University of Minnesota, School of Mathematics

Math 5705: Enumerative Combinatorics, Fall 2018: Homework 2

Darij Grinberg

October 25, 2019

1 Exercise 1

1.1 Problem

For any nonnegative integers a and b and any real x, prove that

$$\binom{x}{a}\binom{x}{b} = \sum_{r=\max\{a,b\}}^{a+b} \binom{a}{a+b-r}\binom{r}{a}\binom{x}{r}. \tag{1}$$

1.2 Solution sketch

1.2.1 First solution

Let a and b be nonnegative integers. Let x be a real. Whenever $k \in \mathbb{N}$, we shall use the standard notation $x^{\underline{k}}$ for the lower factorial $x(x-1)(x-2)\cdots(x-k+1)$. Recall that

$$\binom{x}{k} = \frac{x^{\underline{k}}}{k!} \qquad \text{for each } k \in \mathbb{N}. \tag{2}$$

Applying this to $k = r$, we obtain

$$\binom{x}{r} = \frac{x^{\underline{r}}}{r!}. \tag{3}$$

Let us also recall the following classical formula:

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \qquad \text{for any } n \in \mathbb{N} \text{ and } k \in \mathbb{N} \text{ satisfying } n \geq k. \tag{4}$$

But Exercise 7 on homework set #1 yields

$$x^{\underline{a}}x^{\underline{b}} = \sum_{r=\max\{a,b\}}^{a+b} \frac{a!b!}{(r-a)!\,(r-b)!\,(a+b-r)!}x^{\underline{r}}. \tag{5}$$

Next, we claim:

Claim 1: Let r be an integer such that $\max\{a,b\} \leq r \leq a+b$. Then, $\dfrac{1}{(r-a)!\,(r-b)!\,(a+b-r)!}$ is well-defined and satisfies

$$\frac{1}{(r-a)!\,(r-b)!\,(a+b-r)!} = \frac{1}{r!}\binom{a}{a+b-r}\binom{r}{a}. \tag{6}$$

[*Proof of Claim 1:* We have $a \leq \max\{a,b\} \leq r$, thus $r-a \geq 0$ and therefore $r-a \in \mathbb{N}$. Hence, $(r-a)!$ is a well-defined positive integer. The same argument (applied to b instead of a) shows that $(r-b)!$ is a well-defined positive integer. Also, $a+b-r \geq 0$ (since $r \leq a+b$), and thus $a+b-r \in \mathbb{N}$; hence, $(a+b-r)!$ is a well-defined positive integer. Now we know that all three factorials $(r-a)!$, $(r-b)!$ and $(a+b-r)!$ are well-defined positive integers; thus, their product $(r-a)!\,(r-b)!\,(a+b-r)!$ is a well-defined positive integer as well. Hence, this product is nonzero. Thus, $\dfrac{1}{(r-a)!\,(r-b)!\,(a+b-r)!}$ is well-defined. It remains to prove the equality (6).

From $r-a \geq 0$, we obtain $r \geq a$. We have $b \leq \max\{a,b\} \leq r$, thus $r-b \geq 0$. We have $a \in \mathbb{N}$ and $a+b-r \in \mathbb{N}$ and $a \geq a+b-r$ (since $a-(a+b-r) = r-b \geq 0$). Thus, (4) (applied to $n=a$ and $k=a+b-r$) yields

$$\binom{a}{a+b-r} = \frac{a!}{(a+b-r)!\,(a-(a+b-r))!} = \frac{a!}{(a+b-r)!\,(r-b)!}.$$

Also, (4) (applied to $n=r$ and $k=a$) yields

$$\binom{r}{a} = \frac{r!}{a!\,(r-a)!} \qquad (\text{since } r \in \mathbb{N} \text{ and } a \in \mathbb{N} \text{ and } r \geq a).$$

Multiplying the last two equalities, we find

$$\binom{a}{a+b-r}\binom{r}{a} = \frac{a!}{(a+b-r)!\,(r-b)!} \cdot \frac{r!}{a!\,(r-a)!} = \frac{r!}{(r-a)!\,(r-b)!\,(a+b-r)!}.$$

Multiplying both sides of this equality by $\dfrac{1}{r!}$, we obtain

$$\frac{1}{r!}\binom{a}{a+b-r}\binom{r}{a} = \frac{1}{r!} \cdot \frac{r!}{(r-a)!\,(r-b)!\,(a+b-r)!} = \frac{1}{(r-a)!\,(r-b)!\,(a+b-r)!}.$$

This proves (6). Hence, Claim 1 is proven.]

Now, applying (3) to $r=a$, we find

$$\binom{x}{a} = \frac{x^{\underline{a}}}{a!}.$$

Also, applying (3) to $r=b$, we find

$$\binom{x}{b} = \frac{x^{\underline{b}}}{b!}.$$

Multiplying these two equalities, we obtain

$$\begin{aligned}
\binom{x}{a}\binom{x}{b} &= \frac{x^{\underline{a}}}{a!}\cdot\frac{x^{\underline{b}}}{b!} = \frac{1}{a!}\cdot\frac{1}{b!}\cdot x^{\underline{a}}x^{\underline{b}} \\
&= \frac{1}{a!}\cdot\frac{1}{b!}\cdot\sum_{r=\max\{a,b\}}^{a+b}\frac{a!b!}{(r-a)!\,(r-b)!\,(a+b-r)!}x^{\underline{r}} \qquad \text{(by (5))} \\
&= \sum_{r=\max\{a,b\}}^{a+b}\underbrace{\frac{1}{(r-a)!\,(r-b)!\,(a+b-r)!}}_{\substack{=\frac{1}{r!}\binom{a}{a+b-r}\binom{r}{a} \\ \text{(by (6))}}}x^{\underline{r}} = \sum_{r=\max\{a,b\}}^{a+b}\frac{1}{r!}\binom{a}{a+b-r}\binom{r}{a}x^{\underline{r}} \\
&= \sum_{r=\max\{a,b\}}^{a+b}\binom{a}{a+b-r}\binom{r}{a}\underbrace{\frac{x^{\underline{r}}}{r!}}_{\substack{=\binom{x}{r} \\ \text{(by (3))}}} = \sum_{r=\max\{a,b\}}^{a+b}\binom{a}{a+b-r}\binom{r}{a}\binom{x}{r}.
\end{aligned}$$

This solves the exercise.

1.2.2 Second solution

Let me outline a different solution, which relies on the following fact:

Theorem 1.1. *Let P and Q be two polynomials with real coefficients. Assume that $P(x) = Q(x)$ for every $x \in \mathbb{N}$. Then, $P = Q$ (as polynomials).*

This theorem is essentially Theorem 2.20 (c) from the blackboard work on 26 September 2018 (except that the polynomials have real coefficients, not rational coefficients; but this makes no difference to the proof). It is a consequence of the fact that a nonzero polynomial (with real coefficients) cannot have infinitely many roots. We call it the "polynomial identity trick" in class.

Next, we prove the particular case of the exercise in which x is a nonnegative integer:

Claim 2: Let $a \in \mathbb{N}$, $b \in \mathbb{N}$ and $x \in \mathbb{N}$. Then,

$$\binom{x}{a}\binom{x}{b} = \sum_{r=\max\{a,b\}}^{a+b}\binom{a}{a+b-r}\binom{r}{a}\binom{x}{r}.$$

[*Proof of Claim 2:* Fix an x-element set X. Let us count all pairs (A, B) consisting of an a-element subset A of X and a b-element subset B of X.

1st method: Clearly, we can choose such a pair by first choosing A and then choosing B. Thus, the number of such pairs is $\binom{x}{a}\binom{x}{b}$ (since we have $\binom{x}{a}$ many options for A, and $\binom{x}{b}$ many options for B).

2nd method: Here is another method to construct such a pair:

- First, decide which size the union $U := A \cup B$ is going to have. Let r be this size. Thus, r must be an integer satisfying $\max\{a,b\} \leq r \leq a+b$ (because any two finite sets A and B satisfy $\max\{|A|,|B|\} \leq |A \cup B| \leq |A| + |B|$).

- Then, choose this U itself. This has to be an r-element subset of X; thus, there are $\binom{x}{r}$ many options for it.
- Next, we choose A. This has to be an a-element subset of U; thus, there are $\binom{r}{a}$ many options for it.
- Finally, we choose B. This has to be a b-element subset of U whose complement $U \setminus B$ is a subset of A (because otherwise, $A \cup B$ would not be U). Thus, there are $\binom{a}{r-b}$ many options for it (since choosing such a B is tantamount to choosing its complement $U \setminus B$, which is merely required to be an $(r-b)$-element subset of A).

This gives us $\sum\limits_{r=\max\{a,b\}}^{a+b} \binom{r}{a}\binom{a}{r-b}\binom{x}{r}$ many options in total.

Comparing the results of these two methods, we obtain

$$\binom{x}{a}\binom{x}{b} = \sum_{r=\max\{a,b\}}^{a+b} \binom{r}{a} \underbrace{\binom{a}{r-b}}_{\substack{=\binom{a}{a-(r-b)} \\ \text{(by the symmetry of the} \\ \text{binomial coefficients)}}} \binom{x}{r} = \sum_{r=\max\{a,b\}}^{a+b} \binom{r}{a} \underbrace{\binom{a}{a-(r-b)}}_{=\binom{a}{a+b-r}} \binom{x}{r}$$
$$= \sum_{r=\max\{a,b\}}^{a+b} \binom{a}{a+b-r}\binom{r}{a}\binom{x}{r}.$$

Hence, Claim 2 is proven.]

Now, let a and b be nonnegative integers. Define two polynomials P and Q (in one indeterminate X, with real coefficients) by

$$P = \binom{X}{a}\binom{X}{b} \qquad \text{and} \qquad Q = \sum_{r=\max\{a,b\}}^{a+b} \binom{a}{a+b-r}\binom{r}{a}\binom{X}{r}.$$

(These are indeed polynomials, since $\binom{X}{k}$ is a polynomial for each $k \in \mathbb{N}$.) Claim 2 shows that $P(x) = Q(x)$ for each $x \in \mathbb{N}$. Thus, Theorem 1.1 shows that $P = Q$. Hence, $P(x) = Q(x)$ for every real x. In other words,

$$\binom{x}{a}\binom{x}{b} = \sum_{r=\max\{a,b\}}^{a+b} \binom{a}{a+b-r}\binom{r}{a}\binom{x}{r}.$$

This solves the exercise once again.

1.3 Remark

Note that if we use the Second solution to solve the exercise, then we can walk the First solution backwards to obtain a new solution to Exercise 7 on Homework set #1.

2 Exercise 2

2.1 Problem

Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Prove that

$$\sum_{i=0}^{n} \binom{n}{i} \binom{n-i}{k-2i} 2^{k-2i} = \binom{2n}{k}. \tag{7}$$

[**Hint:** You have n pairs of shoes $(L_1, R_1), (L_2, R_2), \ldots, (L_n, R_n)$, where the $2n$ shoes $L_1, R_1, L_2, R_2, \ldots, L_n, R_n$ are all distinguishable. You grab k of these $2n$ shoes at random (i.e., pick a k-element subset of the set of all $2n$ shoes). For a given $i \in \{0, 1, \ldots, n\}$, what is the probability that among your k shoes are exactly i pairs?]

2.2 Solution sketch

2.2.1 First solution

We follow the hint (but, to stay true to our genre, we speak of counting instead of probabilities).

Let S be a set consisting of $2n$ distinct elements $L_1, R_1, L_2, R_2, \ldots, L_n, R_n$. (For the sake of definiteness, you can set $L_i = i$ and $R_i = -i$ for each $i \in [n]$.) The elements of S will be called *shoes*.

