Mathematical Foundations of Computer Science

CS 499, Shanghai Jiao Tong University, Dominik Scheder

Group Mogicians

- Monday, 2018-03-19, homework handed out
- Sunday, 2018-03-25, 12:00: submit questions and first submissions. You'll get feedback until Wednesday.
- Sunday, 2018-03-29 (Wednesday), 18:00: submit your review of the other group's first submission.
- 2018-04-01: submit final solution.

4 Pascal's Triangle Modulo 2

4.1 Lucas Theorem: $\binom{n}{k} \mod 2$

Theorem 4.1. *Let $n, k \in \mathbb{N}_0$. Then $\binom{n}{k}$ is odd if $k \preceq n$ and even otherwise.*

Note that this theorem lets us compute $\binom{n}{k} \mod 2$ quickly for numbers n, k having millions of digits, whereas no computer on Earth has the memory to evaluate the formula

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+2) \cdot (n-k+1)}{k \cdot (k-1) \cdot (k-2) \cdot \dots \cdot 2 \cdot 1}$$

for values that large. Let me now walk you through a proof of this theorem.

Definition 4.2. *For a natural number $n \in \mathbb{N}$, let $|n|_1$ be the number of 1's in the binary representation of n. For example, $|1|_1 = |2|_1 = |4|_1 = 1$ but $|3|_1 = 2$ and $|7|_1 = 3$.*

Definition 4.3. *For a natural number $a \in \mathbb{N}$ define $f(a)$ as the number of times the factor 2 appears in a. Formally,*

$$f(a) := \max\{k \mid 2^k \text{ divides } a\} .$$

For example, $f(24) = 3$ since 8 divides 24 but 16 does not.

Exercise 4.4. Find a closed formula for $f(n!)$ in terms of n and $|n|_1$.

Answer The function $f(a)$ means the biggest number x, which makes 2^x divides a. If we convert a to a binary form $a_{0,1}$, there will be another interpretation, that the output of $f(a)$ is the lowest position of number 1 in $a_{0,1}$. As we know, if 2 can divide the binary number $a_{0,1}$, $a_{0,1}$ must be even (0 at the end of $a_{0,1}$) and $a_{0,1}/2$ means a right shift of $a_{0,1}$. Now the function can be interpreted as calculating how many factor 2 does a has. The sum of factor 2 in $n!$ is $n/2 + n/2^2 + n/2^3 + \ldots$. Suppose that

$$n_{0,1} = b_N b_{N-1} b_{N-2} \ldots b_0, b_i \in \{0, 1\}$$

Then

$$\begin{aligned} f(n!) &= n/2 + n/2^2 + n/2^3 + \ldots \\ &= b_N b_{N-1} \ldots b_1 + b_N b_{N-1} \ldots b_2 + \cdots + b_N b_{N-1} + b_N \end{aligned}$$

We let both sides of the equation be multiplied by 2

$$2 * f(n!) = b_N b_{N-1} \ldots b_1 0 + b_N b_{N-1} \ldots b_2 0 + \cdots + b_N b_{N-1} 0 + b_N 0 + 0$$

After that, we subtract the above two equations

$$\begin{aligned} f(n!) &= b_N b_{N-1} \ldots b_1 0 \\ &\quad + (b_N b_{N-1} \ldots b_2 0 - b_N b_{N-1} \ldots b_1) + \ldots \\ &\quad + (b_N b_{N-1} 0 - b_N b_{N-1} b_{N-2}) + (b_N 0 - b_N b_{N-1}) + (0 - b_N) \\ &= n - (b_0 + b_1 + \cdots + b_n) \end{aligned}$$

Since $b_0 + b_1 + \cdots + b_n = |n|_1$, we can get the answer by $n - |n|_1$.

Exercise 4.5. Find a closed formula for $f\left(\binom{n}{k}\right)$ in terms of $n, k, |n|_1$, and so on.

