Math 4707 & Math 4990 Fall 2017 (Darij Grinberg): homework set 2 with solutions

Contents

0.1. More on binomial coefficients

Recall the following formula (which we have already seen in the solutions to homework set 1):

Proposition 0.1. Let a and b be two integers such that $a \geq b \geq 0$. Then, $\dbinom{a}{b} = \dfrac{a!}{b!\,(a-b)!}$.

Also, recall some more fundamental properties of binomial coefficients:

Proposition 0.2. We have
$$\dbinom{m}{n} = 0$$
for every $m \in \mathbb{N}$ and $n \in \mathbb{N}$ satisfying $m < n$.

Proposition 0.3. We have
$$\dbinom{m}{n} = \dbinom{m-1}{n-1} + \dbinom{m-1}{n} \qquad (1)$$
for any $m \in \mathbb{Z}$ and $n \in \{1, 2, 3, \ldots\}$.

Proposition 0.4. We have $\dbinom{n}{n} = 1$ for each $n \in \mathbb{N}$.

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

(a) Prove that
$$(2n-1) \cdot (2n-3) \cdot \cdots \cdot 1 = \frac{(2n)!}{2^n n!}.$$
(The left hand side is understood to be the product of all odd integers from 1 to $2n-1$.)

(b) Prove that
$$\binom{-1/2}{n} = \left(\frac{-1}{4}\right)^n \binom{2n}{n}.$$

(c) Prove that
$$\binom{-1/3}{n}\binom{-2/3}{n} = \frac{(3n)!}{(3^n n!)^3}.$$

Solution to Exercise 1. **(a)** We have

$$\begin{aligned}
(2n)! &= 1 \cdot 2 \cdot \cdots \cdot (2n) = \prod_{k \in \{1,2,\ldots,2n\}} k = \underbrace{\left(\prod_{\substack{k \in \{1,2,\ldots,2n\};\\ k \text{ is even}}} k\right)}_{\substack{=2\cdot 4\cdot 6\cdot\cdots\cdot(2n) \\ =\prod_{i=1}^{n}(2i) \\ =2^n \prod_{i=1}^{n} i}} \underbrace{\left(\prod_{\substack{k \in \{1,2,\ldots,2n\};\\ k \text{ is odd}}} k\right)}_{=1\cdot 3\cdot 5\cdot\cdots\cdot(2n-1)} \\
&\qquad \left(\begin{array}{c}\text{here, we have split the product } \prod_{k \in \{1,2,\ldots,2n\}} k \text{ into one product} \\ \text{containing all even } k \text{ and one product containing all odd } k\end{array}\right) \\
&= 2^n \underbrace{\left(\prod_{i=1}^{n} i\right)}_{=1\cdot 2\cdot\cdots\cdot n = n!} \cdot (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)) \\
&= 2^n n! \cdot (1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)).
\end{aligned}$$

Dividing this equality by $2^n n!$, we obtain

$$\frac{(2n)!}{2^n n!} = 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1) = (2n-1) \cdot (2n-3) \cdot \cdots \cdot 1.$$

This solves Exercise 1 **(a)**.

(b) We have $2n \geq n \geq 0$. Hence, Proposition 0.1 (applied to $a = 2n$ and $b = n$) yields

$$\binom{2n}{n} = \frac{(2n)!}{n!\,(2n-n)!} = \frac{(2n)!}{n!n!}. \qquad (2)$$

The definition of $\dbinom{-1/2}{n}$ yields

$$\begin{aligned}
\dbinom{-1/2}{n} &= \frac{(-1/2)(-1/2-1)\cdots(-1/2-n+1)}{n!} \\
&= \frac{1}{n!}\cdot \underbrace{(-1/2)(-1/2-1)\cdots(-1/2-n+1)}_{=\prod_{k=0}^{n-1}(-1/2-k)} \\
&= \frac{1}{n!}\cdot \prod_{k=0}^{n-1} \underbrace{(-1/2-k)}_{=\frac{-1}{2}(2k+1)} = \frac{1}{n!}\cdot \underbrace{\prod_{k=0}^{n-1}\left(\frac{-1}{2}(2k+1)\right)}_{=\left(\frac{-1}{2}\right)^n \prod_{k=0}^{n-1}(2k+1)} \\
&= \frac{1}{n!}\cdot \left(\frac{-1}{2}\right)^n \underbrace{\prod_{k=0}^{n-1}(2k+1)}_{\substack{=1\cdot 3\cdot 5\cdot\cdots\cdot(2(n-1)+1) \\ =1\cdot 3\cdot 5\cdot\cdots\cdot(2n-1) \\ \text{(since } 2(n-1)+1=2n-1\text{)}}} = \frac{1}{n!}\cdot \left(\frac{-1}{2}\right)^n \underbrace{(1\cdot 3\cdot 5\cdot\cdots\cdot(2n-1))}_{\substack{=(2n-1)\cdot(2n-3)\cdot\cdots\cdot 1 \\ =\frac{(2n)!}{2^n n!} \\ \text{(by Exercise 1 } \textbf{(a)}\text{)}}} \\
&= \frac{1}{n!}\cdot \left(\frac{-1}{2}\right)^n \cdot \frac{(2n)!}{2^n n!} = \left(\frac{-1}{2}\right)^n \cdot \underbrace{\frac{1}{2^n}}_{=\left(\frac{1}{2}\right)^n} \cdot \frac{(2n)!}{n!n!} = \left(\frac{-1}{2}\right)^n \cdot \left(\frac{1}{2}\right)^n \cdot \frac{(2n)!}{n!n!}.
\end{aligned}$$

Comparing this with

$$\left(\underbrace{\frac{-1}{4}}_{=\frac{-1}{2}\cdot\frac{1}{2}}\right)^n \underbrace{\dbinom{2n}{n}}_{\substack{=\frac{(2n)!}{n!n!} \\ \text{(by (2))}}} = \underbrace{\left(\frac{-1}{2}\cdot\frac{1}{2}\right)^n}_{=\left(\frac{-1}{2}\right)^n\cdot\left(\frac{1}{2}\right)^n} \cdot \frac{(2n)!}{n!n!} = \left(\frac{-1}{2}\right)^n \cdot \left(\frac{1}{2}\right)^n \cdot \frac{(2n)!}{n!n!},$$

we obtain $\dbinom{-1/2}{n} = \left(\frac{-1}{4}\right)^n \dbinom{2n}{n}$. This solves Exercise 1 **(b)**.

(c) We have

$$\begin{aligned}
(3n)! = 1\cdot 2\cdot\cdots\cdot(3n) &= \prod_{k\in\{1,2,\ldots,3n\}} k \\
&= \left(\prod_{\substack{k\in\{1,2,\ldots,3n\}; \\ k\equiv 0 \bmod 3}} k\right)\left(\prod_{\substack{k\in\{1,2,\ldots,3n\}; \\ k\equiv 1 \bmod 3}} k\right)\left(\prod_{\substack{k\in\{1,2,\ldots,3n\}; \\ k\equiv 2 \bmod 3}} k\right)
\end{aligned}$$

(here, we have split the product $\prod_{k\in\{1,2,\ldots,3n\}} k$ into three smaller products, because each $k \in \{1,2,\ldots,3n\}$ must satisfy exactly one of the three conditions $k \equiv 0 \mod 3$, $k \equiv 1 \mod 3$ and $k \equiv 2 \mod 3$). Thus,

$$\begin{aligned}
(3n)! &= \underbrace{\left(\prod_{\substack{k\in\{1,2,\ldots,3n\};\\ k\equiv 0 \mod 3}} k\right)}_{\substack{=3\cdot 6\cdot 9\cdot\cdots\cdot(3n)\\ =\prod_{i=1}^{n}(3i)\\ =3^n\prod_{i=1}^{n} i}} \underbrace{\left(\prod_{\substack{k\in\{1,2,\ldots,3n\};\\ k\equiv 1 \mod 3}} k\right)}_{\substack{=1\cdot 4\cdot 7\cdot\cdots\cdot(3n-2)\\ =\prod_{i=0}^{n-1}(3i+1)}} \underbrace{\left(\prod_{\substack{k\in\{1,2,\ldots,3n\};\\ k\equiv 2 \mod 3}} k\right)}_{\substack{=2\cdot 5\cdot 8\cdot\cdots\cdot(3n-1)\\ =\prod_{i=0}^{n-1}(3i+2)}} \\
&= 3^n \underbrace{\left(\prod_{i=1}^{n} i\right)}_{=n!} \left(\prod_{i=0}^{n-1}(3i+1)\right) \left(\prod_{i=0}^{n-1}(3i+2)\right) \\
&= 3^n n! \left(\prod_{i=0}^{n-1}(3i+1)\right) \left(\prod_{i=0}^{n-1}(3i+2)\right). \qquad (3)
\end{aligned}$$

On the other hand, for each $g \in \mathbb{Z}$, we have

$$\begin{aligned}
\binom{-g/3}{n} &= \frac{(-g/3)(-g/3-1)\cdots(-g/3-n+1)}{n!} \\
&\qquad \left(\text{by the definition of } \binom{-g/3}{n}\right) \\
&= \frac{1}{n!}\cdot \underbrace{(-g/3)(-g/3-1)\cdots(-g/3-n+1)}_{=\prod_{i=0}^{n-1}(-g/3-i)} \\
&= \frac{1}{n!}\cdot \prod_{i=0}^{n-1} \underbrace{(-g/3-i)}_{=\frac{-1}{3}(3i+g)} = \frac{1}{n!}\cdot \underbrace{\prod_{i=0}^{n-1}\left(\frac{-1}{3}(3i+g)\right)}_{=\left(\frac{-1}{3}\right)^n \prod_{i=0}^{n-1}(3i+g)} \\
&= \frac{1}{n!}\cdot \left(\frac{-1}{3}\right)^n \prod_{i=0}^{n-1}(3i+g). \qquad (4)
\end{aligned}$$

Now,

$$\begin{aligned}
&\underbrace{(3^n n!)^3}_{=3^n n! \cdot 3^n n! \cdot 3^n n!} \underbrace{\binom{-1/3}{n}}_{\substack{=\frac{1}{n!} \cdot \left(\frac{-1}{3}\right)^n \prod_{i=0}^{n-1} (3i+1) \\ \text{(by (4), applied to } g=1)}} \underbrace{\binom{-2/3}{n}}_{\substack{=\frac{1}{n!} \cdot \left(\frac{-1}{3}\right)^n \prod_{i=0}^{n-1} (3i+2) \\ \text{(by (4), applied to } g=2)}} \\
&= 3^n n! \cdot 3^n n! \cdot 3^n n! \cdot \left(\frac{1}{n!} \cdot \left(\frac{-1}{3}\right)^n \prod_{i=0}^{n-1} (3i+1)\right) \cdot \left(\frac{1}{n!} \cdot \left(\frac{-1}{3}\right)^n \prod_{i=0}^{n-1} (3i+2)\right) \\
&= \underbrace{3^n \cdot 3^n \cdot 3^n \cdot \left(\frac{-1}{3}\right)^n \left(\frac{-1}{3}\right)^n}_{=\left(3 \cdot 3 \cdot 3 \cdot \frac{-1}{3} \cdot \frac{-1}{3}\right)^n} n! \left(\prod_{i=0}^{n-1} (3i+1)\right) \left(\prod_{i=0}^{n-1} (3i+2)\right) \\
&= \left(\underbrace{3 \cdot 3 \cdot 3 \cdot \frac{-1}{3} \cdot \frac{-1}{3}}_{=3}\right)^n n! \left(\prod_{i=0}^{n-1} (3i+1)\right) \left(\prod_{i=0}^{n-1} (3i+2)\right) \\
&= 3^n n! \left(\prod_{i=0}^{n-1} (3i+1)\right) \left(\prod_{i=0}^{n-1} (3i+2)\right).
\end{aligned}$$

Comparing this with (3), we obtain $(3^n n!)^3 \binom{-1/3}{n} \binom{-2/3}{n} = (3n)!$. Dividing this equality by $(3^n n!)^3$, we find $\binom{-1/3}{n} \binom{-2/3}{n} = \frac{(3n)!}{(3^n n!)^3}$. This solves Exercise 1 **(c)**. $\square$

Remark 0.5. A generalization of parts **(b)** and **(c)** of Exercise 1 (provable in a similar way) is the following identity, true for each positive integer h:

$$\prod_{g=1}^{h-1} \binom{-g/h}{n} = \left(\frac{-1}{h}\right)^{n(h-1)} \cdot \frac{(hn)!}{h^n n!^h}.$$

Exercise 2. Let $n \in \mathbb{Q}$, $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

(a) Prove that every integer $j \geq a$ satisfies

$$\binom{n}{j} \binom{j}{a} \binom{n-j}{b} = \binom{n}{a} \binom{n-a}{b} \binom{n-a-b}{j-a}.$$

(b) Compute the sum $\sum_{j=a}^{n} \binom{n}{j} \binom{j}{a} \binom{n-j}{b}$ for every integer $n \geq a$. (The result should contain no summation signs.)

