 1. Let $n \in \mathbb{N}$.

(a) Find the number of all triples (A, B, C) of subsets of $[n]$ satisfying $A \cup B \cup C = [n]$ and $A \cap B \cap C = \varnothing$.

(b) Find the number of all triples (A, B, C) of subsets of $[n]$ satisfying $B \cap C = C \cap A = A \cap B$.

(c) Find the number of all triples (A, B, C) of subsets of $[n]$ satisfying $A \cap B = A \cap C$.

Solution to Exercise 1 (sketched). **(a)** The number of such triples is 6^n.

Proof. Let me first give a quick but informal argument.

Clearly, a triple (A, B, C) of subsets of $[n]$ satisfies $A \cup B \cup C = [n]$ and $A \cap B \cap C = \varnothing$ if and only if it has the following property: Each $i \in [n]$ belongs to **at least one** of the three sets A, B, C, but **no** $i \in [n]$ belongs to **all three** of them. Thus, the following simple algorithm constructs every triple (A, B, C) of subsets of $[n]$ satisfying $A \cup B \cup C = [n]$ and $A \cap B \cap C = \varnothing$: For each $i \in [n]$, we decide whether the element i should be contained in the set A only (i.e., in A but not in B and not in C), or in the set B only, or in the set C only, or in the sets A and B only (i.e., in A and B but not in C), or in the sets A and C only, or in the sets B and C only. There are clearly 6 options to choose from in this decision. Thus, in total, there are 6^n possible triples (because we are making this decision once for each of the n elements i of $[n]$). This completes our informal proof.

A rigorous way to present the above argument is the following: Let $\mathfrak{A}$ be the set of all triples (A, B, C) of subsets of $[n]$ satisfies $A \cup B \cup C = [n]$ and $A \cap B \cap C = \varnothing$. We must show that $|\mathfrak{A}| = 6^n$. We know that the set $[6]^{[n]}$ (that is, the set of all maps $[n] \to [6]$) has size $\left|[6]^{[n]}\right| = |[6]|^{|[n]|} = 6^n$; thus, it will suffice to exhibit a bijection $\mathfrak{A} \to [6]^{[n]}$.

We define such a bijection $\Xi : \mathfrak{A} \to [6]^{[n]}$ as follows: It should send any triple $(A, B, C) \in \mathfrak{A}$ to the map $f : [n] \to [6]$ that sends each $i \in [n]$ to

$$\begin{cases} 1, & \text{if } i \in A \text{ but } i \notin B \text{ and } i \notin C; \\ 2, & \text{if } i \in B \text{ but } i \notin C \text{ and } i \notin A; \\ 3, & \text{if } i \in C \text{ but } i \notin A \text{ and } i \notin B; \\ 4, & \text{if } i \in A \text{ and } i \in B \text{ but } i \notin C; \\ 5, & \text{if } i \in A \text{ and } i \in C \text{ but } i \notin B; \\ 6, & \text{if } i \in B \text{ and } i \in C \text{ but } i \notin A \end{cases} \qquad (1)$$

[1]. (As I said, this is merely a translation of our above informal argument into rigorous language; in particular, the 6 possible values in (1) are our "6 options", and we are defining a map $f : [n] \to [6]$ because we are choosing among these 6 options for each element of $[n]$.)

We are not yet done. We must prove, first of all, that the expression in (1) is well-defined, i.e., that each $i \in [n]$ will satisfy exactly one of the conditions "$i \in A$ but $i \notin B$ and $i \notin C$" and "$i \in B$ but $i \notin C$ and $i \notin A$" and "$i \in C$ but $i \notin A$ and $i \notin B$" and "$i \in A$ and $i \in B$ but $i \notin C$" and "$i \in A$ and $i \in C$ but $i \notin B$" and "$i \in B$ and $i \in C$ but $i \notin A$". This is easy[2]. This shows that the map $f : [n] \to [6]$ is well-defined for each $(A, B, C) \in \mathfrak{A}$, and therefore the map $\Xi : \mathfrak{A} \to [6]^{[n]}$ is well-defined. In order to prove that this Ξ is a bijection, it is most reasonable to construct an inverse for Ξ.

I claim that such an inverse is the map $[6]^{[n]} \to \mathfrak{A}$ that sends each $f : [n] \to [6]$ to the triple (A, B, C), where

$$A = \{i \in [n] \mid f(i) \in \{1, 4, 5\}\};$$
$$B = \{i \in [n] \mid f(i) \in \{2, 4, 6\}\};$$
$$C = \{i \in [n] \mid f(i) \in \{3, 5, 6\}\}.$$

Indeed, it is straightforward to check that this map is well-defined, and actually inverse to Ξ. (How did I come up with this map? Well, I wanted an inverse to Ξ, so I was looking for a map that reconstructs any triple $(A, B, C) \in \mathfrak{A}$ from the map $f : [n] \to [6]$ that sends each $i \in [n]$ to (1). This is a rather simple reconstruction problem: For example, the first entry A of this triple (A, B, C) can be reconstructed from f as the set $\{i \in [n] \mid f(i) \in \{1, 4, 5\}\}$, because the elements of A are exactly

[1]From the point of view of logic, the word "but" is merely a synonym for "and". But in this definition, it is meant to reinforce the intuition: We say "if $i \in A$ but $i \notin B$ and $i \notin C$" because we clearly want to contrast the sets to which i belongs on one side against the sets to which i does not belong on the other.

[2]It is clear enough that i cannot satisfy more than one of these conditions. In order to see that i has to satisfy at least one of them, we must rule out the possibilities that ($i \in A$ and $i \in B$ and $i \in C$) and ($i \notin A$ and $i \notin B$ and $i \notin C$). But this is easy: The first of these possibilities is ruled out by $A \cap B \cap C = \varnothing$, while the second is ruled out by $A \cup B \cup C = [n]$.

those elements $i \in [n]$ whose image under f is 1, 4 or 5.) This completes the rigorous proof of **(a)**.

(b) The number of such triples is 5^n.

Proof. I shall give an informal proof only, trusting that you can translate it into a rigorous bijective argument as I've done above for part **(a)**.

Clearly, a triple (A, B, C) of subsets of $[n]$ satisfies $B \cap C = C \cap A = A \cap B$ if and only if it has the following property: Each $i \in [n]$ **either belongs to at most one** of the three sets A, B, C, **or belongs to all three** of them. Thus, the following simple algorithm constructs every triple (A, B, C) of subsets of $[n]$ satisfying $B \cap C = C \cap A = A \cap B$: For each $i \in [n]$, we decide whether the element i should be contained in none of the sets A, B and C, or in the set A only (i.e., in A but not in B and not in C), or in the set B only, or in the set C only, or in all three sets A, B and C. There are clearly 5 options to choose from in this decision. Thus, in total, there are 5^n possible triples (because we are making this decision once for each of the n elements i of $[n]$). This completes our informal proof.