Answer With the conclusions in Exercise 4.4, $f\left(\binom{n}{k}\right) = f(\frac{n!}{k!(n-k)!}) = f(n!) - f(k!) - f((n-k)!) = n - |n|_1 - (k - |k|_1) - (n - k - |n-k|_1) = |n-k|_1 - |n|_1 + |k|_1$.

Exercise 4.6. Prove Theorem 4.1. With our new notation, prove that $f\left(\binom{n}{k}\right)$ is 0 if $k \preceq n$ and at least 1 if $k \not\preceq n$.

Proof. We can acquire the parity of $\binom{n}{k}$ by calculating whether it has the factor 2. As is shown in Exercise 4.4 and 4.5, if $|n-k|_1 - |n|_1 + |k|_1 > 0$, $\binom{n}{k}$ has the factor 2. If $k \preceq n$, $|n-k|_1 - |n|_1 + |k|_1 = 0$ so that $\binom{n}{k}$ is odd and $f(\binom{n}{k}) = 0$. Notice that when we add $k_{0,1}$ and $(n-k)_{0,1}$ together, the result will lose a number 1 if a carry happens since there are only two conditions that are $1+1+0 = 10$ and $1+1+1 = 11$ and both of them will lose an 1. If $k \not\preceq n$, the carry must happen which makes $|n-k|_1 + |k|_1 > |(n-k)+k|_1 = |n|_1$. Therefore, $|n-k|_1 - |n|_1 + |k|_1 > 0$ so that $\binom{n}{k}$ is even and $f(\binom{n}{k})$ is at least 1.

□

4.2 Almost Empty Rows

One feature of the Sierpinski triangle is that some rows are almost empty. For example, row 64 has a black dot at the very left and the very right, and only white space in between. This is because

Theorem 4.7. *Let $d \in \mathbb{N}_0$ and $0 < k < 2^d$. Then $\binom{2^d}{k}$ is even.*

Although this theorem follows easily from Lucas' Theorem, I want you to think about an alternative proof. Intuitively, if some number is even, then one suspects it can be proved by "pairing things up" perfectly. After all, if you can prove that in a set S, every element can be "married" to another element, you have partitioned S into couples and thus $|S|$ must be even. So let's see whether there is a proof of Theorem 4.7 along these lines. This is also valuable because it lets you practice with notions of sets and functions.

Consider the set $\{0,1\}^d$. You can view this as the set of all binary strings of length d. This set has size $2^d = n$. For $1 \leq i \leq d$ and $x \in \{0,1\}^d$ let $f_i(x)$ be x with the i^{th} position flipped. For example, $f_3(11011) = 11111$.

Exercise 4.8. Show that f_i is an involution without a fixed point. That is, $f(f(x)) = x$ and $f(x) \neq x$ for all $x \in \{0,1\}^d$.

Answer Consider x is $\underbrace{\cdots x_i \cdots}_{n \text{ numbers}}$. The ith item in x is x_i. We can easily get that $f_i(x) = \cdots x_i' \cdots$.
x_i' means that when $x_i = 0$ $x_i' = 1$ or $x_i = 0$ $x_i' = 1$. So obviously $f_i(x)$ is not equal to x.
Because of the definition of f_i we can get that $f_i(f_i(x)) = \cdots x_i \cdots = f_i(x)$.
Let $S \subseteq \{0,1\}^d$. We define $f_i(S)$ as the set arising from applying f_i to every element of S. Formally,

$$f_i(S) := \{f_i(x) \mid x \in S\} .$$

Given a set $S \subseteq \{0,1\}^d$, we call an index $i \in [n]$ *active* for S if $f_i(S) \neq S$.

Exercise 4.9. Let $d = 3$ and $S = \{000, 100\}$. Which of the indices $1, 2, 3$ are active?

Answer The index 1 is not active because $f_1(S) = \{f_1(000), f_1(100)\} = \{100, 000\} = S$.
The index 2 is active because $f_2(S) = \{f_2(000), f_2(100)\} = \{010, 110\} \neq S$
The index 3 is active because $f_3(S) = \{f_3(000), f_3(100)\} = \{001, 101\} \neq S$

Exercise 4.10. Let $S \subseteq \{0,1\}^d$. Show that if $S \neq \emptyset$ and $S \neq \{0,1\}^d$ then S has at least one active index.