Before we come to the solution, let us recall a fundamental fact (which has already been proven in the solutions to homework set 1):

Proposition 0.6. Let $m \in \mathbb{N}$. Then,

$$\sum_{k=0}^{m} \binom{m}{k} = 2^m.$$

Let us modify this proposition a little bit by pushing additional zero addends into the sum:

Proposition 0.7. Let $m \in \mathbb{N}$ and $p \in \mathbb{N}$ be such that $p \geq m$. Then,

$$\sum_{k=0}^{p} \binom{m}{k} = 2^m.$$

Proof of Proposition 0.7. We have $p \geq m \geq 0$. Thus, the sum $\sum\limits_{k=0}^{p} \binom{m}{k}$ can be split as follows:

$$\sum_{k=0}^{p} \binom{m}{k} = \sum_{k=0}^{m} \binom{m}{k} + \sum_{k=m+1}^{p} \underbrace{\binom{m}{k}}_{\substack{=0 \\ \text{(by Proposition 0.2, applied to } n=k \\ \text{(since } k \geq m+1 > m \text{ and thus } m<k))}} = \sum_{k=0}^{m} \binom{m}{k} + \underbrace{\sum_{k=m+1}^{p} 0}_{=0}$$

$$= \sum_{k=0}^{m} \binom{m}{k} = 2^m \qquad \text{(by Proposition 0.6)}.$$

This proves Proposition 0.7. $\square$

Solution to Exercise 2. **(a)** For each $k \in \mathbb{N}$, we have

$$\underbrace{\binom{n}{k}}_{\substack{= \frac{n(n-1)\cdots(n-k+1)}{k!} \\ \text{(by the definition of } \binom{n}{k})}} \underbrace{\binom{n-k}{b}}_{\substack{= \frac{(n-k)(n-k-1)\cdots(n-k-b+1)}{b!} \\ \text{(by the definition of } \binom{n-k}{b})}}$$

$$= \frac{n(n-1)\cdots(n-k+1)}{k!} \cdot \frac{(n-k)(n-k-1)\cdots(n-k-b+1)}{b!}$$

$$= \frac{1}{k!b!} \cdot \underbrace{(n(n-1)\cdots(n-k+1)) \cdot ((n-k)(n-k-1)\cdots(n-k-b+1))}_{=n(n-1)\cdots(n-k-b+1)}$$

$$= \frac{1}{k!b!} \cdot (n(n-1)\cdots(n-k-b+1)). \qquad (5)$$

Let $j \geq a$ be an integer. Then, Proposition 0.1 (applied to j and a instead of a and b) shows that

$$\binom{j}{a} = \frac{j!}{a!\,(j-a)!}.$$

But (5) (applied to $k = j$) shows that

$$\binom{n}{j}\binom{n-j}{b} = \frac{1}{j!b!} \cdot (n\,(n-1)\cdots(n-j-b+1)).$$

Multiplying these two equalities, we obtain

$$\binom{j}{a}\binom{n}{j}\binom{n-j}{b} = \frac{j!}{a!\,(j-a)!} \cdot \frac{1}{j!b!} \cdot (n\,(n-1)\cdots(n-j-b+1)) = \frac{1}{a!\,(j-a)!b!} \cdot (n\,(n-1)\cdots(n-j-b+1)). \qquad (6)$$

On the other hand, $j - a \in \mathbb{N}$ (since $j \geq a$), and thus the binomial coefficient $\binom{n-a-b}{j-a}$ is well-defined. We have

$$\begin{aligned}
&\underbrace{\binom{n}{a}\binom{n-a}{b}}_{\substack{=\frac{1}{a!b!}\cdot(n(n-1)\cdots(n-a-b+1)) \\ \text{(by (5), applied to } k=a)}} \underbrace{\binom{n-a-b}{j-a}}_{\substack{=\frac{(n-a-b)(n-a-b-1)\cdots(n-a-b-(j-a)+1)}{(j-a)!} \\ \text{(by the definition of } \binom{n-a-b}{j-a})}} \\
&= \frac{1}{a!b!} \cdot (n\,(n-1)\cdots(n-a-b+1)) \cdot \frac{(n-a-b)\,(n-a-b-1)\cdots(n-a-b-(j-a)+1)}{(j-a)!} \\
&= \frac{1}{a!\,(j-a)!b!} \\
&\qquad \cdot \underbrace{(n\,(n-1)\cdots(n-a-b+1)) \cdot ((n-a-b)\,(n-a-b-1)\cdots(n-a-b-(j-a)+1))}_{\substack{=n(n-1)\cdots(n-a-b-(j-a)+1) \\ =n(n-1)\cdots(n-j-b+1) \\ \text{(since } n-a-b-(j-a)+1=n-j-b+1)}} \\
&= \frac{1}{a!\,(j-a)!b!} \cdot (n\,(n-1)\cdots(n-j-b+1)).
\end{aligned}$$

Comparing this with (6), we obtain

$$\binom{n}{a}\binom{n-a}{b}\binom{n-a-b}{j-a} = \binom{j}{a}\binom{n}{j}\binom{n-j}{b} = \binom{n}{j}\binom{j}{a}\binom{n-j}{b}.$$

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

(b) Let $n \geq a$ be an integer. Thus, $n - a \in \mathbb{N}$. Now, we claim that

$$\sum_{j=a}^{n} \binom{n}{j} \binom{j}{a} \binom{n-j}{b} = \binom{n}{a} \binom{n-a}{b} 2^{n-a-b}. \tag{7}$$

[*Proof of (7):* First of all, (7) holds if $n - a - b < 0$ [1]. Hence, for the rest of this proof, we WLOG assume that we don't have $n - a - b < 0$. Thus, we have $n - a - b \geq 0$, so that $n - a - b \in \mathbb{N}$. Thus, we have $n - a \in \mathbb{N}$ and $n - a - b \in \mathbb{N}$ and $n - a \geq n - a - b$ (since $b \geq 0$). Hence, Proposition 0.7 (applied to $m = n - a - b$ and $p = n - a$) yields

$$\sum_{k=0}^{n-a} \binom{n-a-b}{k} = 2^{n-a-b}.$$

[1] *Proof.* Assume that $n - a - b < 0$. Thus, $n - a < b$. Hence, Proposition 0.2 (applied to $n - a$ and b instead of m and n) shows that $\binom{n-a}{b} = 0$ (since $n - a \in \mathbb{N}$). But

$$\begin{aligned}\sum_{j=a}^{n} \underbrace{\binom{n}{j} \binom{j}{a} \binom{n-j}{b}}_{\substack{=\binom{n}{a}\binom{n-a}{b}\binom{n-a-b}{j-a} \\ \text{(by Exercise 2 (a))}}} &= \sum_{j=a}^{n} \binom{n}{a} \underbrace{\binom{n-a}{b}}_{=0} \binom{n-a-b}{j-a} \\ &= \sum_{j=a}^{n} \binom{n}{a} 0 \binom{n-a-b}{j-a} = 0.\end{aligned}$$

Comparing this with

$$\binom{n}{a} \underbrace{\binom{n-a}{b}}_{=0} 2^{n-a-b} = 0,$$

we obtain $\sum\limits_{j=a}^{n} \binom{n}{j} \binom{j}{a} \binom{n-j}{b} = \binom{n}{a} \binom{n-a}{b} 2^{n-a-b}$. Hence, (7) is proven under the assumption that $n - a - b < 0$.

Now,

$$\begin{aligned}
&\sum_{j=a}^{n} \underbrace{\binom{n}{j}\binom{j}{a}\binom{n-j}{b}}_{\substack{=\binom{n}{a}\binom{n-a}{b}\binom{n-a-b}{j-a} \\ \text{(by Exercise 2 (a))}}} \\
&= \sum_{j=a}^{n} \binom{n}{a}\binom{n-a}{b}\binom{n-a-b}{j-a} = \binom{n}{a}\binom{n-a}{b}\sum_{j=a}^{n}\binom{n-a-b}{j-a} \\
&= \binom{n}{a}\binom{n-a}{b}\underbrace{\sum_{k=0}^{n-a}\binom{n-a-b}{k}}_{=2^{n-a-b}} \\
&\qquad \text{(here, we have substituted } k \text{ for } j-a \text{ in the sum)} \\
&= \binom{n}{a}\binom{n-a}{b}2^{n-a-b}.
\end{aligned}$$

This proves (7).] □

0.2. Counting lacunar subsets by size

Recall the concept of lacunar sets, as defined in homework set 1. Recall also the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ defined by $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. Exercise 4 **(c)** on homework set 1 told us that the number $g(n)$ of all lacunar subsets of $[n]$ is f_{n+2}. We shall now see more.

Exercise 3. Let $n \in \mathbb{N}$.

(a) For any $k \in \{0, 1, \ldots, n+1\}$, prove that the number of all lacunar k-element subsets of $[n]$ is $\dbinom{n-k+1}{k}$.

[Notice that this equals 0 whenever $2k > n+1$. You shouldn't need a separate argument for this case, but make sure you understand why the 0 is not surprising.]

(b) Conclude that

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

Remark 0.8. Exercise 3 **(a)** fails to hold when $k > n+1$. In fact, in this case, the number of all lacunar k-element subsets of $[n]$ is 0, whereas the binomial coefficient $\dbinom{n-k+1}{k}$ is nonzero (since $n-k+1$ is a negative integer).

Solution to Exercise 3. **(a)** *First solution to Exercise 3* ***(a)*** *(sketched):* Let $k \in \{0, 1, \ldots, n+1\}$. Thus, $n - k + 1 \in \mathbb{N}$.

Let $\operatorname{Lac}_k(n)$ be the set of all lacunar k-element subsets of $[n]$. Thus, the number of all lacunar k-element subsets of $[n]$ is $|\operatorname{Lac}_k(n)|$.

For any set S, we let $\mathcal{P}_k(S)$ be the set of all k-element subsets of S. Thus, $|\mathcal{P}_k(S)| = \dbinom{|S|}{k}$ for any finite set S. Applying this to $S = [n-k+1]$, we obtain

$$|\mathcal{P}_k([n-k+1])| = \binom{|[n-k+1]|}{k} = \binom{n-k+1}{k}$$

(since $|[n-k+1]| = n-k+1$ [2]).

Now, we are going to construct a bijection from $\operatorname{Lac}_k(n)$ to $\mathcal{P}_k([n-k+1])$.

Namely, we define a map $\Phi : \operatorname{Lac}_k(n) \to \mathcal{P}_k([n-k+1])$ as follows: For every lacunar k-element subset $S = \{s_1 < s_2 < \cdots < s_k\}$ [3] of $[n]$, we let $\Phi(S)$ be the k-element subset

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

of $[n-k+1]$. It is fairly easy to see that this is well-defined; visually speaking, what the map Φ does is "herding the elements of S closer together", or, to be a bit more specific, moving each element of S (except for the first one) one step closer to its neighbor on the left (thus making each gap between two neighboring elements of S shorter by 1). The reason why the resulting set is still a k-element set is that there was at least one "empty spot" between any two neighboring elements of S (since S is lacunar), and so the "herding" does not cause any two elements to collide.