(c) The number of such triples is 6^n.

Proof. I shall give an informal proof only, trusting that you can translate it into a rigorous bijective argument as I've done above for part **(a)**.

Clearly, a triple (A, B, C) of subsets of $[n]$ satisfies $A \cap B = A \cap C$ if and only if it has the following property: Each $i \in [n]$ **either belongs to at most one** of the three sets A, B, C, **or belongs to** B **and** C **only, or belongs to all three** of them. Thus, the following simple algorithm constructs every triple (A, B, C) of subsets of $[n]$ satisfying $A \cap B = A \cap C$: For each $i \in [n]$, we decide whether the element i should be contained in none of the sets A, B and C, or in the set A only (i.e., in A but not in B and not in C), or in the set B only, or in the set C only, or in the sets B and C only (i.e., in B and in C but not in A), or in all three sets A, B and C. There are clearly 6 options to choose from in this decision. Thus, in total, there are 6^n possible triples (because we are making this decision once for each of the n elements i of $[n]$). This completes our informal proof. □

0.2. Stirling numbers of the 2nd kind, again

Recall that if $n \in \mathbb{N}$ and $k \in \mathbb{N}$, then $\operatorname{sur}(n, k)$ denotes the number of surjections $[n] \to [k]$, and $\left\{ n \atop k \right\}$ denotes the Stirling number of the 2nd kind (defined as $\operatorname{sur}(n, k) / k!$).

Recall furthermore that we are using the convention that $\dbinom{a}{b} = 0$ when $b \notin \mathbb{N}$.

Exercise 2. Let n be a positive integer. Let $k \in \mathbb{N}$.

(a) Prove that

$$\operatorname{sur}(n, k) = k \sum_{i=0}^{k} (-1)^{k-i} \binom{k-1}{i-1} i^{n-1}.$$

(b) Prove that

$$\left\{ {n \atop k} \right\} = \sum_{i=0}^{k} (-1)^{k-i} \frac{i^n}{i!\,(k-i)!}.$$

Solution to Exercise 2. Exercise 4 on Math 4990 homework set #2 showed that

$$\operatorname{sur}(n,k) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n. \tag{2}$$

But Exercise 2 **(b)** on Math 4990 homework set #1 showed that

$$K \binom{N}{K} = N \binom{N-1}{K-1} \tag{3}$$

for any $N \in \mathbb{Q}$ and any positive integer K. (The variables N and K in this equality have been called n and k in the exercise we have cited, but we are using the notations n and k for different purposes here.) Furthermore, we know that

$$\binom{N}{K} = \frac{N!}{K!\,(N-K)!} \tag{4}$$

for each $N \in \mathbb{N}$ and each $K \in \{0, 1, \ldots, N\}$.

(a) From (2), we obtain

$$\begin{aligned}
\operatorname{sur}(n,k) &= \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n = (-1)^{k-0} \binom{k}{0} \underbrace{0^n}_{\substack{=0 \\ \text{(since } n \text{ is positive)}}} + \sum_{i=1}^{k} (-1)^{k-i} \binom{k}{i} i^n \\
&= \underbrace{(-1)^{k-0} \binom{k}{0} 0}_{=0} + \sum_{i=1}^{k} (-1)^{k-i} \binom{k}{i} i^n = \sum_{i=1}^{k} (-1)^{k-i} \binom{k}{i} \underbrace{i^n}_{\substack{=ii^{n-1} \\ \text{(since } n \text{ is positive)}}} \\
&= \sum_{i=1}^{k} (-1)^{k-i} \underbrace{\binom{k}{i} i}_{=i\binom{k}{i}} i^{n-1} = \sum_{i=1}^{k} (-1)^{k-i} \underbrace{i \binom{k}{i}}_{\substack{=k\binom{k-1}{i-1} \\ \text{(by (3), applied} \\ \text{to } N=k \text{ and } K=i)}} i^{n-1} \\
&= \sum_{i=1}^{k} (-1)^{k-i} k \binom{k-1}{i-1} i^{n-1} = k \sum_{i=1}^{k} (-1)^{k-i} \binom{k-1}{i-1} i^{n-1}.
\end{aligned}$$

Comparing this with

$$\begin{aligned}
k & \underbrace{\sum_{i=0}^{k} (-1)^{k-i} \dbinom{k-1}{i-1} i^{n-1}}_{=(-1)^{k-0}\dbinom{k-1}{0-1}0^{n-1}+\sum_{i=1}^{k}(-1)^{k-i}\dbinom{k-1}{i-1}i^{n-1}} \\
&= k \left((-1)^{k-0} \underbrace{\dbinom{k-1}{0-1}}_{\substack{=0 \\ \text{(since } 0-1<0)}} 0^{n-1} + \sum_{i=1}^{k} (-1)^{k-i} \dbinom{k-1}{i-1} i^{n-1} \right) \\
&= k \left(\underbrace{(-1)^{k-0} 0 \cdot 0^{n-1}}_{=0} + \sum_{i=1}^{k} (-1)^{k-i} \dbinom{k-1}{i-1} i^{n-1} \right) \\
&= k \sum_{i=1}^{k} (-1)^{k-i} \dbinom{k-1}{i-1} i^{n-1},
\end{aligned}$$

we obtain

$$\operatorname{sur}(n,k) = k \sum_{i=0}^{k} (-1)^{k-i} \dbinom{k-1}{i-1} i^{n-1}.$$

This solves Exercise 2 **(a)**.

(b) We know from class that

$$\begin{aligned}
\left\{ \begin{matrix} n \\ k \end{matrix} \right\} &= \frac{\operatorname{sur}(n,k)}{k!} = \frac{1}{k!} \underbrace{\operatorname{sur}(n,k)}_{\substack{=\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i} i^n \\ \text{(by (2))}}} = \frac{1}{k!} \cdot \sum_{i=0}^{k} (-1)^{k-i} \underbrace{\dbinom{k}{i}}_{\substack{=\frac{k!}{i!(k-i)!} \\ \text{(by (4), applied} \\ \text{to } N=k \text{ and } K=i)}} i^n \\
&= \frac{1}{k!} \cdot \sum_{i=0}^{k} (-1)^{k-i} \frac{k!}{i!(k-i)!} i^n = \underbrace{\frac{1}{k!} \cdot k!}_{=1} \sum_{i=0}^{k} (-1)^{k-i} \frac{1}{i!(k-i)!} i^n \\
&= \sum_{i=0}^{k} (-1)^{k-i} \frac{1}{i!(k-i)!} i^n = \sum_{i=0}^{k} (-1)^{k-i} \frac{i^n}{i!(k-i)!}.
\end{aligned}$$

This solves Exercise 2 **(b)**. □

0.3. Counting 2-lacunar subsets

Exercise 3. A set S of integers is said to be 2-*lacunar* if every $i \in S$ satisfies $i+1 \notin S$ and $i+2 \notin S$. (That is, any two distinct elements of S are at least a distance of 3 apart on the real axis.) For example, $\{1,5,8\}$ is 2-lacunar, but $\{1,5,7\}$ is not.