The 2-element subsets $\{L_1, R_1\}, \{L_2, R_2\}, \ldots, \{L_n, R_n\}$ of S will be called *shoe-pairs*. Thus, there are exactly n shoe-pairs, and they are distinct 2-element subsets of S and cover the whole S.

We say that a subset T *contains* a shoe-pair P if and only if $P \subseteq T$. (That is, "contains" means "contains as a subset", not "contains as an element", in this context.)

Now we claim the following:

> *Claim 1:* Let $i \in \{0, 1, \ldots, n\}$. Then, the number of k-element subsets of S that contain exactly i shoe-pairs is
>
> $$\binom{n}{i} \binom{n-i}{k-2i} 2^{k-2i}.$$

Note that we are not requiring $k - 2i \geq 0$ in Claim 1. Convince yourself that both the claim and the proof that we will now give are valid whether or not $k - 2i$ is nonnegative.

[*Proof of Claim 1:* Any k-element subset X of S that contains exactly i shoe-pairs can be constructed (uniquely) by the following procedure:

- First, we choose which i shoe-pairs our subset X will contain. We have $\binom{n}{i}$ many options in this choice (since we must choose i out of the n shoe-pairs).
- We shall refer to the chosen i shoe-pairs as *taken*; the remaining $n - i$ shoe-pairs will be called *untaken*. Our subset X must contain all taken shoe-pairs but none of the untaken shoe-pairs. Thus, X must contain all the $2i$ shoes in the i taken shoe-pairs.
- We now need to pick $k - 2i$ further shoes for X; these shoes need to come from the untaken shoe-pairs. However, we can only pick **at most one** shoe from each untaken shoe-pair, because otherwise our set X would contain the whole shoe-pair, which would

contradict the fact that X must contain none of the untaken shoe-pairs. Thus, we need to pick $k-2i$ shoes from the untaken shoe-pairs, in such a way that at most one shoe from each untaken shoe-pair is picked.

- We do this as follows: First, we choose the shoe-pairs from which we are going to pick **exactly one** shoe. In other words, we choose the set

$$Q := \{P \text{ is a shoe-pair } \mid X \text{ contains exactly one shoe from } P\}.$$

This set Q must be a subset of the set of all the $n-i$ untaken shoe-pairs (because if P is a shoe-pair contained in Q, then X contains exactly one shoe from P, and thus X cannot contain P fully; but this means that P is untaken), and must have size $k-2i$ [1]. Thus, we can choose Q in exactly $\binom{n-i}{k-2i}$ many ways.

- Finally, for each shoe-pair $P \in Q$, we choose exactly one shoe from P to be included in X. This choice can be made in 2^{k-2i} many ways (since there are $k-2i$ many shoe-pairs $P \in Q$, and for each of these shoe-pairs, we have exactly 2 options).

Thus, this procedure can be performed in precisely $\binom{n}{i}\binom{n-i}{k-2i}2^{k-2i}$ many ways. Hence, the number of k-element subsets X of S that contain exactly i shoe-pairs is

$$\binom{n}{i}\binom{n-i}{k-2i}2^{k-2i}.$$

This proves Claim 1.]

[1] *Proof.* Assume that X is already chosen. We know that X must contain a total of k shoes, and that exactly $2i$ of these k shoes come from the taken shoe-pairs. The remaining $k-2i$ shoes in X must therefore come from untaken shoe-pairs. In other words,

$$(\text{the number of shoes in } X \text{ contributed by untaken shoe-pairs}) = k-2i.$$

Each shoe-pair in Q contributes exactly one shoe to X (by the definition of Q). Thus,

$$(\text{the number of shoes in } X \text{ contributed by shoe-pairs in } Q) = |Q|. \tag{8}$$

Now, we observe the following:

- Any untaken shoe-pair that contributes a shoe to X must belong to Q. (Indeed, if it would contribute **both** of its shoes to X, then it would be a taken shoe-pair, which contradicts that it is untaken; therefore, it must contribute exactly one shoe to X, and therefore must belong to Q (by the definition of Q).)
- Conversely, any shoe-pair in Q must be untaken (since Q is a subset of the set of all untaken shoe-pairs) and must contribute a shoe to X (by the definition of Q).

Combining these two observations, we conclude that the shoe-pairs in Q are precisely the untaken shoe-pairs that contribute a shoe to X. Hence, a shoe in X is contributed by a shoe-pair in Q if and only if it is contributed by an untaken shoe-pair. Hence,

$$\begin{aligned}&(\text{the number of shoes in } X \text{ contributed by shoe-pairs in } Q)\\&= (\text{the number of shoes in } X \text{ contributed by untaken shoe-pairs}) = k-2i.\end{aligned}$$

Comparing this with (8), we obtain $|Q| = k-2i$. In other words, the set Q has size $k-2i$, qed.

The set S has $2n$ elements. Hence, the number of k-element subsets of S is $\dbinom{2n}{k}$. Thus,

$$\begin{aligned}\binom{2n}{k} &= (\text{the number of } k\text{-element subsets of } S)\\ &= \sum_{i=0}^{n} \underbrace{(\text{the number of } k\text{-element subsets of } S \text{ that contain exactly } i \text{ shoe-pairs})}_{\substack{=\binom{n}{i}\binom{n-i}{k-2i}2^{k-2i} \\ (\text{by Claim 1})}}\\ &\qquad \left(\begin{array}{c}\text{because for any } k\text{-element subset } I \text{ of } S\text{, there is a}\\ \text{unique } i \in \{0,1,\ldots,n\} \text{ such that } I \text{ contains exactly } i \text{ shoe-pairs}\end{array}\right)\\ &= \sum_{i=0}^{n} \binom{n}{i}\binom{n-i}{k-2i}2^{k-2i}.\end{aligned}$$

This solves the exercise.

2.2.2 Second solution

Let us now give an algebraic proof. Let us forget that we fixed n and k. We will first prove the following fact (Theorem 2 in `https://artofproblemsolving.com/community/c6h87265`):

Claim 2: Let $n \in \mathbb{N}$ and $u \in \mathbb{Z}$. Then,

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

[*Proof of Claim 2:* Recall that for any integer u, we have

$$\binom{0}{u} = [u=0] \qquad \text{and} \tag{9}$$

$$\binom{u}{0} = 1. \tag{10}$$

(Here, we are using the Iverson bracket notation; thus, $[u=0]$ means $\begin{cases}1, & \text{if } u=0;\\ 0, & \text{if } u \neq 0\end{cases}$.)

We will use Knuth's sum convention: The summation sign "$\sum\limits_k$" shall always mean a sum over all $k \in \mathbb{Z}$. Such a sum is well-defined whenever it has only finitely many nonzero addends. The sums that will appear in the following argument do have this property, and thus are well-defined.

First we observe the following:

$$\text{For every } k \in \mathbb{Z} \setminus \{0,1,\ldots,n\}\text{, we have } \binom{n}{2k+u}\binom{2k+u}{k} = 0. \tag{11}$$

[*Proof of* (11): Let $k \in \mathbb{Z} \setminus \{0,1,\ldots,n\}$. For the sake of contradiction, assume that $\dbinom{n}{2k+u}\dbinom{2k+u}{k} \neq 0$. Thus, $\dbinom{n}{2k+u} \neq 0$ and $\dbinom{2k+u}{k} \neq 0$.

From $\dbinom{n}{2k+u} \neq 0$ and $n \geq 0$, we conclude that $2k+u \geq 0$ and $2k+u \leq n$. From $\dbinom{2k+u}{k} \neq 0$ and $2k+u \geq 0$, we conclude that $k \geq 0$ and $k \leq 2k+u$. Now, $k \leq 2k+u$ and $2k+u \leq n$ yield $k \leq n$.

Now, $k \geq 0$ and $k \leq n$ yield $k \in \{0,1,\ldots,n\}$, contradicting $k \in \mathbb{Z} \setminus \{0,1,\ldots,n\}$. This contradiction shows that our assumption (that $\dbinom{n}{2k+u}\dbinom{2k+u}{k} \neq 0$) was wrong. Hence, we have $\dbinom{n}{2k+u}\dbinom{2k+u}{k} = 0$. This proves (11).]

Next, we are going to prove that any integers $n \geq 0$ and u satisfy

$$\sum_{k=0}^{n} 2^{n-2k-u}\binom{n}{2k+u}\binom{2k+u}{k} = \sum_{k} 2^{n-2k-u}\binom{n}{2k+u}\binom{2k+u}{k} \tag{12}$$

and

$$\sum_{k} 2^{n-2k-u}\binom{n}{2k+u}\binom{2k+u}{k} = \binom{2n}{n+u}. \tag{13}$$

[*Proof of* (12)*:* Let $n \geq 0$ and u be two integers. Then,

$$\begin{aligned}&\sum_{k} 2^{n-2k-u}\binom{n}{2k+u}\binom{2k+u}{k}\\ &= \sum_{k=0}^{n} 2^{n-2k-u}\binom{n}{2k+u}\binom{2k+u}{k} + \sum_{k\in\mathbb{Z}\setminus\{0,1,\ldots,n\}} 2^{n-2k-u}\underbrace{\binom{n}{2k+u}\binom{2k+u}{k}}_{\substack{=0\\ \text{(by (11))}}}\\ &= \sum_{k=0}^{n} 2^{n-2k-u}\binom{n}{2k+u}\binom{2k+u}{k}.\end{aligned}$$

This proves (12).]

[*Proof of* (13)*:* We shall prove (13) by induction over n:

Induction base: Let us first notice that $2^{-u}[u=0] = [u=0]$. [2]

[2] *Proof:* We shall prove this equality by considering the cases $u \neq 0$ and $u = 0$ separately:

- In the case when $u \neq 0$, this equality holds because both of its sides are 0 (since $[u=0] = 0$ in this case).
- In the case when $u = 0$, this equality also holds (since $2^{-u} = 2^{-0} = 1$ in this case).

Thus, this equality always holds.

For $n = 0$, we have

$$\begin{aligned}
&\sum_k 2^{n-2k-u} \binom{n}{2k+u} \binom{2k+u}{k} \\
&= \sum_{k=0}^{n} 2^{n-2k-u} \binom{n}{2k+u} \binom{2k+u}{k} \qquad \text{(by (12))} \\
&= \sum_{k=0}^{0} 2^{0-2k-u} \binom{0}{2k+u} \binom{2k+u}{k} \qquad \text{(since } n = 0\text{)} \\
&= 2^{0-2\cdot 0-u} \binom{0}{2\cdot 0+u} \binom{2\cdot 0+u}{0} = 2^{-u} \underbrace{\binom{0}{u}}_{\substack{=[u=0] \\ \text{(by (9))}}} \underbrace{\binom{u}{0}}_{=1} = 2^{-u} [u=0] \\
&= [u=0] = \binom{0}{u} \qquad \text{(by (9))} \\
&= \binom{2\cdot 0}{0+u} = \binom{2n}{n+u}
\end{aligned}$$

(since $0 = n$). Thus, (13) is proven for $n = 0$. This completes the induction base.

Induction step: Let $N \geq 0$ be an integer. Assume that (13) is proven for $n = N$. We have to prove (13) for $n = N + 1$.

Let U be an integer. We have assumed that the equality (13) is proven for $n = N$; thus, we can apply it to $n = N$ and every $u \in \mathbb{Z}$.

