Экономия случайных битов для RP алгоритмов

$x \in L \Rightarrow \Pr_{z} [A(x, z) = 1] \geq \frac{1}{2}$

$x \notin L \Rightarrow \Pr_{z} (A(x,z) = 0) = 1$

Можно сгенерировать t раз строку z: $z_1, \ldots z_t$ и тем самым снизить вероятность ошибки до $\left(\frac{1}{2}\right)^t$. Тем самым будет использовано $t \cdot |z|$ случайных битов.

Возьмем простое $n \geq 2^{|z|}$.

Сгенерируем a, b из $\mathbb{Z}_n$.

Запуск $A(x,a)$, $A(x,b)$ дает ошибку с вер $\frac{1}{4}$.

положим $z_i = ai + b \quad \forall i = \overline{1, t}$.

запустим $A(x, z_i)$, z_i и z_j - попарно независимы $\Rightarrow$ $A(x,z_i)$ и $A(x,z_j)$ тоже.

Пусть $Y = \sum_i A(x, z_i)$

Если $x \in L$, то $E(Y) \geq \frac{t}{2}$, $D(Y) = \sum_i D(X_i) \leq \frac{t}{4}$

в виду попарной независимости.

$\Rightarrow \sigma_Y \leq \frac{\sqrt{t}}{2}$.

$\Pr_z[Y = 0] \leq \Pr_z [|Y - E(Y)| \geq \frac{t}{2}] =$

$= \Pr_z [|Y - E(Y)| \geq \sqrt{t} \cdot \frac{\sqrt{t}}{2}] \leq \frac{1}{(\sqrt{t})^2} = \frac{1}{t}$.

Т.е. вероятность ошибки $\leq \frac{1}{t}$.

Тем самым мы использовали всего $2 \log n$ ~~случайных~~ битов.

Stable Marriage Problem

n больниц и n врачей

Полный лист предпочтений у больниц и у врачей.

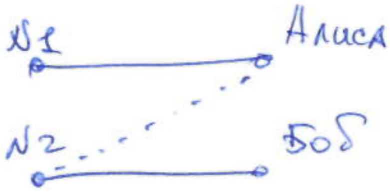
Вы знаете решение за $O(n^2)$.

Госпиталь предлагает работу наиболее необходимому ~~из свободных~~ из тех кому не предлагали врачу, врач соглашается если это лучшее место для него, чем его текущее.

Врач никогда не теряет работу получив её однажды.

1) ~~Врач~~ У больницы всегда есть выбор.

2) В итоге стабильный matching. Пр. пр.



Поликлиника №2 до того как предложить работу Бобу должна была предложить работу Алисе, но Алиса не согласилась или позже отказалась, значит её тек. место её устраивает больше чем поликлиника №2.

Алгоритм работает пропорционально числу предложений о работе. Оценим ~~время~~ мат. ожидание числа предложений в случае ~~вероятностных~~ случайного распределения преференций.

Отступление

Разложим 52 карты по 13 стопкам по 4 карты

Т, 2, 3, ... 10, В, Д, К.

Берём отсюда карту и смотрим на её ном на которое след стопки и т.д.

Описать все расположения когда дом. достигнуто очень сложно. ~~Давайте~~ их строить, пока достаём карты. Вероятность на ~~первом~~ первом ходе вытащить какую-то конкретную карту $\frac{1}{52}$.

на втором это $\frac{1}{51} \cdot \frac{51}{52} = \frac{1}{52}$.

на третьем это $\frac{1}{50} \cdot \frac{50}{51} \cdot \frac{51}{52} = \frac{1}{52}$.

Мы выигрываем если на последнем ходе вытащим короля $\Rightarrow$ вер. выигрыша $\frac{4}{52} = \frac{1}{13}$.

т.е. мы смогли легко решить задачу если ~~не знаем о расположении карт отложили на~~ благодаря тому что отложили решение о расположении карт.

Госпитали определяют свои предпочтения по ходу.
Выбор врачей сейчас слишком зафиксированным.
То есть везде. выбирают след предпочтение когда
в этом понадобится необх.
Давайте все уходили и будет след вдруг брать
след не из оставшихся, а у всех от этого
кол-во предложений только увеличится.

~~А это же~~ А теперь искомое число это ровно
количество времени необходимое для изменения всех
купонов, если они равновероятны.