For any $n \in \mathbb{N}$, we let $h(n)$ denote the number of all 2-lacunar subsets of $[n]$.

(a) Prove that $h(n) = h(n-1) + h(n-3)$ for each $n \geq 3$.

(b) Prove that $h(n) = \sum\limits_{\substack{k\in\mathbb{N};\\ 2k\leq n+2}} \dbinom{n+2-2k}{k}$ for each $n \in \mathbb{N}$.

Solution to Exercise 3 (sketched). Most of the arguments used in this exercise are straightforward adaptations of arguments used in Exercise 4 **(b)** on Math 4990 homework set #1 and in Exercise 3 on Math 4990 homework set #2. Thus, we shall be very brief this time, pointing out only the differences.

(a) Exercise 3 is solved in the same way as Exercise 4 **(b)** on Math 4990 homework set #1 was solved. This time, of course, instead of finding a bijection from $\{S \subseteq [n] \mid S \text{ is lacunar and } n \in S\}$ to $\{S \subseteq [n-2] \mid S \text{ is lacunar}\}$, we need to find a a bijection from $\{S \subseteq [n] \mid S \text{ is 2-lacunar and } n \in S\}$ to $\{S \subseteq [n-3] \mid S \text{ is 2-lacunar}\}$. The bijection is defined in exactly the same way as before: It sends each T to $T \setminus \{n\}$.

(b) We begin with the following fact:

Observation 0: Let S be a 2-lacunar subset of $[n]$. Then,

$$|S| \leq \frac{n+2}{3}.$$

[*Proof of Observation 0:* Let S' be the subset $\{s+1 \mid s \in S\}$ of $[n+1]$. Let S'' be the subset $\{s+2 \mid s \in S\}$ of $[n+2]$. Both subsets S' and S'' are just copies of S, shifted by 1 and by 2, respectively; thus, their sizes are the same as the size of S: that is, we have $|S| = |S'| = |S''|$. Also, it is easy to see that the three sets S, S', S'' are disjoint[3]. Hence, $|S \cup S' \cup S''| = |S| + |S'| + |S''| = 3|S|$ (since $|S| = |S'| = |S''|$). But S, S' and S'' are subsets of $[n+2]$; therefore, so is $S \cup S' \cup S''$. Hence, $|S \cup S' \cup S''| \leq |[n+2]| = n+2$. In view of $|S \cup S' \cup S''| = 3|S|$, this rewrites as $3|S| \leq n+2$, so that $|S| \leq \dfrac{n+2}{3}$. This proves Observation 0.]

Next, we need to prove the following statement:

Observation 1: Let $n \in \mathbb{N}$. For any $k \in \mathbb{N}$ satisfying $2k \leq n+2$, the number of all 2-lacunar k-element subsets of $[n]$ is $\dbinom{n-2k+2}{k}$.

[3] *Proof.* Let us just check that S and S'' are disjoint. (The other two statements are proven similarly.) Indeed, let $j \in S \cap S''$. Then, $j \in S$ and $j \in S''$. From $j \in S''$, it follows that $j = s+2$ for some $s \in S$ (by the definition of S''). Consider this s. Now, recall that every $i \in S$ satisfies $i+2 \notin S$ (since S is 2-lacunar). Applying this to $i = s$, we obtain $s+2 \notin S$. This contradicts $s+2 = j \in S$.

Now, forget that we fixed j. We thus have obtained a contradiction for each $j \in S \cap S''$. Hence, there exists no $j \in S \cap S''$. In other words, the sets S and S'' are disjoint.

[*Proof of Observation 1:* One way to prove this is analogous to the first solution of Exercise 3 **(a)** on Math 4990 homework set #2. The main differences are:

- The set $\operatorname{Lac}_k(n)$ of all lacunar k-element subsets of $[n]$ is replaced by the set $\operatorname{Lac}_{k,2}(n)$ of all 2-lacunar k-element subsets of $[n]$.
- The maps $\Phi : \operatorname{Lac}_k(n) \to \mathcal{P}_k([n-k+1])$ and $\Psi : \mathcal{P}_k([n-k+1]) \to \operatorname{Lac}_k(n)$ are replaced by maps $\widetilde{\Phi} : \operatorname{Lac}_{k,2}(n) \to \mathcal{P}_k([n-2k+2])$ and $\widetilde{\Psi} : \mathcal{P}_k([n-2k+2]) \to \operatorname{Lac}_{k,2}(n)$ defined as follows: $\widetilde{\Phi}$ sends any $S = \{s_1 < s_2 < \cdots < s_k\} \in \operatorname{Lac}_{k,2}(n)$ to

  $$\{s_1 - 0 < s_2 - 2 < s_3 - 4 < \cdots < s_k - 2(k-1)\} = \{s_i - 2(i-1) \mid i \in [k]\},$$

  whereas $\widetilde{\Psi}$ sends any $T = \{t_1 < t_2 < \cdots < t_k\} \in \mathcal{P}_k([n-2k+2])$ to

  $$\{t_1 + 0 < t_2 + 2 < t_3 + 4 < \cdots < t_k + 2(k-1)\} = \{t_i + 2(i-1) \mid i \in [k]\}.$$

  (In other words, instead of increasing/decreasing gaps between neighboring elements of the subset by 1, we are now increasing/decreasing them by 2.)

Alternatively, Observation 1 can also be proven similarly to the second solution of Exercise 3 **(a)** on Math 4990 homework set #2. The analogue of Claim 1 should now state that $g_k(n) = g_k(n-1) + g_{k-1}(n-3)$ for all $n \geq 1$ and $k \in \mathbb{Z}$ (where $g_k(n)$ denotes the number of all 2-lacunar k-element subsets of $[n]$); and the analogue of Claim 2 should now state that each $n \in \{-2, -1, 0, 1, 2, \ldots\}$ and $k \in \mathbb{N}$ with $2k \leq n+2$ satisfy $g_k(n) = \dbinom{n-2k+2}{k}$. (In the proof of Claim 2, the case of $2k = m+2$ needs to be treated separately, in the same way as we had to treat the case $k = m+1$ separately back in homework set #2. This is slightly harder this time, however. Observation 0 shows that a k-element 2-lacunar subset of $[m]$ must have size $k \leq \dfrac{m+2}{3} < \dfrac{m+2}{2}$, whence it cannot satisfy $2k = m+2$ unless $m = -2$.)

Either way, Observation 1 is eventually proven.]

