Math 4990 Fall 2017 (Darij Grinberg): homework set 5 with solutions (preliminary version)

Contents

0.1. The binomial transform, again

If $\mathbf{a} = (a_0, a_1, \ldots, a_N)$ is a list[1] of rational numbers, then the *binomial transform* of this list $\mathbf{a}$ is defined to be the list $(b_0, b_1, \ldots, b_N)$ of rational numbers, where

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \{0, 1, \ldots, N\}.$$

We shall denote the binomial transform of the list $\mathbf{a}$ by $B(\mathbf{a})$. We have already studied binomial transforms implicitly on the previous homework set: Namely, Exercise 5 on homework set #4 says that if $\mathbf{b}$ is the binomial transform of a list $\mathbf{a}$, then $\mathbf{a}$ is (in turn) the binomial transform of $\mathbf{b}$. In other words: If $\mathbf{b} = B(\mathbf{a})$, then $\mathbf{a} = B(\mathbf{b})$. In other words, if we regard B as a map that transforms lists into lists, then $B^2 = B \circ B = \mathrm{id}$.

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

(a) Find the binomial transform of the list $(1, 1, \ldots, 1)$ (with $N+1$ entries).

(b) For any given $a \in \mathbb{N}$, find the binomial transform of the list $\left(\binom{0}{a}, \binom{1}{a}, \ldots, \binom{N}{a}\right)$.

(c) For any given $q \in \mathbb{Z}$, find the binomial transform of the list $\left(q^0, q^1, \ldots, q^N\right)$.

(d) Find the binomial transform of the list $(1, 0, 1, 0, 1, 0, \ldots)$ (this ends with 1 if N is even, and with 0 if N is odd).

Before we solve this exercise, let us recall some fundamental facts about binomial coefficients:

Proposition 0.1. Let $n \in \mathbb{N}$. Let $x \in \mathbb{Q}$ and $y \in \mathbb{Q}$. Then,

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

[1] The words "finite list", "tuple" and "finite sequence" mean the same thing. I only consider finite lists on this homework set.

Proposition 0.2. We have

$$\binom{m}{n} = 0$$

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

Corollary 0.3. Let $n \in \mathbb{N}$. Let $i \in \{0, 1, \ldots, n\}$. Then,

$$\sum_{j=i}^{n} (-1)^{j+i} \binom{n}{j} \binom{j}{i} = [i = n].$$

Proposition 0.1 is simply the binomial formula. Proposition 0.2 is fundamental and easy to prove. Corollary 0.3 was proven in the solutions to homework set #4.

Let us derive a few simple corollaries from these facts.

Corollary 0.4. Let $n \in \mathbb{N}$ and $q \in \mathbb{Q}$. Then,

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} q^i = (1-q)^n.$$

Proof of Corollary 0.4. We have

$$\left(\underbrace{1-q}_{=(-q)+1}\right)^n = ((-q)+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-q)^k \underbrace{1^{n-k}}_{=1}$$

(by Proposition 0.1, applied to $x = -q$ and $y = 1$)

$$= \sum_{k=0}^{n} \binom{n}{k} \underbrace{(-q)^k}_{=(-1)^k q^k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k q^k$$

$$= \sum_{k=0}^{n} (-1)^k \binom{n}{k} q^k = \sum_{i=0}^{n} (-1)^i \binom{n}{i} q^i$$

(here, we have renamed the summation index k as i). This proves Corollary 0.4. □

Corollary 0.5. Let $n \in \mathbb{N}$. Let $i \in \mathbb{N}$. Then,

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} \binom{j}{i} = (-1)^i [n = i].$$

Proof of Corollary 0.5. Notice that each $j \in \{0, 1, \ldots, i-1\}$ satisfies

$$\binom{j}{i} = 0 \tag{1}$$

[2].

We are in one of the following two cases:

Case 1: We have $i \leq n$.

Case 2: We have $i > n$.

Let us first consider Case 1. In this case, we have $i \leq n$. Thus, $i \in \{0,1,\ldots,n\}$. Now,

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j}\binom{j}{i}$$

$$= \sum_{j=0}^{i-1} (-1)^j \binom{n}{j} \underbrace{\binom{j}{i}}_{\substack{=0 \\ \text{(by (1))}}} + \sum_{j=i}^{n} \underbrace{(-1)^j}_{\substack{=(-1)^{i+(j+i)} \\ \text{(since } j \equiv 2i+j = i+(j+i) \bmod 2\text{)}}} \binom{n}{j}\binom{j}{i}$$

(here, we have split the sum at $j = i$, since $0 \leq i \leq n$)

$$= \underbrace{\sum_{j=0}^{i-1} (-1)^j \binom{n}{j} 0}_{=0} + \sum_{j=i}^{n} (-1)^{i+(j+i)} \binom{n}{j}\binom{j}{i} = \sum_{j=i}^{n} \underbrace{(-1)^{i+(j+i)}}_{=(-1)^i(-1)^{j+i}} \binom{n}{j}\binom{j}{i}$$

$$= \sum_{j=i}^{n} (-1)^i (-1)^{j+i} \binom{n}{j}\binom{j}{i} = (-1)^i \underbrace{\sum_{j=i}^{n} (-1)^{j+i} \binom{n}{j}\binom{j}{i}}_{\substack{=[i=n] \\ \text{(by Corollary 0.3)}}}$$

$$= (-1)^i \left[\underbrace{i = n}_{\iff (n=i)} \right] = (-1)^i [n = i].$$

Hence, Corollary 0.5 is proven in Case 1.

Let us now consider Case 2. In this case, we have $i > n$. Thus, $n < i$, so that $n \in \{0,1,\ldots,i-1\}$ (since $n \in \mathbb{N}$). But we don't have $n = i$ (since we have $n < i$); thus, we have $[n = i] = 0$. Hence, $(-1)^i \underbrace{[n = i]}_{=0} = 0$. But

$$\sum_{j=0}^{n} (-1)^j \binom{n}{j} \underbrace{\binom{j}{i}}_{\substack{=0 \\ \text{(by (1)} \\ \text{(since } j \in \{0,1,\ldots,i-1\} \\ \text{(because } j \leq n < i \text{ and } j \in \mathbb{N})\text{)}}} = \sum_{j=0}^{n} (-1)^j \binom{n}{j} 0 = 0 = (-1)^i [n = i].$$

Hence, Corollary 0.5 is proven in Case 2.

[2] *Proof:* Let $j \in \{0,1,\ldots,i-1\}$. Thus, $j \leq i-1 < i$ and $j \in \mathbb{N}$. Hence, Proposition 0.2 (applied to j and i instead of m and n) shows that $\binom{j}{i} = 0$. This proves (1).

We have now proven Corollary 0.5 in both Cases 1 and 2. Hence, Corollary 0.5 always holds. □

Solution to Exercise 1. **(b)**

Claim 1: Let $a \in \mathbb{N}$. The binomial transform of the list $\left(\binom{0}{a}, \binom{1}{a}, \ldots, \binom{N}{a}\right)$ is the list

$$\left((-1)^a [0=a], (-1)^a [1=a], \ldots, (-1)^a [N=a]\right).$$

(This is the list whose entries are all 0 except for the a-th entry – counted from 0 –, which is $(-1)^a$. However, if $a > N$, then this list has no a-th entry, and thus all of its entries are 0.)

[*Proof of Claim 1:* Let $(b_0, b_1, \ldots, b_N)$ be the binomial transform of the list $\left(\binom{0}{a}, \binom{1}{a}, \ldots, \binom{N}{a}\right)$. Thus,

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i}\binom{i}{a} \qquad \text{for each } n \in \{0,1,\ldots,N\}$$

(by the definition of the binomial transform).

