Тасування карт і ланцюги Маркова

Кучеренко Анастасія, Хілько Данило
Київський національний університет ім. Тараса Шевченка і Ecole normale supérieure de Paris

> У карти, так обшмульгані, що аж,
> засіли пан різник і пан музика.
> Була спокуса виграшу велика,
> а за вікном був гомін і пейзаж.
>
> Юрій Андрухович

Партію зіграно і тепер картярі мають добре перетасувати колоду, щоб розпочати наступну. Що означає "добре перетасувати колоду"? Після завершення партії гравці мають доволі багато інформації про розташування карт в колоді: вони можуть пам'ятати останню карту, в деяких іграх колоду можна розділити на пари сусідніх карт однієї масті, а у випадку виграшу в пасьянс карти будуть впорядковані по масті і номіналу. Отже, для старту нової партії потрібно позбутися цієї інформації. Можна було б сказати, що після перетасування карти мають йти у деякому фіксованому "хаотичному" порядку. Але тоді той, хто цей фіксований "хаотичний" порядок знає, мав би серйозну перевагу, що неприпустимо. Тож після перетасування ми маємо досягти ситуації, за якої *всі можливі впорядкування карт є рівноймовірними* — хоч би таке впорядкування було "хаотичним"чи "не хаотичним"в наївному розумінні. Зрозуміло, що ніщо не гарантує нам досягнення такої ситуації. Тож потрібно перетасувати карти, щоб так було *наближено.*

Необхідно також визначитись із процесом тасування. Для простоти вважатимемо, що під час кожного кроку ми навмання обираємо карту з колоди незалежно від попередніх виборів і перекладаємо її нагору. Таку дію ми називатимемо *перетасуванням.*

Нехай E — деяка множина, а $\mathscr{P}$ клас всіх її підмножин. *Мірою* на E називається функція $\mu : \mathscr{P} \to \mathbb{R}$, для якої виконується $\mu(\emptyset) = 0$ і для довільних неперетинних підмножин A і B

$$\mu(A \cup B) = \mu(A) + \mu(B).$$

Це не є цілком коректним означенням міри. Зокрема, на деяких складних множинах неможливо визначити бажану міру на класі всіх підмножин, тож необхідно обмежитись деяким вужчим класом. Однак нам такого означення вистачатиме. Так чи інакше, це означення відображає ідею процесу вимірювання: кожній підмножині деякої множини ми ставимо у відповідність певну вагу так, щоби виконувався ряд природніх правил — вага порожньої множини була нульовою, а вага об'єднання двох неперетинних множин дорівнювала сумі ваг цих двох множин. Нехай тепер E буде скінченною, тобто $E = \{e_1, \ldots, e_k\}$. Через $|E|$ позначатимемо кількість елементів в E, тобто тут $|E| = k$. В цьому випадку кожна міра μ на E ототожнюється з $(\mu(\{e_1\}), \dots, \mu(\{e_k\}))$ — вектором, складеним з мір кожного з елементів E. Справді, для довільного $A \subset E$

$$\mu(A) = \sum_{e \in A} \mu(\{e\}).$$

Надалі для позначення міри одного елементу замість $\mu(\{e\})$ вживатимемо $\mu(e)$, хоча такий запис не є цілком коректним. В нашому випадку E буде множиною всіх $n!$ впорядкувань колоди з n карт. На цьому етапі потрібно розуміти, що на E можна визначити багато різних мір, більше того, кожен вектор з $|E|$ чисел визначає свою міру. Отже можна говорити про множину всіх мір на E як про певний об'єкт.

Нехай X — випадкова величина зі значеннями в E. Формально кажучи, X є функцією, що визначена на ймовірнісному просторі (Ω, P) і діє в E. В нашому випадку Ω можна уявляти як множину варіантів "вибору навмання" карти, яку ми перекладаємо нагору. Зауважимо, що в такому разі кожне $\omega \in \Omega$ складається з компонент, кожна з яких відповідає вибору карти на кожному кроці, тобто $\omega = (i_1, \dots, i_m, \dots)$, де i_j номер обраної карти на кроці j. Інакше кажучи, ми вибираємо все майбутнє відразу. Насправді, Ω слід розуміти лише як генератор випадковості, все найцікавіше відбуватиметься на множині E.

Розподілом X на E називається така міра X_*, визначена на E, що для довільного вимірного $B \subset E$

$$X_*(B) = P(\{\omega : X(\omega) \in B\}).$$

Ця міра відповідає вектору

$$(P(X = e_1), \dots, P(X = e_k))$$

Зауважимо, що вона є *ймовірнісною*, тобто що $X_*(E) = 1$. Справді,

$$P(\{\omega : X(\omega) \in E\}) = P(\Omega) = 1$$

.