Now, we proceed similarly to the solution of Exercise 3 on Math 4990 homework set #2: Fix $n \in \mathbb{N}$. The size of any 2-lacunar subset of $[n]$ is a $k \in \mathbb{N}$ satisfying

$2k \leq n+2$ (because Observation 0 yields that it is $\leq \dfrac{n+2}{3} \leq \dfrac{n+2}{2}$). Now,

$$\begin{aligned} h(n) &= (\text{the number of all 2-lacunar subsets of } [n]) \\ &\qquad (\text{by the definition of } h(n)) \\ &= \sum_{\substack{k\in\mathbb{N};\\ 2k\leq n+2}} \underbrace{(\text{the number of all 2-lacunar subsets of } [n] \text{ having size } k)}_{\substack{=(\text{the number of all 2-lacunar } k\text{-element subsets of } [n]) \\ =\binom{n-2k+2}{k} \\ (\text{by Observation 1})}} \\ &\qquad \left(\begin{array}{c} \text{because the size of any 2-lacunar subset of } [n] \\ \text{is a } k\in\mathbb{N} \text{ satisfying } 2k\leq n+2 \end{array}\right) \\ &= \sum_{\substack{k\in\mathbb{N};\\ 2k\leq n+2}} \binom{n-2k+2}{k} = \sum_{\substack{k\in\mathbb{N};\\ 2k\leq n+2}} \binom{n+2-2k}{k}. \end{aligned}$$

This solves Exercise 3 **(b)**. □

0.4. Counting shadowed subsets

Exercise 4. A set S of integers is said to be *shadowed* if it has the following property: Whenever an **odd** integer i belongs to S, the next integer $i+1$ must also belong to S. (For example, $\varnothing$, $\{2,4\}$ and $\{1,2,5,6,8\}$ are shadowed, but $\{1,5,6\}$ is not, since 1 belongs to $\{1,5,6\}$ but 2 does not.)

(a) Let $n \in \mathbb{N}$ be even. How many shadowed subsets of $[n]$ exist?

(b) Let $n \in \mathbb{N}$ be odd. How many shadowed subsets of $[n]$ exist?

Solution to Exercise 4 (sketched). **(a)** The number of shadowed subsets of $[n]$ is $3^{n/2}$.

Proof. Here is an informal argument:

The definition of a "shadowed" set can be rewritten as follows: A set S of integers is shadowed if and only if, for each integer i, it either contains **none** of the two integers $2i-1$ and $2i$, or it contains $2i$ **but not** $2i-1$, or it contains **both** $2i-1$ and $2i$. (What it cannot do is contain $2i-1$ but not $2i$.) When we are studying subsets of $[n]$, we can restrict ourselves to only considering the integers $i \in [n/2]$, because each of the elements of $[n]$ can be uniquely represented in the form $2i-1$ or in the form $2i$ for some $i \in [n/2]$. Thus, a subset S of $[n]$ is shadowed if and only if, for each $i \in [n/2]$, it either contains **none** of the two integers $2i-1$ and $2i$, or it contains $2i$ **but not** $2i-1$, or it contains **both** $2i-1$ and $2i$. Furthermore, if we know for each $i \in [n/2]$ which of these three options it satisfies, then we know the whole subset S.

Thus, the following simple algorithm constructs every shadowed subset of $[n]$: For each $i \in [n/2]$, we decide whether our subset should contain **none** of the two integers $2i-1$ and $2i$, or it should contain $2i$ **but not** $2i-1$, or it should contain **both** $2i-1$ and $2i$. There are clearly 3 options to choose from in this decision. Thus, in total, there are $3^{n/2}$ possible shadowed subsets of $[n]$ (because we are making this decision once for each of the $n/2$ elements i of $[n/2]$). This completes our informal proof.

This argument can be translated into a formal proof (by bijection) in the same way as this was done in our solution to Exercise 1 **(a)** above. Let me be very brief: Let $\mathfrak{A}$ be the set of all shadowed subsets of $[n]$. We must show that $|\mathfrak{A}| = 3^{n/2}$. It will suffice to exhibit a bijection $\mathfrak{A} \to [3]^{[n/2]}$.

We define such a bijection $\Xi : \mathfrak{A} \to [3]^{[n/2]}$ as follows: It should send any shadowed subset S of $[n]$ to the map $f : [n/2] \to [3]$ that sends each $i \in [n/2]$ to

$$\begin{cases} 1, & \text{if } S \text{ contains } \textbf{none} \text{ of } 2i-1 \text{ and } 2i; \\ 2, & \text{if } S \text{ contains } 2i \textbf{ but not } 2i-1; \\ 3, & \text{if } S \text{ contains } \textbf{both } 2i-1 \text{ and } 2i \end{cases}.$$

The reader can easily check that this Ξ is well-defined and has an inverse, and that completes the proof.

(b) The number of shadowed subsets of $[n]$ is $3^{(n-1)/2}$.

Proof. We know that $n \neq 0$ (since n is odd); thus, n is a positive integer (since $n \in \mathbb{N}$). Hence, $n-1 \in \mathbb{N}$. Moreover, $n-1$ is even (since n is odd). Hence, Exercise 4 **(a)** (applied to $n-1$ instead of n) shows that the number of shadowed subsets of $[n-1]$ is $3^{(n-1)/2}$.

But any shadowed subset of $[n]$ must be a subset of $[n-1]$ [4]. Hence, the shadowed subsets of $[n]$ are precisely the shadowed subsets of $[n-1]$; consequently, their number is $3^{(n-1)/2}$ (because we have just shown that the number of shadowed subsets of $[n-1]$ is $3^{(n-1)/2}$). This completes the proof. □

0.5. Counting smords (Smirnov words, or Carlitz words)

Exercise 5. Let n and k be positive integers. A *k-smord* will mean a k-tuple $(a_1, a_2, \ldots, a_k) \in [n]^k$ such that no two consecutive entries of the k-tuple are equal (i.e., we have $a_i \neq a_{i+1}$ for all $i \in [k-1]$). For example, $(3,1,3,2)$ is a 4-smord (when $n \geq 3$), but $(1,3,3,2)$ is not.

(a) Compute the number of all k-smords.

(b) A k-smord $(a_1, a_2, \ldots, a_k)$ is said to be *rounded* if it furthermore satisfies $a_k \neq a_1$. Compute the number of all rounded k-smords.

---

[4] *Proof.* Let S be a shadowed subset of $[n]$. We must show that S is a subset of $[n-1]$.

We know that S is shadowed. In other words, whenever an **odd** integer i belongs to S, the next integer $i+1$ must also belong to S. Applying this to $i = n$, we conclude that if n belongs to S, then $n+1$ must also belong to S (since n is an odd integer). Therefore, n cannot belong to S (since $n+1$ cannot belong to S (because S is a subset of $[n]$, and $n+1$ does not belong to $[n]$)). Therefore, S is a subset of $[n] \setminus \{n\} = [n-1]$. Qed.