Proof. Assume $S \subset \{0,1\}^d$ has no active index, and $\exists x_0 \in S$.
Define all the sequences that have i different bits with x_0 are contained in a set L_i, $0 \leq i \leq d$.
Apparently, $\forall 0 \leq i < j \leq d$, $|L_i \cap L_j| = 0$; $\forall x \in \{0,1\}^d$, $\exists 0 \leq i \leq d$, $x \in L_i$; $L_0 = \{x_0\}$.
This means $\bigcup_{i=0}^{d} L_i = \{0,1\}^d$.
Because S has no active index, we can get a statement as follows.

$$\forall x \in S,\ \forall 1 \leq i \leq d,\ f_i(x) \in S. \tag{1}$$

According to the statement above and the definition of L_i, we can see if $L_i \subset S$, $L_{i+1} \subset S$.
Now we have $x_0 \in S$, in other words, $L_0 \subset S$. By induction, $\forall 1 \leq i \leq d$, $L_i \subset S$. Then $S = \bigcup_{i=0}^{d} L_i = \{0,1\}^d$, which is inconsistent with the assumption $S \subset \{0,1\}^d$.
So S has at least one active index.

□

Given $S \subseteq \{0,1\}^d$, define $f(S)$ as follows: if $S = \emptyset$ or $S = \{0,1\}^d$ define $f(S) = S$. Otherwise, let $f(S) := f_i(S)$ where i is the smallest active index of S (which exists by the previous exercise).

Exercise 4.11. Show that f is an involution. That is, $f(f(S)) = S$. Furthermore, show that the only fixed points of f are $\emptyset$ and $\{0,1\}^d$.

Proof. If $S = \emptyset$ or $S = \{0,1\}^d$, the equation is easy to prove. Otherwise, let i be the smallest active index of S, $S' = f(S) = f_i(S)$. From the above Exercise, we know that $f_i(S') = \{f_i(f_i(x))|x \in S\} = \{x|x \in S\} = S$. Next we need to prove that i is the smallest active index of S'.

It is obvious if $i = 1$. If $i > 1$, take any j such that $1 \leq j < i$. $\forall x \in S$, $x = (\cdots, x_j, \cdots, x_i, \cdots)$, $\exists y \in S$, $y = (\cdots, 1 - x_j, \cdots, x_i, \cdots)$, we find that $f_j(x) = y \in S$ and $f_j(y) = x \in S$. Then $x' = f_i(x) = (\cdots, x_j, \cdots, 1 - x_i, \cdots)$, $y' = f_i(y) = (\cdots, 1 - x_j, \cdots, 1 - x_i, \cdots)$. We also have $f_j(x') = y' \in S'$. That is to say, $\forall x' \in S'$, $f_j(x') = y' \in S'$. So j is not an active index of S', and i is the smallest one.

Since $f(S) = f_i(S) \neq S$, the only fixed points of f are $\emptyset$ and $\{0,1\}^d$. $\square$

Exercise 4.12. Let $\mathcal{S} = \binom{\{0,1\}^d}{k}$. This is a set of sets, and each set $S \in \mathcal{S}$ consists of exactly k strings from $\{0,1\}^d$. Prove the following statements:

1. f is a bijection from $\mathcal{S}$ to $\mathcal{S}$.
2. For $1 \leq k \leq 2^d - 1$, this bijection is an involution without fixed points.
3. $|\mathcal{S}|$ is even for $1 \leq k \leq 2^d - 1$.

Proof.