Hence, each $n \in \{0,1,\ldots,N\}$ satisfies

$$\begin{aligned} b_n &= \sum_{i=0}^{n} (-1)^i \binom{n}{i}\binom{i}{a} = \sum_{j=0}^{n} (-1)^j \binom{n}{j}\binom{j}{a} \\ &\qquad \text{(here, we have renamed the summation index } i \text{ as } j) \\ &= (-1)^a [n=a] \qquad \text{(by Corollary 0.5, applied to } i=a). \end{aligned}$$

In other words,

$$(b_0, b_1, \ldots, b_N) = \left((-1)^a [0=a], (-1)^a [1=a], \ldots, (-1)^a [N=a]\right).$$

Thus, the binomial transform of the list $\left(\binom{0}{a}, \binom{1}{a}, \ldots, \binom{N}{a}\right)$ is $\left((-1)^a [0=a], (-1)^a [1=a], \ldots, (-1)^a [N=a]\right)$ (since the binomial transform of the list $\left(\binom{0}{a}, \binom{1}{a}, \ldots, \binom{N}{a}\right)$ is $(b_0, b_1, \ldots, b_N)$). This proves Claim 1.]

Thus, Exercise 1 **(b)** is solved.

(a)

Claim 2: The binomial transform of the list $(1,1,\ldots,1)$ (with $N+1$ entries) is the list $(1,0,0,\ldots,0)$ (with one 1 and N zeroes).

[*Proof of Claim 2:* We have $\binom{n}{0} = 1$ for each $n \in \{0,1,\ldots,N\}$. Hence,

$$\left(\binom{0}{0}, \binom{1}{0}, \ldots, \binom{N}{0}\right) = (1,1,\ldots,1) \tag{2}$$

(with $N+1$ entries).

But Claim 1 (applied to $a = 0$) shows that the binomial transform of the list $\left(\binom{0}{0}, \binom{1}{0}, \ldots, \binom{N}{0}\right)$ is the list

$$\begin{aligned}&\left(\underbrace{(-1)^0}_{=1}[0=0], \underbrace{(-1)^0}_{=1}[1=0], \ldots, \underbrace{(-1)^0}_{=1}[N=0]\right)\\ &= ([0=0], [1=0], \ldots, [N=0]) = (1,0,0,\ldots,0)\end{aligned}$$

(with one 1 and N zeroes). In view of (2), this rewrites as follows: The binomial transform of the list $(1,1,\ldots,1)$ (with $N+1$ entries) is the list $(1,0,0,\ldots,0)$ (with one 1 and N zeroes). This proves Claim 2.]

Thus, Exercise 1 **(a)** is solved.

(c)

Claim 3: Let $q \in \mathbb{Z}$. The binomial transform of the list $\left(q^0, q^1, \ldots, q^N\right)$ is $\left((1-q)^0, (1-q)^1, \ldots, (1-q)^N\right)$.

[*Proof of Claim 3:* Let $(b_0, b_1, \ldots, b_N)$ be the binomial transform of the list $\left(q^0, q^1, \ldots, q^N\right)$. Thus,

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} q^i \qquad \text{for each } n \in \{0,1,\ldots,N\}$$

(by the definition of the binomial transform). Hence, each $n \in \{0,1,\ldots,N\}$ satisfies

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} q^i = (1-q)^n$$

(by Corollary 0.4). In other words, $(b_0, b_1, \ldots, b_N) = \left((1-q)^0, (1-q)^1, \ldots, (1-q)^N\right)$. Thus, the binomial transform of the list $\left(q^0, q^1, \ldots, q^N\right)$ is $\left((1-q)^0, (1-q)^1, \ldots, (1-q)^N\right)$ (since the binomial transform of the list $\left(q^0, q^1, \ldots, q^N\right)$ is $(b_0, b_1, \ldots, b_N)$). This proves Claim 3.]

Thus, Exercise 1 **(c)** is solved.

(d)

Claim 4: The binomial transform of the list $(1,0,1,0,1,0,\ldots)$ (with $N+1$ entries) is $\left(1, 2^0, 2^1, \ldots, 2^{N-1}\right)$.

[*Proof of Claim 4:* Let $(a_0, a_1, \ldots, a_N)$ be the list $(1, 0, 1, 0, 1, 0, \ldots)$ (with $N+1$ entries). Thus, for each $i \in \{0, 1, \ldots, N\}$, we have

$$a_i = \begin{cases} 1, & \text{if } i \text{ is even;} \\ 0, & \text{if } i \text{ is odd} \end{cases} = \frac{1}{2}\left(1 + (-1)^i\right). \tag{3}$$

(In fact, the last equality is easy to check: If i is even, then $(-1)^i = 1$ and thus $\frac{1}{2}\left(1 + (-1)^i\right) = \frac{1}{2}(1+1) = 1$; but if i is odd, then $(-1)^i = -1$ and therefore $\frac{1}{2}\left(1 + (-1)^i\right) = 0$.)

Let $(b_0, b_1, \ldots, b_N)$ be the binomial transform of the list $(1, 0, 1, 0, 1, 0, \ldots)$ (with $N+1$ entries). Thus, $(b_0, b_1, \ldots, b_N)$ is the binomial transform of the list $(a_0, a_1, \ldots, a_N)$ (because the list $(1, 0, 1, 0, 1, 0, \ldots)$ (with $N+1$ entries) is precisely $(a_0, a_1, \ldots, a_N)$). Hence,

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \{0, 1, \ldots, N\}$$

(by the definition of the binomial transform). Thus, for each $n \in \{0, 1, \ldots, N\}$, we

obtain

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} \underbrace{a_i}_{\substack{=\frac{1}{2}\left(1+(-1)^i\right) \\ \text{(by (3))}}} = \sum_{i=0}^{n} \underbrace{(-1)^i \binom{n}{i} \cdot \frac{1}{2}\left(1+(-1)^i\right)}_{=\frac{1}{2}(-1)^i\binom{n}{i}\cdot 1+\frac{1}{2}(-1)^i\binom{n}{i}(-1)^i}$$

$$= \sum_{i=0}^{n} \left(\frac{1}{2}(-1)^i \binom{n}{i} \cdot 1 + \frac{1}{2}(-1)^i \binom{n}{i} (-1)^i \right)$$

$$= \frac{1}{2} \sum_{i=0}^{n} (-1)^i \binom{n}{i} \cdot \underbrace{1}_{=1^i} + \frac{1}{2} \sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^i$$

$$= \frac{1}{2} \underbrace{\sum_{i=0}^{n} (-1)^i \binom{n}{i} \cdot 1^i}_{\substack{=(1-1)^n \\ \text{(by Corollary 0.4, applied to } q=1\text{)}}} + \frac{1}{2} \underbrace{\sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^i}_{\substack{=(1-(-1))^n \\ \text{(by Corollary 0.4, applied to } q=-1\text{)}}}$$

$$= \frac{1}{2} \left(\underbrace{1-1}_{=0} \right)^n + \frac{1}{2} \left(\underbrace{1-(-1)}_{=2} \right)^n = \frac{1}{2} \underbrace{0^n}_{=\begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n > 0 \end{cases}} + \underbrace{\frac{1}{2} 2^n}_{=2^{n-1}}$$

$$= \frac{1}{2} \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n > 0 \end{cases} + 2^{n-1} = \begin{cases} \frac{1}{2} \cdot 1 + 2^{n-1}, & \text{if } n = 0; \\ \frac{1}{2} \cdot 0 + 2^{n-1}, & \text{if } n > 0 \end{cases}$$

$$= \begin{cases} 1, & \text{if } n = 0; \\ 2^{n-1}, & \text{if } n > 0 \end{cases}$$

(because $\frac{1}{2} \cdot 1 + 2^{n-1} = 1$ in the case when $n = 0$, whereas $\frac{1}{2} \cdot 0 + 2^{n-1} = 2^{n-1}$ in the case when $n > 0$). In other words, $(b_0, b_1, \ldots, b_N) = \left(1, 2^0, 2^1, \ldots, 2^{N-1}\right)$. Thus, the binomial transform of the list $(1, 0, 1, 0, 1, 0, \ldots)$ (with $N+1$ entries) is $\left(1, 2^0, 2^1, \ldots, 2^{N-1}\right)$ (since the binomial transform of the list $(1, 0, 1, 0, 1, 0, \ldots)$ (with $N+1$ entries) is $(b_0, b_1, \ldots, b_N)$). This proves Claim 4.]