Геометрическое распределение

Монетка: орел $- p$, решка $- 1-p=q$ ~~не включительно~~.
~~Сколько раз~~ Кол-во раз до первого орла ~~включительно~~ включительно

$$E(\xi) = p + 2qp + 3q^2p + \dots$$

$$E(\xi) = p + (1-p)(E(\xi)+1)$$

$$pE\xi = 1 \Rightarrow E\xi = \frac{1}{p}.$$

$$D\xi = E\xi^2 - (E\xi)^2 = E(\xi(\xi-1)) + E(\xi) - (E\xi)^2$$

$$\sum_1 k(k-1)p(1-p)^{k-1}$$

$$Var(\xi) = \frac{1-p}{p^2}$$

$$X = X_0 + X_1 + \dots + X_{n-1}$$

$$p_i = \frac{n-i}{n} \Rightarrow E(X) = \sum_i E(X_i) = \sum_{i=0}^{n-1} \frac{n}{n-i} = n\sum_{i=1}^{n} \frac{1}{i} = nH_n.$$

$$H_n = \ln n + \Theta(1).$$

$$\sigma_X^2 = \sum_{i=0}^{n-1} \sigma_{X_i}^2 = \sum \frac{ni}{(n-i)^2} = \sum \frac{n(n-i)}{i^2} =$$

$$= n^2 \sum_1 \frac{1}{i^2} - nH_n$$

$$\Rightarrow \quad \lim \frac{\sigma_X^2}{n^2} = \frac{\pi^2}{6}$$

$\mathcal{E}_i^R$ – i-купон не собран в первых R шагов.

$$P_2(\mathcal{E}_i^R) = \left(1 - \frac{1}{n}\right)^R \le e^{-\frac{R}{n}}$$

$R = \beta n \ln n$

$$P_2[X > 2] = P_2[\bigcup_i \mathcal{E}_i^R] \le \sum P_2[\mathcal{E}_i^R] \le$$

$$\le n^{-\beta} = n^{-(\beta-1)}.$$

Теорема Для константы $c \in \mathbb{R}$ для $m = n\ln n + cn$

$$\lim_{n\to\infty} \Pr[X > m] = 1 - e^{-e^{-c}}$$

Док-во: $X > m = \cup \mathcal{E}_i^m$

$$\Pr[\cup \mathcal{E}_i^m] = \sum (-1)^{k+1} P_k^n$$

$$P_k^n = \sum_{1 \le i_1 < \dots < i_k \le n} \Pr\left(\cap \mathcal{E}_{i_j}^m\right), \quad S_k^n = P_1^n - P_2^n + \dots (-1)^{k+1} P_k^n$$

Буль-Бонферрони:

$$S_{2k}^n \le \Pr[\cup \mathcal{E}_i^m] \le S_{2k+1}^n$$

$$P_k^n = \binom{n}{k} \Pr[\cap \mathcal{E}_i^m] = \binom{n}{k} \cdot \left(1 - \frac{k}{n}\right)^m \xrightarrow{\lim} \frac{e^{-ck}}{k!} = P_k$$

$$S_k = \sum (-1)^{j+1} P_j = \sum (-1)^{j+1} \frac{e^{-cj}}{j!} \to 1 - e^{-e^{-c}}$$

$$\lim P_k^n = P_k \Rightarrow \lim S_k^n = S_k$$

$$\lim S_k = 1 - e^{-e^{-c}} \Rightarrow \Pr[\cap \mathcal{E}_i^m] \to 1 - e^{-e^{-c}}.$$

$$\Rightarrow \lim_{n\to\infty} \Pr[X \geq n(\ln n + c)] = 1 - e^{-e^{-c}}.$$

Occupancy Problem

Во 1-ой корзине i шаров.

$$\binom{n}{i}\left(\frac{1}{n}\right)^{i}\left(1-\frac{1}{n}\right)^{n-i} \le \binom{n}{i}\left(\frac{1}{n}\right)^{i} \le \left(\frac{ne}{i}\right)^{i}\left(\frac{1}{n}\right)^{i} = \left(\frac{e}{i}\right)^{i}$$

$$\Pr[\mathcal{E}_1(k)] \le \sum_{i=k}^{n}\left(\frac{e}{i}\right)^{i} = \left(\frac{e}{k}\right)^{k}\left(1+\frac{e}{k}+\left(\frac{e}{k}\right)^{2}+\dots\right)$$

$$\Pr(\mathcal{E}_1(k^*)) \le \left(\frac{e}{k^*}\right)^{k^*}\frac{1}{1-e/k^*} \le \frac{1}{n^{-2}}$$

$$k^* = \frac{3\ln n}{\ln\ln n}$$

$$\cancel{\left(\frac{e\ln\ln n}{3\ln n}\right)^{\frac{3\ln n}{\ln\ln n}}}$$

$$\cancel{\left(\frac{e}{k^*}\right)^{k^*} = e^{\left(\ln\frac{e}{k^*}\right)k'} = e^{(\ln e-\ln k')k'} =}$$

$$\cancel{= e^{k' - (\ln 3\ln n - \ln\ln\ln n)\frac{3\ln n}{\ln\ln n}}}$$

$$\Pr\left[\cup\, \mathcal{E}_i(k^*)\right] \le \sum \Pr[\mathcal{E}_i(k^*)] \le \frac{1}{n}.$$

~~with~~ с вер $1-\frac{1}{n}$ нет корзины с более

$\frac{3\ln n}{\ln\ln n}$ шарами.