In particular:

- We can apply (13) to $n = N$ and $u = U$ and get
$$\sum_k 2^{N-2k-U} \binom{N}{2k+U} \binom{2k+U}{k} = \binom{2N}{N+U}. \qquad (14)$$

- We can apply (13) to $n = N$ and $u = U - 1$ and get
$$\sum_k 2^{N-2k-(U-1)} \binom{N}{2k+(U-1)} \binom{2k+(U-1)}{k} = \binom{2N}{N+(U-1)}. \qquad (15)$$

- We can apply (13) to $n = N$ and $u = U + 1$ and get
$$\sum_k 2^{N-2k-(U+1)} \binom{N}{2k+(U+1)} \binom{2k+(U+1)}{k} = \binom{2N}{N+(U+1)}. \qquad (16)$$

Now,

$$\begin{aligned}
&\sum_k 2^{(N+1)-2k-U} \underbrace{\binom{N+1}{2k+U}}_{\substack{=\binom{N}{2k+U}+\binom{N}{2k+U-1} \\ \text{(by the recurrence relation of binomial coefficients)}}} \binom{2k+U}{k} \\
&= \sum_k 2^{(N+1)-2k-U} \left(\binom{N}{2k+U}+\binom{N}{2k+U-1}\right)\binom{2k+U}{k} \\
&= \sum_k \underbrace{2^{(N+1)-2k-U}}_{=2\cdot 2^{N-2k-U}} \binom{N}{2k+U}\binom{2k+U}{k} + \sum_k 2^{(N+1)-2k-U}\binom{N}{2k+U-1}\binom{2k+U}{k} \\
&= 2\cdot\sum_k 2^{N-2k-U}\binom{N}{2k+U}\binom{2k+U}{k} \\
&\quad + \sum_k 2^{(N+1)-2k-U}\binom{N}{2k+U-1} \underbrace{\binom{2k+U}{k}}_{\substack{=\binom{2k+U-1}{k}+\binom{2k+U-1}{k-1} \\ \text{(by the recurrence relation of binomial coefficients)}}} \\
&= 2\cdot\sum_k 2^{N-2k-U}\binom{N}{2k+U}\binom{2k+U}{k} \\
&\quad + \sum_k 2^{(N+1)-2k-U}\binom{N}{2k+U-1}\left(\binom{2k+U-1}{k}+\binom{2k+U-1}{k-1}\right) \\
&= 2\cdot\sum_k 2^{N-2k-U}\binom{N}{2k+U}\binom{2k+U}{k} \\
&\quad + \sum_k \underbrace{2^{(N+1)-2k-U}}_{=2^{N-2k-(U-1)}} \underbrace{\binom{N}{2k+U-1}}_{=\binom{N}{2k+(U-1)}} \underbrace{\binom{2k+U-1}{k}}_{=\binom{2k+(U-1)}{k}} \\
&\quad + \sum_k \underbrace{2^{(N+1)-2k-U}}_{=2^{N-2(k-1)-(U+1)}} \underbrace{\binom{N}{2k+U-1}}_{=\binom{N}{2(k-1)+(U+1)}} \underbrace{\binom{2k+U-1}{k-1}}_{=\binom{2(k-1)+(U+1)}{k-1}} \\
&= 2\cdot\sum_k 2^{N-2k-U}\binom{N}{2k+U}\binom{2k+U}{k} \\
&\quad + \sum_k 2^{N-2k-(U-1)}\binom{N}{2k+(U-1)}\binom{2k+(U-1)}{k} \\
&\quad + \sum_k 2^{N-2(k-1)-(U+1)}\binom{N}{2(k-1)+(U+1)}\binom{2(k-1)+(U+1)}{k-1}
\end{aligned}$$

$$\begin{aligned}
&= 2 \cdot \sum_k 2^{N-2k-U} \binom{N}{2k+U} \binom{2k+U}{k} \\
&\qquad + \sum_k 2^{N-2k-(U-1)} \binom{N}{2k+(U-1)} \binom{2k+(U-1)}{k} \\
&\qquad + \sum_k 2^{N-2k-(U+1)} \binom{N}{2k+(U+1)} \binom{2k+(U+1)}{k} \\
&\qquad \text{(here we substituted } k \text{ for } k-1 \text{ in the last sum)} \\
&= 2 \cdot \binom{2N}{N+U} + \binom{2N}{N+(U-1)} + \binom{2N}{N+(U+1)} \qquad \text{(by (14), (15) and (16))} \\
&= 2 \cdot \binom{2N}{N+U} + \binom{2N}{N+U-1} + \binom{2N}{N+U+1} \\
&= \underbrace{\left(\binom{2N}{N+U} + \binom{2N}{N+U-1}\right)}_{\substack{=\binom{2N+1}{N+U} \\ \text{(by the recurrence relation of binomial coefficients)}}} + \underbrace{\left(\binom{2N}{N+U+1} + \binom{2N}{N+U}\right)}_{\substack{=\binom{2N+1}{N+U+1} \\ \text{(by the recurrence relation of binomial coefficients)}}} \\
&= \binom{2N+1}{N+U} + \binom{2N+1}{N+U+1} \\
&= \binom{2N+2}{N+U+1} \qquad \text{(by the recurrence relation of binomial coefficients)} \\
&= \binom{2(N+1)}{(N+1)+U}.
\end{aligned}$$

We have proven this for every integer U. If we rename U as u, this becomes

$$\sum_k 2^{(N+1)-2k-u} \binom{N+1}{2k+u} \binom{2k+u}{k} = \binom{2(N+1)}{(N+1)+u}.$$

In other words, (13) holds for $n = N+1$. This completes the induction step. Hence, (13) is proven for any integers $n \geq 0$ and u.]

Now, let $n \in \mathbb{N}$ and $u \in \mathbb{Z}$. Then, (12) becomes

$$\sum_{k=0}^{n} 2^{n-2k-u} \binom{n}{2k+u} \binom{2k+u}{k} = \sum_k 2^{n-2k-u} \binom{n}{2k+u} \binom{2k+u}{k} = \binom{2n}{n+u}$$

(by (13)). This proves Claim 2.]

We still haven't solved the exercise. To do that, we need to recall two further identities for binomial coefficients:

- The *trinomial revision identity* (Proposition 2.2 in blackboard work from 17 September 2018) says that

  $$\binom{n}{a}\binom{a}{b} = \binom{n}{b}\binom{n-b}{a-b} \qquad \text{for all reals } n,\ a \text{ and } b. \tag{17}$$

  (We shall only use it in the case when n, a and b are integers.)

- The *symmetry identity* (Theorem 1.17 in blackboard work from 10 September 2018) says that
$$\binom{n}{k} = \binom{n}{n-k} \qquad \text{for all } n \in \mathbb{N} \text{ and } k \in \mathbb{Z}. \tag{18}$$

We can use these to further transform Claim 2 into the following:

Claim 3: Let $n \in \mathbb{N}$ and $u \in \mathbb{Z}$. Then,
$$\sum_{i=0}^{n} 2^{n-2i-u} \binom{n}{i} \binom{n-i}{n-2i-u} = \binom{2n}{n+u}.$$

[*Proof of Claim 3:* Let $i \in \{0, 1, \ldots, n\}$. Then, $i \leq n$, so that $n - i \geq 0$ and thus $n - i \in \mathbb{N}$. Hence, (18) (applied to $n-i$ and $i+u$ instead of n and k) yields
$$\binom{n-i}{i+u} = \binom{n-i}{(n-i)-(i+u)} = \binom{n-i}{n-2i-u}.$$
But (17) (applied to $a = 2i + u$ and $b = i$) yields
$$\binom{n}{2i+u}\binom{2i+u}{i} = \binom{n}{i} \underbrace{\binom{n-i}{(2i+u)-i}}_{=\binom{n-i}{i+u}=\binom{n-i}{n-2i-u}} = \binom{n}{i}\binom{n-i}{n-2i-u}. \tag{19}$$

Now, forget that we fixed i. We thus have proven (19) for each $i \in \{0, 1, \ldots, n\}$.

Now, Claim 2 yields
$$\sum_{k=0}^{n} 2^{n-2k-u} \binom{n}{2k+u}\binom{2k+u}{k} = \binom{2n}{n+u}.$$
Hence,
$$\binom{2n}{n+u} = \sum_{k=0}^{n} 2^{n-2k-u} \binom{n}{2k+u}\binom{2k+u}{k} = \sum_{i=0}^{n} 2^{n-2i-u} \underbrace{\binom{n}{2i+u}\binom{2i+u}{i}}_{\substack{=\binom{n}{i}\binom{n-i}{n-2i-u} \\ \text{(by (19))}}}$$
$$\text{(here, we have renamed the summation index } k \text{ as } i\text{)}$$
$$= \sum_{i=0}^{n} 2^{n-2i-u} \binom{n}{i}\binom{n-i}{n-2i-u}.$$
This proves Claim 3.]

Now, let $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Claim 3 (applied to $u = n - k$) yields
$$\sum_{i=0}^{n} 2^{n-2i-(n-k)} \binom{n}{i}\binom{n-i}{n-2i-(n-k)}$$
$$= \binom{2n}{n+(n-k)} = \binom{2n}{2n-k} = \binom{2n}{2n-(2n-k)}$$
$$\text{(by (18), applied to } 2n \text{ and } 2n-k \text{ instead of } n \text{ and } k\text{)}$$
$$= \binom{2n}{k}.$$

Hence,

$$\binom{2n}{k} = \sum_{i=0}^{n} \underbrace{2^{n-2i-(n-k)}}_{=2^{k-2i}} \binom{n}{i} \underbrace{\binom{n-i}{n-2i-(n-k)}}_{=\binom{n-i}{k-2i}}$$
$$= \sum_{i=0}^{n} 2^{k-2i} \binom{n}{i} \binom{n-i}{k-2i} = \sum_{i=0}^{n} \binom{n}{i} \binom{n-i}{k-2i} 2^{k-2i}.$$

This solves the exercise again.

2.3 Remark

The addends $\binom{n}{i}\binom{n-i}{k-2i}2^{k-2i}$ in the sum on the left hand side of (7) equal 0 when $i > n$ (because $\binom{n}{i} = 0$ in this case) and also equal 0 when $i > k$ (because in this case, we have $k - 2i < k - 2k = -k \leq 0$ and thus $\binom{n-i}{k-2i} = 0$). Hence, we can replace the "$\sum_{i=0}^{n}$" sign by a "$\sum_{i=0}^{k}$" sign without changing the value of the sum. Thus, the identity (7) can be rewritten as

$$\sum_{i=0}^{k} \binom{n}{i} \binom{n-i}{k-2i} 2^{k-2i} = \binom{2n}{k}. \tag{20}$$

This equality (20) has the nice property that both of its sides are polynomial functions in n; in other words, it can be restated as $P(n) = Q(n)$, where P and Q are two polynomials (in one variable X) defined by

$$P = \sum_{i=0}^{k} \binom{X}{i} \binom{X-i}{k-2i} 2^{k-2i} \qquad \text{and} \qquad Q = \binom{2X}{k}.$$

Thus, Theorem 1.1 yields that $P = Q$ (since the exercise yields $P(n) = Q(n)$ for all $n \in \mathbb{N}$). Hence, $P(x) = Q(x)$ for each $x \in \mathbb{R}$. In other words,

$$\sum_{i=0}^{k} \binom{x}{i} \binom{x-i}{k-2i} 2^{k-2i} = \binom{2x}{k} \qquad \text{for each } x \in \mathbb{R}.$$

---

3 Exercise 3

3.1 Problem

Let $n \in \mathbb{N}$. For each $i \in \{0, 1, 2\}$, we let $g_{n,i}$ denote the number of all subsets S of $[n]$ satisfying $|S| \equiv i \mod 3$.