Before I come to the solution of this exercise, let me quickly comment on where it comes from. What I call "k-smords" in Exercise 5 is usually called "*Smirnov words*"[5] or "*Carlitz words*" (of length k, over the alphabet $[n]$). Generally, combinatorialists often use the word "word of length k over an alphabet A" as a synonym for "k-tuple of elements of A", with no linguistic or semantic connotations in mind.

The exercise, however, has a deeper significance in combinatorics: It provides two simple examples for the computation of a *chromatic polynomial*. I hope we will come to see the general case in class.

Solution to Exercise 5 (sketched). **(a)** The number of all k-smords is $n(n-1)^{k-1}$.

Proof. A k-smord is simply a k-tuple of elements of $[n]$ such that each entry (apart from the first) is distinct from the previous entry. Thus, the following algorithm constructs each k-smord:

- First, choose the first entry of the k-smord. There are n choices here.
- Then, choose the second entry of the k-smord. There are $n-1$ choices for this, because it has to be distinct from the previous entry.
- Then, choose the third entry of the k-smord. There are $n-1$ choices for this, because it has to be distinct from the previous entry.
- And so on, until all entries have been chosen.

Thus, in total, there are

$$n\underbrace{(n-1)(n-1)\cdots(n-1)}_{k-1 \text{ times}} = n(n-1)^{k-1}$$

ways to perform this algorithm. Hence, the number of all k-smords is $n(n-1)^{k-1}$.

(b) The number of all rounded k-smords is $(n-1)^k + (-1)^k(n-1)$.

Proof. Let $r_k(n)$ denote the number of all rounded k-smords. We must prove that

$$r_k(n) = (n-1)^k + (-1)^k(n-1). \tag{5}$$

Let us forget that we fixed k. We shall now prove (5) by induction over k:

Induction base: A 1-smord (a) is rounded if and only if it satisfies $a \neq a$ (by the definition of "rounded"); thus, there exist no rounded 1-smords (because $a \neq a$ never holds). Hence, the number of all rounded 1-smords is 0. In other words, $r_1(n) = 0$ (since $r_1(n)$ was defined to be the number of all rounded 1-smords). Comparing this with $(n-1)^1 + (-1)^1(n-1) = 0$, we obtain $r_1(n) = (n-1)^1 + (-1)^1(n-1)$. In other words, (5) holds for $k=1$. This completes the induction base.

[5] I have abbreviated this to "smords" in the exercise to make it harder to google. The definition of "smord" in Urban Dictionary is an (unintended) red herring.

Induction step: You have seen lots of induction steps by now, so let me take away one piece of railing for the sake of brevity. Namely, instead of stepping "from $k = m$ to $k = m + 1$", I shall simply "step from k to $k + 1$". This is just a matter of notation, which at this point should not be too confusing any longer.

So let k be a positive integer, and assume (as our induction hypothesis) that (5) holds "for this particular k" (that is, we have $r_k(n) = (n-1)^k + (-1)^k (n-1)$). Then, we must show that (5) holds "for $k+1$ as well" (that is, we must show that $r_{k+1}(n) = (n-1)^{k+1} + (-1)^{k+1}(n-1)$).

We say that a $(k+1)$-smord is *non-rounded* if it is not rounded. (Duh.)

Exercise 5 **(a)** (applied to $k+1$ instead of k) shows that the number of all $(k+1)$-smords is $n(n-1)^{(k+1)-1} = n(n-1)^k$. Hence,

$$\begin{aligned} n(n-1)^k &= (\text{the number of all } (k+1)\text{-smords}) \\ &= (\text{the number of all rounded } (k+1)\text{-smords}) \\ &\qquad + (\text{the number of all non-rounded } (k+1)\text{-smords}) . \end{aligned} \tag{6}$$

We shall now find the number of all non-rounded $(k+1)$-smords.

A $(k+1)$-smord $(a_1, a_2, \ldots, a_{k+1})$ is rounded if and only if it satisfies $a_{k+1} \neq a_1$ (by the definition of "rounded"). Hence, a $(k+1)$-smord $(a_1, a_2, \ldots, a_{k+1})$ is non-rounded if and only if it satisfies $a_{k+1} = a_1$. Thus, a non-rounded $(k+1)$-smord $(a_1, a_2, \ldots, a_{k+1})$ is uniquely determined by its first k entries $a_1, a_2, \ldots, a_k$. Moreover, these first k entries must themselves form a k-smord (since $a_i \neq a_{i+1}$ holds for all $i \in [k]$ and therefore also for all $i \in [k-1]$), and this k-smord $(a_1, a_2, \ldots, a_k)$ is rounded (because $a_i \neq a_{i+1}$ for all $i \in [k]$, whence $a_k \neq a_{k+1} = a_1$, but this says precisely that the k-smord $(a_1, a_2, \ldots, a_k)$ is rounded). Hence, we can define a map

$$\begin{aligned} \phi : \{\text{non-rounded } (k+1)\text{-smords}\} &\to \{\text{rounded } k\text{-smords}\} , \\ (a_1, a_2, \ldots, a_{k+1}) &\mapsto (a_1, a_2, \ldots, a_k) . \end{aligned}$$

Conversely, if $(a_1, a_2, \ldots, a_k)$ is a rounded k-smord, then $(a_1, a_2, \ldots, a_k, a_1)$ is a non-rounded $(k+1)$-smord (in fact, it is a $(k+1)$-smord because the roundedness of $(a_1, a_2, \ldots, a_k)$ leads to $a_k \neq a_1$; and it is non-rounded because $a_1 = a_1$). Thus, we can define a map

$$\begin{aligned} \psi : \{\text{rounded } k\text{-smords}\} &\to \{\text{non-rounded } (k+1)\text{-smords}\} , \\ (a_1, a_2, \ldots, a_k) &\mapsto (a_1, a_2, \ldots, a_k, a_1) . \end{aligned}$$

The two maps ϕ and ψ are mutually inverse (to check this, just remember that any non-rounded $(k+1)$-smord $(a_1, a_2, \ldots, a_{k+1})$ must satisfy $a_{k+1} = a_1$, so it is identical with $(a_1, a_2, \ldots, a_k, a_1)$), and thus are bijections. Hence, we have found a bijection from $\{\text{non-rounded } (k+1)\text{-smords}\}$ to $\{\text{rounded } k\text{-smords}\}$ (namely, ϕ). Therefore,

$$\begin{aligned} &(\text{the number of all non-rounded } (k+1)\text{-smords}) \\ &= (\text{the number of all rounded } k\text{-smords}) . \end{aligned}$$

Thus, (6) becomes

$$n(n-1)^k = \underbrace{(\text{the number of all rounded } (k+1)\text{-smords})}_{\substack{=r_{k+1}(n) \\ (\text{since } r_{k+1}(n) \text{ is defined as the number of all rounded } (k+1)\text{-smords})}} + \underbrace{(\text{the number of all non-rounded } (k+1)\text{-smords})}_{\substack{=(\text{the number of all rounded } k\text{-smords})=r_k(n) \\ (\text{since } r_k(n) \text{ is defined as the number of all rounded } k\text{-smords})}} = r_{k+1}(n) + r_k(n).$$