An inverse to the map Φ is easily constructed. Namely, we define a map $\Psi : \mathcal{P}_k([n-k+1]) \to \operatorname{Lac}_k(n)$ as follows: For every k-element subset $T = \{t_1 < t_2 < \cdots < t_k\}$ of $[n-k+1]$, we let $\Psi(T)$ be the lacunar k-element subset

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

of $[n]$. Again, it is easy to check that this is well-defined (the resulting subset $\Psi(T)$ is built from T by "spreading the elements of T further apart", making each gap between two neighboring elements of T longer by 1; thus, $\Psi(T)$ is lacunar).

Finally, it is more-or-less obvious that the maps Φ and Ψ are mutually inverse, and therefore bijections. Hence, we have found a bijection $\operatorname{Lac}_k(n) \to \mathcal{P}_k([n-k+1])$ (namely, Φ); this allows us to conclude that $|\operatorname{Lac}_k(n)| = |\mathcal{P}_k([n-k+1])| = \dbinom{n-k+1}{k}$.

[2] This follows from $n-k+1 \in \mathbb{N}$. The reason why I am spelling out this obvious argument in such detail is that it hides a slippery point: If we hadn't assumed $k \in \{0, 1, \ldots, n+1\}$, then $n-k+1$ could be negative, and then $|[n-k+1]|$ would equal 0 rather than $n-k+1$, which would render the whole proof incorrect.

[3] I hope that this notation ("$S = \{s_1 < s_2 < \cdots < s_k\}$") is self-explanatory. If not, let me spell it out: By saying "$S = \{s_1 < s_2 < \cdots < s_k\}$", I mean that $s_1, s_2, \ldots, s_k$ are all the elements of S in increasing order (in other words, I mean that $S = \{s_1, s_2, \ldots, s_k\}$ and $s_1 < s_2 < \cdots < s_k$).

Hence, the number of all lacunar k-element subsets of $[n]$ is $|\operatorname{Lac}_k(n)| = \dbinom{n-k+1}{k}$. This solves Exercise 3 **(a)**.

Second solution to Exercise 3 ***(a)*** *(sketched):* Let us also show how Exercise 3 **(a)** can be proven by strong induction over n. More precisely, we proceed as follows: Let us first forget that we fixed n. For each $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$, we let $g_k(n)$ denote the number of all lacunar k-element subsets of $[n]$. (Here, $[n]$ is understood to be $\varnothing$ when n is negative.) Now we claim that the following recursive formula holds (similar to the answer to Exercise 4 **(b)** on homework set 1):

> *Claim 1:* We have $g_k(n) = g_k(n-1) + g_{k-1}(n-2)$ for all $n \geq 1$ and $k \in \mathbb{Z}$.

The proof of Claim 1 is almost completely analogous to the solution to Exercise 4 **(b)** on homework set 1:

[*Proof of Claim 1:* Let $n \geq 1$ and $k \in \mathbb{Z}$. The definition of $g_k(n)$ yields

$$\begin{aligned} g_k(n) &= (\text{the number of lacunar } k\text{-element subsets of } [n]) \\ &= |\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k\}| . \end{aligned} \tag{8}$$

Similarly,

$$g_k(n-1) = |\{S \subseteq [n-1] \mid S \text{ is lacunar, and } |S| = k\}| \tag{9}$$

and

$$g_{k-1}(n-2) = |\{S \subseteq [n-2] \mid S \text{ is lacunar, and } |S| = k-1\}| . \tag{10}$$

Now, the lacunar k-element subsets of $[n]$ that don't contain n are precisely the lacunar k-element subsets of $[n-1]$ (because a subset of $[n]$ that doesn't contain n is nothing other than a subset of $[n-1]$). In other words,

$$\begin{aligned} &\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \notin S\} \\ &= \{S \subseteq [n-1] \mid S \text{ is lacunar, and } |S| = k\} . \end{aligned}$$

Therefore,

$$\begin{aligned} &|\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \notin S\}| \\ &= |\{S \subseteq [n-1] \mid S \text{ is lacunar, and } |S| = k\}| = g_k(n-1) \end{aligned} \tag{11}$$

(by (9)).

On the other hand, consider the lacunar k-element subsets of $[n]$ that do contain n. If T is such a subset, then $T \setminus \{n\}$ is a lacunar $(k-1)$-element subset of $[n-2]$ [4]. Hence, we can define a map

$$\begin{aligned} \alpha : \{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \in S\} \\ \to \{S \subseteq [n-2] \mid S \text{ is lacunar, and } |S| = k-1\} , \\ T \mapsto T \setminus \{n\} . \end{aligned}$$

[4] *Proof.* Let T be a lacunar k-element subset of $[n]$ that contains n. We must prove that $T \setminus \{n\}$ is a lacunar $(k-1)$-element subset of $[n-2]$.

On the other hand, if R is any lacunar $(k-1)$-element subset of $[n-2]$, then $R \cup \{n\}$ is a lacunar k-element subset of $[n]$ [5] and satisfies $n \in R \cup \{n\}$. Hence, we can define a map

$$\begin{aligned} \beta : \{S \subseteq [n-2] \mid S \text{ is lacunar, and } |S| = k-1\} \\ \to \{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \in S\}, \\ R \mapsto R \cup \{n\}. \end{aligned}$$

The two maps α and β we have just defined are mutually inverse[6], and thus are bijections. Hence, we have found a bijection from

---

Clearly, any subset of a lacunar set is lacunar. Thus, the set $T \setminus \{n\}$ is lacunar (since it is a subset of the lacunar set T).

Also, T contains n. Hence, $|T \setminus \{n\}| = |T| - 1 = k - 1$ (since $|T| = k$ (since T is a k-element set)). In other words, $T \setminus \{n\}$ is a $(k-1)$-element set.

Recall that the set T is lacunar. In other words, there exists no $i \in \mathbb{Z}$ such that both i and $i+1$ belong to T. Applying this to $i = n-1$, we conclude that $n-1$ and $(n-1)+1$ cannot both belong to T. In other words, $n-1$ and n cannot both belong to T. Since n does belong to T (by definition of T), we thus conclude that $n-1$ cannot belong to T. In other words, $n-1 \notin T$. Hence, $n-1 \notin T \setminus \{n\}$.

Now we know that $T \setminus \{n\}$ is a subset of $[n]$ (since $T \setminus \{n\} \subseteq T \subseteq [n]$) that contains neither $n-1$ nor n (since $n-1 \notin T \setminus \{n\}$ and $n \notin T \setminus \{n\}$). In other words, $T \setminus \{n\}$ is a subset of $[n] \setminus \{n-1, n\} = [n-2]$. Thus, $T \setminus \{n\}$ is a lacunar $(k-1)$-element subset of $[n-2]$ (since we already know that $T \setminus \{n\}$ is lacunar and is a $(k-1)$-element set).

[5] *Proof.* Let R be a lacunar $(k-1)$-element subset of $[n-2]$. We must prove that $R \cup \{n\}$ is a lacunar k-element subset of $[n]$.

Clearly, $R \subseteq [n-2] \subseteq [n]$ and $\{n\} \subseteq [n]$. Thus, $\underbrace{R}_{\subseteq [n]} \cup \underbrace{\{n\}}_{\subseteq [n]} \subseteq [n] \cup [n] = [n]$. Hence, $R \cup \{n\}$ is a subset of $[n]$. Moreover, $n \notin R$ (because otherwise, we would have $n \in R \subseteq [n-2]$, so that $n \leq n-2$, which would contradict $n > n-2$). Hence, $|R \cup \{n\}| = |R| + 1 = k$ (since $|R| = k-1$ (since R is a $(k-1)$-element set)). Thus, $R \cup \{n\}$ is a k-element subset of $[n]$ (since $R \cup \{n\}$ is a subset of $[n]$).

It remains to prove that R is lacunar.

Indeed, let $i \in \mathbb{Z}$ be such that both i and $i+1$ belong to $R \cup \{n\}$. We shall derive a contradiction.

We have $i + 1 \in R \cup \{n\} \subseteq [n]$, so that $i + 1 \leq n$, hence $i \leq n-1$ and therefore $i \neq n$. Combining this with $i \in R \cup \{n\}$, we obtain $i \in (R \cup \{n\}) \setminus \{n\} \subseteq R$. In other words, i belongs to R.

It is impossible that both i and $i+1$ belong to R (because R is lacunar). Hence, at least one of i and $i+1$ does not belong to R. Since we know that i belongs to R, we thus conclude that $i+1$ does not belong to R. Combining this with $i+1 \in R \cup \{n\}$, we obtain $i+1 \in (R \cup \{n\}) \setminus R \subseteq \{n\}$, so that $i+1 = n$. Hence, $i = n-1$. But $i \in R \subseteq [n-2]$, so that $i \leq n-2 < n-1$. This contradicts $i = n-1$.

Now, forget that we fixed i. We thus have obtained a contradiction for each $i \in \mathbb{Z}$ such that both i and $i+1$ belong to $R \cup \{n\}$. Hence, there exists no $i \in \mathbb{Z}$ such that both i and $i+1$ belong to $R \cup \{n\}$. In other words, the set $R \cup \{n\}$ is lacunar. Thus, $R \cup \{n\}$ is a lacunar k-element subset of $[n]$.

[6] This is easy to check: For example, each $T \in \{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \in S\}$ is easily seen to satisfy $(\beta \circ \alpha)(T) = (T \setminus \{n\}) \cup \{n\} = T$, because of $n \in T$; therefore, $\beta \circ \alpha = \text{id}$. Also, each $R \in \{S \subseteq [n-2] \mid S \text{ is lacunar, and } |S| = k-1\}$ is easily seen to satisfy $(\alpha \circ \beta)(R) = (R \cup \{n\}) \setminus \{n\} = R$, because of $n \notin R$ (which in turn is a consequence of $R \subseteq [n-2]$); thus, $\alpha \circ \beta = \text{id}$.

$\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \in S\}$ to
$\{S \subseteq [n-2] \mid S \text{ is lacunar, and } |S| = k-1\}$. Thus,

$$\begin{aligned} &|\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \in S\}| \\ &= |\{S \subseteq [n-2] \mid S \text{ is lacunar, and } |S| = k-1\}| = g_{k-1}(n-2) \end{aligned} \tag{12}$$

(by (10)).

Now, (8) becomes

$$\begin{aligned} g_k(n) &= |\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k\}| \\ &= \underbrace{|\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \notin S\}|}_{\substack{=g_k(n-1) \\ \text{(by (11))}}} \\ &\qquad + \underbrace{|\{S \subseteq [n] \mid S \text{ is lacunar, and } |S| = k \text{ and } n \in S\}|}_{\substack{=g_{k-1}(n-2) \\ \text{(by (12))}}} \\ &\qquad \left(\begin{array}{c} \text{since each } S \subseteq [n] \text{ satisfies either } n \notin S \text{ or } n \in S \\ \text{(but not both)} \end{array}\right) \\ &= g_k(n-1) + g_{k-1}(n-2). \end{aligned}$$

This proves Claim 1.]

Now, we claim the following:

Claim 2: Let $n \in \{-1, 0, 1, 2, \ldots\}$. Then, each $k \in \{0, 1, \ldots, n+1\}$ satisfies

$$g_k(n) = \binom{n-k+1}{k}.$$

Notice that we allowed n to be -1 in Claim 2 in order to have a smoother induction step in the proof.

[*Proof of Claim 2:* Let us prove Claim 2 by strong induction on n.

Here is the induction step: Fix any $m \in \{-1, 0, 1, 2, \ldots\}$. Assume (as the induction hypothesis) that Claim 2 holds whenever $n < m$. We must prove that Claim 2 holds for $n = m$. In other words, we must prove that every $k \in \{0, 1, \ldots, m+1\}$ satisfies $g_k(m) = \binom{m-k+1}{k}$.