(a) Show that if $n > 0$, then

$$g_{n,0} = g_{n-1,0} + g_{n-1,2}; \qquad g_{n,1} = g_{n-1,1} + g_{n-1,0}; \qquad g_{n,2} = g_{n-1,2} + g_{n-1,1}.$$

(b) Find closed-form expressions (with no summation signs) for $g_{n,0}, g_{n,1}, g_{n,2}$ depending on the remainder of n upon division by 3.

3.2 Remark

Remark 3.1. The combinatorial interpretation of binomial coefficients shows that

$$g_{n,i} = \sum_{\substack{k\in\mathbb{Z};\\ k\equiv i \mod 3}} \binom{n}{k} \qquad \text{for each } i.$$

This is not what the problem is asking for – find formulas with no summation signs.

3.3 Solution sketch

3.3.1 Solution to part (a)

(a) Let us extend the definition $g_{n,i}$ to the case when i is an arbitrary integer (as opposed to being an element of $\{0,1,2\}$). Then, of course, if i and j are two integers satisfying $i \equiv j \mod 3$, and if $n \in \mathbb{N}$, then $g_{n,i} = g_{n,j}$ (because a subset S of $[n]$ satisfies $|S| \equiv i \mod 3$ if and only if it satisfies $|S| \equiv j \mod 3$). Applying this equality to $i = -1$ and $j = 2$, we obtain

$$g_{n,-1} = g_{n,2} \tag{21}$$

(since $-1 \equiv 2 \mod 3$).

Next, I will prove the following:

Claim 1: Let $i \in \mathbb{Z}$. Let $n > 0$ be an integer. Then, $g_{n,i} = g_{n-1,i} + g_{n-1,i-1}$.

[*Proof of Claim 1:* The map

$$\begin{aligned}&\{\text{subsets } S \text{ of } [n-1] \text{ satisfying } |S| \equiv i \mod 3\}\\ \to &\{\text{subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \notin T\}\end{aligned}$$

that sends each S to S itself is well-defined and bijective (since the subsets S of $[n-1]$ satisfying $|S| \equiv i \mod 3$ are exactly the subsets T of $[n]$ satisfying $|T| \equiv i \mod 3$ and $n \notin T$). Thus,

$$\begin{aligned}&|\{\text{subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \notin T\}|\\ =&|\{\text{subsets } S \text{ of } [n-1] \text{ satisfying } |S| \equiv i \mod 3\}|.\end{aligned}$$

In other words,

$$\begin{aligned}&(\text{the number of subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \notin T)\\ =&(\text{the number of subsets } S \text{ of } [n-1] \text{ satisfying } |S| \equiv i \mod 3)\\ =&\, g_{n-1,i}\end{aligned} \tag{22}$$

(since $g_{n-1,i}$ was defined as the number of subsets S of $[n-1]$ satisfying $|S| \equiv i \mod 3$).

The map

$$\begin{aligned}&\{\text{subsets } S \text{ of } [n-1] \text{ satisfying } |S| \equiv i-1 \mod 3\}\\ \to &\{\text{subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \in T\}\end{aligned}$$

that sends each S to $S \cup \{n\}$ is well-defined and bijective (in fact, its inverse map sends each T to $T \setminus \{n\}$). Thus,

$$\begin{aligned} & \left|\{\text{subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \in T\}\right| \\ = & \left|\{\text{subsets } S \text{ of } [n-1] \text{ satisfying } |S| \equiv i-1 \mod 3\}\right|. \end{aligned}$$

In other words,

$$\begin{aligned} & (\text{the number of subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \in T) \\ = & (\text{the number of subsets } S \text{ of } [n-1] \text{ satisfying } |S| \equiv i-1 \mod 3) \\ = & \ g_{n-1,i-1} \end{aligned} \tag{23}$$

(since $g_{n-1,i-1}$ was defined as the number of subsets S of $[n-1]$ satisfying $|S| \equiv i-1 \mod 3$).

Now, the definition of $g_{n,i}$ yields

$$\begin{aligned} g_{n,i} &= (\text{the number of subsets } S \text{ of } [n] \text{ satisfying } |S| \equiv i \mod 3) \\ &= (\text{the number of subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3) \\ &= \underbrace{(\text{the number of subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \notin T)}_{\substack{=g_{n-1,i} \\ \text{(by (22))}}} \\ &\qquad + \underbrace{(\text{the number of subsets } T \text{ of } [n] \text{ satisfying } |T| \equiv i \mod 3 \text{ and } n \in T)}_{\substack{=g_{n-1,i-1} \\ \text{(by (23))}}} \\ &= g_{n-1,i} + g_{n-1,i-1}. \end{aligned}$$

This proves Claim 1.]

Now, let $n > 0$ be an integer. Claim 1 (applied to $i = 0$) yields

$$g_{n,0} = g_{n-1,0} + \underbrace{g_{n-1,-1}}_{\substack{=g_{n-1,2} \\ \text{(by (21))}}} = g_{n-1,0} + g_{n-1,2}.$$

Claim 1 (applied to $i = 1$) yields

$$g_{n,1} = g_{n-1,1} + g_{n-1,0}.$$

Claim 1 (applied to $i = 2$) yields

$$g_{n,2} = g_{n-1,2} + g_{n-1,1}.$$

Thus, part **(a)** of the exercise is solved.

3.3.2 Solution to part (b)

(b) We claim that every $n \in \mathbb{N}$ and $i \in \{0, 1, 2\}$ satisfy

$$g_{n,i} = \frac{2^n - (-1)^n}{3} + (-1)^n [n \equiv -i \mod 3] \tag{24}$$

(where we are using the Iverson bracket notation).

This can be proven by a straightforward induction on n, where the induction step relies on the recurrences proven in part **(a)** of the exercise[3]. We leave the details to the reader.

[3] It also relies on the fact that

$$[n \equiv -i \mod 3] + [n-1 \equiv -i \mod 3] + [n-1 \equiv -(i-1) \mod 3] = 1$$

for any integers n and i. This fact is a consequence of the fact that every integer n is congruent to exactly one of the three numbers $0, 1, 2$ modulo 3.

3.4 Remark

There is also a different approach to solving part **(b)**, using the so-called *roots-of-unity filter*. See the proof of Proposition 2.32 in the class work from 3 October 2018 for an outline of this approach (and `https://math.stackexchange.com/questions/1960129` for further information).

Here is a different comment: How could you come up with the answer (24)? Here is one way: Tabulate the values of $g_{n,i}$ for the first few values of n and each of $i \in \{0, 1, 2\}$. You will soon observe (experimentally, so far) that for each $n \in \mathbb{N}$, two of the three values $g_{n,0}$, $g_{n,1}$ and $g_{n,2}$ are equal, whereas the third of these three values differs from these two by 1. But the sum $g_{n,0} + g_{n,1} + g_{n,2}$ of these three values is 2^n (since it counts all subsets of $[n]$). Hence, these three values $g_{n,0}$, $g_{n,1}$ and $g_{n,2}$ divide 2^n into three parts that are "as close to each other as possible" while being integers (since we cannot divide 2^n evenly by 3). This lets you find an explicit formula for these parts. It is also not hard to see the pattern that governs which two of the parts are equal. After some work, the formula (24) (or an equivalent formula) emerges.

4 Exercise 4

4.1 Problem

Let $n \in \mathbb{N}$ be positive. Let $m \in \mathbb{N}$. Prove that

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m}. \tag{25}$$

4.2 Solution sketch

4.2.1 First solution

We can prove (25) by induction on m:

Induction base: We have $\binom{n}{0} = \binom{n-1}{0}$ (since both sides of this equality equal 1). Now,

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

In other words, (25) holds for $m = 0$. This completes the induction base.

Induction step: Let $p \in \mathbb{N}$. Assume that (25) holds for $m = p$. We must now prove that (25) holds for $m = p + 1$.

We have assumed that (25) holds for $m = p$. In other words, we have

$$\sum_{k=0}^{p} (-1)^k \binom{n}{k} = (-1)^p \binom{n-1}{p}. \tag{26}$$

But the recurrence relation of the binomial coefficients yields

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

Hence,

$$\begin{aligned}\sum_{k=0}^{p+1}(-1)^k\binom{n}{k} &= \underbrace{\sum_{k=0}^{p}(-1)^k\binom{n}{k}}_{=(-1)^p\binom{n-1}{p}} + \underbrace{(-1)^{p+1}}_{=-(-1)^p}\underbrace{\binom{n}{p+1}}_{=\binom{n-1}{p}+\binom{n-1}{p+1}} \\ &= (-1)^p\binom{n-1}{p} + \left(-(-1)^p\right)\left(\binom{n-1}{p}+\binom{n-1}{p+1}\right) \\ &= (-1)^p\binom{n-1}{p} - (-1)^p\binom{n-1}{p} - (-1)^p\binom{n-1}{p+1} \\ &= \underbrace{-(-1)^p}_{=(-1)^{p+1}}\binom{n-1}{p+1} = (-1)^{p+1}\binom{n-1}{p+1}.\end{aligned}$$

In other words, (25) holds for $m = p+1$. This completes the induction step. Thus, (25) is proven by induction. This solves the exercise.

4.2.2 Second solution

Recall the telescope principle (which we have already encountered in the solutions to homework set #0):

Proposition 4.1. *Let $m \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_m$ be $m+1$ real numbers. Then,*

$$\sum_{i=1}^{m}(a_i - a_{i-1}) = a_m - a_0.$$

Let us restate this proposition in a slightly modified way:

Proposition 4.2. *Let $m \in \{-1, 0, 1, 2, \ldots\}$. Let $a_{-1}, a_0, \ldots, a_m$ be $m+2$ real numbers. Then,*

$$\sum_{i=0}^{m}(a_i - a_{i-1}) = a_m - a_{-1}.$$

Proof of Proposition 4.2. Proposition 4.1 (applied to $m+1$ and a_{j-1} instead of m and a_j) yields

$$\sum_{i=1}^{m+1}\left(a_{i-1} - a_{(i-1)-1}\right) = a_{(m+1)-1} - a_{0-1} = a_m - a_{-1}.$$

Comparing this with

$$\sum_{i=1}^{m+1}\left(a_{i-1} - a_{(i-1)-1}\right) = \sum_{i=0}^{m}(a_i - a_{i-1}) \qquad \text{(here, we have substituted } i \text{ for } i-1 \text{ in the sum)},$$

we obtain

$$\sum_{i=0}^{m}(a_i - a_{i-1}) = a_m - a_{-1}.$$

This proves Proposition 4.2. □

Every $i \in \mathbb{Z}$ satisfies

$$\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i}$$

(by the recurrence relation of the binomial coefficients) and therefore

$$\begin{aligned}
(-1)^i \binom{n}{i} &= (-1)^i \left(\binom{n-1}{i-1} + \binom{n-1}{i} \right) = \underbrace{(-1)^i}_{=-(-1)^{i-1}} \binom{n-1}{i-1} + (-1)^i \binom{n-1}{i} \\
&= -(-1)^{i-1} \binom{n-1}{i-1} + (-1)^i \binom{n-1}{i} \\
&= (-1)^i \binom{n-1}{i} - (-1)^{i-1} \binom{n-1}{i-1}. \qquad (27)
\end{aligned}$$

Now,

$$\begin{aligned}
\sum_{k=0}^{m} (-1)^k \binom{n}{k} &= \sum_{i=0}^{m} \underbrace{(-1)^i \binom{n}{i}}_{\substack{=(-1)^i \binom{n-1}{i} - (-1)^{i-1} \binom{n-1}{i-1} \\ \text{(by (27))}}} \\
&= \sum_{i=0}^{m} \left((-1)^i \binom{n-1}{i} - (-1)^{i-1} \binom{n-1}{i-1} \right) \\
&= (-1)^m \binom{n-1}{m} - (-1)^{-1} \underbrace{\binom{n-1}{-1}}_{\substack{=0 \\ \text{(since } -1<0)}} \\
&\qquad \left(\text{by Proposition 4.2, applied to } a_j = (-1)^j \binom{n-1}{j} \right) \\
&= (-1)^m \binom{n-1}{m}.
\end{aligned}$$

This solves the exercise.