Therefore,

$$r_{k+1}(n) = n(n-1)^k - \underbrace{r_k(n)}_{\substack{=(n-1)^k+(-1)^k(n-1) \\ (\text{by the induction hypothesis})}} = n(n-1)^k - \left((n-1)^k + (-1)^k(n-1)\right)$$
$$= \underbrace{n(n-1)^k - (n-1)^k}_{=(n-1)(n-1)^k=(n-1)^{k+1}} - \underbrace{(-1)^k}_{=-(-1)^{k+1}} (n-1) = (n-1)^{k+1} - \left(\left(-1\right)^{k+1}\right)(n-1)$$
$$= (n-1)^{k+1} + (-1)^{k+1}(n-1).$$

In other words, (5) holds "for $k+1$ as well". This completes the induction step. Thus, the induction proof of (5) is finished, and with it the solution of Exercise 5 **(b)**. □

0.6. Necklaces 2: rotational equivalence of tuples

Let us recall a basic property of maps (proven in Exercise 6 **(a)** on Math 4990 homework set #2): If S is a set, and if $f : S \to S$ a map, then

$$f^n \circ f^m = f^{n+m} \qquad (7)$$

for each $n, m \in \mathbb{N}$.

Exercise 6. This continues Exercise 7 from Math 4990 homework set #2.

Let n be a positive integer. Let X be a set.

We define a map $c : X^n \to X^n$ by

$$c(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1) \qquad \text{for all } (x_1, x_2, \ldots, x_n) \in X^n.$$

(In other words, the map c transforms any n-tuple $(x_1, x_2, \ldots, x_n) \in X^n$ by "rotating" it one step to the left, or, equivalently, moving its first entry to the last position.)

For two n-tuples $\mathbf{x}$ and $\mathbf{y}$, we say that $\mathbf{x} \sim \mathbf{y}$ if there exists some $k \in \mathbb{N}$ such that $\mathbf{y} = c^k(\mathbf{x})$. (For example, $(1,5,2,4) \sim (2,4,1,5)$, because $(2,4,1,5) = c^2(1,5,2,4)$.)

> **(a)** Prove that $\sim$ is an equivalence relation, i.e., is reflexive, transitive and symmetric. (For example, symmetry boils down to showing that if there exists some $k \in \mathbb{N}$ satisfying $\mathbf{y} = c^k(\mathbf{x})$, then there exists some $\ell \in \mathbb{N}$ satisfying $\mathbf{x} = c^\ell(\mathbf{y})$.)
>
> **(b)** An *n-necklace* (over X) shall mean a $\sim$-equivalence class. We denote the $\sim$-equivalence class of a tuple $\mathbf{x} \in X^n$ by $[\mathbf{x}]_\sim$.
>
> Let $\mathbf{x} \in X^n$ be an n-tuple. Let m be the smallest nonzero period of the n-tuple $\mathbf{x} \in X^n$.
>
> Prove that $[\mathbf{x}]_\sim = \left\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\right\}$.
>
> **(c)** Show that the m tuples $c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})$ are distinct. Conclude that $|[\mathbf{x}]_\sim| = m$.

Solution to Exercise 6. Before we properly start solving this exercise, let us make some basic observations:

> *Observation 1:* We have $c^n(\mathbf{x}) = \mathbf{x}$ for each $\mathbf{x} \in X^n$.

[*Proof of Observation 1:* Let $\mathbf{x} \in X^n$. We have proven $c^n(\mathbf{x}) = \mathbf{x}$ during our solution to Exercise 7 **(d)** on Math 4990 homework set #2. Thus, Observation 1 follows.]

> *Observation 2:* Let $\mathbf{x} \in X^n$. Let $p \in \mathbb{N}$ be such that $c^p(\mathbf{x}) = \mathbf{x}$. Then, $c^{kp}(\mathbf{x}) = \mathbf{x}$ for each $k \in \mathbb{N}$.

[*Proof of Observation 2:* Observation 2 is intuitively obvious: All it says is that if applying the map c to $\mathbf{x}$ a total of p times brings you back to $\mathbf{x}$, then applying the map c to $\mathbf{x}$ a total of kp times brings you back to $\mathbf{x}$ as well. This intuition can easily be translated into a rigorous argument:

We shall prove Observation 2 by induction over k:

Induction base: We have $c^{0p} = c^0 = \mathrm{id}_{X^n}$, so that $c^{0p}(\mathbf{x}) = \mathrm{id}_{X^n}(\mathbf{x}) = \mathbf{x}$. Thus, Observation 2 holds for $k = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that Observation 2 holds for $k = m$. We must prove that Observation 2 holds for $k = m + 1$.

Let $\mathbf{x} \in X^n$. Let $p \in \mathbb{N}$ be such that $c^p(\mathbf{x}) = \mathbf{x}$. Then, $c^{mp}(\mathbf{x}) = \mathbf{x}$ (since Observation 2 holds for $k = m$). But (7) (applied to X^n, c, mp and p instead of S, f, n and m) yields $c^{mp} \circ c^p = c^{mp+p} = c^{(m+1)p}$. Hence, $(c^{mp} \circ c^p)(\mathbf{x}) = c^{(m+1)p}(\mathbf{x})$, and therefore

$$c^{(m+1)p}(\mathbf{x}) = (c^{mp} \circ c^p)(\mathbf{x}) = c^{mp}\left(\underbrace{c^p(\mathbf{x})}_{=\mathbf{x}}\right) = c^{mp}(\mathbf{x}) = \mathbf{x}.$$

In other words, Observation 2 holds for $k = m + 1$. This completes the induction step. Thus, Observation 2 is proven.]

Now, we must show that $\sim$ is an equivalence relation. Indeed, the relation $\sim$ is reflexive[6], symmetric[7] and transitive[8]. In other words, the relation $\sim$ is an equivalence relation. This solves Exercise 6 **(a)**.

(b) The number m is the smallest nonzero period of the n-tuple $\mathbf{x} \in X^n$. In particular, m is a period of $\mathbf{x}$. In other words, $m \in \mathbb{N}$ and $c^m(\mathbf{x}) = \mathbf{x}$.

The definition of the equivalence class $[\mathbf{x}]_\sim$ of $\mathbf{x}$ shows that

$$[\mathbf{x}]_\sim = \{\mathbf{y} \in X^n \mid \mathbf{y} \sim \mathbf{x}\}. \tag{8}$$

Let S denote the set $\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\}$. Then, $S \subseteq [\mathbf{x}]_\sim$ [9].