Thus, Exercise 1 **(d)** is solved. □

Exercise 2. Let $N \in \mathbb{N}$. If $\mathbf{a} = (a_0, a_1, \ldots, a_N)$ is a list of $N+1$ rational numbers, then $W(\mathbf{a})$ denotes the list $\left((-1)^N a_N, (-1)^N a_{N-1}, \ldots, (-1)^N a_0\right)$ of rational numbers. (Thus, the list $W(\mathbf{a})$ is obtained by reversing the list $\mathbf{a}$ and then multiplying each of its entries by $(-1)^N$.) Hence, W and B are two maps, each transforming lists into lists.

Prove that $B \circ W \circ B = W \circ B \circ W$ and $(B \circ W)^3 = \mathrm{id}$.

The equality $(B \circ W)^3 = \mathrm{id}$, spelt out in words, says that if we start with a list, apply the map W, apply the binomial transform, then apply the map W to the result, then again apply the binomial transform, then again apply the map W to the result, then apply the binomial transform once again, then we end up with the original list.

Before we solve Exercise 2, we shall arm ourselves with an identity:

Lemma 0.6. Let N, n and j be nonnegative integers such that $N \geq n$ and $N \geq j$. Then,

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

There are two ways to prove Lemma 0.6. One way is combinatorial (using the principle of inclusion and exclusion) and is explained in [Galvin17, proof of Identity 17.1].

The other way is algebraic. It relies on the following identity:

Lemma 0.7. For every $x \in \mathbb{N}$ and $y \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $x \leq n$, we have

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

Lemma 0.7 is precisely [Grinbe16, Proposition 3.32 **(e)**] (where it is proven using the Vandermonde convolution identity).

To derive Lemma 0.6 from Lemma 0.7, we will need the upper negation formula:

Proposition 0.8. We have

$$\binom{n}{k} = (-1)^k \binom{k-n-1}{k}$$

for any $n \in \mathbb{Q}$ and $k \in \mathbb{N}$.

Proposition 0.8 is Exercise 2 **(a)** in homework set 1.

Proof of Lemma 0.6. We have $j \leq N$ (since $N \geq j$). Thus, Lemma 0.7 (applied to j, n

and N instead of x, y and n) yields

$$\begin{aligned}\binom{n-j-1}{N-j} &= \sum_{k=0}^{N} \underbrace{(-1)^{k-j}}_{\substack{=(-1)^{(N-j)+(N-k)} \\ \text{(since } k-j \equiv 2N+k-j=(N-j)+(N-k) \bmod 2\text{)}}} \binom{k}{j}\binom{n}{N-k} \\ &= \sum_{k=0}^{N} \underbrace{(-1)^{(N-j)+(N-k)}}_{=(-1)^{N-j}(-1)^{N-k}} \binom{k}{j}\binom{n}{N-k} \\ &= \sum_{k=0}^{N} (-1)^{N-j}(-1)^{N-k}\binom{k}{j}\binom{n}{N-k}. \end{aligned} \tag{4}$$

But $N-j \geq 0$ (since $N \geq j$), so that $N-j \in \mathbb{N}$. Hence, Proposition 0.8 (applied to $N-n$ and $N-j$ instead of n and k) yields

$$\begin{aligned}\binom{N-n}{N-j} &= (-1)^{N-j} \underbrace{\binom{(N-j)-(N-n)-1}{N-j}}_{=\binom{n-j-1}{N-j}} \\ &\qquad = \underbrace{\sum_{k=0}^{N} (-1)^{N-j}(-1)^{N-k}\binom{k}{j}\binom{n}{N-k}}_{\text{(by (4))}} \\ &= (-1)^{N-j} \sum_{k=0}^{N} (-1)^{N-j}(-1)^{N-k}\binom{k}{j}\binom{n}{N-k} \\ &= \underbrace{(-1)^{N-j}(-1)^{N-j}}_{=((-1)\cdot(-1))^{N-j}=1^{N-j}=1} \sum_{k=0}^{N} (-1)^{N-k}\binom{k}{j}\binom{n}{N-k} \\ &= \sum_{k=0}^{N} (-1)^{N-k}\binom{k}{j}\binom{n}{N-k}. \end{aligned} \tag{5}$$

But $0 \leq n \leq N$ (since $N \geq n$). Hence, we can split the sum $\sum_{i=0}^{N} (-1)^{i}\binom{n}{i}\binom{N-i}{j}$

at $i = n$. We thus find

$$\begin{aligned}
&\sum_{i=0}^{N} (-1)^i \binom{n}{i} \binom{N-i}{j} \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{N-i}{j} + \sum_{i=n+1}^{N} (-1)^i \underbrace{\binom{n}{i}}_{\substack{=0 \\ \text{(by Proposition 0.2,} \\ \text{applied to } n \text{ and } i \text{ instead of } m \text{ and } n \\ \text{(since } n<i \text{ (since } i \geq n+1>n)))}} \binom{N-i}{j} \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{N-i}{j} + \underbrace{\sum_{i=n+1}^{N} (-1)^i 0 \binom{N-i}{j}}_{=0} \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{N-i}{j}.
\end{aligned}$$

Hence,

$$\begin{aligned}
&\sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{N-i}{j} \\
&= \sum_{i=0}^{N} (-1)^i \binom{n}{i} \binom{N-i}{j} \\
&= \sum_{k=0}^{N} (-1)^{N-k} \binom{n}{N-k} \underbrace{\binom{N-(N-k)}{j}}_{=\binom{k}{j}} \\
&\qquad \text{(here, we have substituted } N-k \text{ for } i \text{ in the sum)} \\
&= \sum_{k=0}^{N} (-1)^{N-k} \underbrace{\binom{n}{N-k}\binom{k}{j}}_{=\binom{k}{j}\binom{n}{N-k}} \\
&= \sum_{k=0}^{N} (-1)^{N-k} \binom{k}{j} \binom{n}{N-k} = \binom{N-n}{N-j}
\end{aligned}$$

(by (5)). This proves Lemma 0.6. □

We are now ready to solve Exercise 2.

First solution to Exercise 2. Let us first focus on proving that $B \circ W \circ B = W \circ B \circ W$.

Indeed, let $\mathbf{a}$ be a list of $N+1$ rational numbers. Write $\mathbf{a}$ in the form $\mathbf{a} = (a_0, a_1, \ldots, a_N)$.

Let $\mathbf{b}$ be the list $B(\mathbf{a})$. Write the list $\mathbf{b}$ in the form $\mathbf{b} = (b_0, b_1, \ldots, b_N)$. Recall that $B(\mathbf{a})$ is the binomial transform of the list $\mathbf{a}$. In other words, $(b_0, b_1, \ldots, b_N)$ is the binomial transform of the list $(a_0, a_1, \ldots, a_N)$ (since $\mathbf{a} = (a_0, a_1, \ldots, a_N)$ and $B(\mathbf{a}) = \mathbf{b} = (b_0, b_1, \ldots, b_N)$). Thus,

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \{0, 1, \ldots, N\} \tag{6}$$

(by the definition of the binomial transform). Thus,

$$b_n = \sum_{i=0}^{N} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \{0, 1, \ldots, N\} \tag{7}$$

[3].