4.2.3 Third solution

Let me sketch a combinatorial proof, similar to the 3rd proof of Corollary 2.3 in the blackboard work on 19 September 2018 (but written up more systematically, since our situation is more complicated).

If S is any set, then $\mathcal{P}(S)$ shall denote the set of all subsets of S. This is called the *powerset* (or *power set*) of S.

If S is any set and i is any integer, then:

- We let $\mathcal{P}_i(S)$ denote the set of all i-element subsets of S.
- We let $\mathcal{P}_{\leq i}(S)$ denote the set of all subsets of S that have at most i elements.

(Thus, $\mathcal{P}_{\leq i}(S) = \mathcal{P}_0(S) \cup \mathcal{P}_1(S) \cup \cdots \cup \mathcal{P}_i(S)$ for any i and S.)

The core of our argument can be abstracted into the following general lemma:

Lemma 4.3. *Let S be a finite set. Let X be a subset of $\mathcal{P}(S)$. (That is, X is a set of subsets of S.) Let $f : X \to X$ be a bijection. Assume that*

$$|f(I)| \equiv |I| + 1 \mod 2 \qquad \text{for each } I \in X. \tag{28}$$

Then,

$$\sum_{I \in X} (-1)^{|I|} = 0.$$

Roughly speaking, Lemma 4.3 says that if X is a set of subsets of a finite set S, and there exists a permutation f of X that flips the parity of the size of every subset it is applied to, then X contains equally many even-sized sets as it contains odd-sized sets (indeed, this is what the equality $\sum_{I \in X} (-1)^{|I|} = 0$ says). The intuitive reason for this is that the bijection f "matches" the even-sized sets in X with the odd-sized sets in X (though we need to be careful here, since we are not requiring $f \circ f$ to be id). The following proof of this lemma formalizes this intuition:

Proof of Lemma 4.3. Every $I \in X$ is a subset of S, and thus a finite set (since S is finite). Thus, $|I|$ is well-defined for every $I \in X$.

If $I \in X$ is such that $|I|$ is odd, then $|f(I)|$ is even[4]. Hence, the map

$$\{I \in X \mid |I| \text{ is odd}\} \to \{I \in X \mid |I| \text{ is even}\},$$
$$I \mapsto f(I)$$

is well-defined. Let us denote this map by p.

On the other hand, the map $f : X \to X$ is a bijection; thus, the map $f^{-1} : X \to X$ is well-defined. If $I \in X$ is such that $|I|$ is even, then $|f^{-1}(I)|$ is odd[5]. Hence, the map

$$\{I \in X \mid |I| \text{ is even}\} \to \{I \in X \mid |I| \text{ is odd}\},$$
$$I \mapsto f^{-1}(I)$$

is well-defined. Let us denote this map by q.

The maps p and q are mutually inverse (since p is a restriction of f, whereas q is a restriction of f^{-1}). Thus, the map p is invertible, i.e., a bijection.

Now, if $I \in X$, then $|I|$ is either even or odd (but not both at the same time). Hence,

[4] because (28) yields $|f(I)| \equiv \underbrace{|I|}_{\substack{\equiv 1 \mod 2 \\ (\text{since } |I| \text{ is odd})}} + 1 \equiv 1 + 1 \equiv 0 \mod 2$

[5] because (28) (applied to $f^{-1}(I)$ instead of I) yields $\left|f\left(f^{-1}(I)\right)\right| \equiv \left|f^{-1}(I)\right| + 1 \mod 2$, which leads to $\left|f^{-1}(I)\right| + 1 \equiv \left|\underbrace{f\left(f^{-1}(I)\right)}_{=I}\right| = |I| \equiv 0 \mod 2$ (since $|I|$ is even), which leads to $\left|f^{-1}(I)\right| \equiv 0 - 1 \equiv 1 \mod 2$

we can split the sum $\sum\limits_{I\in X}(-1)^{|I|}=0$ as follows:

$$\begin{aligned}\sum_{I\in X}(-1)^{|I|}&=\sum_{\substack{I\in X;\\|I|\text{ is even}}}\underbrace{(-1)^{|I|}}_{\substack{=1\\(\text{since }|I|\text{ is even})}}+\sum_{\substack{I\in X;\\|I|\text{ is odd}}}\underbrace{(-1)^{|I|}}_{\substack{=-1\\(\text{since }|I|\text{ is odd})}}\\&=\sum_{\substack{I\in X;\\|I|\text{ is even}}}1+\sum_{\substack{I\in X;\\|I|\text{ is odd}}}(-1)\\&=\sum_{\substack{I\in X;\\|I|\text{ is odd}}}1+\sum_{\substack{I\in X;\\|I|\text{ is odd}}}(-1)\\&\qquad\left(\begin{array}{c}\text{here, we have substituted }p(I)\text{ for }I\text{ in the first sum, since the map}\\p:\{I\in X\ \mid\ |I|\text{ is odd}\}\to\{I\in X\ \mid\ |I|\text{ is even}\}\\\text{is a bijection}\end{array}\right)\\&=\sum_{\substack{I\in X;\\|I|\text{ is odd}}}\underbrace{(1+(-1))}_{=0}=\sum_{\substack{I\in X;\\|I|\text{ is odd}}}0=0.\end{aligned}$$

This proves Lemma 4.3. □

Now, recall once again the concept of a symmetric difference: If X and Y are two sets, then the *symmetric difference* of X and Y is the set $X\triangle Y$, defined by

$$X\triangle Y=(X\cup Y)\setminus(X\cap Y)=(X\setminus Y)\cup(Y\setminus X).$$

Thus, in particular, if I is any set and a is any object, then

$$I\triangle\{a\}=\begin{cases}I\cup\{a\}, & \text{if }a\notin I;\\I\setminus\{a\}, & \text{if }a\in I.\end{cases}$$

Thus, if I is any finite set, and if a is any object, then the set $I\triangle\{a\}$ is finite again, and satisfies

$$|I\triangle\{a\}|\equiv|I|+1\mod 2\qquad(29)$$

(in fact, $|I\triangle\{a\}|$ is either $|I|+1$ or $|I|-1$, depending on whether $a\notin I$ or $a\in I$).

Furthermore, any set I and any object a satisfy

$$(I\triangle\{a\})\triangle\{a\}=I.\qquad(30)$$

Now, let us return to the exercise. Let X be the subset $\mathcal{P}_{\leq m}([n])\setminus\mathcal{P}_m([n-1])$ of $\mathcal{P}([n])$. This subset X consists of all subsets S of $[n]$ that

- belong to $\mathcal{P}_{\leq m}([n])$ (i.e., have at most m elements), and
- do not belong to $\mathcal{P}_m([n-1])$ (i.e., are not m-element subsets of $[n-1]$).

In other words, a subset S of $[n]$ belongs to X if and only if it has at most m elements and has the property that **if** it has **exactly** m elements, then it must contain n (since this is what it means to not be a subset of $[n-1]$).

Now, it is easy to see that for each $I\in X$, we have $I\triangle\{n\}\in X$. [6] Hence, we can define a map

$$\begin{aligned}X&\to X,\\I&\mapsto I\triangle\{n\}.\end{aligned}$$

[6] *Proof.* Let $I\in X$. Thus, I belongs to $\mathcal{P}_{\leq m}([n])$ but does not belong to $\mathcal{P}_m([n-1])$ (by the definition of X). From $I\in\mathcal{P}_{\leq m}([n])$, we obtain $|I|\leq m$.

Let us denote this map by f.

The equality (30) (applied to $a = n$) shows that $(I \triangle \{n\}) \triangle \{n\} = I$ for each $I \in X$. In other words, $f(f(I)) = I$ for each $I \in X$. Thus, $f \circ f = \operatorname{id}$. Thus, the maps f and f are mutually inverse. Hence, the map f is invertible, i.e., a bijection. Moreover, it satisfies

$$|f(I)| \equiv |I| + 1 \mod 2 \qquad \text{for each } I \in X$$

(by (29), applied to $a = n$).

Hence, Lemma 4.3 (applied to $S = [n]$) yields that

$$\sum_{I \in X} (-1)^{|I|} = 0.$$

In view of $X = \mathcal{P}_{\leq m}([n]) \setminus \mathcal{P}_m([n-1])$, this rewrites as

$$\sum_{I \in \mathcal{P}_{\leq m}([n]) \setminus \mathcal{P}_m([n-1])} (-1)^{|I|} = 0.$$

But each m-element subset of $[n-1]$ is clearly a subset of $[n]$ that has at most m elements. In other words, $\mathcal{P}_m([n-1])$ is a subset of $\mathcal{P}_{\leq m}([n])$. Each $I \in \mathcal{P}_{\leq m}([n])$ satisfies either $I \in \mathcal{P}_m([n-1])$ or $I \notin \mathcal{P}_m([n-1])$ (but not both). Thus,

$$\sum_{I \in \mathcal{P}_{\leq m}([n])} (-1)^{|I|} = \sum_{\substack{I \in \mathcal{P}_{\leq m}([n]); \\ I \in \mathcal{P}_m([n-1])}} (-1)^{|I|} + \sum_{\substack{I \in \mathcal{P}_{\leq m}([n]); \\ I \notin \mathcal{P}_m([n-1])}} (-1)^{|I|}. \tag{31}$$

On the right hand side of this equality, we can replace the summation sign "$\sum\limits_{\substack{I \in \mathcal{P}_{\leq m}([n]); \\ I \in \mathcal{P}_m([n-1])}}$" by "$\sum\limits_{I \in \mathcal{P}_m([n-1])}$" (since $\mathcal{P}_m([n-1])$ is a subset of $\mathcal{P}_{\leq m}([n])$), and we can also replace the

Now, we must prove that $I \triangle \{n\} \in X$. We are in one of the following two cases:

- *Case 1:* We have $n \in I$.
- *Case 2:* We have $n \notin I$.

Let us first consider Case 1. In this case, we have $n \in I$. Hence, $I \triangle \{n\} = I \setminus \{n\}$, so that $|I \triangle \{n\}| = |I \setminus \{n\}| = |I| - 1$ (since $n \in I$). Thus, $|I \triangle \{n\}| = |I| - 1 \leq m - 1$ (since $|I| \leq m$), so that $|I \triangle \{n\}| \neq m$. Now, the set $I \triangle \{n\}$ belongs to $\mathcal{P}_{\leq m}([n])$ (since $I \triangle \{n\} \subseteq [n]$ and $|I \triangle \{n\}| \leq m - 1 \leq m$) and does not belong to $\mathcal{P}_m([n-1])$ (since $|I \triangle \{n\}| \neq m$). In other words, $I \triangle \{n\} \in X$ (by the definition of X). Hence, $I \triangle \{n\} \in X$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $n \notin I$. Hence, $I \triangle \{n\} = I \cup \{n\}$, so that $|I \triangle \{n\}| = |I \cup \{n\}| = |I| + 1$ (since $n \in I$). Also, I is a subset of $[n]$ satisfying $n \notin I$; thus, I is a subset of $[n] \setminus \{n\} = [n-1]$. Hence, if we had $|I| = m$, then we would have $I \in \mathcal{P}_m([n-1])$ (since I would be an m-element subset of $[n-1]$), which would contradict the fact that I does not belong to $\mathcal{P}_m([n-1])$. Hence, we cannot have $|I| = m$. Thus, $|I| \neq m$. Combined with $|I| \leq m$, this yields $|I| < m$, so that $|I| \leq m - 1$ (since $|I|$ and m are integers). Thus, $|I| + 1 \leq m$. Furthermore, the set $I \triangle \{n\} = I \cup \{n\}$ contains n (since $n \in \{n\}$), and thus cannot be a subset of $[n-1]$. In other words, $I \triangle \{n\} \not\subseteq [n-1]$.