Відтак, для кожного натурального m визначимо випадкову величину X_m зі значеннями в E — впорядкування карт в колоді після здійснення m перетасувань. Процес перетасування буде успішним, якщо вектор $(P(X_m = e_1), \dots, P(X_m = e_k))$ з плином часу (тобто зі збільшенням m) буде наближатися до $(1/(n!), \dots, 1/(n!))$, тобто якщо розподіл X_{m*} наближатиметься до рівномірної міри на E.

Отже, нам потрібно надати сенс слову "наближатися" тобто вміти вимірювати *відстань* між двома мірами на E. Зрозуміло, що визначати відстань можна по-різному. Важливим поняттям, що виникає в різних частинах прикладної математики, є відстань *Кульбака-Лейблера.* Відстані *Гелінджера* та *хі-квадрат* виявляються зручними в деяких задачах статистики. Ми ж в подальшому будемо розглядати, можливо, найприроднішу відстань — *відстань повної варіації* (total variation distance), що визначається за формулою

$$d_{TV}(\mu, \nu) = \frac{1}{2} \sum_{e \in E} |\mu(e) - \nu(e)| \, .$$

Тут для того, щоб міра μ була близькою до міри ν, ми вимагаємо, щоб для кожного елементу e його μ-міра була близькою до його ν-міри. Зокрема, колода з n карт буде добре перемішаною, якщо відстань d_{TV} між *реальним* розподілом і *ідеальним* — коли всі $n!$ порядків розташування карт в колоді рівноймовірні — є малою.

Нагадаємо також, що таке математичне сподівання $\mathbb{E}(X)$ та дисперсія $D(X)$ випадкової величини, що може набувати зліченну множину числових значень $\{a_1, \dots, a_n, \dots\}$. Перше з них показує "середнє" всіх можливих значень. Ми б могли порахувати просто їхнє середнє арифметичне, але щоб "врівноважити" всі значення, їх домножують на ймовірність, з якою вони можуть прийматись. Виводимо строгу формулу: $\mathbb{E}(X) = \sum_{n=1}^{\infty} a_n \cdot P(X = a_n)$. Дисперсія ж описує наскільки допустимі значення відхилені від математичного сподівання, тобто математичне сподівання самих відхилень. Щоб відхилення в один бік не компенсували відхилення в інший бік, беруть математичне сподівання квадратів відхилень: $D(X) = \mathbb{E}(X - \mathbb{E}(X))^2$. Для довільних випадкових величин X, Y математичне сподівання є лінійним:

$$\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y),$$

а якщо X, Y незалежні, то дисперсія теж:

$$D(X + Y) = D(X) + D(Y)$$

В цій статті ми переконаємося, що наш процес справді "добре перемішує карти" а також спробуємо дослідити скільки кроків необхідно зробити, щоб колода була "добре перетасованою" в залежності від кількості карт.

1 Ланцюги Маркова

Теорія ланцюгів Маркова є головним інструментом в розв'язанні цієї задачі.

Розглянемо ситуацію на кроці m. Карти розташовані в деякому порядку e. Далі ми обираємо навмання карту і потрапляємо в деяке впорядкування e'. Що важливо: ймовірність потрапити з впорядкування e у впорядкування e' не залежить ні від моменту m, ні від історії перетасування до моменту m, а залежить тільки від станів e і e'.

В цьому розділі позначення E, Ω, P, $(X_m)_{m=0}^{\infty}$ ми будемо використовувати в найширшому значенні, тобто E — довільна скінчена множина, (Ω, P) — вимірний простір, $(X_m)_{m=0}^{\infty}$ — послідовність випадкових величин зі значеннями в E. Але E, Ω, $(X_m)_{m=0}^{\infty}$ з задачі про перетасування карт, яку ми розглянемо потім, треба тримати в голові в якості найпершого прикладу.

Означення 1. *Послідовність $(X_m)_{m=0}^{\infty}$ випадкових величин зі значеннями в E називається ланцюгом Маркова (або процесом Маркова) на множині станів E, якщо задовольняє умову:*

$$P\{X_m = e_m | X_{m-1} = e_{m-1}, \ldots, X_0 = e_0\} = \\ = P\{X_m = e_m | X_{m-1} = e_{m-1}\} = Q(e_{m-1}, e_m),$$

якщо

$$P(X_{m-1} = e_{m-1}, \ldots, X_1 = e_1) > 0$$

Через $Q(e_{m-1}, e_m)$ позначено ймовірність переходу зі стану e_{m-1} в e_m. Набір чисел $Q(e, e')$ формує матрицю Q розміру $|E| \times |E|$, яку називають матрицею переходу.