We have $\mathbf{b} = (b_0, b_1, \ldots, b_N)$. Thus, $W(\mathbf{b}) = \left((-1)^N b_N, (-1)^N b_{N-1}, \ldots, (-1)^N b_0\right)$ (by the definition of the list $W(\mathbf{b})$).

Now, let $\mathbf{c}$ be the binomial transform of the list $W(\mathbf{b})$. Thus, $\mathbf{c} = B(W(\mathbf{b}))$.

Write the list $\mathbf{c}$ in the form $\mathbf{c} = (c_0, c_1, \ldots, c_N)$. Recall that $\mathbf{c}$ is the binomial transform of the list $W(\mathbf{b})$. In other words, $(c_0, c_1, \ldots, c_N)$ is the binomial transform of the list $\left((-1)^N b_N, (-1)^N b_{N-1}, \ldots, (-1)^N b_0\right)$ (since $\mathbf{c} = (c_0, c_1, \ldots, c_N)$ and $W(\mathbf{b}) = \left((-1)^N b_N, (-1)^N b_{N-1}, \ldots, (-1)^N b_0\right)$). Thus,

$$c_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^N b_{N-i} \qquad \text{for each } n \in \{0, 1, \ldots, N\} \tag{8}$$

(by the definition of the binomial transform).

On the other hand, $\mathbf{a} = (a_0, a_1, \ldots, a_N)$. Thus, $W(\mathbf{a}) = \left((-1)^N a_N, (-1)^N a_{N-1}, \ldots, (-1)^N a_0\right)$ (by the definition of $W(\mathbf{a})$). Let $\mathbf{d}$ be the binomial transform of the list $W(\mathbf{a})$. Thus, $\mathbf{d} = B(W(\mathbf{a}))$.

---

[3] *Proof of (7):* Let $n \in \{0, 1, \ldots, N\}$. Then, $0 \leq n \leq N$. Hence, we can split the sum $\sum_{i=0}^{N} (-1)^i \binom{n}{i} a_i$ at $i = n$. We thus find

$$\begin{aligned}
&\sum_{i=0}^{N} (-1)^i \binom{n}{i} a_i \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i + \sum_{i=n+1}^{N} (-1)^i \underbrace{\binom{n}{i}}_{\substack{=0 \\ \text{(by Proposition 0.2,} \\ \text{applied to } n \text{ and } i \text{ instead of } m \text{ and } n \\ \text{(since } n<i \text{ (since } i \geq n+1>n)))}} a_i \\
&= \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i + \underbrace{\sum_{i=n+1}^{N} (-1)^i 0 a_i}_{=0} = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i = b_n
\end{aligned}$$

(by (6)). This proves (7).

Write the list $\mathbf{d}$ in the form $\mathbf{d} = (d_0, d_1, \ldots, d_N)$. Recall that $\mathbf{d}$ is the binomial transform of the list $W(\mathbf{a})$. In other words, $(d_0, d_1, \ldots, d_N)$ is the binomial transform of the list $\left((-1)^N a_N, (-1)^N a_{N-1}, \ldots, (-1)^N a_0\right)$ (since $\mathbf{d} = (d_0, d_1, \ldots, d_N)$ and $W(\mathbf{a}) = \left((-1)^N a_N, (-1)^N a_{N-1}, \ldots, (-1)^N a_0\right)$). Thus,

$$d_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^N a_{N-i} \qquad \text{for each } n \in \{0, 1, \ldots, N\} \tag{9}$$

(by the definition of the binomial transform).

Finally, from $\mathbf{d} = (d_0, d_1, \ldots, d_N)$, we obtain

$$W(\mathbf{d}) = \left((-1)^N d_N, (-1)^N d_{N-1}, \ldots, (-1)^N d_0\right) \tag{10}$$

(by the definition of $W(\mathbf{d})$).

We have

$$(B \circ W \circ B)(\mathbf{a}) = B\left(W\left(\underbrace{B(\mathbf{a})}_{=\mathbf{b}}\right)\right) = B(W(\mathbf{b})) = \mathbf{c}$$

and

$$(W \circ B \circ W)(\mathbf{a}) = W\left(\underbrace{B(W(\mathbf{a}))}_{=\mathbf{d}}\right) = W(\mathbf{d}).$$

We shall now show that $\mathbf{c} = W(\mathbf{d})$.

Indeed, for any $g \in \{0, 1, \ldots, N\}$, we have

$$\begin{aligned} b_g &= \sum_{i=0}^{N} (-1)^i \binom{g}{i} a_i \qquad \text{(by (7), applied to } n = g\text{)} \\ &= \sum_{j=0}^{N} (-1)^j \binom{g}{j} a_j \end{aligned} \tag{11}$$

(here, we have renamed the summation index i as j).

Now, let $n \in \{0, 1, \ldots, N\}$ be arbitrary. Then, $n \leq N$, so that $N \geq n$. Hence,

$N - n \geq 0$, so that $0 \leq N - n \leq N$. But (8) becomes

$$c_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^N \underbrace{b_{N-i}}_{= \sum_{j=0}^{N} (-1)^j \binom{N-i}{j} a_j \text{ (by (11), applied to } g = N-i)}$$

$$= \sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^N \sum_{j=0}^{N} (-1)^j \binom{N-i}{j} a_j$$

$$= \underbrace{\sum_{i=0}^{n} \sum_{j=0}^{N}}_{= \sum_{j=0}^{N} \sum_{i=0}^{n}} (-1)^i \binom{n}{i} (-1)^N (-1)^j \binom{N-i}{j} a_j$$

$$= \sum_{j=0}^{N} \sum_{i=0}^{n} (-1)^i \binom{n}{i} (-1)^N (-1)^j \binom{N-i}{j} a_j$$

$$= \sum_{j=0}^{N} \underbrace{(-1)^N (-1)^j}_{= (-1)^{N+j} = (-1)^{N-j} \text{ (since } N+j \equiv N-j \bmod 2)} \underbrace{\left(\sum_{i=0}^{n} (-1)^i \binom{n}{i} \binom{N-i}{j} \right)}_{= \binom{N-n}{N-j} \text{ (by Lemma 0.6 (since } N \geq j))} \underbrace{a_j}_{= a_{N-(N-j)} \text{ (since } j = N-(N-j))}$$

$$= \sum_{j=0}^{N} (-1)^{N-j} \binom{N-n}{N-j} a_{N-(N-j)} = \sum_{i=0}^{N} (-1)^i \binom{N-n}{i} a_{N-i}$$

(here, we have substituted i for $N - j$ in the sum)

$$= \sum_{i=0}^{N-n} (-1)^i \binom{N-n}{i} a_{N-i} + \sum_{i=N-n+1}^{N} (-1)^i \underbrace{\binom{N-n}{i}}_{= 0 \text{ (by Proposition 0.2, applied to } N-n \text{ and } i \text{ instead of } m \text{ and } n \text{ (since } N-n < i \text{ (since } i \geq N-n+1 > N-n))\text{)}} a_{N-i}$$

(here, we have split the sum at $i = N - n$ (because $0 \leq N - n \leq N$))

$$= \sum_{i=0}^{N-n} (-1)^i \binom{N-n}{i} a_{N-i} + \underbrace{\sum_{i=N-n+1}^{N} (-1)^i 0 a_{N-i}}_{=0} = \sum_{i=0}^{N-n} (-1)^i \binom{N-n}{i} a_{N-i}.$$

Comparing this with

$$\begin{aligned}
&(-1)^N \underbrace{d_{N-n}}_{\substack{=\sum_{i=0}^{N-n}(-1)^i\binom{N-n}{i}(-1)^N a_{N-i} \\ \text{(by (9), applied to } N-n \\ \text{instead of } n)}} \\
&= (-1)^N \left(\sum_{i=0}^{N-n} (-1)^i \binom{N-n}{i} (-1)^N a_{N-i} \right) \\
&= \sum_{i=0}^{N-n} (-1)^i \binom{N-n}{i} \underbrace{(-1)^N (-1)^N}_{=((-1)(-1))^N = 1^N = 1} a_{N-i} = \sum_{i=0}^{N-n} (-1)^i \binom{N-n}{i} a_{N-i},
\end{aligned}$$

we obtain $c_n = (-1)^N d_{N-n}$.