On the other hand, we claim the following:

---

[6] *Proof.* Let $\mathbf{x} \in X^n$. We shall show that $\mathbf{x} \sim \mathbf{x}$.

Indeed, $c^0 = \mathrm{id}_{X^n}$, so that $c^0(\mathbf{x}) = \mathrm{id}_{X^n}(\mathbf{x}) = \mathbf{x}$. Hence, there exists some $k \in \mathbb{N}$ such that $\mathbf{x} = c^k(\mathbf{x})$ (namely, $k = 0$). In other words, $\mathbf{x} \sim \mathbf{x}$ (by the definition of the relation $\sim$).

Now, forget that we fixed $\mathbf{x}$. We thus have shown that every $\mathbf{x} \in X^n$ satisfies $\mathbf{x} \sim \mathbf{x}$. In other words, the relation $\sim$ is reflexive.

[7] *Proof.* Let $\mathbf{x} \in X^n$ and $\mathbf{y} \in X^n$ be such that $\mathbf{x} \sim \mathbf{y}$. We shall show that $\mathbf{y} \sim \mathbf{x}$.

Indeed, we have $\mathbf{x} \sim \mathbf{y}$. In other words, there exists some $k \in \mathbb{N}$ such that $\mathbf{y} = c^k(\mathbf{x})$ (by the definition of the relation $\sim$). Consider such a k, and denote it by u. Thus, $u \in \mathbb{N}$ satisfies $\mathbf{y} = c^u(\mathbf{x})$.

Observation 1 yields $c^n(\mathbf{x}) = \mathbf{x}$. Hence, Observation 2 (applied to $p = n$ and $k = u$) yields $c^{un}(\mathbf{x}) = \mathbf{x}$. But n is positive; hence, $n \geq 1$ and thus $un \geq u1 = u$. Hence, $un - u \in \mathbb{N}$. Applying (7) to X^n, c, $un - u$ and u instead of S, f, n and m, we obtain $c^{un-u} \circ c^u = c^{(un-u)+u} = c^{un}$. Thus, $(c^{un-u} \circ c^u)(\mathbf{x}) = c^{un}(\mathbf{x}) = \mathbf{x}$. Hence, $\mathbf{x} = (c^{un-u} \circ c^u)(\mathbf{x}) = c^{un-u}\left(\underbrace{c^u(\mathbf{x})}_{=\mathbf{y}}\right) = c^{un-u}(\mathbf{y})$. Thus, there exists some $k \in \mathbb{N}$ such that $\mathbf{x} = c^k(\mathbf{y})$ (namely, $k = un - u$). In other words, $\mathbf{y} \sim \mathbf{x}$ (by the definition of the relation $\sim$).

Now, forget that we fixed $\mathbf{x}$ and $\mathbf{y}$. We thus have shown that if $\mathbf{x} \in X^n$ and $\mathbf{y} \in X^n$ satisfy $\mathbf{x} \sim \mathbf{y}$, then $\mathbf{y} \sim \mathbf{x}$. In other words, the relation $\sim$ is symmetric.

[8] *Proof.* Let $\mathbf{x} \in X^n$, $\mathbf{y} \in X^n$ and $\mathbf{z} \in X^n$ be such that $\mathbf{x} \sim \mathbf{y}$ and $\mathbf{y} \sim \mathbf{z}$. We shall show that $\mathbf{x} \sim \mathbf{z}$.

Indeed, we have $\mathbf{x} \sim \mathbf{y}$. In other words, there exists some $k \in \mathbb{N}$ such that $\mathbf{y} = c^k(\mathbf{x})$ (by the definition of the relation $\sim$). Consider such a k, and denote it by u. Thus, $u \in \mathbb{N}$ satisfies $\mathbf{y} = c^u(\mathbf{x})$.

Also, we have $\mathbf{y} \sim \mathbf{z}$. In other words, there exists some $k \in \mathbb{N}$ such that $\mathbf{z} = c^k(\mathbf{y})$ (by the definition of the relation $\sim$). Consider such a k, and denote it by v. Thus, $v \in \mathbb{N}$ satisfies $\mathbf{z} = c^v(\mathbf{y})$.

Applying (7) to X^n, c, v and u instead of S, f, n and m, we obtain $c^v \circ c^u = c^{v+u}$. Thus, $(c^v \circ c^u)(\mathbf{x}) = c^{v+u}(\mathbf{x})$. In view of $(c^v \circ c^u)(\mathbf{x}) = c^v\left(\underbrace{c^u(\mathbf{x})}_{=\mathbf{y}}\right) = c^v(\mathbf{y}) = \mathbf{z}$, this rewrites as $\mathbf{z} = c^{v+u}(\mathbf{x})$. Thus, there exists some $k \in \mathbb{N}$ such that $\mathbf{z} = c^k(\mathbf{x})$ (namely, $k = v + u$). In other words, $\mathbf{x} \sim \mathbf{z}$ (by the definition of the relation $\sim$).

Now, forget that we fixed $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$. We thus have shown that if $\mathbf{x} \in X^n$, $\mathbf{y} \in X^n$ and $\mathbf{z} \in X^n$ satisfy $\mathbf{x} \sim \mathbf{y}$ and $\mathbf{y} \sim \mathbf{z}$, then $\mathbf{x} \sim \mathbf{z}$. In other words, the relation $\sim$ is transitive.

[9] *Proof.* Let $\mathbf{s} \in S$. Then, $\mathbf{s} \in S = \{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\}$. In other words, $\mathbf{s} = c^i(\mathbf{x})$ for some $i \in \{0, 1, \ldots, m-1\}$. Consider this i.

Hence, $\mathbf{s} \in X^n$. Furthermore, there exists some $k \in \mathbb{N}$ such that $\mathbf{s} = c^k(\mathbf{x})$ (namely, $k = i$). In other words, $\mathbf{x} \sim \mathbf{s}$ (by the definition of the relation $\sim$). Hence, $\mathbf{s} \sim \mathbf{x}$ (since the relation $\sim$ is symmetric). Therefore, $\mathbf{s} \in \{\mathbf{y} \in X^n \mid \mathbf{y} \sim \mathbf{x}\}$. In light of (8), this rewrites as $\mathbf{s} \in [\mathbf{x}]_\sim$.

> *Observation 3:* We have $c^k(\mathbf{x}) \in S$ for each $k \in \mathbb{N}$.

[*Proof of Observation 3:* We proceed by strong induction over k:

Induction step: Let $h \in \mathbb{N}$. Assume that Observation 3 holds whenever $k < h$. We now must prove that Observation 3 holds for $k = h$. In other words, we must prove that $c^h(\mathbf{x}) \in S$.

If $h < m$, then this is obvious[10]. Hence, for the rest of this proof (i.e., of the induction step), we WLOG assume that we don't have $h < m$. Thus, $h \geq m$, so that $h - m \in \mathbb{N}$.