Let $k \in \{0, 1, \ldots, m+1\}$. We must show that $g_k(m) = \binom{m-k+1}{k}$. If $k = 0$, then this is obvious[7]. Hence, we WLOG assume that $k \neq 0$.

[7] *Proof.* The only 0-element subset of $[m]$ is the empty set $\varnothing$. Thus, there is only one lacunar 0-element subset of $[m]$, namely the empty set $\varnothing$ (since $\varnothing$ is clearly lacunar).

The definition of $g_0(m)$ yields

$$g_0(m) = (\text{the number of all lacunar 0-element subsets of } [m]) = 1$$

We also clearly have $g_k(m) = \dbinom{m-k+1}{k}$ if $k = m+1$ [8]. Hence, we WLOG assume that $k \neq m+1$.

Combining $k \in \{0,1,\ldots,m+1\}$ with $k \neq 0$, we obtain $k \in \{0,1,\ldots,m+1\} \setminus \{0\} = \{1,2,\ldots,m+1\} = [m+1]$. Combining this with $k \neq m+1$, we find $k \in [m+1] \setminus \{m+1\} = [m]$. Hence, $1 \leq k \leq m$, so that $m \geq 1$. Therefore, both $m-1$ and $m-2$ are elements of $\{-1,0,1,2,\ldots\}$. In particular $m-1$ is an element of $\{-1,0,1,2,\ldots\}$ satisfying $m-1 < m$; thus, Claim 2 holds for $n = m-1$ (by our induction hypothesis). Hence, we can apply Claim 2 to $m-1$ instead of m (because $k \in [m] \subseteq \{0,1,\ldots,m\} = \{0,1,\ldots,(m-1)+1\}$). We conclude that

$$g_k(m-1) = \binom{(m-1)-k+1}{k} = \binom{m-k}{k}.$$

Also, $k \in [m] = \{1,2,\ldots,m\}$, so that $k-1 \in \{0,1,\ldots,m-1\} = \{0,1,\ldots,(m-2)+1\}$. But $m-2$ is an element of $\{-1,0,1,2,\ldots\}$ satisfying $m-2 < m$; thus, Claim 2 holds for $n = m-2$ (by our induction hypothesis). Therefore, we can apply Claim 2 to $m-2$ and $k-1$ instead of m and k (since $k-1 \in \{0,1,\ldots,(m-2)+1\}$). We conclude that

$$g_{k-1}(m-2) = \binom{(m-2)-(k-1)+1}{k-1} = \binom{m-k}{k-1}.$$

But $m \geq 1$. Hence, Claim 1 (applied to $n = m$) yields

$$\begin{aligned} g_k(m) &= \underbrace{g_k(m-1)}_{=\binom{m-k}{k}} + \underbrace{g_{k-1}(m-2)}_{=\binom{m-k}{k-1}} \\ &= \binom{m-k}{k} + \binom{m-k}{k-1} = \binom{m-k}{k-1} + \binom{m-k}{k}. \end{aligned}$$

(since there is only one lacunar 0-element subset of $[m]$). Comparing this with $\dbinom{m-0+1}{0} = 1$, we obtain $g_0(m) = \dbinom{m-0+1}{0}$. In other words, $g_k(m) = \dbinom{m-k+1}{k}$ holds for $k = 0$. Qed.

[8] *Proof.* There exist no $(m+1)$-element subsets of $[m]$ (since the set $[m]$ has only m elements). In particular, there exist no lacunar $(m+1)$-element subsets of $[m]$.

The definition of $g_{m+1}(m)$ yields

$$g_{m+1}(m) = (\text{the number of all lacunar } (m+1)\text{-element subsets of } [m]) = 0$$

(since there exist no lacunar $(m+1)$-element subsets of $[m]$). Comparing this with

$$\begin{aligned} \binom{m-(m+1)+1}{m+1} &= \binom{0}{m+1} = [m+1=0] \qquad \left(\text{since } \binom{0}{g} = [g=0] \text{ for each } g \in \mathbb{N}\right) \\ &= 0 \qquad (\text{since we don't have } m+1=0), \end{aligned}$$

we obtain $g_{m+1}(m) = \dbinom{m-(m+1)+1}{m+1}$. In other words, $g_k(m) = \dbinom{m-k+1}{k}$ holds for $k = m+1$. Qed.

Meanwhile, Proposition 0.3 (applied to $m-k+1$ and k instead of m and n) shows that

$$\binom{m-k+1}{k} = \binom{(m-k+1)-1}{k-1} + \binom{(m-k+1)-1}{k} = \binom{m-k}{k-1} + \binom{m-k}{k}.$$

Comparing these two equalities, we find that $g_k(m) = \binom{m-k+1}{k}$.

Now, forget that we fixed k. We thus have shown that every $k \in \{0,1,\ldots,m+1\}$ satisfies $g_k(m) = \binom{m-k+1}{k}$. Thus, the induction step is complete, so that Claim 2 is proven by strong induction.]

Now that Claim 2 is proven, we have solved Exercise 3 **(a)**.

(b) Fix $n \in \mathbb{N}$. The size of any subset of $[n]$ is an integer between 0 and n (inclusive). Thus, in particular, the size of any lacunar subset of $[n]$ is an integer between 0 and n (inclusive).

Let $g(n)$ denote the number of all lacunar subsets of $[n]$. Then, Exercise 4 **(c)** on homework set 1 shows that $g(n) = f_{n+2}$. Hence,

$$\begin{aligned} f_{n+2} = g(n) &= (\text{the number of all lacunar subsets of } [n]) \\ &\qquad (\text{by the definition of } g(n)) \\ &= \sum_{k=0}^{n} \underbrace{(\text{the number of all lacunar subsets of } [n] \text{ having size } k)}_{\substack{=(\text{the number of all lacunar } k\text{-element subsets of } [n]) \\ = \binom{n-k+1}{k} \\ (\text{by Exercise 3 (a)})}} \\ &\qquad \left(\begin{array}{c} \text{because the size of a lacunar subset of } [n] \\ \text{is an integer between 0 and } n \text{ (inclusive)} \end{array}\right) \\ &= \sum_{k=0}^{n} \binom{n-k+1}{k}. \end{aligned}$$

This solves Exercise 3 **(b)**. □

0.3. A formula for the $\operatorname{sur}(n,k)$ numbers

Recall that if $n \in \mathbb{N}$ and $k \in \mathbb{N}$, then $\operatorname{sur}(n,k)$ denotes the number of surjections $[n] \to [k]$. In class, we have shown the following two recursive formulas:

- We have

$$\operatorname{sur}(n,0) = [n=0] \qquad \text{for all } n \in \mathbb{N},$$

  and

$$\operatorname{sur}(n,k) = \sum_{j=0}^{n-1} \binom{n}{j} \operatorname{sur}(j,k-1) \qquad \text{for all } n \in \mathbb{N} \text{ and } k > 0. \tag{13}$$

- We have
$$\operatorname{sur}(n,0) = [n=0] \qquad \text{for all } n \in \mathbb{N}, \tag{14}$$
$$\operatorname{sur}(0,k) = [k=0] \qquad \text{for all } k \in \mathbb{N}, \tag{15}$$
and
$$\operatorname{sur}(n,k) = k\left(\operatorname{sur}(n-1,k) + \operatorname{sur}(n-1,k-1)\right) \qquad \text{for all } n > 0 \text{ and } k > 0.$$

Exercise 4. Prove that
$$\operatorname{sur}(n,k) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n$$
for every $n \in \mathbb{N}$ and $k \in \mathbb{N}$.

Before we come to the solution of this exercise, let us recall the *binomial formula*:

Proposition 0.9. Let $n \in \mathbb{N}$. Let $x, y \in \mathbb{Q}$. Then,
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

We will use this formula via two simple corollaries:

Corollary 0.10. Let $n \in \mathbb{N}$. Then, $\sum\limits_{i=0}^{n} (-1)^{n-i} \binom{n}{i} = [n=0]$.

Proof of Corollary 0.10. Applying Proposition 0.9 to $x = 1$ and $y = -1$, we obtain
$$(1+(-1))^n = \sum_{k=0}^{n} \binom{n}{k} \underbrace{1^k}_{=1} (-1)^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k}$$
$$= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i}$$
(here, we have renamed the summation index k as i). Thus,
$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} = \Big(\underbrace{1+(-1)}_{=0}\Big)^n = 0^n = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases}.$$
Comparing this with $[n=0] = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases}$ (this follows from the definition of the truth value $[n=0]$), we obtain $\sum\limits_{i=0}^{n} (-1)^{n-i} \binom{n}{i} = [n=0]$. This proves Corollary 0.10. $\square$

Corollary 0.11. Let $x \in \mathbb{Q}$ and $n \in \mathbb{N}$. Then,

$$(x+1)^n - x^n = \sum_{j=0}^{n-1} \binom{n}{j} x^j.$$

Proof of Corollary 0.11. Applying Proposition 0.9 to $y = 1$, we obtain

$$\begin{aligned}(x+1)^n &= \sum_{k=0}^{n} \binom{n}{k} x^k \underbrace{1^{n-k}}_{=1} = \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{j=0}^{n} \binom{n}{j} x^j \\ &\qquad \text{(here, we have renamed the summation index } k \text{ as } j) \\ &= \sum_{j=0}^{n-1} \binom{n}{j} x^j + \underbrace{\binom{n}{n}}_{\substack{=1 \\ \text{(by Proposition 0.4)}}} x^n = \sum_{j=0}^{n-1} \binom{n}{j} x^j + x^n.\end{aligned}$$

Subtracting x^n from this equality, we find $(x+1)^n - x^n = \sum_{j=0}^{n-1} \binom{n}{j} x^j$. This proves Corollary 0.11. □

Solution to Exercise 4 (sketched). We shall solve Exercise 4 by strong induction over n:

Induction step: Let $m \in \mathbb{N}$. Assume that Exercise 4 holds for all $n < m$. We must now prove that Exercise 4 holds for $n = m$.

We have assumed that Exercise 4 holds for $n < m$. In other words, we have

$$\operatorname{sur}(n,k) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^n \qquad (16)$$

for every $n \in \mathbb{N}$ and $k \in \mathbb{N}$ satisfying $n < m$.

Now, let $k \in \mathbb{N}$. We are going to prove that

$$\operatorname{sur}(m,k) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^m. \qquad (17)$$

[*Proof of (17):* If $m = 0$, then (17) is easy to check[9]. Hence, for the rest of this

[9] *Proof.* Assume that $m = 0$. Then,

$$\begin{aligned}\sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^m &= \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} \underbrace{i^0}_{=1} \qquad (\text{since } m = 0) \\ &= \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} = [k = 0] \qquad (\text{by Corollary 0.10, applied to } n = k) \\ &= \operatorname{sur}(0,k) \qquad (\text{by (15)}) \\ &= \operatorname{sur}(m,k) \qquad (\text{since } 0 = m).\end{aligned}$$

Thus, we have proven (17) under the assumption that $m = 0$.

proof, we WLOG assume that $m \neq 0$. Hence, $m \in \{1, 2, 3, \ldots\}$ (since $m \in \mathbb{N}$), so that $m > 0$. Since $m \neq 0$, we have $[m = 0] = 0$.

If $k = 0$, then (17) is also easy to check[10]. Hence, for the rest of this proof, we WLOG assume that $k \neq 0$. Hence, $k \in \{1, 2, 3, \ldots\}$ (since $k \in \mathbb{N}$), so that $k > 0$. Hence, $k - 1 \in \mathbb{N}$.