Now, forget that we fixed n. We thus have proven that $c_n = (-1)^N d_{N-n}$ for each $n \in \{0, 1, \ldots, N\}$. In other words,

$$(c_0, c_1, \ldots, c_N) = \left((-1)^N d_N, (-1)^N d_{N-1}, \ldots, (-1)^N d_0 \right).$$

Thus,

$$\begin{aligned}
(B \circ W \circ B)(\mathbf{a}) &= B\left(W\left(\underbrace{B(\mathbf{a})}_{=\mathbf{b}} \right) \right) = B(W(\mathbf{b})) = \mathbf{c} \\
&= (c_0, c_1, \ldots, c_N) = \left((-1)^N d_N, (-1)^N d_{N-1}, \ldots, (-1)^N d_0 \right) \\
&= W\left(\underbrace{\mathbf{d}}_{=B(W(\mathbf{a}))} \right) \qquad \text{(by (10))} \\
&= W(B(W(\mathbf{a}))) = (W \circ B \circ W)(\mathbf{a}).
\end{aligned}$$

Now, forget that we fixed $\mathbf{a}$. We thus have proven that $(B \circ W \circ B)(\mathbf{a}) = (W \circ B \circ W)(\mathbf{a})$ for each list $\mathbf{a}$ of $N+1$ rational numbers. In other words,

$$B \circ W \circ B = W \circ B \circ W. \tag{12}$$

Next, we notice that

$$B \circ B = \mathrm{id} \tag{13}$$

[4] and

$$W \circ W = \mathrm{id} \tag{16}$$

[4] *Proof.* Let $\mathbf{a}$ be a list of $N+1$ rational numbers. Write $\mathbf{a}$ in the form $\mathbf{a} = (a_0, a_1, \ldots, a_N)$.

Let $\mathbf{b}$ be the list $B(\mathbf{a})$. Write the list $\mathbf{b}$ in the form $\mathbf{b} = (b_0, b_1, \ldots, b_N)$. Recall that $B(\mathbf{a})$ is the binomial transform of the list $\mathbf{a}$. In other words, $(b_0, b_1, \ldots, b_N)$ is the binomial transform of the

list $(a_0, a_1, \ldots, a_N)$ (since $\mathbf{a} = (a_0, a_1, \ldots, a_N)$ and $B(\mathbf{a}) = \mathbf{b} = (b_0, b_1, \ldots, b_N)$). Thus,

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \{0, 1, \ldots, N\}$$

(by the definition of the binomial transform). Hence, Exercise 5 on homework set #4 says that

$$a_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \qquad \text{for each } n \in \{0, 1, \ldots, N\}. \tag{14}$$

Let $\mathbf{c}$ be the list $B(\mathbf{b})$. Write the list $\mathbf{c}$ in the form $\mathbf{c} = (c_0, c_1, \ldots, c_N)$. Recall that $B(\mathbf{b})$ is the binomial transform of the list $\mathbf{b}$. In other words, $(c_0, c_1, \ldots, c_N)$ is the binomial transform of the list $(b_0, b_1, \ldots, b_N)$ (since $\mathbf{b} = (b_0, b_1, \ldots, b_N)$ and $B(\mathbf{b}) = \mathbf{c} = (c_0, c_1, \ldots, c_N)$). Thus,

$$c_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \qquad \text{for each } n \in \{0, 1, \ldots, N\} \tag{15}$$

(by the definition of the binomial transform).

Now, for each $n \in \{0, 1, \ldots, N\}$, we have

$$\begin{aligned} c_n &= \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \qquad \text{(by (15))} \\ &= a_n \qquad \text{(by (14))}. \end{aligned}$$

In other words, $(c_0, c_1, \ldots, c_N) = (a_0, a_1, \ldots, a_N)$. Thus,

$$\begin{aligned} (B \circ B)(\mathbf{a}) &= B\left(\underbrace{B(\mathbf{a})}_{=\mathbf{b}}\right) = B(\mathbf{b}) = \mathbf{c} = (c_0, c_1, \ldots, c_N) = (a_0, a_1, \ldots, a_N) \\ &= \mathbf{a} = \mathrm{id}(\mathbf{a}). \end{aligned}$$

Now, forget that we fixed $\mathbf{a}$. We thus have shown that $(B \circ B)(\mathbf{a}) = \mathrm{id}(\mathbf{a})$ for each list $\mathbf{a}$ of $N+1$ rational numbers. In other words, $B \circ B = \mathrm{id}$. This proves (13).

[5]. Hence,

$$(B \circ W)^3 = \underbrace{B \circ W \circ B}_{\substack{=W \circ B \circ W \\ \text{(by (12))}}} \circ W \circ B \circ W = W \circ B \circ \underbrace{W \circ W}_{\substack{=\mathrm{id} \\ \text{(by (16))}}} \circ B \circ W$$
$$= W \circ \underbrace{B \circ B}_{\substack{=\mathrm{id} \\ \text{(by (13))}}} \circ W = W \circ W = \mathrm{id} \qquad \text{(by (16))}\,.$$

This completes the solution of Exercise 2. □

TODO: Write up the second solution.

0.2. Another recurrence

Exercise 3. Consider the sequence $(a_0, a_1, a_2, \ldots)$ of integers given by

$$a_0 = 2, \qquad a_1 = 20, \qquad a_n = 20a_{n-1} - 99a_{n-2} \qquad \text{for } n \geq 2.$$

Find an explicit formula for a_n.

[5] *Proof.* Let $\mathbf{a}$ be a list of $N+1$ rational numbers. Write $\mathbf{a}$ in the form $\mathbf{a} = (a_0, a_1, \ldots, a_N)$.

Let $\mathbf{b}$ be the list $W(\mathbf{a})$. Write the list $\mathbf{b}$ in the form $\mathbf{b} = (b_0, b_1, \ldots, b_N)$. Thus, $(b_0, b_1, \ldots, b_N) = \mathbf{b} = W(\mathbf{a}) = \left((-1)^N a_N, (-1)^N a_{N-1}, \ldots, (-1)^N a_0\right)$ (by the definition of $W(\mathbf{a})$, because $\mathbf{a} = (a_0, a_1, \ldots, a_N)$). In other words,

$$b_n = (-1)^N a_{N-n} \qquad \text{for each } n \in \{0, 1, \ldots, N\}\,. \tag{17}$$

Hence, for each $n \in \{0, 1, \ldots, N\}$, we have

$$(-1)^N \underbrace{b_{N-n}}_{\substack{=(-1)^N a_{N-(N-n)} \\ \text{(by (17), applied} \\ \text{to } N-n \text{ instead of } n)}} = \underbrace{(-1)^N (-1)^N}_{=((-1)(-1))^N = 1^N = 1} a_{N-(N-n)} = a_{N-(N-n)} = a_n$$

(since $N - (N-n) = n$). In other words,

$$\left((-1)^N b_N, (-1)^N b_{N-1}, \ldots, (-1)^N b_0\right) = (a_0, a_1, \ldots, a_N)\,.$$

But recall that $\mathbf{b} = (b_0, b_1, \ldots, b_N)$. Hence, the definition of $W(\mathbf{b})$ yields

$$W(\mathbf{b}) = \left((-1)^N b_N, (-1)^N b_{N-1}, \ldots, (-1)^N b_0\right) = (a_0, a_1, \ldots, a_N) = \mathbf{a}.$$

Thus,

$$(W \circ W)(\mathbf{a}) = W\left(\underbrace{W(\mathbf{a})}_{=\mathbf{b}}\right) = W(\mathbf{b}) = \mathbf{a} = \mathrm{id}(\mathbf{a})\,.$$

Now, forget that we fixed $\mathbf{a}$. We thus have shown that $(W \circ W)(\mathbf{a}) = \mathrm{id}(\mathbf{a})$ for each list $\mathbf{a}$ of $N+1$ rational numbers. In other words, $W \circ W = \mathrm{id}$. This proves (16).