Now, the set $I \triangle \{n\}$ belongs to $\mathcal{P}_{\leq m}([n])$ (since $I \triangle \{n\} \subseteq [n]$ and $|I \triangle \{n\}| = |I| + 1 \leq m$) and does not belong to $\mathcal{P}_m([n-1])$ (since $I \triangle \{n\} \not\subseteq [n-1]$). In other words, $I \triangle \{n\} \in X$ (by the definition of X). Hence, $I \triangle \{n\} \in X$ is proven in Case 2.

We have now proven $I \triangle \{n\} \in X$ in each of the two Cases 1 and 2. Thus, $I \triangle \{n\} \in X$ always holds. Qed.

summation sign "$\sum\limits_{\substack{I\in\mathcal{P}_{\leq m}([n]);\\ I\notin\mathcal{P}_m([n-1])}}$" by "$\sum\limits_{I\in\mathcal{P}_{\leq m}([n])\setminus\mathcal{P}_m([n-1])}$". Thus, (31) rewrites as

$$\begin{aligned}\sum_{I\in\mathcal{P}_{\leq m}([n])}(-1)^{|I|} &= \sum_{I\in\mathcal{P}_m([n-1])}(-1)^{|I|} + \underbrace{\sum_{I\in\mathcal{P}_{\leq m}([n])\setminus\mathcal{P}_m([n-1])}(-1)^{|I|}}_{=0} \\ &= \sum_{I\in\mathcal{P}_m([n-1])}\underbrace{(-1)^{|I|}}_{\substack{=(-1)^m\\ (\text{since } |I|=m \text{ (because } I\in\mathcal{P}_m([n-1])))}} = \sum_{I\in\mathcal{P}_m([n-1])}(-1)^m \\ &= \underbrace{|\mathcal{P}_m([n-1])|}_{\substack{=(\text{the number of all } m\text{-element subsets of } [n-1])\\ =\binom{n-1}{m}\\ (\text{since } n-1\in\mathbb{N})}}\cdot(-1)^m = \binom{n-1}{m}\cdot(-1)^m \\ &= (-1)^m\binom{n-1}{m}.\end{aligned}$$

On the other hand, the $I\in\mathcal{P}_{\leq m}([n])$ are precisely the subsets I of $[n]$ that satisfy $|I|\leq m$. In other words, the $I\in\mathcal{P}_{\leq m}([n])$ are precisely the subsets I of $[n]$ that satisfy $|I|\in\{0,1,\ldots,m\}$. Thus,

$$\begin{aligned}\sum_{I\in\mathcal{P}_{\leq m}([n])}(-1)^{|I|} &= \sum_{\substack{I\in\mathcal{P}([n]);\\ |I|\in\{0,1,\ldots,m\}}}(-1)^{|I|} = \sum_{k\in\{0,1,\ldots,m\}}\sum_{\substack{I\in\mathcal{P}([n]);\\ |I|=k}}\underbrace{(-1)^{|I|}}_{\substack{=(-1)^k\\ (\text{since } |I|=k)}} \\ &= \sum_{k\in\{0,1,\ldots,m\}}\underbrace{\sum_{\substack{I\in\mathcal{P}([n]);\\ |I|=k}}(-1)^k}_{=(\text{the number of all } I\in\mathcal{P}([n]) \text{ satisfying } |I|=k)\cdot(-1)^k} \\ &= \underbrace{\sum_{k\in\{0,1,\ldots,m\}}}_{=\sum_{k=0}^{m}}\underbrace{(\text{the number of all } I\in\mathcal{P}([n]) \text{ satisfying } |I|=k)}_{\substack{=(\text{the number of all } k\text{-element subsets of } [n])\\ =\binom{n}{k}}}\cdot(-1)^k \\ &= \sum_{k=0}^{m}\binom{n}{k}\cdot(-1)^k = \sum_{k=0}^{m}(-1)^k\binom{n}{k}.\end{aligned}$$

Hence,

$$\sum_{k=0}^{m}(-1)^k\binom{n}{k} = \sum_{I\in\mathcal{P}_{\leq m}([n])}(-1)^{|I|} = (-1)^m\binom{n-1}{m}.$$

Thus, the exercise is solved again.

4.3 Remark

The equality (25) holds not only for any positive integer n, but also for any real number n. Indeed, the first and second solutions given above still apply in this generality (although the third solution does not).

Let us also remark that this exercise generalizes the following known fact (which was Corollary 2.3 in the blackboard work on 19 September 2018):

Corollary 4.4. *Let $n \in \mathbb{N}$. Then,*

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

(where we are using the Iverson bracket notation).

To derive this corollary from the exercise, we recall the following fact (that we proved in class):

Proposition 4.5. *Let $m \in \mathbb{N}$ and $n \in \mathbb{N}$ be such that $m < n$. Then, $\binom{m}{n} = 0$.*

Proof of Corollary 4.4. In the case when $n = 0$, it is straightforward to verify Corollary 4.4 by direct computation (it simply becomes $1 = 1$ in this case). Thus, for the rest of this proof, we WLOG assume that we don't have $n = 0$. Thus, $n \neq 0$, so that n is a positive integer and satisfies $[n = 0] = 0$.

Also, $n - 1 \in \mathbb{N}$ (since n is a positive integer) and $n - 1 < n$. Hence, Proposition 4.5 (applied to $m = n - 1$) yields $\binom{n-1}{n} = 0$.

Now, (25) (applied to $m = n$) yields

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

This proves Corollary 4.4. □

5 Exercise 5

5.1 Problem

Let $n \in \mathbb{N}$. If $\mathbf{i} = (i_1, i_2, \ldots, i_n) \in \{0, 1\}^n$ and $k \in [n]$, then

- we say that k is a *1-position* of $\mathbf{i}$ if $i_k = 1$;
- we say that k is a *10-position* of $\mathbf{i}$ if $k < n$, $i_k = 1$ and $i_{k+1} = 0$.

For example, the 7-tuple $(0, 1, 1, 0, 1, 0, 1)$ has 1-positions $2, 3, 5, 7$ and 10-positions $3, 5$.

It is easy to see that for each $k \in \mathbb{Z}$, the number of all n-tuples $\mathbf{i} \in \{0, 1\}^n$ having exactly k 1-positions is $\binom{n}{k}$. (In fact, these n-tuples are in bijection with the k-element subsets of $[n]$.) In this problem, we shall count the n-tuples having exactly k 10-positions.

We use the notation $a\%b$ for the remainder of an integer a upon division by a positive integer b. For example, $5\%3 = 2$. Also, $\lfloor x \rfloor$ denotes the integer part (i.e., floor) of a real number x (that is, the largest integer that is smaller or equal to x).

Let $A : \{0, 1\}^n \to \{0, 1\}^n$ be the map that sends any n-tuple $(i_1, i_2, \ldots, i_n)$ to the n-tuple $(j_1, j_2, \ldots, j_n)$, where

$$j_k = (i_1 + i_2 + \cdots + i_k) \%2 \qquad \text{for all } k.$$

For example, $A((0, 1, 1, 0, 0, 1, 0)) = (0, 1, 0, 0, 0, 1, 1)$.

Prove the following:

(a) The map A is bijective.

(b) If the number of 1-positions of some n-tuple $\mathbf{i} \in \{0,1\}^n$ is p, then the number of 10-positions of the n-tuple $A(\mathbf{i})$ is $\lfloor p/2 \rfloor$.

(c) Let $k \in \mathbb{Z}$. Then, the number of n-tuples $\mathbf{i} \in \{0,1\}^n$ having exactly k 10-positions is $\dbinom{n+1}{2k+1}$.

5.2 Solution sketch

Before we step to the actual problem, let us notice two simple facts about remainders modulo 2:

- For any integer u, we have
$$u \equiv u\%2 \mod 2. \tag{32}$$
- If u and v are two integers satisfying $u \equiv v \mod 2$, then
$$u\%2 = v\%2. \tag{33}$$

(Both of these facts remain true if 2 is replaced by any other positive integer.)

(a) Let $B : \{0,1\}^n \to \{0,1\}^n$ be the map that sends any n-tuple $(j_1, j_2, \ldots, j_n)$ to the n-tuple $(i_1, i_2, \ldots, i_n)$, where

$$i_k = (j_k - j_{k-1})\,\%2 \qquad \text{for all } k,$$

where j_0 is understood to be 0. For example, $B((0,1,1,0,0,1,0)) = (0,1,0,1,0,1,1)$.

We shall show that the maps A and B are mutually inverse. Indeed:

- Let us first check that $B \circ A = \operatorname{id}$.

  Indeed, let $\mathbf{i} \in \{0,1\}^n$ be arbitrary. Write $\mathbf{i}$ in the form $\mathbf{i} = (i_1, i_2, \ldots, i_n)$. Set
$$j_k = (i_1 + i_2 + \cdots + i_k)\,\%2 \qquad \text{for all } k \in [n]. \tag{34}$$
  Then, $A(\mathbf{i}) = (j_1, j_2, \ldots, j_n)$ (by the definition of A).

  Next, set $j_0 = 0$. Set
$$h_k = (j_k - j_{k-1})\,\%2 \qquad \text{for all } k \in [n]. \tag{35}$$
  Then, $B(A(\mathbf{i})) = (h_1, h_2, \ldots, h_n)$ (by the definition of B, because $A(\mathbf{i}) = (j_1, j_2, \ldots, j_n)$).

  For each $k \in [n]$, we have
$$\begin{aligned} j_k &= (i_1 + i_2 + \cdots + i_k)\,\%2 \qquad (\text{by } (34)) \\ &\equiv i_1 + i_2 + \cdots + i_k \mod 2 \qquad (\text{by } (32), \text{ applied to } u = i_1 + i_2 + \cdots + i_k). \end{aligned}$$
  This congruence also holds for $k = 0$ (since $j_0 = 0 \equiv 0 = i_1 + i_2 + \cdots + i_0 \mod 2$). Thus, it holds for all $k \in \{0, 1, \ldots, n\}$. In other words, we have
$$j_k \equiv i_1 + i_2 + \cdots + i_k \mod 2 \qquad \text{for all } k \in \{0, 1, \ldots, n\}. \tag{36}$$

Now, let $k \in [n]$. Then,

$$\underbrace{j_k}_{\substack{\equiv i_1+i_2+\cdots+i_k \mod 2 \\ \text{(by (36))}}} - \underbrace{j_{k-1}}_{\substack{\equiv i_1+i_2+\cdots+i_{k-1} \mod 2 \\ \text{(by (36), applied to } k-1 \text{ instead of } k\text{)}}}$$
$$\equiv (i_1+i_2+\cdots+i_k) - (i_1+i_2+\cdots+i_{k-1}) = i_k \mod 2.$$

Hence, (33) (applied to $u = j_k - j_{k-1}$ and $v = i_k$) yields $(j_k - j_{k-1}) \%2 = i_k\%2$. But $i_k \in \{0,1\}$; thus, i_k is its own remainder upon division by 2. In other words, $i_k\%2 = i_k$. Hence, $(j_k - j_{k-1})\%2 = i_k\%2 = i_k$. Now, (35) becomes $h_k = (j_k - j_{k-1})\%2 = i_k$.