Іншими словами, в Марківському процесі є кілька станів, в яких ми можемо бути. Спочатку ми перебуваємо в деякому положенні $X_0 = e_0$ (можливо — випадковому), а потім на кожному кроці з певною ймовірністю переходимо зі стану в стан. Ймовірність $Q(e, e')$ перейти зі стану e в стан e' залежить лише від e і e'. Для передбачення майбутнього X_{m+1} вся історія $(X_0, \ldots, X_m)$ не дає більше інформації, ніж X_m.

Всю інформацію про ланцюг Маркова відображено в матриці переходу Q. Справді, неважко переконатися, що

$$P(X_m = e_m, X_{m-1} = e_{m-1}, \ldots, X_0 = e_0) = \\ = P(X_0 = e_0) Q(e_0, e_1) \ldots Q(e_{m-1}, e_m).$$

Бачимо, що динаміка ланцюга повністю визначається початковим розподілом — тобто мірою X_{0*} — і матрицею переходу Q.

Насамкінець, використовуючи означення, неважко переконатися, що для довільного $e \in E$

$$\sum_{e' \in E} Q(e, e') = 1.$$

Це відображає не несподівану властивість ланцюгів Маркова, що з положення e ми повинні перейти в якесь інше положення обов'язково всередині E. Насправді, цієї умови в якомусь сенсі достатньо: якщо задано матрицю невід'ємних чисел Q розміру $|E| \times |E|$, для якої виконується умова вище, то можна побудувати ймовірнісний простір Ω і послідовність випадкових величин $X_0, \ldots X_m, \ldots$ зі значеннями в E такі, що $(X_m)_{m=0}^{\infty}$ є ланцюгом Маркова з матрицею переходу Q.

Уявімо собі ланцюг Маркова $X_0, \ldots, X_n, \ldots$ з матрицею переходу Q, що визначається так:

$$Q(e, e') = \begin{cases} 1 \text{ якщо } e = e' \\ 0 \text{ інакше.} \end{cases}$$

Тут кожен зі станів є, так би мовити, стаціонарним. Це означає, що якщо ми починаємо зі стану e, то не зможемо з нього вийти і будемо в ньому завжди. Отже, всередині E можна взяти підмножину — $\{e\}$ для якого-небудь $e \in E$ — яка є своєрідним ланцюгом Маркова з одним станом, в якому ми є завжди. В свою чергу цей "малий" ланцюг Маркова є в певному сенсі "мінімальним", що означає, що в ньому не можна знайти менший ланцюг, який би був замкненою системою. Зрозуміло, що будь-який ланцюг з $|E| = 1$ є "мінімальним", бо в ньому надто мало елементів. Як формально описати "мінімальні" ланцюги з $|E| > 1$? Для цього нам потрібно наступне означення. Спочатку не є цілком зрозумілим яким чином воно стосується цього неформального пояснення, однак наступна після означення теорема має його розтлумачити.

Означення 2. *Марківський ланцюг, в якому, починаючи з будь-якого стану, можна з ненульовою ймовірністю досягти будь-який інший стан за скінченну кількість кроків, називається незвідним.*

Теорема 1. *Нехай E скінченна і $X_0, X_1, \ldots$ — незвідний ланцюг Маркова на E. Тоді для довільного $e \in E$*

$$P(\textit{існує безліч } m \textit{ для яких } X_m = e) = 1.$$

Ідея доведення. Оскільки E — скінченне, можна довести, що знайдеться хоча б один потрібний стан, тобто таке $s \in E$, що

$$P(\text{існує безліч } m \text{ для яких } X_n = s) = 1.$$

Це є посиленням того очевидного факту, що для кожної окремої траекторії (що відповідає певному $\omega \in \Omega$) буде існувати стан, через який ланцюг проходитиме безліч разів. Тепер, ми маємо позитивні шанси p потрапити з стану s в довільний інший стан $e \in E$, оскільки ланцюг незвідний. Але тоді, якщо не існуватиме безлічі моментів часу m, за яких $X_m = e$, то з якогось моменту, кожного разу проходячи через s, ми повинні уникати e, що відбувається з ймовірністю $1 - p$. Але це є неможливим. □

Зауважимо, що хоч з ймовірністю 1 ми матимемо безліч m для яких $X_m = e$, не є правильним те, що для кожного $\omega \in \Omega$

траєкторія ланцюга проходитиме через e безліч разів. Просто множина таких поганих ω є дуже малою. Якщо $P(A) = 1$ для деякої події A, то кажуть, що подія A виконується *майже напевно*.