Applying (13) to $n = m$, we find

$$\begin{aligned}
\operatorname{sur}(m,k) &= \sum_{j=0}^{m-1} \binom{m}{j} \underbrace{\operatorname{sur}(j, k-1)}_{\substack{= \sum\limits_{i=0}^{k-1} (-1)^{(k-1)-i} \binom{k-1}{i} i^j \\ \text{(by (16), applied to } j \text{ and } k-1 \\ \text{instead of } n \text{ and } k \text{ (since } j \leq m-1 < m,\ j \in \mathbb{N} \text{ and } k-1 \in \mathbb{N}))}} \\
&= \sum_{j=0}^{m-1} \binom{m}{j} \sum_{i=0}^{k-1} (-1)^{(k-1)-i} \binom{k-1}{i} i^j = \underbrace{\sum_{j=0}^{m-1} \sum_{i=0}^{k-1}}_{= \sum_{i=0}^{k-1} \sum_{j=0}^{m-1}} \binom{m}{j} (-1)^{(k-1)-i} \binom{k-1}{i} i^j \\
&= \sum_{i=0}^{k-1} \sum_{j=0}^{m-1} \binom{m}{j} (-1)^{(k-1)-i} \binom{k-1}{i} i^j \\
&= \sum_{i=0}^{k-1} (-1)^{(k-1)-i} \binom{k-1}{i} \sum_{j=0}^{m-1} \binom{m}{j} i^j. \qquad (18)
\end{aligned}$$

It is easy to show that

$$\binom{k-1}{k} k^m = 0 \qquad (19)$$

[11].

[10] *Proof.* Assume that $k = 0$. Thus, $\operatorname{sur}(m,k) = \operatorname{sur}(m,0) = [m = 0]$ (by (14), applied to $n = m$). But from $k = 0$, we also conclude that

$$\begin{aligned}
\sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^m &= \sum_{i=0}^{0} (-1)^{0-i} \binom{0}{i} i^m = \underbrace{(-1)^{0-0}}_{=1} \underbrace{\binom{0}{0}}_{=1} 0^m = 0^m = 0 \qquad (\text{since } m > 0) \\
&= [m = 0] = \operatorname{sur}(m,k).
\end{aligned}$$

Thus, we have proven (17) under the assumption that $k = 0$.

[11] *Proof of (19):* If $k = 0$, then this follows from $\binom{k-1}{k} \underbrace{k^m}_{\substack{=0^m \\ (\text{since } k=0)}} = \binom{k-1}{k} \underbrace{0^m}_{\substack{=0 \\ (\text{since } m>0)}} = 0$. Thus, for the rest of this proof, we WLOG assume that $k \neq 0$. Hence, $k \in \{1, 2, 3, \ldots\}$ (since $k \in \mathbb{N}$), so that $k - 1 \in \mathbb{N}$. Therefore, Proposition 0.2 (applied to $k - 1$ and k instead of m and n) shows that $\binom{k-1}{k} = 0$ (since $k - 1 < k$). Hence, $\underbrace{\binom{k-1}{k}}_{=0} k^m = 0$. This proves (19).

Now, every $g \in \mathbb{Z}$ satisfies

$$\begin{aligned}
\sum_{i=0}^{k} (-1)^{k-i} \binom{g}{i} i^m &= \sum_{i=1}^{k} (-1)^{k-i} \binom{g}{i} i^m + (-1)^{k-0} \binom{g}{0} \underbrace{0^m}_{\substack{=0 \\ \text{(since } m>0)}} \\
&= \sum_{i=1}^{k} (-1)^{k-i} \binom{g}{i} i^m + \underbrace{(-1)^{k-0} \binom{g}{0} 0}_{=0} \\
&= \sum_{i=1}^{k} (-1)^{k-i} \binom{g}{i} i^m . \qquad (20)
\end{aligned}$$

Applying this to $g = k$, we obtain

$$\begin{aligned}
\sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^m &= \sum_{i=1}^{k} (-1)^{k-i} \underbrace{\binom{k}{i}}_{\substack{= \binom{k-1}{i-1} + \binom{k-1}{i} \\ \text{(by Proposition 0.3, applied to } k \text{ and } i \\ \text{instead of } m \text{ and } n)}} i^m \\
&= \sum_{i=1}^{k} (-1)^{k-i} \left(\binom{k-1}{i-1} + \binom{k-1}{i} \right) i^m \\
&= \sum_{i=1}^{k} (-1)^{k-i} \binom{k-1}{i-1} i^m + \sum_{i=1}^{k} (-1)^{k-i} \binom{k-1}{i} i^m . \qquad (21)
\end{aligned}$$

But

$$\begin{aligned}
\sum_{i=1}^{k} (-1)^{k-i} \binom{k-1}{i-1} i^m &= \sum_{i=0}^{k-1} \underbrace{(-1)^{k-(i+1)}}_{=(-1)^{k-i-1}} \underbrace{\binom{k-1}{(i+1)-1}}_{= \binom{k-1}{i}} (i+1)^m \\
&\qquad \left(\text{here, we have substituted } i+1 \text{ for } i \text{ in the sum}\right) \\
&= \sum_{i=0}^{k-1} (-1)^{k-i-1} \binom{k-1}{i} (i+1)^m . \qquad (22)
\end{aligned}$$

Also, (20) (applied to $g = k-1$) yields

$$\sum_{i=0}^{k} (-1)^{k-i} \binom{k-1}{i} i^m = \sum_{i=1}^{k} (-1)^{k-i} \binom{k-1}{i} i^m ,$$

and thus we have

$$\begin{aligned}
\sum_{i=1}^{k}(-1)^{k-i}\binom{k-1}{i}i^m &= \sum_{i=0}^{k}(-1)^{k-i}\binom{k-1}{i}i^m \\
&= \sum_{i=0}^{k-1}\underbrace{(-1)^{k-i}}_{=-(-1)^{k-i-1}}\binom{k-1}{i}i^m + (-1)^{k-k}\underbrace{\binom{k-1}{k}k^m}_{\substack{=0 \\ \text{(by (19))}}} \\
&= \sum_{i=0}^{k-1}\left(-(-1)^{k-i-1}\right)\binom{k-1}{i}i^m + \underbrace{(-1)^{k-k}0}_{=0} \\
&= \sum_{i=0}^{k-1}\left(-(-1)^{k-i-1}\right)\binom{k-1}{i}i^m \\
&= -\sum_{i=0}^{k-1}(-1)^{k-i-1}\binom{k-1}{i}i^m. \qquad (23)
\end{aligned}$$

Now, (21) becomes

$$\begin{aligned}
&\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^m \\
&= \underbrace{\sum_{i=1}^{k}(-1)^{k-i}\binom{k-1}{i-1}i^m}_{\substack{=\sum_{i=0}^{k-1}(-1)^{k-i-1}\binom{k-1}{i}(i+1)^m \\ \text{(by (22))}}} + \underbrace{\sum_{i=1}^{k}(-1)^{k-i}\binom{k-1}{i}i^m}_{\substack{=-\sum_{i=0}^{k-1}(-1)^{k-i-1}\binom{k-1}{i}i^m \\ \text{(by (23))}}} \\
&= \sum_{i=0}^{k-1}(-1)^{k-i-1}\binom{k-1}{i}(i+1)^m + \left(-\sum_{i=0}^{k-1}(-1)^{k-i-1}\binom{k-1}{i}i^m\right) \\
&= \sum_{i=0}^{k-1}(-1)^{k-i-1}\binom{k-1}{i}(i+1)^m - \sum_{i=0}^{k-1}(-1)^{k-i-1}\binom{k-1}{i}i^m \\
&= \sum_{i=0}^{k-1}\underbrace{(-1)^{k-i-1}}_{=(-1)^{(k-1)-i}}\binom{k-1}{i}\underbrace{\left((i+1)^m - i^m\right)}_{\substack{=\sum_{j=0}^{m-1}\binom{m}{j}i^j \\ \text{(by Corollary 0.11, applied to } m \\ \text{and } i \text{ instead of } n \text{ and } x)}} \\
&= \sum_{i=0}^{k-1}(-1)^{(k-1)-i}\binom{k-1}{i}\sum_{j=0}^{m-1}\binom{m}{j}i^j.
\end{aligned}$$

Comparing this with (18), we obtain

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

This proves (17).]

Now, forget that we fixed k. We thus have proven that $\operatorname{sur}(m,k) = \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i} i^m$ for every $k \in \mathbb{N}$. In other words, Exercise 4 holds for $n = m$. This completes the induction step. Thus, Exercise 4 is solved. □

0.4. "Oddlike" permutations

> **Exercise 5.** Let $n \in \mathbb{N}$. Let me call a permutation of $[n]$ *oddlike* if it sends every odd element of $[n]$ to an odd element of $[n]$. (For example, the permutation of $[5]$ sending $1,2,3,4,5$ to $3,4,5,2,1$ is oddlike.)
>
> **(a)** Prove that any oddlike permutation of $[n]$ must also send every even element of $[n]$ to an even element of $[n]$.
>
> **(b)** Find a formula for the number of oddlike permutations of $[n]$. [**Hint:** The answer may depend on the parity of n.]

Solution to Exercise 5 (sketched). **(a)** Let σ be any oddlike permutation of $[n]$. We must show that σ sends every even element of $[n]$ to an even element of $[n]$.

Let A be the set of all odd elements of $[n]$. The permutation σ is oddlike. In other words, σ sends every odd element of $[n]$ to an odd element of $[n]$ (by the definition of "oddlike"). In other words, σ sends every element of A to an element of A (because the elements of A are precisely the odd elements of $[n]$). In other words[12], $\sigma(A) \subseteq A$.

Let i be any even element of $[n]$. Then, $i \notin A$ (because i is even, whereas the elements of A are odd), and thus $|A \cup \{i\}| = |A| + 1$. On the other hand, the map σ is a permutation, thus a bijection; therefore, $|\sigma(S)| = |S|$ for each subset S of $[n]$. Applying this to $S = A \cup \{i\}$, we obtain $|\sigma(A \cup \{i\})| = |A \cup \{i\}| = |A| + 1 > |A|$.

Now, let us prove that $\sigma(i)$ is even. Indeed, assume the contrary. Thus, $\sigma(i)$ is odd. In other words, $\sigma(i) \in A$ (since A is the set of all odd elements of $[n]$). Now,

$$\sigma(A \cup \{i\}) = \underbrace{\sigma(A)}_{\subseteq A} \cup \underbrace{\sigma(\{i\})}_{\substack{=\{\sigma(i)\} \subseteq A \\ (\text{since } \sigma(i) \in A)}} \subseteq A \cup A = A.$$

Hence, $|\sigma(A \cup \{i\})| \leq |A|$ (because clearly, any subset B of A must satisfy $|B| \leq |A|$). This contradicts $|\sigma(A \cup \{i\})| > |A|$.

[12] Recall that if $f : X \to Y$ is a map between two sets, and if T is a subset of X, then $f(T)$ denotes the subset $\{f(t) \mid t \in T\}$ of Y.

We thus have found a contradiction. This contradiction shows that our assumption was wrong; thus, we have shown that $\sigma(i)$ is even.

Now, forget that we fixed i. We thus have proven that if i is any even element of $[n]$, then $\sigma(i)$ is even. In other words, σ sends every even element of $[n]$ to an even element of $[n]$. This solves Exercise 5 **(a)**.

(b) We *claim* that the number of oddlike permutations of $[n]$ is

$$\begin{cases} \left(\frac{n}{2}\right)!^2, & \text{if } n \text{ is even;} \\ \left(\frac{n-1}{2}\right)!\left(\frac{n+1}{2}\right)!, & \text{if } n \text{ is odd} \end{cases}.$$

Let us prove this claim. We must be in one of the following two cases:

Case 1: The number n is even.

Case 2: The number n is odd.

Let us consider Case 2 first. In this case, the number n is odd.