4.12.1 From the above Exercise, we know that $\forall S_1 \in \mathcal{S}$, $\exists S_2 \in \mathcal{S}$, $S_1 \neq S_2$ and $f(S_1) = S_2$, $f(S_2) = f(f(S_1)) = S_1$. So f is surjective. f is injective because for any two different S_1 and S_2, $S_1 = f(f(S_1))$, $S_2 = f(f(S_2))$, that is to say, $f(f(S_1)) \neq f(f(S_2))$, so $f(S_1) \neq f(S_2)$. So $\mathcal{S}$ is a bijection from $\mathcal{S}$ to $\mathcal{S}$.

4.12.2 From the Exercise 4.11, we know that since $1 \leq k \leq 2^d - 1$, $\mathcal{S} \neq \emptyset$ and $\mathcal{S} \neq \{0,1\}^d$. So $f(S) \neq S$, the bijection is an involution without fixed points.

4.12.3 $\forall S_1 \in \mathcal{S}$, $\exists S_2 \in \mathcal{S}$. Let $\mathcal{S}' = \mathcal{S} \setminus \{S1, S2\}$. Suppose $|\mathcal{S}|$ is odd for $1 \leq k \leq 2^d - 1$, we can do the above delete process for $\frac{|\mathcal{S}|-1}{2}$ times, and at last there is only one element S. This situation cannot exist because $\exists S' \in \mathcal{S}$, $S' = f(S) \neq S$. When $\mathcal{S}$ deletes S', it also deletes S. So $|\mathcal{S}|$ is even for $1 \leq k \leq 2^d - 1$.

$\square$

Exercise 4.13. Complete the proof of Theorem 4.7.

Proof. Let $d \in \mathbb{N}_0$ and $0 < k < 2^d$. From Exercise 4.12, $|\mathcal{S}|$ is even. Because $|\mathcal{S}| = \binom{2^d}{k}$, $\binom{2^d}{k}$ is even. □

***Exercise 4.14.** *Generalize the above "combinatorial" proof to show the following theorem:*

Theorem 4.15. *Let $n = p^d$ where p is a prime number. Then p divides $\binom{n}{k}$ unless $k = 0$ or $k = n$.*

Proof. Consider the set $\mathbb{Z}_p^d$. You can view this set as the set of all **vectors** whose components are non-negative integers less than p. This set has size p^d.

Definition 4.16. *For $1 \leq i \leq d$, let $f_i : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$, its components are defined as:*

$$f_i(\boldsymbol{x})_j = \begin{cases} x_j, & j \neq i \\ x_j + 1 \mod p, & j = i \end{cases}$$

Given a set $S \in \mathbb{Z}_p^d$, define:

$$f_i(S) = \{f_i(\boldsymbol{x}) | \boldsymbol{x} \in S\}$$

For example, when p is 5, $f_3((1,2,3,4)) = (1,2,4,4)$ and $f_3((1,2,4,4)) = (1,2,0,4)$

Definition 4.17. *Define:* $\underbrace{f \circ f \circ \cdots \circ f}_{n} \triangleq f^n$

*A function f is **n-involution** if:*

$$f^n = id$$

So a regular involution function is "2-involution".

Lemma 4.18. *$f_i(\boldsymbol{x})$ is p-involution.*

Proof. Let $F_i = \underbrace{f_i \circ \cdots \circ f_i}_{n}$, then

$$\begin{aligned} F_i(\boldsymbol{x})_j &= \begin{cases} x_j, & j \neq i \\ x_j + p \mod p, & j = i \end{cases} \\ &= x_j \end{aligned}$$

□

Definition 4.19. *$S \in \mathbb{Z}_p^d$, we call an index $i \in [n]$ active for S if $f_i(S) \neq S$*

Let $f(S) = f_i(S)$ where i is the smallest active index of S, and if $S \in \{\emptyset,\ \mathbb{Z}_p^d\}$, $f(S) = S$.