Тепер розглянемо інший ланцюг Маркова. Уявімо собі шахівницю і короля, що випадковим чином блукає на ній — тобто на кожному кроці переходить на випадковим чином обране сусіднє по стороні поле. Блукання короля є ланцюгом Маркова на множині E, що складається з 64 клітинок шахівниці. Оскільки після кожного кроку колір поля, на якому стоїть король, змінюється на протилежний, в своє початкове поле король зможе повернутися тільки на парному кроці. Інакше кажучи, $P(X_{2m+1} = X_0) = 0$. Отже, динаміка цього ланцюга Маркова, попри свою непередбачуваність, має структурне правило: король може повертатися в початкове положення тільки на парних кроках. Ланцюги, які подібного структурного правила не мають, називаються *аперіодичними*.

Означення 3. *Стан e ланцюга Маркова називають аперіодичним, якщо*

$$\text{НСД}(n : P\{X_n = e|X_0 = e\} > 0) = 1.$$

Якщо всі стани ланцюга є аперіодичними, то такий ланцюг називається аперіодичним.

У прикладі з шахівницею і королем можемо бачити, що жоден зі станів не є аперіодичним, точніше, для кожного поля e

$$\text{НСД}(n : P\{X_n = e|X_0 = e\} > 0) = 2.$$

Означення 4. *Міра μ на E, що відповідає вектору $(\mu(e_1), \dots, \mu(e_{|E|}))$, де $\sum_{i=1}^{|E|} \mu(e_i) = 1$ називається стаціонарним розподілом ланцюга Маркова, якщо для довільного $e \in E\, \forall j = \overline{1, N}$*

$$\mu(e) = \sum_{e' \in E} \mu(e') Q(e', e)$$

Це нове означення потрібно прокоментувати. Припустимо, що $X_{0*} = \mu$ є стаціонарним розподілом. Тоді з формули в означенні випливає, що $X_{m*} = \mu$ для довільного $m \geq 0$. Справді, якщо $X_{m-1*} = \mu$, то для кожного $e \in E$

$$P(X_m = e) = \sum_{e' \in E} P(X_m = e, X_{m-1} = e') =$$
$$= \sum_{e' \in E} P(X_{m-1} = e') Q(e', e) = \mu(e)$$

Отже це така міра, починаючи з якої, ми завжди "в ній" і залишатимемось.

Теорема 2. *Кожний незвідний і аперіодичний марківський ланцюг має рівно один стаціонарний розподіл μ. Яким би не був розподіл X_0 (тобто якою б не була міра X_{0*}) X_{m*} збігатиметься до цього стаціонарного розподілу при $m \to +\infty$, тобто*

$$d_{TV}(X_{m*}, \mu) \to 0, \;\; m \to +\infty.$$

Ідея доведення. Ми покажемо тільки другу частину — про збіжність. Розглянемо ще один ланцюг Маркова $(\widetilde{X}_m)_{m=0}^{\infty}$. Він має таку ж матрицю переходу, що і $(X_m)_{m=0}^{\infty}$, але нехай X_{0*} буде стаціонарною мірою на E. Тепер розглянемо пару $(X_m, \widetilde{X}_m)_{m=0}^{\infty}$. Це є ланцюг Маркова на множині пар $(e, e') \in E \times E$ з матрицею переходу Q', що визначається за формулою:

$$Q'((e_1, e_1'), (e_2, e_2')) = Q(e_1, e_2) Q(e_1', e_2').$$

Тоді можна показати, що цей ланцюг, що діє на парах елементів з E, є незвідним, а тому з ймовірністю 1 ми побуваємо безліч разів в кожному зі станів, зокрема в (s, s) для якогось $s \in E$. Позначимо тоді $T = \min\{m \geq 0 : X_m = e, \widetilde{X}_m = e\}$. Тоді з ймовірністю 1 величина T є скінченною. T є прикладом *моменту зупинки*. Ми не будемо розглядати це поняття надто детально, потрібно лише розуміти, що T є випадковою величиною зі значеннями в $\{0\} \cup \mathbb{N} \cup \{+\infty\}$, тобто що T діє з Ω в $\{0\} \cup \mathbb{N} \cup \{+\infty\}$.

Тепер зафіксуємо m і нехай $T < m$. Це означає, що два ланцюги зустрілися до моменту m. Але тоді в них буде спільна динаміка з моменту T, тобто ймовірність потрапити в деякий стан e для X_m після зустрічі з $\widetilde{X_m}$ є такою ж, як і для $\widetilde{X_m}$! Тобто

$$P(X_m = e, T < m) = P(\widetilde{X_m} = e, T < m)$$

Отже,

$$\sum_{e \in E} |P(X_m = e) - \mu(e)| =$$

$$= \sum_{e \in E} |P(X_m = e) - P(\widetilde{X}_m = e)| =$$

$$= |P(X_m = e, T \geq m) - P(\widetilde{X}_m = e, T \geq m)|$$

$$\leq 2P(T \geq m) \to 0,$$

оскільки $P(T \geq m) \xrightarrow{m \to +\infty} 0$. Це завершує доведення.