We know that m is nonzero, and therefore positive (since $m \in \mathbb{N}$). Hence, $h - m < h$. Therefore (and because of $h - m \in \mathbb{N}$), we can apply Observation 3 to $k = h - m$ (since we have assumed that Observation 3 holds whenever $k < h$). We thus obtain $c^{h-m}(\mathbf{x}) \in S$.

But (7) (applied to X^n, c, $h - m$ and m instead of S, f, n and m) shows that $c^{h-m} \circ c^m = c^{(h-m)+m} = c^h$. Hence, $\left(c^{h-m} \circ c^m\right)(\mathbf{x}) = c^h(\mathbf{x})$, so that

$$c^h(\mathbf{x}) = \left(c^{h-m} \circ c^m\right)(\mathbf{x}) = c^{h-m}\left(\underbrace{c^m(\mathbf{x})}_{=\mathbf{x}}\right) = c^{h-m}(\mathbf{x}) \in S.$$

In other words, Observation 3 holds for $k = h$. This completes the induction step. Observation 3 is thus proven.]

Now, it is easy to see that $[\mathbf{x}]_\sim \subseteq S$ [11]. Combining this with $S \subseteq [\mathbf{x}]_\sim$, we obtain $[\mathbf{x}]_\sim = S = \left\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\right\}$ (by the definition of S). This solves Exercise 6 **(b)**.

(c) We observe that $m \in \mathbb{N}$ and $c^m(\mathbf{x}) = \mathbf{x}$ (as we have already seen in the solution to part **(b)**).

Now, we are going to show the following:

> *Observation 4:* Let i and j be two distinct elements of $\{0, 1, \ldots, m-1\}$. Then, $c^i(\mathbf{x}) \neq c^j(\mathbf{x})$.

[*Proof of Observation 4:* We WLOG assume that $i \leq j$ (since otherwise, we can simply switch i with j to ensure that $i \leq j$). Hence, $i < j$ (since i and j are distinct).

Now, forget that we fixed $\mathbf{s}$. We thus have shown that $\mathbf{s} \in [\mathbf{x}]_\sim$ for each $\mathbf{s} \in S$. In other words, $S \subseteq [\mathbf{x}]_\sim$.

[10] *Proof.* Assume that $h < m$. Thus, $h \in \{0, 1, \ldots, m-1\}$ (since $h \in \mathbb{N}$), and thus $c^h(\mathbf{x}) \in \left\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\right\} = S$, qed.

[11] *Proof.* Let $\mathbf{s} \in [\mathbf{x}]_\sim$. Then, $\mathbf{s} \in [\mathbf{x}]_\sim = \{\mathbf{y} \in X^n \mid \mathbf{y} \sim \mathbf{x}\}$ (by (8)). In other words, $\mathbf{s} \in X^n$ and $\mathbf{s} \sim \mathbf{x}$. From $\mathbf{s} \sim \mathbf{x}$, we obtain $\mathbf{x} \sim \mathbf{s}$ (since the relation $\sim$ is symmetric). In other words, there exists some $k \in \mathbb{N}$ such that $\mathbf{s} = c^k(\mathbf{x})$ (by the definition of the relation $\sim$). Consider this k. Now, Observation 3 yields $c^k(\mathbf{x}) \in S$. Hence, $\mathbf{s} = c^k(\mathbf{x}) \in S$.

Now, forget that we fixed $\mathbf{s}$. We thus have shown that $\mathbf{s} \in S$ for each $\mathbf{s} \in [\mathbf{x}]_\sim$. In other words, $[\mathbf{x}]_\sim \subseteq S$.

Assume (for the sake of contradiction) that $c^i(\mathbf{x}) = c^j(\mathbf{x})$. Since $j \in \{0, 1, \ldots, m-1\}$, we have $j \leq m - 1 < m$. Hence, $\left(m - \underbrace{j}_{<m}\right) + i > (m - m) + i = i \geq 0$.

Also $m - j \in \mathbb{N}$ (since $j < m$). Therefore, (7) (applied to X^n, c, $m - j$ and j instead of S, f, n and m) shows that $c^{m-j} \circ c^j = c^{(m-j)+j} = c^m$. Hence, $\left(c^{m-j} \circ c^j\right)(\mathbf{x}) = c^m(\mathbf{x}) = \mathbf{x}$. Therefore,

$$\mathbf{x} = \left(c^{m-j} \circ c^j\right)(\mathbf{x}) = c^{m-j}\left(c^j(\mathbf{x})\right). \tag{9}$$

On the other hand, (7) (applied to X^n, c, $m - j$ and i instead of S, f, n and m) shows that $c^{m-j} \circ c^i = c^{(m-j)+i}$. Hence, $\left(c^{m-j} \circ c^i\right)(\mathbf{x}) = c^{(m-j)+i}(\mathbf{x})$. Therefore,

$$c^{(m-j)+i}(\mathbf{x}) = \left(c^{m-j} \circ c^i\right)(\mathbf{x}) = c^{m-j}\left(\underbrace{c^i(\mathbf{x})}_{\substack{=c^j(\mathbf{x}) \\ \text{(by our assumption)}}}\right) = c^{m-j}\left(c^j(\mathbf{x})\right) = \mathbf{x}$$

(by (9)).

Now, the integer $(m - j) + i$ belongs to $\mathbb{N}$ (since $(m - j) + i > 0$) and satisfies $c^{(m-j)+i}(\mathbf{x}) = \mathbf{x}$. In other words, $(m - j) + i$ is a period of $\mathbf{x}$ (by the definition of a "period"). Moreover, this period $(m - j) + i$ is nonzero (since $(m - j) + i > 0$).

Recall that m is the **smallest** nonzero period of the n-tuple $\mathbf{x} \in X^n$. Hence, every nonzero period p of $\mathbf{x}$ satisfies $p \geq m$. Applying this to $p = (m - j) + i$, we obtain $(m - j) + i \geq m$ (since $(m - j) + i$ is a nonzero period of $\mathbf{x}$). This contradicts $(m - j) + \underbrace{i}_{<j} < (m - j) + j = m$. This contradiction shows that our assumption (that $c^i(\mathbf{x}) = c^j(\mathbf{x})$) was wrong. Hence, $c^i(\mathbf{x}) \neq c^j(\mathbf{x})$. This proves Observation 4.]

Observation 4 shows that the m tuples $c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})$ are distinct. Hence, the set $\left\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\right\}$ contains m distinct elements. Therefore, $\left|\left\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\right\}\right| = m$. But Exercise 6 **(b)** shows that $[\mathbf{x}]_\sim = \left\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\right\}$. Thus, $\left|[\mathbf{x}]_\sim\right| = \left|\left\{c^0(\mathbf{x}), c^1(\mathbf{x}), \ldots, c^{m-1}(\mathbf{x})\right\}\right| = m$. This solves Exercise 6 **(c)**. $\square$