Lemma 4.20. *If $S \neq \emptyset$ and $S \neq \mathbb{Z}_p^d$, then S has at least one active index*

Proof. Obviously $\emptyset$ has no active index because $\forall i \in [d],\ f_i(\emptyset) = \emptyset$

If S is not empty and has no active index, that is to say, $\forall \boldsymbol{x} \in S, \forall i \in [d], f_i(\boldsymbol{x}) \in S$. By induction, we know: $f_1^{k_1} \circ f_2^{k_2} \circ \cdots \circ f_d^{k_d}(\boldsymbol{x}) \in S,\ k_i \in \mathbb{N}$

So select $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in S$, every elements $\boldsymbol{x} = (x_1, \ldots, x_d) \in \mathbb{Z}_p^d$ can be represented as:

$$f_1^{x_1+p-\alpha_1} \circ f_2^{x_2+p-\alpha_2} \circ \cdots \circ f_d^{x_d+p-\alpha_d}(\boldsymbol{\alpha})$$

And it's in S for the previous conclusion. So $S = \mathbb{Z}_p^d$ is the only non-empty set without an active index. □

Lemma 4.21. *Function $f_i(S)$ will not change a set's smallest active index.*

Proof. Let i be the smallest active index of S, and j be that of $f(S)$.

If $j < i$, because f_i will not change the j^{th} components of vectors in S and j is active for S, j can be the smallest active index of S rather than i.

If $j > i$, which means i is no longer an active index after applying f_i. Let $S' = f(S) = f_i(S)$, we can know that $S' \neq S$ for i is active at that time. So by induction, $f_i^{p-1}(S') = f_i^{-1}(S') = S'$ (because f_i is p-involution). However, $f_i^{-1}(S') = S$, which contradict to the previous conclusion.

So $i = j$. □

Definition 4.22. *x_0 is an r-fixed point of $f(x)$ if $f^r(x_0) = x_0$*

Lemma 4.23. *f is p-involution. And $\emptyset$ and $\mathbb{Z}_p^d$ are the only fixed points of $f(S)$*

Proof. Function f will not change the smallest active index of the set, so for the given set S, $\exists i,\ f \equiv f_i$. So f is p-involution because f_i is.

Obviously $\emptyset$ and $\mathbb{Z}_p^d$ are fixed points because of the definition of f. For the other sets, they have at least one active index, so $f(S) \neq S$ and they're not fixed points. □

Lemma 4.24. *f has an r-fixed point if and only if $gcd(r, p) \neq 1$*

Proof. Assume that S_0 is an r-fixed point of f. For a given S_0, $\exists i,\ f = f_i$ (because of lemma 4.21). So we define:

$$T = \{x_i | \boldsymbol{x} \in S_0\}$$

$$g_r(x) = x + r \mod p$$

So

$$f_i(\boldsymbol{x})_j = \begin{cases} x_j, & j \neq i \\ g_r(x_j), & j = i \end{cases}$$

We can know that $\forall x_0 \in S_0,\ g_r(x_0) \in S_0$. So by induction, $g_r^k(x_0) \in S_0$. Then $S_0 = \{y | y = g_r^k(x_0),\ k \in [p]\}$,and it is an r-fixed point of f if and only if $S_0 \neq [p]$(if not, i will not be an active index).

Now the target becomes proving $\{y | y = x_0 + kr \mod p\} \neq [p]$, or in other words, $y = h(k) = x_0 + kr \mod p$ is a bijection on $[n]$. Consider the condition of the existence of inverse element on addictive group on integers modulo p, we can conclude that $gcd(r, p) \neq 1$ □

Let $\boldsymbol{S} = \binom{\mathbb{Z}_p^d}{k},\ 1 \leq k \leq 2^d - 1$. For each set $S \in \boldsymbol{S}$, define

$$T_S = \{S' | S' = f^c(S), c \in \mathbb{N}\}$$

f has no r-fixed point for $r < p$ because p is a prime number. So we can know that $T_S \subset \boldsymbol{S}$ and $|T_S| = p$ because f is p-involution. Every S is in a certain set T, so $\boldsymbol{S}$ is divided into a few subset T in this way. Therefore, $p \mid |\binom{\mathbb{Z}_p^d}{k}|$, or, $p \mid \binom{p^d}{k}$

□