Найважливішою ж ідеєю тут було розглядати $(\widetilde{X}_m)_{m=0}^{\infty}$. Ми повернемося до неї в останньому розділі. □

2 Тасування колоди з n карт

В цій частині ми будемо тасувати колоду з n карт, де n фіксоване.

Нехай E — множина всіх можливих впорядкувань колоди з n карт. Зрозуміло, $|E| = n!$. Через X_m позначатимемо (випадкове) упорядкування колоди після m кроків тасування.

Для простоти вважатимемо, що всі карти пронумеровані від 1 до n і в такому ж зростаючому (якщо дивитись згори вниз) порядку лежать в колоді перед початком тасування: 1 - зверху колоди, а n - знизу. Тобто початкове впорядкування є фіксованим і відомим, тобто X_0 невипадкове і дорівнює $(1, 2, \ldots, n)$ (для довільного $\omega \in \Omega$ $X_0(\omega) = (1, 2, \ldots, n)$).

На початку попереднього розділу ми зауважували, що ймовірність потрапити на кроці m з упорядкування e в інше впорядкування e' залежить тільки від e, e' і не залежить від моменту часу m і історії тасування до m. Тож $(X_m)_{m=0}^{\infty}$ є ланцюгом Маркова. Його матриця переходу Q визначається за формулою

$$Q(e, e') = \begin{cases} \frac{1}{n} \text{ якщо з } e \text{ можна потрапити в } e' \\ 0 \text{ інакше} \end{cases}$$

Справді, з положення e можна потрапити в рівно n інших: ми обираємо одну з n карт колоди і перекладаємо її нагору. Всі n отриманих впорядкувань будуть різними, хоча б тому, що всі вони матимуть різні карти нагорі. Оскільки карта обирається навмання, всі n впорядкувань будуть рівноймовірними.

Через μ позначимо рівномірний розподіл на E — наш бажаний розподіл, якого ми хочемо досягнути після поважної кількості перетасувань.

Наступний результат стверджує, що наш процес є справді ефективним — він добре перетасовує колоду.

Теорема 3. *Якщо кількість перемішувань прямує до нескінченності, то розподіл ймовірностей на множині всіх можливих перестановок прямує до рівномірного. Інакше кажучи,*

$$d_{TV}(\mu, X_{m*}) \xrightarrow{m \to +\infty} 0$$

Доведення. Уважний читач міг би помітити подібність цієї теореми до останньої теореми минулого розділу. Справді, щоб застосувати Теорему 2, нам потрібно тільки перевірити, що

1) ланцюг є незвідним;

2) ланцюг є аперіодичним;

3) рівномірний розподіл на E є стаціонарним.

Так загальні теоретичні результати допомагають в математичних моделях реальних процесів!

Аперіодичність випливає з того, що з кожного стану ми можемо потрапити в себе з ненульовою ймовірністю $\frac{1}{n}$ (коли ми випадковим чином вибрали саме верхню карту).

З будь-якого порядку колоди $(a_1, a_2, \dots a_n)$ ми можемо з ненульовою ймовірністю отримати будь-який $(b_1, b_2, \dots b_n)$, послідовно вибираючи карти $b_n, b_{n-1}, \dots b_1$ в початковому розміщенні і перекладаючи їх вгору. Тож ланцюг є незвідним.

Так як стаціонарний розподіл у кожного ланцюга єдиний, покажемо, що для нашого ланцюга таким є рівномірний розподіл μ. Для цього пригадаймо, що ймовірність кожного розміщення колоди при рівномірному розподілу рівна $\frac{1}{n!}$ і запишемо умову стаціонарності

$$\mu(e) = \sum_{e' \in E} \mu(e') Q(e', e).$$

Підставимо числа з нашої задачі:

$$\frac{1}{n!} = \sum_{e' \in E} \frac{1}{n!} Q(e', e).$$

Бачимо, що умова стаціонарності теж виконується.

Тож згідно до Теореми 2

$$\lim_{m \to +\infty} d_{TV}(X_{m*}, \mu) = 0.$$

□

3 Тасування колоди з нефіксованою кількістю карт

Отже дійсно, для нескінченної кількості перетасувань ми будемо прямувати до рівномірного розподілу. Ось лише постає питання — наскільки швидко це буде відбуватись?

Ми не можемо дати відповідь на питання про швидкість збіжності. Натомість ми сформулюємо своє питання інакше: скільки перетасувань *асимптотично* досить для того, щоби перетасувати колоду з n карт при $n \to +\infty$? А скільки — точно не вистачить? Відповідь на це питання дає наступна теорема, яка є головним результатом цього розділу.