Now, forget that we fixed k. We thus have shown that $h_k = i_k$ for each $k \in [n]$. In other words, $(h_1, h_2, \ldots, h_n) = (i_1, i_2, \ldots, i_n)$. Now,

$$(B \circ A)(\mathbf{i}) = B(A(\mathbf{i})) = (h_1, h_2, \ldots, h_n) = (i_1, i_2, \ldots, i_n) = \mathbf{i} = \operatorname{id}(\mathbf{i}).$$

Now, forget that we fixed $\mathbf{i}$. We thus have shown that $(B \circ A)(\mathbf{i}) = \operatorname{id}(\mathbf{i})$ for each $\mathbf{i} \in \{0,1\}^n$. In other words, $B \circ A = \operatorname{id}$.

- Let us now prove that $A \circ B = \operatorname{id}$.

  Indeed, let $\mathbf{j} \in \{0,1\}^n$ be arbitrary. Write $\mathbf{j}$ in the form $\mathbf{j} = (j_1, j_2, \ldots, j_n)$. Set $j_0 = 0$. Now, set
  $$i_k = (j_k - j_{k-1})\%2 \qquad \text{for all } k \in [n]. \tag{37}$$
  Then, $B(\mathbf{j}) = (i_1, i_2, \ldots, i_n)$ (by the definition of B).

  Next, set
  $$j'_k = (i_1 + i_2 + \cdots + i_k)\%2 \qquad \text{for all } k \in [n]. \tag{38}$$
  Then, $A(B(\mathbf{j})) = (j'_1, j'_2, \ldots, j'_n)$ (by the definition of A, because $B(\mathbf{j}) = (i_1, i_2, \ldots, i_n)$).

  The equality (37) shows that for each $k \in [n]$, we have
  $$i_k = (j_k - j_{k-1})\%2 \equiv j_k - j_{k-1} \mod 2 \tag{39}$$
  (by (32), applied to $u = j_k - j_{k-1}$).

  For each $m \in [n]$, we have
  $$\begin{aligned} i_1 + i_2 + \cdots + i_m &= \sum_{k=1}^{m} \underbrace{i_k}_{\substack{\equiv j_k - j_{k-1} \mod 2 \\ \text{(by (39))}}} \equiv \sum_{k=1}^{m} (j_k - j_{k-1}) \\ &= j_m - \underbrace{j_0}_{=0} \qquad \text{(by the telescope principle)} \\ &= j_m \mod 2, \end{aligned}$$
  and therefore
  $$\begin{aligned} &(i_1 + i_2 + \cdots + i_m)\%2 \\ &= j_m\%2 \qquad \text{(by (33), applied to } u = i_1 + i_2 + \cdots + i_k \text{ and } v = j_m\text{)} \\ &= j_m \qquad (\text{since } j_m \in \{0,1\}). \end{aligned} \tag{40}$$

  Now, for each $k \in [n]$, we have
  $$\begin{aligned} j'_k &= (i_1 + i_2 + \cdots + i_k)\%2 \qquad \text{(by (34))} \\ &= j_k \end{aligned}$$

(by (40), applied to $m = k$). In other words, we have $(j'_1, j'_2, \ldots, j'_n) = (j_1, j_2, \ldots, j_n)$. Now,

$$(A \circ B)(\mathbf{j}) = A(B(\mathbf{j})) = (j'_1, j'_2, \ldots, j'_n) = (j_1, j_2, \ldots, j_n) = \mathbf{j} = \operatorname{id}(\mathbf{j}).$$

Now, forget that we fixed $\mathbf{j}$. We thus have shown that $(A \circ B)(\mathbf{j}) = \operatorname{id}(\mathbf{j})$ for each $\mathbf{j} \in \{0,1\}^n$. In other words, $A \circ B = \operatorname{id}$.

Combining $A \circ B = \operatorname{id}$ with $B \circ A = \operatorname{id}$, we conclude that the maps A and B are mutually inverse. Thus, the map A is invertible, i.e., bijective.

(b) Let $\mathbf{i} \in \{0,1\}^n$ be an n-tuple. Let p be the number of 1-positions of $\mathbf{i}$. We need to prove that the number of 10-positions of the n-tuple $A(\mathbf{i})$ is $\lfloor p/2 \rfloor$.

Indeed, let $h_1, h_2, \ldots, h_p$ be the 1-positions of $\mathbf{i}$, labeled from first to last (so that $h_1 < h_2 < \cdots < h_p$). We shall prove that $h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1$ are the 10-positions of the n-tuple $A(\mathbf{i})$. In other words, we shall prove that

$$\left\{h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1\right\} = \{10\text{-positions of } A(\mathbf{i})\}.$$

This will, of course, entail that the number of 10-positions of the n-tuple $A(\mathbf{i})$ is $\lfloor p/2 \rfloor$ (since $h_2 - 1 < h_4 - 1 < \cdots < h_{2\lfloor p/2 \rfloor} - 1$).

But first, let us write $\mathbf{i}$ in the form $\mathbf{i} = (i_1, i_2, \ldots, i_n)$. Set

$$j_k = (i_1 + i_2 + \cdots + i_k) \% 2 \qquad \text{for all } k \in [n]. \tag{41}$$

Then, $A(\mathbf{i}) = (j_1, j_2, \ldots, j_n)$ (by the definition of A).

Now we claim that every $k \in [n]$ satisfies

$$j_k = (\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq k) \% 2. \tag{42}$$

[*Proof of* (42)*:* Let $k \in [n]$. Then,

$$\begin{aligned}
i_1 + i_2 + \cdots + i_k &= \sum_{r \in [k]} i_r = \sum_{\substack{r \in [k];\\ i_r = 0}} \underbrace{i_r}_{=0} + \sum_{\substack{r \in [k];\\ i_r = 1}} \underbrace{i_r}_{=1} \\
&\qquad \left(\text{since each } r \in [k] \text{ satisfies either } i_r = 0 \text{ or } i_r = 1 \text{ (but not both)}\right) \\
&= \underbrace{\sum_{\substack{r \in [k];\\ i_r = 0}} 0}_{=0} + \sum_{\substack{r \in [k];\\ i_r = 1}} 1 = \sum_{\substack{r \in [k];\\ i_r = 1}} 1 \\
&= (\text{the number of all } r \in [k] \text{ satisfying } i_r = 1) \cdot 1 \\
&= (\text{the number of all } r \in [k] \text{ satisfying } i_r = 1) \\
&= (\text{the number of all 1-positions of } \mathbf{i} \text{ that belong to } [k]) \\
&\qquad \left(\begin{array}{c}\text{since the } r \in [k] \text{ satisfying } i_r = 1 \text{ are precisely} \\ \text{the 1-positions of } \mathbf{i} \text{ that belong to } [k]\end{array}\right) \\
&= (\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq k)
\end{aligned}$$

(since the 1-positions of $\mathbf{i}$ that belong to $[k]$ are precisely the 1-positions of $\mathbf{i}$ that are $\leq k$). Hence, (41) yields

$$\begin{aligned}
j_k &= \underbrace{(i_1 + i_2 + \cdots + i_k)}_{=(\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq k)} \% 2 \\
&= (\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq k) \% 2.
\end{aligned}$$

This proves (42).]

Next, we claim that

$$\left\{h_2-1, h_4-1, \ldots, h_{2\lfloor p/2\rfloor}-1\right\} \subseteq \{\text{10-positions of } A(\mathbf{i})\}. \tag{43}$$

[*Proof of* (43): Let $q \in \left\{h_2-1, h_4-1, \ldots, h_{2\lfloor p/2\rfloor}-1\right\}$. We need to show that $q \in \{\text{10-positions of } A(\mathbf{i})\}$.

We have $q \in \left\{h_2-1, h_4-1, \ldots, h_{2\lfloor p/2\rfloor}-1\right\}$; thus, $q = h_x - 1$ for some even $x \in [p]$. Consider this x.

We know that x is even; thus, $x-1$ is odd.

We have $x \geq 2$ (since $x \in [p]$ is even). But $h_1 < h_2 < \cdots < h_p$; thus, $h_1 < h_x$ (since $x \geq 2 > 1$). Hence, $h_x > h_1 \geq 1$, so that $h_x - 1 > 0$. Hence, $q = h_x - 1 > 0$. Combined with $q = h_x - 1 < h_x \leq n$, this yields $q \in [n-1]$. Thus, j_q and j_{q+1} are well-defined.

Recall that the 1-positions of $\mathbf{i}$ are $h_1, h_2, \ldots, h_p$; these 1-positions are listed in strictly increasing order (i.e., we have $h_1 < h_2 < \cdots < h_p$). Hence, the first $x-1$ of these 1-positions are $< h_x$, whereas the remaining $p-x+1$ of these 1-positions are $\geq h_x$. Thus, the 1-positions of $\mathbf{i}$ that are $< h_x$ are precisely $h_1, h_2, \ldots, h_{x-1}$. Similar reasoning shows that the 1-positions of $\mathbf{i}$ that are $\leq h_x$ are precisely $h_1, h_2, \ldots, h_x$.

From (42) (applied to $k = q$), we obtain

$$\begin{aligned} j_q &= (\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq q)\,\%2 \\ &= \underbrace{(\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq h_x - 1)}_{\substack{=(\text{the number of 1-positions of } \mathbf{i} \text{ that are } < h_x) \\ = x-1 \\ (\text{since the 1-positions of } \mathbf{i} \text{ that are } < h_x \text{ are precisely } h_1, h_2, \ldots, h_{x-1})}}\,\%2 \qquad (\text{since } q = h_x - 1) \\ &= (x-1)\,\%2 = 1 \end{aligned}$$

(since $x-1$ is odd).

But $q+1 = h_x$ (since $q = h_x - 1$). From (42) (applied to $k = q+1$), we obtain

$$\begin{aligned} j_{q+1} &= (\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq q+1)\,\%2 \\ &= \underbrace{(\text{the number of 1-positions of } \mathbf{i} \text{ that are} \leq h_x)}_{\substack{= x \\ (\text{since the 1-positions of } \mathbf{i} \text{ that are } \leq h_x \text{ are precisely } h_1, h_2, \ldots, h_x)}}\,\%2 \qquad (\text{since } q+1 = h_x) \\ &= x\%2 = 0 \end{aligned}$$

(since x is even).

Recall that $A(\mathbf{i}) = (j_1, j_2, \ldots, j_n)$. Thus, an integer $k \in [n]$ is a 10-position of $A(\mathbf{i})$ if and only if $k < n$, $j_k = 1$ and $j_{k+1} = 0$ (by the definition of a "10-position"). We can apply this to $k = q$ (since $q \in [n-1] \subseteq [n]$); thus, we conclude that q is a 10-position of $A(\mathbf{i})$ (since it does satisfy $q < n$ and $j_q = 1$ and $j_{q+1} = 0$). In other words, $q \in \{\text{10-positions of } A(\mathbf{i})\}$.

Now, forget that we fixed q. We thus have shown that $q \in \{\text{10-positions of } A(\mathbf{i})\}$ for each $q \in \left\{h_2-1, h_4-1, \ldots, h_{2\lfloor p/2\rfloor}-1\right\}$. In other words, $\left\{h_2-1, h_4-1, \ldots, h_{2\lfloor p/2\rfloor}-1\right\} \subseteq \{\text{10-positions of } A(\mathbf{i})\}$. This proves (43).]

Next, we claim that

$$\{\text{10-positions of } A(\mathbf{i})\} \subseteq \left\{h_2-1, h_4-1, \ldots, h_{2\lfloor p/2\rfloor}-1\right\}. \tag{44}$$

[*Proof of* (43): Let $q \in \{\text{10-positions of } A(\mathbf{i})\}$. We need to show that $q \in \left\{h_2-1, h_4-1, \ldots, h_{2\lfloor p/2\rfloor}-1\right\}$.