[**Hint:** Use of generating functions is allowed. To solve Exercise 3 in the same way as I proved Binet's formula in class, partial fraction decomposition is needed. The Wikipedia examples can be useful.]

Solution to Exercise 3 (sketched). The answer is $a_n = 9^n + 11^n$. Once you have guessed this, you can of course prove this by a strong induction over n. But how can you find this?

Essentially every way to prove the Binet formula for the Fibonacci sequence can be repurposed to prove $a_n = 9^n + 11^n$. Let me outline how this can be done using generating functions: Define the generating function $A(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ (a formal power series in the indeterminate x over $\mathbb{C}$). Then,

$$\begin{aligned}
A(x) &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \cdots \\
&= 2 + 20x + (20a_1 - 99a_0) x^2 + (20a_2 - 99a_1) x^3 + (20a_3 - 99a_2) x^4 + \cdots \\
&\qquad \text{(by the recursive definition of our sequence)} \\
&= 2 + 20x + 20x \underbrace{\left(a_1 x + a_2 x^2 + a_3 x^3 + \cdots\right)}_{= A(x) - a_0 = A(x) - 2} - 99x^2 \underbrace{\left(a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots\right)}_{= A(x)} \\
&= 2 + 20x + 20x\left(A(x) - 2\right) - 99x^2 A(x) \\
&= 2 - 20x + 20xA(x) - 99x^2 A(x).
\end{aligned}$$

This is a linear equation in $A(x)$. Solving it results in

$$A(x) = \frac{2 - 20x}{1 - 20x + 99x^2}.$$

The denominator $1 - 20x + 99x^2$ can be factored as $(1 - 9x)(1 - 11x)$ (and you can find this factorization easily by finding the roots of $1 - 20x + 99x^2$, using the quadratic formula). Thus,

$$\begin{aligned}
A(x) = \frac{2 - 20x}{(1 - 9x)(1 - 11x)} &= \underbrace{\frac{1}{1 - 9x}}_{= \sum_{n \geq 0} (9x)^n = \sum_{n \geq 0} 9^n x^n} + \underbrace{\frac{1}{1 - 11x}}_{= \sum_{n \geq 0} (11x)^n = \sum_{n \geq 0} 11^n x^n} \\
&\qquad \text{(by partial fraction decomposition)} \\
&= \sum_{n \geq 0} 9^n x^n + \sum_{n \geq 0} 11^n x^n = \sum_{n \geq 0} \left(9^n + 11^n\right) x^n.
\end{aligned}$$

Comparing coefficients of x^n, we obtain $a_n = 9^n + 11^n$ (since the coefficient of x^n in $A(x)$ is a_n). □

0.3. Counting permutations by descents

If σ is a permutation of $[n]$ for some $n \in \mathbb{N}$, then a *descent* of σ means an element $i \in [n-1]$ satisfying $\sigma(i) > \sigma(i+1)$. For example, the permutation σ of $[5]$ with

$(\sigma(1), \sigma(2), \sigma(3), \sigma(4), \sigma(5)) = (3,1,4,5,2)$ has descents 1 (since $3 > 1$) and 4 (since $5 > 2$).

Exercise 4. Let n be a positive integer. How many permutations of $[n]$ have at most 1 descent?

(For example, the permutation σ of $[5]$ with $(\sigma(1), \sigma(2), \sigma(3), \sigma(4), \sigma(5)) = (1,4,2,3,5)$ has exactly 1 descent: namely, 2 is its only descent.)

Solution to Exercise 4 (sketched). The answer is $2^n - n$. Let me give a proof.

How many permutations of $[n]$ have no descents? These are clearly the permutations σ of $[n]$ satisfying $\sigma(1) \leq \sigma(2) \leq \cdots \leq \sigma(n)$. There is only one such permutation: namely, id. (See [Grinbe16, Exercise 5.2 **(d)**] for the rigorous proof.) Thus,

$$(\text{the number of permutations of } [n] \text{ having no descents}) = 1. \tag{18}$$

Now, fix $k \in [n-1]$. How many permutations of $[n]$ have k as their only descent?

Let us ask a somewhat simpler question: How many permutations of $[n]$ have no descents apart from k (but may or may not have k as a descent)? These are the permutations σ of $[n]$ satisfying

$$\sigma(1) \leq \sigma(2) \leq \cdots \leq \sigma(k) \qquad \text{and} \qquad \sigma(k+1) \leq \sigma(k+2) \leq \cdots \leq \sigma(n).$$

Here is one way to construct such a permutation σ:

- First, choose a k-element subset S of $[n]$ to become the set $\{\sigma(1), \sigma(2), \ldots, \sigma(k)\}$. There are $\dbinom{n}{k}$ choices here.
- Then, the values of $\sigma(1), \sigma(2), \ldots, \sigma(k)$ are uniquely determined (indeed, they have to be the k elements of S in increasing order).
- Furthermore, the values of $\sigma(k+1), \sigma(k+2), \ldots, \sigma(n)$ are also uniquely determined (indeed, they have to be the $n-k$ elements of $[n] \setminus S$ in increasing order).

Thus, in total, we have $\dbinom{n}{k}$ options. Hence,

$$(\text{the number of permutations of } [n] \text{ having no descents apart from } k) = \binom{n}{k}.$$

Hencce,

$$\begin{aligned}
&\binom{n}{k} \\
&= (\text{the number of permutations of } [n] \text{ having no descents apart from } k) \\
&= (\text{the number of permutations of } [n] \text{ having } k \text{ as their only descent}) \\
&\qquad + \underbrace{(\text{the number of permutations of } [n] \text{ having no descents})}_{\substack{=1 \\ \text{(by (18))}}} \\
&= (\text{the number of permutations of } [n] \text{ having } k \text{ as their only descent}) + 1.
\end{aligned}$$

Hence,

$$\begin{aligned}
&(\text{the number of permutations of } [n] \text{ having } k \text{ as their only descent}) \\
&= \binom{n}{k} - 1. \qquad (19)
\end{aligned}$$

Now, forget that we fixed k. We thus have proven (19) for each $k \in [n-1]$.