Теорема 4. *Нехай μ — рівномірний розподіл на E, де E є множиною всіх впорядкувань колоди з n карт, де n — не фіксоване. Для довільного $\varepsilon > 0$ малого*

(i) якщо $m = (1 - \varepsilon) n \ln n$, то

$$d_{TV}(X_{m*}, \mu) \to 1, \quad n \to +\infty.$$

(ii) якщо $m = (1 + \varepsilon) n \ln n$, то

$$d_{TV}(X_{m*}, \mu) \to 0, \quad n \to +\infty.$$

Ця теорема є результатом з теорії часів перемішування ланцюгів Маркова (mixing time theory). Тут ми спостерігаємо дещо дивне явище. Інтуїція помилково підказує: карти мають перемішуватися поступово. Але для великого n колода буде дуже погано перетасованою до часу $0.99 n \log(n)$ і стає добре перетасованою після часу $1.01 n \log(n)$. Тобто в порівняно недовгий період відбуваються "найважливіші" перемішування.

Спочатку ми доведемо першу частину теореми, тобто що $(1 - \varepsilon) n \ln n$ перетасувань недостатньо.

Нехай $A_0 = \emptyset$. Позначимо через A_k множину всіх карт, що принаймі один раз знаходились зверху колоди від початку до часу k (вважаємо, що одна одиниця часу позначає одне перекладання карти). Інакше кажучи, множина A_k — це множина тих карт, які хоча би раз обиралися і перекладалися нагору під час перших k перетасовувань. Множини A_k формують зростаючу послідовність випадкових множин, тобто $A_0 \subset A_1 \subset A_2 \subset \ldots$

Позначимо

$$T_i = min\{k \geq 0, \text{що } |A_k| \geq i\}.$$

T_i є моментом часу k, коли кількість елементів множини A_k вперше дорівнює i. Зрозуміло, що в момент T_i ми маємо обрати і покласти нагору карту, яка до того не була згори колоди (за винятком, можливо, вихідного положення).

Лема 1. *Для довільної пари фіксованих ε та j ми маємо*

$$P(1-\varepsilon \leq \frac{T_{n-j}}{n \ln n} \leq 1+\varepsilon) \to 1, \quad n \to +\infty$$

Ця лема показує, що при великому n майже завжди випадкова величина T_{n-j} концентрується навколо числа $n \ln n$.

Щоб оцінити

$$P\left(\left|\frac{T_{n-j}}{n \ln n} - 1\right| \leq \varepsilon\right),$$

будемо застосовувати нерівність Чебишова, яка дає оцінку ймовірності відхилення випадкової величини від її середнього. Нехай $X : \Omega \to \mathbb{R}$. Тоді нерівність Чебишова стверджує, що для довільного $\varepsilon > 0$

$$P(|X - \mathbb{E}(X)| > \varepsilon) \leq \frac{D(X)}{\varepsilon^2}.$$

Доведення леми. Спочатку ми шукатимемо $\mathbb{E}(T_{n-j})$ і $D(T_{n-j})$. Для цього розглянемо випадкові величини $T_{i+1} - T_i$ для $0 \leq i \leq n-1$. Величина $T_{i+1} - T_i$ є часом очікування від моменту, коли i карт побували вгорі колоди, до моменту, коли множина A_k вперше містить $i+1$ елемент. Оскільки всі кроки перетасування відбуваються незалежно один від одного, величини $T_{i+1} - T_i$ для $0 \leq i \leq n-1$ є незалежними в сукупності. Тоді

$$D(T_{n-j}) = D\left(\sum_{i=0}^{n-j-1} T_{i+1} - T_i\right) = \sum_{i=0}^{n-j-1} D(T_{i+1} - T_i).$$

Для довільного k між T_i і $T_{i+1} - 1$ $|A_k| = i$, тобто $A_k = A_{T_i}$, а в момент T_{i+1} до A_{T_i} додається одна карта, тобто $|A_{T_{i+1}}| = i+1$. Відтак, на кожному кроці k при $T_i \leq k \leq T_{i+1} - 1$ карту для перекладання нагору ми обирали з множини $A_k = A_{A_{T_i}}$. На кожному кроці ймовірність вибрати карту з множини A_{T_i} дорівнює i/n. В момент T_{i+1} ми обрали нову карту, це відбувається з імовірністю $(n-i)/n$. Отже, для довільного натурального l

$$P(T_{i+1} - T_i = l) = \left(\frac{i}{n}\right)^{l-1} \left(1 - \frac{i}{n}\right).$$

Маючи це, можна знайти математичне сподівання і дисперсію величини $T_{i+1} - T_i$:

$$\mathbb{E}(T_{i+1} - Ti) = \frac{n}{n-i}, \; D(T_{i+1} - T_i) = \frac{in}{(n-i)^2}.$$

Цей підрахунок залишимо читачеві. Насправді, $T_{i+1} - T_i$ має *геометричний розподіл* з параметром $(n-i)/n$. Докладну інформацію про геометричний розподіл можна знайти тут [**?**].