We have $q \in \{\text{10-positions of } A(\mathbf{i})\}$. In other words, q is a 10-position of $A(\mathbf{i})$.

Recall that $A(\mathbf{i}) = (j_1, j_2, \ldots, j_n)$. Thus, an integer $k \in [n]$ is a 10-position of $A(\mathbf{i})$ if and only if $k < n$, $j_k = 1$ and $j_{k+1} = 0$ (by the definition of a "10-position"). We can apply this to $k = q$; thus we conclude that $q \in [n]$ satisfies $q < n$, $j_q = 1$ and $j_{q+1} = 0$ (since q is a 10-position of $A(\mathbf{i})$).

From (42) (applied to $k = q$), we obtain

$$j_q = (\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q) \%2. \tag{45}$$

But $q+1 \in [n]$ (since $q \in [n]$ and $q < n$); thus, (42) (applied to $k = q+1$) yields

$$j_{q+1} = (\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q+1) \%2.$$

Hence,

$$\begin{aligned} &(\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q+1) \%2 \\ &= j_{q+1} = 0 \neq 1 = j_q = (\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q) \%2 \end{aligned}$$

(by (45)). Therefore,

$$\begin{aligned} &(\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q+1) \\ &\neq (\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q). \end{aligned} \tag{46}$$

Thus, $q+1$ must be a 1-position of $\mathbf{i}$ (because otherwise, the 1-positions of $\mathbf{i}$ that are $\leq q+1$ would be **exactly** the 1-positions of $\mathbf{i}$ that are $\leq q$; but this would yield

$$\begin{aligned} &(\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q+1) \\ &= (\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q), \end{aligned}$$

which would contradict (46)). In other words, $q+1$ is one of the numbers $h_1, h_2, \ldots, h_p$ (since $h_1, h_2, \ldots, h_p$ are the 1-positions of $\mathbf{i}$). In other words, there exists some $x \in [p]$ such that $q + 1 = h_x$. Consider this x. From $q + 1 = h_x$, we obtain $q = h_x - 1$.

Recall that the 1-positions of $\mathbf{i}$ are $h_1, h_2, \ldots, h_p$; these 1-positions are listed in strictly increasing order (i.e., we have $h_1 < h_2 < \cdots < h_p$). Hence, the first x of these 1-positions are $\leq h_x$, whereas the remaining $p - x$ of these 1-positions are $> h_x$. Thus, the 1-positions of $\mathbf{i}$ that are $\leq h_x$ are precisely $h_1, h_2, \ldots, h_x$.

From (42) (applied to $k = q+1$), we obtain

$$\begin{aligned} j_{q+1} &= (\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq q+1) \%2 \\ &= \underbrace{(\text{the number of 1-positions of } \mathbf{i} \text{ that are } \leq h_x)}_{\substack{=x \\ (\text{since the 1-positions of } \mathbf{i} \text{ that are } \leq h_x \text{ are precisely } h_1, h_2, \ldots, h_x)}} \%2 \qquad (\text{since } q+1 = h_x) \\ &= x\%2. \end{aligned}$$

Therefore, $x\%2 = j_{q+1} = 0$. In other words, x is even.

Now,

$$\begin{aligned} q = h_x - 1 &\in \{h_k - 1 \mid k \in [p] \text{ is even}\} \qquad (\text{since } x \in [p] \text{ is even}) \\ &= \left\{h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1\right\}. \end{aligned}$$

Forget that we fixed q. We thus have shown that $q \in \left\{h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1\right\}$ for each $q \in \{\text{10-positions of } A(\mathbf{i})\}$. In other words, $\{\text{10-positions of } A(\mathbf{i})\} \subseteq \left\{h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1\right\}$. This proves (44).]

Combining (43) with (44), we obtain

$$\{\text{10-positions of } A(\mathbf{i})\} = \left\{h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1\right\}. \tag{47}$$

In other words, the 10-positions of $A(\mathbf{i})$ are precisely $h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1$. Since these $\lfloor p/2 \rfloor$ elements $h_2 - 1, h_4 - 1, \ldots, h_{2\lfloor p/2 \rfloor} - 1$ are distinct[7], we thus conclude that the

[7] This follows easily from $h_1 < h_2 < \cdots < h_p$.

number of 10-positions of $A(\mathbf{i})$ is $\lfloor p/2 \rfloor$. This solves part **(b)** of the exercise.

(c) The map A is bijective (according to part **(a)** of the exercise). Thus,

$$\begin{aligned} & (\text{the number of } \mathbf{i} \in \{0,1\}^n \text{ such that } \mathbf{i} \text{ has exactly } k \text{ 10-positions}) \\ & = (\text{the number of } \mathbf{i} \in \{0,1\}^n \text{ such that } A(\mathbf{i}) \text{ has exactly } k \text{ 10-positions}) \end{aligned} \tag{48}$$

(here, we have substituted $A(\mathbf{i})$ for $\mathbf{i}$ in the count, since the map A is bijective).

But for each n-tuple $\mathbf{i} \in \{0,1\}^n$, we have the following logical equivalence:

$$\begin{aligned} & (A(\mathbf{i}) \text{ has exactly } k \text{ 10-positions}) \\ \Longleftrightarrow\ & (\mathbf{i} \text{ has exactly } 2k \text{ or } 2k+1 \text{ 1-positions}). \end{aligned} \tag{49}$$

[*Proof of* (49)*:* Let $\mathbf{i} \in \{0,1\}^n$ be an n-tuple. Let p be the number of 1-positions of $\mathbf{i}$. Then, part **(b)** of the exercise shows that the number of 10-positions of the n-tuple $A(\mathbf{i})$ is $\lfloor p/2 \rfloor$. Now, we have the following chain of logical equivalences:

$$\begin{aligned} & (A(\mathbf{i}) \text{ has exactly } k \text{ 10-positions}) \\ \Longleftrightarrow\ & (\text{the number of 10-positions of the } n\text{-tuple } A(\mathbf{i}) \text{ is } k) \\ \Longleftrightarrow\ & (\lfloor p/2 \rfloor = k) \\ & \quad (\text{since the number of 10-positions of the } n\text{-tuple } A(\mathbf{i}) \text{ is } \lfloor p/2 \rfloor) \\ \Longleftrightarrow\ & (k \leq p/2 < k+1) \\ & \quad (\text{by the definition of } \lfloor p/2 \rfloor) \\ \Longleftrightarrow\ & (2k \leq p < 2(k+1)) \\ \Longleftrightarrow\ & (p \text{ is either } 2k \text{ or } 2k+1) \\ & \quad (\text{since } p \text{ is an integer}) \\ \Longleftrightarrow\ & (\text{the number of 1-positions of } \mathbf{i} \text{ is either } 2k \text{ or } 2k+1) \\ & \quad (\text{since } p \text{ is the number of 1-positions of } \mathbf{i}) \\ \Longleftrightarrow\ & (\mathbf{i} \text{ has exactly } 2k \text{ or } 2k+1 \text{ 1-positions}). \end{aligned}$$

This proves (49).]

Recall furthermore the following fact (already mentioned in the exercise):

Claim 1: Let $j \in \mathbb{Z}$. Then,

$$(\text{the number of all } n\text{-tuples } \mathbf{i} \in \{0,1\}^n \text{ having exactly } j \text{ 1-positions}) = \binom{n}{j}.$$

[*Proof of Claim 1:* Let $\mathcal{P}_j([n])$ denote the set of all j-element subsets of the set $[n]$. Then, $|\mathcal{P}_j([n])| = \binom{n}{j}$ (by the combinatorial interpretation of the binomial coefficients).

But the map

$$\begin{aligned} \{\mathbf{i} \in \{0,1\}^n \mid \mathbf{i} \text{ has exactly } j \text{ 1-positions}\} &\to \mathcal{P}_j([n]), \\ (i_1, i_2, \ldots, i_n) &\mapsto \{p \in [n] \mid i_p = 1\} \end{aligned}$$

is a bijection (indeed, its inverse is the map

$$\begin{aligned} \mathcal{P}_j([n]) &\to \{\mathbf{i} \in \{0,1\}^n \mid \mathbf{i} \text{ has exactly } j \text{ 1-positions}\}, \\ S &\mapsto ([1 \in S], [2 \in S], \ldots, [n \in S]), \end{aligned}$$

where we are using the Iverson bracket notation). Hence,

$$\left|\left\{\mathbf{i} \in \{0,1\}^n \ \mid \ \mathbf{i} \text{ has exactly } j \text{ 1-positions}\right\}\right| = \left|\mathcal{P}_j\left([n]\right)\right| = \dbinom{n}{j}.$$

Thus,

$$\begin{aligned}&\left(\text{the number of all } n\text{-tuples } \mathbf{i} \in \{0,1\}^n \text{ having exactly } j \text{ 1-positions}\right)\\ &= \left|\left\{\mathbf{i} \in \{0,1\}^n \ \mid \ \mathbf{i} \text{ has exactly } j \text{ 1-positions}\right\}\right| = \dbinom{n}{j}.\end{aligned}$$

This proves Claim 1.]

Now, all we need is to combine what we have proven. We have

$$\begin{aligned}&\left(\text{the number of } n\text{-tuples } \mathbf{i} \in \{0,1\}^n \text{ having exactly } k \text{ 10-positions}\right)\\ &= \left(\text{the number of } \mathbf{i} \in \{0,1\}^n \text{ such that } \mathbf{i} \text{ has exactly } k \text{ 10-positions}\right)\\ &= \underbrace{\left(\text{the number of } \mathbf{i} \in \{0,1\}^n \text{ such that } \underbrace{A\left(\mathbf{i}\right) \text{ has exactly } k \text{ 10-positions}}_{\substack{\Longleftrightarrow (\mathbf{i} \text{ has exactly } 2k \text{ or } 2k+1 \text{ 1-positions})\\ \text{(by (49))}}}\right)}_{}\\ &\qquad \text{(by (48))}\\ &= \left(\text{the number of } \mathbf{i} \in \{0,1\}^n \text{ such that } \mathbf{i} \text{ has exactly } 2k \text{ or } 2k+1 \text{ 1-positions}\right)\\ &= \underbrace{\left(\text{the number of } \mathbf{i} \in \{0,1\}^n \text{ such that } \mathbf{i} \text{ has exactly } 2k \text{ 1-positions}\right)}_{\substack{=(\text{the number of all } n\text{-tuples } \mathbf{i}\in\{0,1\}^n \text{ having exactly } 2k \text{ 1-positions})\\ =\binom{n}{2k}\\ \text{(by Claim 1, applied to } j=2k)}}\\ &\qquad + \underbrace{\left(\text{the number of } \mathbf{i} \in \{0,1\}^n \text{ such that } \mathbf{i} \text{ has exactly } 2k+1 \text{ 1-positions}\right)}_{\substack{=(\text{the number of all } n\text{-tuples } \mathbf{i}\in\{0,1\}^n \text{ having exactly } 2k+1 \text{ 1-positions})\\ =\binom{n}{2k+1}\\ \text{(by Claim 1, applied to } j=2k+1)}}\\ &= \dbinom{n}{2k} + \dbinom{n}{2k+1} = \dbinom{n+1}{2k+1}\end{aligned}$$

(since the recurrence relation of the binomial coefficients yields $\dbinom{n+1}{2k+1} = \dbinom{(n+1)-1}{(2k+1)-1} + \dbinom{(n+1)-1}{2k+1} = \dbinom{n}{2k} + \dbinom{n}{2k+1}$). This solves part **(c)** of the exercise.