We want to count the oddlike permutations of $[n]$. In order to do so, we consider the following algorithm to create an oddlike permutation σ of $[n]$:

- First, we choose the values of σ at all odd elements of $[n]$ (that is, we choose the values $\sigma(1), \sigma(3), \sigma(5), \ldots, \sigma(n)$). The set $[n]$ has $\frac{n+1}{2}$ odd elements (namely, $1, 3, 5, \ldots, n$), and the permutation σ must send each of them to an odd element of $[n]$ again (because we want σ to be oddlike). Thus, there are $\frac{n+1}{2}$ choices for $\sigma(1)$, then $\frac{n+1}{2} - 1$ choices for $\sigma(3)$ (because $\sigma(3)$ must be distinct from $\sigma(1)$ [13]), then $\frac{n+1}{2} - 2$ choices for $\sigma(5)$ (because $\sigma(5)$ must be distinct from the two distinct numbers $\sigma(1)$ and $\sigma(3)$), and so on, until we finally have $\frac{n+1}{2} - \frac{n+1}{2} + 1 = 1$ choices for $\sigma(n)$. Altogether, we thus have

$$\frac{n+1}{2}\left(\frac{n+1}{2} - 1\right)\cdots 1 = \left(\frac{n+1}{2}\right)!$$

choices for the values $\sigma(1), \sigma(3), \sigma(5), \ldots, \sigma(n)$.

- Next, we choose the values of σ at all even elements of $[n]$ (that is, we choose the values $\sigma(2), \sigma(4), \sigma(6), \ldots, \sigma(n-1)$). The set $[n]$ has $\frac{n-1}{2}$ even elements (namely, $2, 4, 6, \ldots, n-1$), and (having already chosen $\frac{n+1}{2}$ values of σ) we have $n - \frac{n+1}{2} = \frac{n-1}{2}$ elements of $[n]$ left to choose our values from (since σ must not take any value twice). Thus, there are $\frac{n-1}{2}$ choices for

[13] Keep in mind that σ is a permutation, so any two values of σ at distinct elements must be distinct.

$\sigma(2)$, then $\dfrac{n-1}{2}-1$ choices for $\sigma(4)$ (because $\sigma(4)$ must be distinct from $\sigma(2)$), then $\dfrac{n-1}{2}-2$ choices for $\sigma(6)$ (because $\sigma(6)$ must be distinct from the two distinct numbers $\sigma(2)$ and $\sigma(4)$), and so on, until we finally have $\dfrac{n-1}{2}-\dfrac{n-1}{2}+1=1$ choices for $\sigma(n-1)$. Altogether, we thus have

$$\frac{n-1}{2}\left(\frac{n-1}{2}-1\right)\cdots 1=\left(\frac{n-1}{2}\right)!$$

choices for the values $\sigma(2), \sigma(4), \sigma(6), \ldots, \sigma(n-1)$.

This algorithm constructs every oddlike permutation of $[n]$ exactly once, and there are clearly $\left(\dfrac{n+1}{2}\right)!\left(\dfrac{n-1}{2}\right)!$ ways to make choices in this algorithm. Hence, the number of oddlike permutations of $[n]$ is

$$\left(\frac{n+1}{2}\right)!\left(\frac{n-1}{2}\right)!=\left(\frac{n-1}{2}\right)!\left(\frac{n+1}{2}\right)!=\begin{cases}\left(\dfrac{n}{2}\right)!^2, & \text{if } n \text{ is even;}\\ \left(\dfrac{n-1}{2}\right)!\left(\dfrac{n+1}{2}\right)!, & \text{if } n \text{ is odd}\end{cases}$$

(since n is odd). This proves our claim in Case 2.

The proof in Case 1 is analogous, except that now both $\dfrac{n+1}{2}$ and $\dfrac{n-1}{2}$ have to be replaced by $\dfrac{n}{2}$ (since the set $[n]$ has $\dfrac{n}{2}$ even elements and $\dfrac{n}{2}$ odd elements). Hence, the claim is finally proven in both cases. This solves Exercise 5 **(b)**. $\square$

0.5. Necklaces 1: rotating tuples

Definition 0.12. Let S be a set. Let $f : S \to S$ be a map from S to S. Then, for every $k \in \mathbb{N}$, the map $f^k : S \to S$ is defined to be

$$\underbrace{f\circ f\circ\cdots\circ f}_{k\text{ times}}.$$

For example, if $f : \mathbb{Z} \to \mathbb{Z}$ is the map $x \mapsto x^2$, then f^k is the map $x \mapsto \underbrace{\left(\left(\left(x^2\right)^2\right)\cdots\right)^2}_{k\text{ squarings}} = x^{\left(2^k\right)}$.

Note that $f^0=\underbrace{f\circ f\circ\cdots\circ f}_{0\text{ times}}=\mathrm{id}_S$, since a composition of no maps ("empty composition") is always understood as the identity map.

Exercise 6. Let S be a set. Let $f : S \to S$ be a map.

(a) Prove that $f^n \circ f^m = f^{n+m}$ for each $n, m \in \mathbb{N}$. [Yes, this is a one-liner; you don't need induction.]

(b) Let $g : S \to S$ be a further map such that $f \circ g = g \circ f$. Prove that $(f \circ g)^n = f^n \circ g^n$ for each $n \in \mathbb{N}$.

(c) Find an example in which the claim of **(b)** fails if we drop the assumption that $f \circ g = g \circ f$.

Solution to Exercise 6. **(a)** *First solution to Exercise 6 **(a)**.* Let $n, m \in \mathbb{N}$. The definition of f^{n+m} shows that

$$f^{n+m} = \underbrace{f \circ f \circ \cdots \circ f}_{n+m \text{ times}}.$$

Comparing this with

$$\underbrace{f^n}_{= \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}} \circ \underbrace{f^m}_{= \underbrace{f \circ f \circ \cdots \circ f}_{m \text{ times}}} = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}} \circ \underbrace{f \circ f \circ \cdots \circ f}_{m \text{ times}} = \underbrace{f \circ f \circ \cdots \circ f}_{n+m \text{ times}},$$

we obtain $f^n \circ f^m = f^{n+m}$. This solves Exercise 6 **(a)**.

Remark: The solution we just gave might be considered somewhat lacking in rigor; after all, it depended on the meaningfulness of an expression like

$$\underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}} \circ \underbrace{f \circ f \circ \cdots \circ f}_{m \text{ times}},$$

that is, a composition of several maps without an explicit parenthesization. Why can we write a composition $f_1 \circ f_2 \circ \cdots \circ f_k$ of multiple maps without specifying (by means of parentheses) in what order it is to be evaluated? Notice that the same objection applies to the very definition of f^k in Definition 0.12.

There are two ways to address this objection. One way is to **prove** that a composition $f_1 \circ f_2 \circ \cdots \circ f_k$ of multiple maps is independent of the order in which they are evaluated (and thus requires no parentheses in order to be unambiguous). This is called the *general associativity theorem*, and is proven in various texts on abstract algebra[14]. Notice that this theorem holds not only when $f_1, f_2, \ldots, f_k$ are maps $S \to S$, but also (more generally) when $f_1, f_2, \ldots, f_k$ are arbitrary maps such that the compositions $f_i \circ f_{i+1}$ (that is, the domain of f_i is the codomain of f_{i+1}) are

[14]For example, this is done in §A-3 of:

- David R. Wilkins, *Module MA3411: Commentary Basic Concepts and Results of Group Theory Michaelmas Term 2009*, `http://www.maths.tcd.ie/~dwilkins/Courses/MA3411/Wrapper_MA3411Mich2009_Commentary_A.pdf` .

Note that this text proves the general associativity theorem for k elements $x_1, x_2, \ldots, x_k$ of a group G rather than for k maps $f_1, f_2, \ldots, f_k$; but the proof is more or less identical.

well-defined for all $i \in [k-1]$. Once this theorem is proven, the above solution to Exercise 6 **(a)** becomes fully justified.

Another way is to ditch Definition 0.12, and instead define f^k (for an arbitrary set S, an arbitrary map $f : S \to S$, and an arbitrary $k \in \mathbb{N}$) by recursion on k, as follows:

$$f^0 = \mathrm{id}_S,$$

and

$$f^k = f \circ f^{k-1} \qquad \text{for each positive integer } k. \tag{24}$$

This recursive definition is formally bulletproof and requires no justification; of course, it is far less intuitive than Definition 0.12. Using this definition, we can now formally solve Exercise 6 **(a)** by induction over n as follows:

*Second solution to Exercise 6 **(a)**.* We shall solve Exercise 6 **(a)** by induction over n:

Induction base: For any $m \in \mathbb{N}$, we have $\underbrace{f^0}_{=\mathrm{id}_S} \circ f^m = \mathrm{id}_S \circ f^m = f^m = f^{0+m}$ (since $m = 0 + m$). In other words, Exercise 6 **(a)** holds for $n = 0$. This completes the induction base.

Induction step: Let k be a positive integer. Assume that Exercise 6 **(a)** holds for $n = k - 1$. We must prove that Exercise 6 **(a)** holds for $n = k$.

Let $m \in \mathbb{N}$. We assumed that Exercise 6 **(a)** holds for $n = k - 1$; thus, we have $f^{k-1} \circ f^m = f^{(k-1)+m} = f^{k+m-1}$. But (24) shows that $f^k = f \circ f^{k-1}$. Hence,

$$\begin{aligned}
\underbrace{f^k}_{=f\circ f^{k-1}} \circ f^m &= \left(f \circ f^{k-1}\right) \circ f^m = f \circ \underbrace{\left(f^{k-1} \circ f^m\right)}_{=f^{k+m-1}} \\
&\qquad \text{(since composition of maps is associative)} \\
&= f \circ f^{k+m-1}.
\end{aligned}$$

Comparing this with

$$f^{k+m} = f \circ f^{k+m-1} \qquad \text{(by (24), applied to } k+m \text{ instead of } k\text{)},$$

we obtain $f^k \circ f^m = f^{k+m}$. In other words, Exercise 6 **(a)** holds for $n = k$. This completes the induction step. Thus, Exercise 6 **(a)** is proven (again).

(b) We shall give three solutions for Exercise 6 **(b)**, on different levels of rigor. The first solution is verbose and relies on a lot of handwaving (it can be "cleaned up" to result in a rigorous proof, but this is not a particularly pleasant job). The second is rather rigorous already (it relies on the general associativity law, as did the first solution to Exercise 6 **(a)** above). The third is fully rigorous.

*First solution to Exercise 6 **(b)**.* Let $n \in \mathbb{N}$. Then,

$$(f \circ g)^n = \underbrace{(f \circ g) \circ (f \circ g) \circ \cdots \circ (f \circ g)}_{n \text{ times}} = f \circ g \circ f \circ g \circ \cdots \circ f \circ g; \tag{25}$$

the right-hand side of this equation is a composition of $2n$ maps, which alternate between f and g. On the other hand,

$$\underbrace{f^n}_{=\underbrace{f\circ f\circ\cdots\circ f}_{n\text{ times}}} \circ \underbrace{g^n}_{=\underbrace{g\circ g\circ\cdots\circ g}_{n\text{ times}}} = \underbrace{f\circ f\circ\cdots\circ f}_{n\text{ times}}\circ\underbrace{g\circ g\circ\cdots\circ g}_{n\text{ times}}$$
$$= f\circ f\circ\cdots\circ f\circ g\circ g\circ\cdots\circ g; \qquad (26)$$

the right-hand side of this equation is a composition of $2n$ maps, the first n of which are f and the last n of which are g. We want to prove that the right-hand sides of (25) and (26) are identical (because this will then show that $(f\circ g)^n = f^n\circ g^n$). In order to do so, it would clearly suffice to show that the expression "$f\circ g\circ f\circ g\circ\cdots\circ f\circ g$" can be transformed into "$f\circ f\circ\cdots\circ f\circ g\circ g\circ\cdots\circ g$" by repeatedly applying the law $g\circ f = f\circ g$ (which is true, because we assumed it to hold in the exercise). For example, here is how this transformation can be done in the case when $n=4$:

$$f\circ\underbrace{g\circ f}_{=f\circ g}\circ\underbrace{g\circ f}_{=f\circ g}\circ\underbrace{g\circ f}_{=f\circ g}\circ g$$
$$= f\circ f\circ\underbrace{g\circ f}_{=f\circ g}\circ\underbrace{g\circ f}_{=f\circ g}\circ g\circ g$$
$$= f\circ f\circ f\circ\underbrace{g\circ f}_{=f\circ g}\circ g\circ g\circ g$$
$$= f\circ f\circ f\circ f\circ g\circ g\circ g\circ g.$$

We need to show that such a transformation can be made for arbitrary n. So let us argue from general principles: An *fg-expression* shall mean an expression of the form "a composition of maps, some of which are f while the others are g". For example, "$f\circ g\circ g\circ f$" and "$g\circ f\circ g\circ g\circ g$" are fg-expressions (and so is the empty composition "id_S" as well as "f" alone). Notice that "$f\circ g\circ f\circ g$" and "$f\circ f\circ g\circ g$" are two different fg-expressions, but they describe the same map (since $f\circ g\circ f\circ g = f\circ f\circ g\circ g$); this is why we put quotation marks around fg-expressions.[15] A *switch* means the operation of replacing a "$g\circ f$" by an "$f\circ g$" in an fg-expression. For example, the fg-expression "$g\circ f\circ f\circ g$" is obtained from the fg-expression "$g\circ f\circ g\circ f$" by a switch (specifically, the switch that replaces the "$g\circ f$" at the end of the expression by an "$f\circ g$"). Notice that a switch changes the **fg-expression**, but does not change the **map** represented by the fg-expression, because we have $g\circ f = f\circ g$.