Відтак,

$$\mathbb{E}(T_{n-j}) = \sum_{i=0}^{n-j-1} \mathbb{E}[T_{i+1} - T_i] =$$

$$= n\sum_{i=0}^{n-j-1} \frac{1}{n-i} = n\left(\sum_{i=0}^{n} \frac{1}{i} - \sum_{i=0}^{j} \frac{1}{i}\right) =$$

$$= n\left(\sum_{i=0}^{n} \frac{1}{i}\right) - nC,$$

де $C = \sum_{i=0}^{j} \frac{1}{i}$ не залежить від n. Оцінимо суму гармонічного ряду $\sum_{i=0}^{n} \frac{1}{i}$. Згідно до [2]

$$\sum_{i=0}^{n} \frac{1}{i} - \ln n = f(n) \xrightarrow{n\to+\infty} \gamma,$$

де $\gamma = 0,577215...$ — стала Ейлера. Отож

$$\mathbb{E}(T_{n-j}) = n\ln n + n(f(n) - C).$$

Також

$$D(T_{n-j}) = \sum_{i=0}^{n-j-1} D(T_{i+1} - T_i) =$$

$$= \sum_{i=0}^{n-j-1} \frac{ni}{(n-i)^2} \leq n^2 \sum_{i=0}^{n-j-1} \frac{1}{(n-i)^2} \leq \frac{\pi^2}{6}n^2$$

Тут ми застосували інший факт з дійсного аналізу [3]:

$$\sum_{i=0}^{n-j-1} \frac{1}{(n-i)^2} \leq \sum_{i=0}^{+\infty} \frac{1}{i^2} = \frac{\pi^2}{6}.$$

Нарешті, застосуємо нерівність Чебишова для випадкової величини T_{n-j} і $\frac{\varepsilon}{2}n\ln n$:

$$P\left(\left|T_{n-j} - (n\ln n + n(f(n) - C))\right| > \frac{\varepsilon}{2}n\ln n\right)$$

$$\leq \frac{\frac{\pi^2}{6}n^2}{\frac{\varepsilon}{2}n\ln n}.$$

Звідси,

$$P\left(\left|\frac{T_{n-j}}{n\ln n} - (1 + \frac{f(n) - C}{\ln n})\right| > \frac{\varepsilon}{2}\right) \leq$$

$$\leq \frac{2\pi^2}{\varepsilon(\ln n)^2}.$$

Тоді для достатньо великих n

$$P\left(\left|\frac{T_{n-j}}{n\ln n} - 1)\right| > \varepsilon\right) \leq$$

$$\leq P\left(\left|\frac{T_{n-j}}{n\ln n} - 1 - \frac{f(n) - C}{\ln n}\right| > \varepsilon/2\right) \leq$$

$$\leq \frac{2\pi^2}{\varepsilon(\ln n)^2},$$

оскільки $\frac{f(n)-C}{\ln n} \xrightarrow{n\to+\infty} 0$. І нарешті з того, що $\frac{2\pi^2}{\varepsilon(\ln n)^2} \to 0$, випливає твердження леми. □

Тепер ми можемо довести першу частину Теореми 4.

Доведення першої частини Теореми 4. Нагадаємо, що карти пронумеровані від 1 до n і початково в такому порядку розташовані в колоді. Нехай $j > 0$ — довільне натуральне число. Позначимо через S_j сукупність всіх таких впорядкувань колоди, для яких карти що лежать на позиціях $n - j + 1, ..., n$ розташовані в порядку зростання, якщо дивитись згори. Тобто карта $n - j + 1$ має більший номер ніж $n - j + 2$-га карта в колоді, карта $n - j + 2$ має більший номер ніж $n - j + 3$-тя і так далі.

Неважко порахувати кількість таких впорядкувань: $|S_j| = (n!)/(j!)$. Тоді $\mu(S_j) = 1/(j!)$, оскільки μ — рівномірне.

З Леми 1 отримуємо, що з ймовірністю, що прямує до 1 при $n \to +\infty$

$$T_{n-j} \geq (1 - \varepsilon)n\ln n$$

Якщо карта ніколи не була "переставленою" то вона з часом опиниться в нижній частині колоди. Таким чином, якщо $T_{n-j} \geq k$, то на час k j нижніх карт колоди ніколи не піднімались вгору, тому не менше j нижніх карт колоди розташовані в зростаючому порядку, отже, $X_k \in S_j$ і $X_{k*}(S_j) \xrightarrow{n\to+\infty} 1$ для фіксованого j та $k = (1-\epsilon)n\log n$.