But any descent of a permutation of $[n]$ must be one of the integers $1, 2, \ldots, n-1$. Hence,

$$\begin{aligned}
&(\text{the number of permutations of } [n] \text{ having exactly 1 descent}) \\
&= \sum_{k=1}^{n-1} \underbrace{(\text{the number of permutations of } [n] \text{ having } k \text{ as their only descent})}_{\substack{=\binom{n}{k}-1 \\ \text{(by (19))}}} \\
&= \sum_{k=1}^{n-1} \left(\binom{n}{k} - 1 \right) = \sum_{k=0}^{n} \left(\binom{n}{k} - 1 \right) - \left(\underbrace{\binom{n}{0}}_{=1} - 1 \right) - \left(\underbrace{\binom{n}{n}}_{=1} - 1 \right) \\
&\qquad \left(\begin{array}{c} \text{because the sum } \sum\limits_{k=1}^{n-1} \left(\binom{n}{k} - 1 \right) \text{ differs from the sum } \sum\limits_{k=0}^{n} \left(\binom{n}{k} - 1 \right) \\ \text{in the lack of the addends for } k = 0 \text{ and for } k = n \end{array} \right) \\
&= \sum_{k=0}^{n} \left(\binom{n}{k} - 1 \right) - (1-1) - (1-1) = \sum_{k=0}^{n} \left(\binom{n}{k} - 1 \right) \\
&= \underbrace{\sum_{k=0}^{n} \binom{n}{k}}_{\substack{=2^n \\ \text{(as you should} \\ \text{know by now)}}} - (n+1) = 2^n - (n+1).
\end{aligned}$$

Finally,

$$\begin{aligned}
&(\text{the number of permutations of } [n] \text{ having at most 1 descent}) \\
&= \underbrace{(\text{the number of permutations of } [n] \text{ having exactly 1 descent})}_{=2^n-(n+1)} \\
&\qquad + \underbrace{(\text{the number of permutations of } [n] \text{ having no descents})}_{\substack{=1 \\ \text{(by (18))}}} \\
&= (2^n - (n+1)) + 1 = 2^n - n.
\end{aligned}$$

□

0.4. Counting derangements squaring to the identity

Exercise 5. Let $n \in \mathbb{N}$. How many derangements σ of $[n]$ satisfy $\sigma^2 = \mathrm{id}$?

(For example, the derangement σ of $[6]$ sending $1,2,3,4,5,6$ to $3,6,1,5,4,2$ satisfies $\sigma^2 = \mathrm{id}$.)

[**Hint:** The answer will depend on whether n is even or odd.]

Solution to Exercise 5 (sketched). The answer is

$$\begin{cases} (n-1)(n-3)\cdots 1, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

The proof in the case of even n is similar to part of the proof of Observation 2 in the solution of Exercise 3 on homework set #4.

TODO: Details. □

0.5. Iteration of maps on finite sets

The next two exercises study what happens if you apply a map from a finite set to itself several times.

Exercise 6. Let $n \in \mathbb{N}$. Let S be an n-element set. Let $f : S \to S$ be any map.

(a) Prove that $f^0(S) \supseteq f^1(S) \supseteq f^2(S) \supseteq \cdots$.

(b) Prove that $f^n(S) = f^k(S)$ for each integer $k \geq n$.

(c) Define a map $g : f^n(S) \to f^n(S)$ by

$$g(x) = f(x) \qquad \text{for each } x \in f^n(S).$$

(Thus, g is the restriction of f onto the image $f^n(S)$, regarded as a map from $f^n(S)$ to $f^n(S)$.)

Prove that g is well-defined (i.e., that $f(x)$ actually belongs to $f^n(S)$ for each $x \in f^n(S)$) and is a permutation of $f^n(S)$.

[**Hint:** For part **(b)**, first prove that there exists some $m \in \{0,1,\ldots,n\}$ such that $f^m(S) = f^{m+1}(S)$. Then argue that $f^n(S) = f^{n+1}(S)$.]

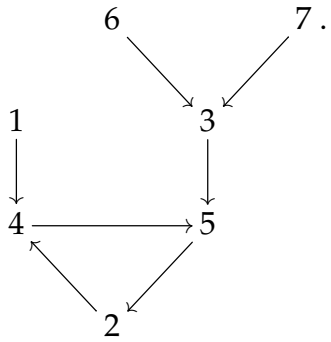
Example 0.9. Let $n = 7$. Let $S = [7]$. Let $f : S \to S$ be the map with

$$(f(1), f(2), f(3), f(4), f(5), f(6), f(7)) = (4,4,5,5,2,3,3).$$

Then,

$$\begin{aligned}
&f^0(S) = S = \{1,2,3,4,5,6,7\};\\
&f^1(S) = f(S) = \{2,3,4,5\};\\
&f^2(S) = \{2,4,5\};\\
&f^k(S) = \{2,4,5\} \qquad \text{for each } k \geq 2.
\end{aligned}$$

Thus, in particular, $f^n(S) = \{2,4,5\}$. The map g is the permutation of this set $f^n(S) = \{2,4,5\}$ sending $2,4,5$ to $4,5,2$, respectively. It is perhaps worthwhile to draw the "cycle digraph" of f (which is not literally a cycle digraph, because f is not a permutation, but is constructed in the same way):



Solution to Exercise 6 (sketched). **(a)** We must show that $f^k(S) \supseteq f^{k+1}(S)$ for each $k \in \mathbb{N}$. But this is clear: If $k \in \mathbb{N}$, then $f^{k+1}(S) = f^k\left(\underbrace{f(S)}_{\subseteq S}\right) \subseteq f^k(S)$.

(b) Part **(a)** shows that $f^0(S) \supseteq f^1(S) \supseteq f^2(S) \supseteq \cdots$. Hence, $\left|f^0(S)\right| \geq \left|f^1(S)\right| \geq \left|f^2(S)\right| \geq \cdots$.

In other words, the sequence $\left(\left|f^0(S)\right|, \left|f^1(S)\right|, \left|f^2(S)\right|, \ldots\right)$ is weakly decreasing. The rough idea of the following argument is to show that this sequence must stagnate somewhere between its first $n+2$ elements (that is, there must exist some $p \in [n+1]$ satisfying $\left|f^{p-1}(S)\right| = \left|f^p(S)\right|$); and then, to show that once it stagnates, it stays constant (i.e., once two consecutive terms of this sequence are equal, all the terms that follow must also be equal).

Here is the rigorous version:

We claim that there exists some $p \in [n+1]$ satisfying $\left|f^{p-1}(S)\right| = \left|f^p(S)\right|$. Indeed, assume the contrary. Thus, each $p \in [n+1]$ satisfies $\left|f^{p-1}(S)\right| \neq \left|f^p(S)\right|$,

and thus $\left|f^{p-1}(S)\right| > \left|f^{p}(S)\right|$ (since $\left|f^{0}(S)\right| \geq \left|f^{1}(S)\right| \geq \left|f^{2}(S)\right| \geq \cdots$). Hence,

$$\left|f^{0}(S)\right| > \left|f^{1}(S)\right| > \cdots > \left|f^{n+1}(S)\right|.$$

Thus, the $n+2$ numbers $\left|f^{0}(S)\right|, \left|f^{1}(S)\right|, \ldots, \left|f^{n+1}(S)\right|$ are distinct. But this is absurd, because these $n+2$ numbers all lie in the $(n+1)$-element set $\{0,1,\ldots,n\}$ (since they are sizes of subsets of the n-element set S) and therefore (by the pigeonhole principle) they cannot be all distinct. Thus, we obtain a contradiction.

Hence, we have shown that there exists some $p \in [n+1]$ satisfying $\left|f^{p-1}(S)\right| = \left|f^{p}(S)\right|$. Consider this p.

Part **(a)** shows that $f^{p-1}(S) \supseteq f^{p}(S)$. Combined with $\left|f^{p-1}(S)\right| = \left|f^{p}(S)\right|$, this yields $f^{p-1}(S) = f^{p}(S)$ [6].

Now, I claim that

$$f^{p-1}(S) = f^{h}(S) \qquad \text{for each } h \geq p-1. \tag{20}$$

[*Proof of (20):* Induction over h.

The *induction base* (the case $h = p-1$) is tautological.

For the *induction step*, assume that $f^{p-1}(S) = f^{h}(S)$ for some $h \geq p-1$; we then must show that $f^{p-1}(S) = f^{h+1}(S)$.