Our goal is now to show that the fg-expression "$f\circ g\circ f\circ g\circ\cdots\circ f\circ g$" (with $2n$ maps in total, which alternate between f and g) can be transformed into the

[15] As an aside, check that the number of fg-expressions with a appearances of "f" and b appearances of "g" is $\dbinom{a+b}{a}$.

fg-expression "$f \circ f \circ \cdots \circ f \circ g \circ g \circ \cdots \circ g$" (with $2n$ maps in total, the first n of which are f and the last n of which are g) by a sequence of switches.

To define the sequence of switches necessary for this transformation, we proceed as follows: Start with the fg-expression "$f \circ g \circ f \circ g \circ \cdots \circ f \circ g$" on the right-hand side of (25), and keep performing switches until no more switches are possible (i.e., until no more "$g \circ f$" occur in the fg-expression). I claim the following:

> *Claim 1:* This will actually happen (i.e., after finitely many switches, we will arrive at an fg-expression in which no more "$g \circ f$" occur).
>
> *Claim 2:* The resulting fg-expression will be precisely the "$f \circ f \circ \cdots \circ f \circ g \circ g \circ \cdots \circ g$" on the right-hand side of (26).

[*Proof of Claim 1:* Claim 1 is easily justified using what is called a *monovariant*: Namely, for any fg-expression E, we define the *grievance* of E to be the number of all pairs of a "g" in E and an "f" in E where the "g" stands further left than the "f". For example, the fg-expression "$f \circ g \circ f \circ g \circ f \circ g$" has grievance 3, because it has 3 such pairs[16].

The grievance of an fg-expression is clearly a nonnegative integer. Every time we apply a switch, this grievance decreases by 1 (check this!). Thus, we cannot keep applying switches eternally (because if we could, then the grievance would eventually become negative, which is absurd). Hence, if we start with any fg-expression and keep applying switches, then eventually, after finitely many switches, we will arrive at an fg-expression in which no more "$g \circ f$" occur. This proves Claim 1.

As I said, this was an example of a "proof by monovariant". This kind of proof is often used to show that a certain type of operation cannot be performed eternally. A *monovariant* is a quantity that keeps decreasing every time the operation is performed (or increasing – but of course, the direction of change has to be the same regardless of the state). In our case, the grievance has served as a monovariant. A monovariant often shows that the operation cannot be performed eternally – for example, if the monovariant is always a nonnegative integer, then this is clear. Sometimes, other justifications are needed.]

[*Proof of Claim 2:* The resulting fg-expression contains no "$g \circ f$" sub-expressions (because no more switches are possible on it). Therefore, if it contains the map "g" anywhere, then the map that follows it (i.e., the map directly to its right) must also be "g", and the map that follows this "g" must again be a "g" as well, and so on. In other words, the fg-expression has the property that the first "g" appearing in it is followed by "g"s all the way until the end of the expression. Similarly, it also has the property that the last "f" appearing in it is preceded by "f"s all the way until

[16] One pair consists of the "g" in position 2 and the "f" in position 3.

Another pair consists of the "g" in position 4 and the "f" in position 5.

The last pair consists of the "g" in position 2 and the "f" in position 5. Notice that the "g" and the "f" don't have to be adjacent in the expression.

the beginning of the expression. Hence, the fg-expression must have the form

$$\text{“}\underbrace{f \circ f \circ \cdots \circ f}_{\textbf{some}\text{ number of “}f\text{”s}} \circ \underbrace{g \circ g \circ \cdots \circ g}_{\textbf{some}\text{ number of “}g\text{”s}}\text{”}.$$

All we have to prove is that there are exactly n “f”s and exactly n “g”s in the fg-expression.

But this becomes clear if we think about how the fg-expression was obtained: Namely, we have obtained it by repeatedly applying switches to the fg-expression “$f \circ g \circ f \circ g \circ \cdots \circ f \circ g$”, which had exactly n “f”s and exactly n “g”s. Since a switch preserves the number of “f”s and the number of “g”s (indeed, as its name suggests, a switch only **switches** two maps), we thus conclude that the resulting fg-expression still has exactly n “f”s and exactly n “g”s. This completes the proof of Claim 2.]

Combining Claim 1 with Claim 2, we conclude that if we start with the fg-expression “$f \circ g \circ f \circ g \circ \cdots \circ f \circ g$” on the right-hand side of (25), and keep performing switches until no more switches are possible (i.e., until no more “$g \circ f$” occur in the fg-expression), then (after finitely many switches) we end up with the “$f \circ f \circ \cdots \circ f \circ g \circ g \circ \cdots \circ g$” on the right-hand side of (26). Thus, the two **maps** $f \circ g \circ f \circ g \circ \cdots \circ f \circ g$ and $f \circ f \circ \cdots \circ f \circ g \circ g \circ \cdots \circ g$ are identical (because a switch does not change the **map** represented by the fg-expression). In other words, the right-hand sides of (25) and (26) are identical. Thus, the left-hand sides of (25) and (26) are identical. In other words, $(f \circ g)^n = f^n \circ g^n$. This solves Exercise 6 **(b)**.

*Second solution to Exercise 6 **(b)**.* We shall solve Exercise 6 **(b)** by induction over n:

Induction base: We have $(f \circ g)^0 = \mathrm{id}_S = \underbrace{\mathrm{id}_S}_{=f^0} \circ \underbrace{\mathrm{id}_S}_{=g^0} = f^0 \circ g^0$. In other words, Exercise 6 **(b)** holds for $n = 0$. This completes the induction base.

Induction step: Let k be a positive integer. Assume that Exercise 6 **(b)** holds for $n = k - 1$. We must prove that Exercise 6 **(b)** holds for $n = k$.

We assumed that Exercise 6 **(b)** holds for $n = k - 1$; thus, we have $(f \circ g)^{k-1} = f^{k-1} \circ g^{k-1}$. But

$$\begin{aligned}
(f \circ g)^k &= \underbrace{(f \circ g) \circ (f \circ g) \circ \cdots \circ (f \circ g)}_{k \text{ times}} = \underbrace{f \circ g \circ f \circ g \circ \cdots \circ f \circ g}_{\substack{\text{a composition of } 2k \text{ maps,} \\ \text{alternating between } f \text{ and } g}} \\
&= f \circ \underbrace{\underbrace{(g \circ f \circ g \circ f \circ \cdots \circ g \circ f)}_{\substack{\text{a composition of } 2(k-1) \text{ maps,} \\ \text{alternating between } g \text{ and } f}}}_{= \underbrace{(g \circ f) \circ (g \circ f) \circ \cdots \circ (g \circ f)}_{k-1 \text{ times}} = (g \circ f)^{k-1}} \circ g \\
&= f \circ \left(\underbrace{g \circ f}_{= f \circ g} \right)^{k-1} \circ g = f \circ \underbrace{(f \circ g)^{k-1}}_{= f^{k-1} \circ g^{k-1}} \circ g = \underbrace{f \circ f^{k-1}}_{= f^k} \circ \underbrace{g^{k-1} \circ g}_{= g^k} = f^k \circ g^k.
\end{aligned}$$

In other words, Exercise 6 **(b)** holds for $n = k$. This completes the induction step. Thus, Exercise 6 **(b)** is solved again.

*Third solution to Exercise 6 **(b)**.* Now, we shall give a fully formal solution, which is not far away from what a proof assistant would accept (if it was written in its programming language). In particular, no "..."s will appear anywhere in the formulas.

We first prove an auxiliary claim:

Claim 3: We have $g \circ f^m = f^m \circ g$ for each $m \in \mathbb{N}$.

[*Proof of Claim 3:* We shall prove Claim 3 by induction over m:

Induction base: Comparing $g \circ \underbrace{f^0}_{=\operatorname{id}_S} = g \circ \operatorname{id}_S = g$ with $\underbrace{f^0}_{=\operatorname{id}_S} \circ g = \operatorname{id}_S \circ g = g$, we obtain $g \circ f^0 = f^0 \circ g$. In other words, Claim 3 holds for $m = 0$. This completes the induction base.

Induction step: Let k be a positive integer. Assume that Claim 3 holds for $m = k - 1$. We must prove that Claim 3 holds for $m = k$.

We assumed that Claim 3 holds for $m = k - 1$; thus, we have $g \circ f^{k-1} = f^{k-1} \circ g$. But (24) yields $f^k = f \circ f^{k-1}$. Hence,

$$\begin{aligned} g \circ \underbrace{f^k}_{=f \circ f^{k-1}} &= g \circ \left(f \circ f^{k-1}\right) = \underbrace{(g \circ f)}_{=f \circ g} \circ f^{k-1} = (f \circ g) \circ f^{k-1} \\ &= f \circ \underbrace{\left(g \circ f^{k-1}\right)}_{=f^{k-1} \circ g} = f \circ \left(f^{k-1} \circ g\right) = \underbrace{\left(f \circ f^{k-1}\right)}_{=f^k} \circ g = f^k \circ g. \end{aligned}$$

In other words, Claim 3 holds for $m = k$. This completes the induction step. Thus, Claim 3 is proven.]

Now that Claim 3 is established, we can comfortably prove Exercise 6 **(b)**. We proceed by induction over n:

Induction base: We have $(f \circ g)^0 = \operatorname{id}_S = \underbrace{\operatorname{id}_S}_{=f^0} \circ \underbrace{\operatorname{id}_S}_{=g^0} = f^0 \circ g^0$. In other words, Exercise 6 **(b)** holds for $n = 0$. This completes the induction base.

Induction step: Let k be a positive integer. Assume that Exercise 6 **(b)** holds for $n = k - 1$. We must prove that Exercise 6 **(b)** holds for $n = k$.

We assumed that Exercise 6 **(b)** holds for $n = k - 1$; thus, we have $(f \circ g)^{k-1} = f^{k-1} \circ g^{k-1}$.

Recall that (24) shows that $f^k = f \circ f^{k-1}$. Similarly, $g^k = g \circ g^{k-1}$. But (24) (applied to $f \circ g$ instead of f) yields

$$\begin{aligned}
(f \circ g)^k &= (f \circ g) \circ \underbrace{(f \circ g)^{k-1}}_{=f^{k-1} \circ g^{k-1}} = (f \circ g) \circ \left(f^{k-1} \circ g^{k-1}\right) = \underbrace{\left((f \circ g) \circ f^{k-1}\right)}_{=f \circ \left(g \circ f^{k-1}\right)} \circ g^{k-1} \\
&= \left(f \circ \underbrace{\left(g \circ f^{k-1}\right)}_{\substack{=f^{k-1} \circ g \\ \text{(by Claim 3, applied to } m=k-1)}} \right) \circ g^{k-1} = \left(\underbrace{f \circ \left(f^{k-1} \circ g\right)}_{=\left(f \circ f^{k-1}\right) \circ g} \right) \circ g^{k-1} \\
&= \left(\left(f \circ f^{k-1} \right) \circ g \right) \circ g^{k-1} = \underbrace{\left(f \circ f^{k-1}\right)}_{=f^k} \circ \underbrace{\left(g \circ g^{k-1}\right)}_{=g^k} = f^k \circ g^k.
\end{aligned}$$

In other words, Exercise 6 **(b)** holds for $n = k$. This completes the induction step. Thus, Exercise 6 **(b)** is solved again (and now completely formally).

(c) Many different answers are possible. For example, we can let $S = \mathbb{Z}$, and define two maps $f : S \to S$ and $g : S \to S$ by

$$f(n) = n + 1 \qquad \text{for each } n \in \mathbb{Z}, \qquad \text{and}$$
$$g(n) = -n \qquad \text{for each } n \in \mathbb{Z}.$$

(Visually speaking, S is the set of all integer points on the real axis, and f is the map that shifts a point 1 step to the right, whereas g is the map that reflects a point around the origin.) Now, it is easy to check that $(f \circ g)(n) = 1 - n$ for each $n \in \mathbb{Z}$. Hence, each $n \in \mathbb{N}$ satisfies

$$(f \circ g)^2 (n) = (f \circ g) \left(\underbrace{(f \circ g)(n)}_{=1-n} \right) = (f \circ g)(1 - n) = 1 - (1 - n) = n.$$

In other words, $(f \circ g)^2 = \mathrm{id}_{\mathbb{Z}}$. But $f^2 \circ g^2 \neq \mathrm{id}_{\mathbb{Z}}$ (indeed, $\left(f^2 \circ g^2\right)(n) = ((-(-n)) + 1) + 1 = n + 2$ for each $n \in \mathbb{Z}$), and thus $(f \circ g)^2 \neq f^2 \circ g^2$.

(With a bit more work, it is possible to check that $(f \circ g)^n \neq f^n \circ g^n$ for **each** $n \geq 2$. But it is sufficient to show that $(f \circ g)^2 \neq f^2 \circ g^2$ to know that Exercise 6 **(b)** cannot hold without the $f \circ g = g \circ f$ assumption.) $\square$

Remark 0.13. Exercise 6 gives two "rules of exponents" for compositions of maps. Here is another: If S is a set and $f : S \to S$ is a map, then $(f^n)^m = f^{nm}$ for any $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Prove this!

Exercise 7. 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.)

(a) Prove that

$$c^k(x_1, x_2, \ldots, x_n) = (x_{k+1}, x_{k+2}, \ldots, x_n, x_1, x_2, \ldots, x_k)$$

for each $k \in \{0, 1, \ldots, n\}$ and each $(x_1, x_2, \ldots, x_n) \in X^n$. (Note that $(x_{k+1}, x_{k+2}, \ldots, x_n, x_1, x_2, \ldots, x_k)$ is to be understood as $(x_1, x_2, \ldots, x_n)$ if k equals either 0 or n.)

[**Note:** This might be intuitively clear – after all, if c rotates a tuple, then c^k rotates it k times, which causes its first k entries to move to the rightmost spot. But the point is to give a rigorous proof. Induction is recommended.]

(b) Let $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be an n-tuple in X^n. A nonnegative integer k is said to be a *period* of $\mathbf{x}$ if it satisfies $c^k(\mathbf{x}) = \mathbf{x}$. (For example, 0 is always a period of $\mathbf{x}$. For another example, the periods of the 6-tuple $(1, 4, 2, 1, 4, 2)$ are $0, 3, 6, 9, \ldots$.)

Prove that if p and q are two periods of $\mathbf{x}$ satisfying $p \geq q$, then $p - q$ is also a period of $\mathbf{x}$.

(c) Let m be the smallest nonzero period of the n-tuple $\mathbf{x} \in X^n$. Prove that m divides any period of $\mathbf{x}$.

(d) Conclude that m divides n.

Solution to Exercise 7. **(a)** We shall solve Exercise 7 **(a)** by induction over k:

Induction base: For each $(x_1, x_2, \ldots, x_n) \in X^n$, we have

$$\underbrace{c^0}_{=\mathrm{id}_{X^n}}(x_1, x_2, \ldots, x_n) = \mathrm{id}_{X^n}(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)$$
$$= (x_{0+1}, x_{0+2}, \ldots, x_n, x_1, x_2, \ldots, x_0)$$

(because $\left(\underbrace{x_{0+1}, x_{0+2}, \ldots, x_n}_{\text{these are the } n \text{ elements } x_1, x_2, \ldots, x_n}, \underbrace{x_1, x_2, \ldots, x_0}_{\text{there is nothing in here}} \right) = (x_1, x_2, \ldots, x_n)$). In other words, Exercise 7 **(a)** holds for $k = 0$. This completes the induction base.

Induction step: Let $p \in \{0, 1, \ldots, n\}$ be positive. Assume that Exercise 7 **(a)** holds for $k = p - 1$. We must show that Exercise 7 **(a)** also holds for $k = p$.

Let $(x_1, x_2, \ldots, x_n) \in X^n$ be arbitrary.

We have $p \in \{1, 2, \ldots, n\}$ (since $p \in \{0, 1, \ldots, n\}$ is positive) and thus $p - 1 \in \{0, 1, \ldots, n-1\} \subseteq \{0, 1, \ldots, n\}$. Recall that Exercise 7 **(a)** holds for $k = p - 1$.

Hence, we can apply Exercise 7 **(a)** to $k = p - 1$, and obtain

$$\begin{aligned} c^{p-1}(x_1, x_2, \ldots, x_n) &= \left(x_{(p-1)+1}, x_{(p-1)+2}, \ldots, x_n, x_1, x_2, \ldots, x_{p-1}\right) \\ &= \left(x_p, x_{p+1}, \ldots, x_n, x_1, x_2, \ldots, x_{p-1}\right). \end{aligned}$$

But now

$$\begin{aligned} \underbrace{c^p}_{=c\circ c^{p-1}}(x_1, x_2, \ldots, x_n) &= \left(c \circ c^{p-1}\right)(x_1, x_2, \ldots, x_n) = c\left(\underbrace{c^{p-1}(x_1, x_2, \ldots, x_n)}_{=\left(x_p, x_{p+1}, \ldots, x_n, x_1, x_2, \ldots, x_{p-1}\right)}\right) \\ &= c\left(x_p, x_{p+1}, \ldots, x_n, x_1, x_2, \ldots, x_{p-1}\right) \\ &= \left(x_{p+1}, x_{p+2}, \ldots, x_n, x_1, x_2, \ldots, x_{p-1}, x_p\right) \\ &\qquad (\text{by the definition of } c) \\ &= \left(x_{p+1}, x_{p+2}, \ldots, x_n, x_1, x_2, \ldots, x_p\right). \end{aligned}$$

Now, forget that we fixed $(x_1, x_2, \ldots, x_n)$. We thus have shown that $c^p(x_1, x_2, \ldots, x_n) = \left(x_{p+1}, x_{p+2}, \ldots, x_n, x_1, x_2, \ldots, x_p\right)$ for each $(x_1, x_2, \ldots, x_n) \in X^n$. In other words, Exercise 7 **(a)** holds for $k = p$. This completes the induction step.

(b) Let p and q be two periods of $\mathbf{x}$ satisfying $p \geq q$. We must show that $p - q$ is also a period of $\mathbf{x}$.

We know that p is a period of $\mathbf{x}$. In other words, p is a nonnegative integer satisfying $c^p(\mathbf{x}) = \mathbf{x}$ (by the definition of "period"). Similarly, q is a nonnegative integer satisfying $c^q(\mathbf{x}) = \mathbf{x}$.

But $p - q \in \mathbb{N}$ (since $p \geq q$). Exercise 6 **(a)** (applied to X^n, c, $p - q$ and q instead of S, f, n and m) shows that $c^{p-q} \circ c^q = c^{(p-q)+q} = c^p$. Hence, $\underbrace{\left(c^{p-q} \circ c^q\right)}_{=c^p}(\mathbf{x}) = c^p(\mathbf{x}) = \mathbf{x}$. Therefore,

$$\mathbf{x} = \left(c^{p-q} \circ c^q\right)(\mathbf{x}) = c^{p-q}\left(\underbrace{c^q(\mathbf{x})}_{=\mathbf{x}}\right) = c^{p-q}(\mathbf{x}).$$

Thus, $c^{p-q}(\mathbf{x}) = \mathbf{x}$. Since $p - q$ is a nonnegative integer (because $p - q \in \mathbb{N}$), this shows that $p - q$ is a period of $\mathbf{x}$ (by the definition of "period"). This solves Exercise 7 **(b)**.

(c) We want to prove the following claim:

> *Claim 1:* Let r be any period of $\mathbf{x}$. Then, m divides r.

[*Proof of Claim 1:* We shall prove Claim 1 by strong induction over r:

Induction step: Let $p \in \mathbb{N}$. Assume that Claim 1 holds whenever $r < p$. We must now prove that Claim 1 holds for $r = p$.

We have assumed that Claim 1 holds whenever $r < p$. In other words,

$$\text{if } r \text{ is any period of } \mathbf{x} \text{ such that } r < p, \text{ then } m \text{ divides } r. \tag{27}$$

Now, let r be any period of $\mathbf{x}$ such that $r = p$. We must show that m divides r.

If $r = 0$, then this is obvious (since m clearly divides 0). Thus, we WLOG assume that $r \neq 0$. In other words, r is nonzero.

Recall that m is the smallest nonzero period of $\mathbf{x}$. Thus, each nonzero period of $\mathbf{x}$ is $\geq m$. Hence, r is $\geq m$ (since r is a nonzero period of $\mathbf{x}$). We thus have shown that $r \geq m$. Hence, Exercise 7 **(b)** (applied to r and m instead of p and q) shows that $r - m$ is also a period of $\mathbf{x}$. Furthermore, m is a nonzero nonnegative integer, and thus is a positive integer. Hence, $m > 0$. Thus, $r - \underbrace{m}_{>0} < r - 0 = r = p$. Therefore, $r - m$ is a period of $\mathbf{x}$ such that $r - m < p$. Hence, (27) (applied to $r - m$ instead of r) shows that m divides $r - m$. In other words, $r - m = km$ for some $k \in \mathbb{Z}$. Consider this k. From $r - m = km$, we obtain $r = km + m = (k+1)m$. Hence, m divides r.

Now, forget that we fixed r. We thus have proven that

$$\text{if } r \text{ is any period of } \mathbf{x} \text{ such that } r = p, \text{ then } m \text{ divides } r.$$

In other words, Claim 1 holds for $r = p$. This completes the induction step, so Claim 1 is proven.]

Claim 1 (which we now have proven) says precisely that m divides any period of $\mathbf{x}$. Thus, Exercise 7 **(c)** is solved.

(d) Write the n-tuple $\mathbf{x} \in X^n$ in the form $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Then,

$$\begin{aligned} c^n \left(\underbrace{\mathbf{x}}_{=(x_1,x_2,\ldots,x_n)} \right) &= c^n (x_1, x_2, \ldots, x_n) = \left(\underbrace{x_{n+1}, x_{n+2}, \ldots, x_n}_{\text{there is nothing in here}}, \underbrace{x_1, x_2, \ldots, x_n}_{\substack{\text{these are the } n \text{ elements} \\ x_1, x_2, \ldots, x_n}} \right) \\ &\qquad (\text{by Exercise 7 } \textbf{(a)}, \text{ applied to } k = n) \\ &= (x_1, x_2, \ldots, x_n) = \mathbf{x}. \end{aligned}$$

Hence, n is a nonnegative integer satisfying $c^n(\mathbf{x}) = \mathbf{x}$. In other words, n is a period of $\mathbf{x}$ (by the definition of "period"). Thus, m divides n (since Exercise 7 **(c)** shows that m divides any period of $\mathbf{x}$). This solves Exercise 7 **(d)**. $\square$