Таким чином $|\mu(S_j) - X_{k*}(S_j)| \geq 1 - \frac{2}{j!}$ для досить великих n. Тоді згідно до еквівалентного означення d_TV (див. Вправу 2) для всіх j справедливо $d_{TV}(X_{k*}, \mu) \geq 1 - \frac{2}{j!}$, що і завершує доведення.

□

А тепер доведемо другу частину Теореми 4.

Доведення другої частини Теореми 4. Додатково до нашої колоди розглянемо ще одну, яка вже є рівномірно перемішаною, тобто вона може бути впорядкована кожним способом з ймовірністю $1/n!$. В кожний момент часу, якщо картка з номером i в першій колоді переміщуватиметься нагору колоди, картку з номером i другої колоди будемо перекладати нагору другої колоди. Позначимо через $\widetilde{X}_k$ впорядкування другої колоди в час k. У кожен момент часу карта, що піднімається в першій колоді, вибирається рівномірно серед $\{1, 2, \ldots, n\}$, тому і карта, що переміщається нагору в другій колоді, обирається рівномірно з $\{1, 2, \ldots, n\}$. І тому $\widetilde{X}$ є ланцюгом Маркова з тією ж матрицею переходу, що і X. Отже в другій колоді також виконуватиметься те, що міра $\widetilde{X}_{k*}$ збігається до стаціонарної і саме рівномірний розподіл буде тут стаціонарним. Порівняйте запровадження нової колоди з ідеєю доведення Теореми 2!

Також для довільних двох карт виконується, що після моменту, коли обидві були вибрані принаймні один раз, їх відносне положення є однаковим в обох колодах (вище буде та карта, яку вибрали пізніше). Тому, як тільки всі карти були вибрані для перестановки принаймі по одному разу, всі відносні позиції для довільних карт i та j однакові, і тому ці дві колоди мають однакове впорядкування.

Таким чином, ми маємо $X_m = \widetilde{X}_m$, коли $m \geq T_n$. Але згідно до Леми 1 $T_n \leq (1+\varepsilon)n \ln n$ з ймовірністю, що прямує до 1. Тоді для $k = (1+\varepsilon)n \ln n$

$$P(X_k = \widetilde{X}_k) \geq P(T_n \leq (1+\varepsilon)n \ln n) \to 1.$$

Тоді довільного $A \subset E$ за рахунок рівномірності X_k маємо:

$$\begin{aligned} |X_{k*}(A) - \widetilde{X}_{k*}(A)| = |P(X_k \in A) - P(\widetilde{X}_k \in A)| \leq \\ \leq P(X_k \notin A, \widetilde{X}_k \in A) + P(X_k \in A, \widetilde{X}_k \notin A) \leq \\ \leq 2P(X_k \neq \widetilde{X}_k) \xrightarrow{n\to+\infty} 0. \end{aligned}$$

□

4 Вправи

Вправа 1. *Нехай E — скінченна множина, а μ, ν — дві міри на ній. Доведіть, що*

$$d_{TV}(\mu, \nu) = \max_{A \subset E} \mu(A) - \nu(A).$$

Вправа 2. *Нехай $(X_m)_{m=0}^{\infty}$ — ланцюг Маркова на скінченній множині E. Доведіть, що для кожного $m \geq 0$*

$$P(X_{m+2} = e''|X_m = e) = \sum_{e' \in E} Q(e, e')Q(e', e'').$$

Нехай Q^2 — квадрат матриці Q. Переконайтеся, що $X_0, X_2, X_4, \ldots$ — ланцюг Маркова з матрицею переходу Q^2.

Вправа 3. *Повернімося до випадкового блукання короля на шахівниці. Якою є матриця переходу цього ланцюга? Чи правда, що $d_{TV}(X_{m*}, \mu)$ прямує до 0, коли m прямує до нескінченності, якщо μ — рівномірна міра?*

Література

[1] М. В. Карташов *Імовірність, процеси, статистика*
Видавничо-поліграфічний центр 'Київський університет'. Київ, 2008.

[2] Вікіпедія. *Стала Ейлера-Маскероні*

[3] Вікіпедія. *Ряд обернених квадратів*

[4] Jean-François Le Gall *Intégration, Probabilités et Processus aléatoires*
https://www.math.u-psud.fr/~jflegall/IPPA2.pdf

[5] В. Н. Андреев, А. Я. Иоффе *Эти замечательные цепи*
М.: Знание, 1987. - 176 с.

[6] David A. Levin, Yuval Peres, Elizabeth L. Wilmer *Markov Chains and Mixing Times*
http://pages.uoregon.edu/dlevin/MARKOV/markovmixing.pdf