Apply the map f to both sides of the equality $f^{p-1}(S) = f^{h}(S)$, we obtain $f\left(f^{p-1}(S)\right) = f\left(f^{h}(S)\right) = f^{h+1}(S)$. Comparing this with $f\left(f^{p-1}(S)\right) = f^{p}(S) = f^{p-1}(S)$, we obtain $f^{p-1}(S) = f^{h+1}(S)$. This completes the induction step. Thus, (20) is proven.]

We have $p \in [n+1]$, so that $p \leq n+1$, so that $n \geq p-1$. Hence, (20) (applied to $h = n$) yields $f^{p-1}(S) = f^{n}(S)$.

Let $k \geq n$ be an integer. Thus, $k \geq n \geq p-1$ and therefore $f^{p-1}(S) = f^{k}(S)$ (by (20), applied to $h = k$). Comparing this with $f^{p-1}(S) = f^{n}(S)$, we obtain $f^{n}(S) = f^{k}(S)$. This solves part **(b)**.

(c) It is straightforward to see that g is well-defined: after all, each $x \in f^{n}(S)$ satisfies $f(x) \in f\left(f^{n}(S)\right) = f^{n+1}(S) = f^{n}\left(\underbrace{f(S)}_{\subseteq S}\right) \subseteq f^{n}(S)$.

It remains to prove that g is a permutation of $f^{n}(S)$. In other words, it remains to prove that g is bijective.

The definition of g shows that $g\left(f^{n}(S)\right) = f\left(f^{n}(S)\right) = f^{n+1}(S)$. But $n+1 \geq n$. Hence, part **(b)** (applied to $k = n+1$) yields $f^{n}(S) = f^{n+1}(S)$. Hence, $g\left(f^{n}(S)\right) = f^{n+1}(S) = f^{n}(S)$. In other words, the map g is surjective. Hence, this map g is bijective (since any surjective map between two finite sets of equal sizes is bijective). As we have said, this completes the solution of part **(c)**.

TODO: More details. □

[6] What we have used here is the fact that if two finite sets A and B satisfy $A \supseteq B$ and $|A| = |B|$, then $A = B$. (We have applied this fact to $A = f^{p-1}(S)$ and $B = f^{p}(S)$.)

Exercise 7. Let $n \in \mathbb{N}$. Let S be an n-element set. Let $f : S \to S$ be any map.

(a) If f is a permutation of S, then prove that there exists some $p \in [n!]$ such that $f^p = \mathrm{id}$.

(b) Prove in general (i.e., not only when f is a permutation) that there exist two integers u and v with $0 \leq u < v \leq n!$ and $f^u = f^v$.

[**Hint:** First prove part **(b)** in the case when f is a permutation (hint: what does the pigeonhole principle say about the permutations $f^0, f^1, \ldots, f^{n!}$?). Then, use this to show part **(a)**. Finally, prove part **(b)** in the general case, by applying part **(a)** to the map g from Exercise 6.]

Solution to Exercise 7 (sketched). **(a)** Assume that f is a permutation of S. Since f is bijective, so are all the $n! + 1$ maps $f^0, f^1, \ldots, f^{n!}$ (since a composition of bijective maps is always bijective). In other words, $f^0, f^1, \ldots, f^{n!}$ are $n! + 1$ permutations of S. But there are only $n!$ permutations of S. Hence, by the pigeonhole principle, (at least) two of these permutations $f^0, f^1, \ldots, f^{n!}$ are equal. That is, there exist two integers u and v with $0 \leq u < v \leq n!$ and $f^u = f^v$. Consider these u and v. Now, $f^u = f^v = f^{v-u} \circ f^u$. Since f^u is bijective, we can cancel f^u from this equality, and thus find $\mathrm{id} = f^{v-u}$. Since $v - u \in [n!]$, we are done with part **(a)**.

(b) If f is surjective, then f must be bijective (since any surjective map between two finite sets of equal sizes is bijective), and therefore f is a permutation of S; but then, the claim of part **(b)** follows from part **(a)**. Hence, we WLOG assume that f is not surjective. Thus, the image $f(S)$ is a **proper** subset of S. Hence, S has a proper subset; thus, $S \neq \varnothing$. Hence, $f^n(S) \neq \varnothing$. Let $q = |f^n(S)|$.

Let g be as in Exercise 6 **(c)**. Then, g is a permutation of $f^n(S)$ (by Exercise 6 **(c)**). Exercise 7 **(a)** (applied to $f^n(S)$, q and g instead of S, n and f) thus shows that there exists some $p \in [q!]$ such that $g^p = \mathrm{id}$. Consider this p.

Each $x \in f^n(S)$ satisfies $g(x) = f(x)$ (by the definition of g) and thus

$$g^r(x) = f^r(x)$$

for each $r \in \mathbb{N}$ (by induction over r). Applying this to $r = p$, we conclude that every $x \in f^n(S)$ satisfies $g^p(x) = f^p(x)$, hence

$$f^p(x) = \underbrace{g^p}_{=\mathrm{id}}(x) = \mathrm{id}(x) = x. \tag{21}$$

Thus,

$$f^n = f^{p+n}. \tag{22}$$

[*Proof of (22):* Let $y \in S$. Then, $f^n(y) \in f^n(S)$. Hence, (21) (applied to $x = f^n(y)$) yields $f^p(f^n(y)) = f^n(y)$. Thus, $f^n(y) = f^p(f^n(y)) = f^{p+n}(y)$. Since we have shown this for each $y \in S$, we thus conclude that $f^n = f^{p+n}$. This proves (22).]

But Exercise 6 **(a)** yields $f^0(S) \supseteq f^1(S) \supseteq f^2(S) \supseteq \cdots$, so that $f^1(S) \supseteq f^n(S)$ (since $n = |S| > 0$ (because $S \neq \varnothing$)). Hence, $f^n(S) \subseteq f^1(S) = f(S)$. Therefore, $f^n(S)$ is a proper subset of S (since $f(S)$ is a proper subset of S). Thus, $|f^n(S)| <$

$|S| = n$. Thus, $q = |f^n(S)| < n$, so that $q \leq n-1$, and thus $q! \leq (n-1)!$ (since $0! \leq 1! \leq 2! \leq \cdots$).

From $p \in [q!]$, we obtain $0 < p \leq q!$.

If $n \leq 2$, then the claim of Exercise 7 **(b)** can easily be checked by hand (since there are at most 4 maps $f : S \to S$ in this case). Thus, WLOG assume that $n > 2$. Thus, $n \geq 3$, and therefore $n \leq (n-1)^2$ (check this!). Hence,

$$\begin{aligned} n \leq (n-1)^2 &= (n-1) \cdot \underbrace{(n-1)}_{\leq 1 \cdot 2 \cdot \cdots \cdot (n-1) = (n-1)!} \leq (n-1) \cdot (n-1)! \\ &= \underbrace{n \cdot (n-1)!}_{=n!} - (n-1)! = n! - (n-1)!. \end{aligned}$$

Hence, $n + (n-1)! \leq n!$, so that $n + \underbrace{q!}_{\leq (n-1)!} \leq n + (n-1)! \leq n!$. Thus,

$$0 \leq n = \underbrace{0}_{<p} + n < \underbrace{p}_{\leq q!} + n \leq q! + n = n + q! \leq n!.$$

Hence, from (22), we conclude that there exist two integers u and v with $0 \leq u < v \leq n!$ and $f^u = f^v$ (namely, $u = n$ and $v = p + n$). This solves Exercise 7 **(b)**.

TODO: More details. □

References

[Galvin17] David Galvin, *Basic discrete mathematics*, 13 December 2017.
`http://www.cip.ifi.lmu.de/~grinberg/t/17f/60610lectures2017-Galvin.pdf`

[Grinbe16] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .