PKU-04833060
算法设计与分析『实验班』

第13讲 随机算法 (下)

罗国杰

gluo@pku.edu.cn

2024年春季学期

主要内容

- 泊松 （Poisson）试验
- 切诺夫（Chernoff）界
- 切诺夫（Chernoff）界的应用
  - 负载均衡算法分析
  - 排列路由问题

马尔可夫（Markov）不等式

- 令 X 为非负随机变量
- 且假设 $E[X]$ 存在
- 则对任意 $t > 0$，有 $P[X \geq t] \leq \frac{E[X]}{t}$

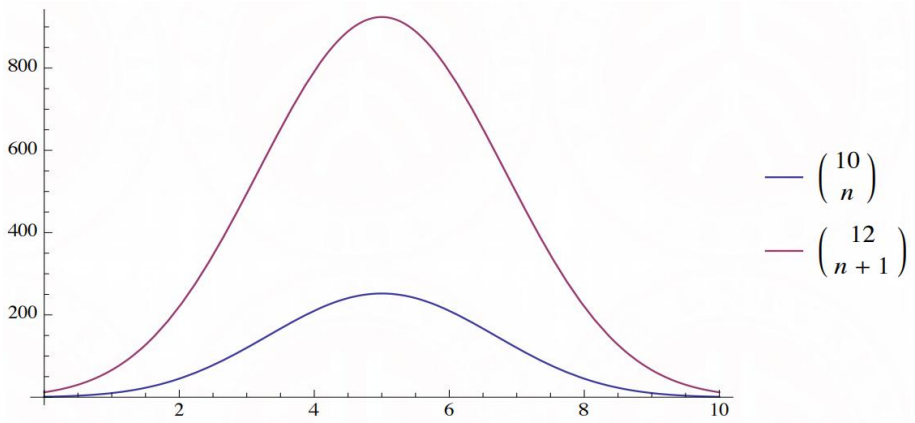
$$
\begin{aligned}
E(X) = \int_0^{\infty} x f(x) dx &= \int_0^{t} x f(x) dx + \int_t^{\infty} x f(x) dx \\
&\geq \int_t^{\infty} x f(x) dx \\
&\geq t \int_t^{\infty} f(x) dx \\
&= tP(X > t)
\end{aligned}
$$

独立伯努利（Bernoulli）试验

- 独立随机变量的和分布的尾概率的一般的界。
- 独立伯努利（Bernoulli）试验
  - 令$X_1, X_2, \ldots, X_n$是独立 Bernoulli 试验，即

$$\mathbf{Pr}[X_i = 1] = p \quad \wedge \quad \mathbf{Pr}[X_i = 0] = 1 - p, \qquad 1 \le i \le n$$

  - 令 $X = \sum_{i=1}^{n} X_i$
  - 则 X 称为具有二项分布。



泊松（Poisson）试验

- 泊松（Poisson）试验（更一般意义的独立随机试验）
  - 令$X_1, X_2, \ldots, X_n$是独立硬币投掷，即

$$\mathbf{Pr}[X_i = 1] = p_i \quad \wedge \quad \mathbf{Pr}[X_i = 0] = 1 - p_i, \qquad 1 \le i \le n$$

  - 称这样的硬币投掷为泊松（Poisson）试验，令

$$X = \sum_{i=1}^{n} X_i \text{，显然，} \mu = \mu_X = \sum_{i=1}^{n} p_i$$

  - 考察 X 偏离其期望 μ 的两个相关问题：

$$\mathbf{Pr}[X > (1+\delta)\mu] < ?$$

$$\mathbf{Pr}[X > (1+\delta)\mu] < \epsilon \Rightarrow \delta > ?$$

切诺夫（Chernoff）界

定理 1 令$X_1, \ldots, X_n$为独立 Poisson 试验，即对于$1 \le i \le n$，有$\Pr[X_i = 1] = p_i$，其中$0 < p_i < 1$。对于$X = \sum_{i=1}^{n} X_i$，$\mu = \mathrm{E}[X] = \sum_{i=1}^{n} p_i$，以及$\forall \delta > 0$，

$$\Pr[X > (1+\delta)\mu] < \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}$$

证明：对于任意的正实数t，

$$\Pr[X > (1+\delta)\mu] = \Pr\left[e^{tX} > e^{t(1+\delta)\mu}\right] < \frac{\mathrm{E}[e^{tX}]}{e^{t(1+\delta)\mu}}$$

注意：此不等式是严格的，因为$0 < p_i < 1$。

定理1 证明（续）

因为$\boldsymbol{X_i}$是独立的，所以$\boldsymbol{e^{tX_i}}$也彼此独立，于是

$$\mathbf{E}[e^{tX}] = \mathbf{E}\left[e^{t\left(\sum_{i=1}^{n} X_i\right)}\right] = \mathbf{E}\left[\prod_{i=1}^{n} e^{tX_i}\right] = \prod_{i=1}^{n} \mathbf{E}[e^{tX_i}]$$

考虑到

$$\mathbf{Pr}[e^{tX_i} = e^t] = \mathbf{Pr}[X_i = 1] = p_i$$

$$\mathbf{Pr}[e^{tX_i} = 1] = \mathbf{Pr}[X_i = 0] = 1\text{-}p_i$$

$$\mathbf{E}[e^{tX_i}] = e^t p_i + (1 - p_i) = (e^t - 1)p_i + 1$$

令$\boldsymbol{x = (e^t - 1)p_i}$，利用$\boldsymbol{1 + x < e^x}$，有

$$\mathbf{Pr}[X > (1+\delta)\mu] < \frac{\prod_{i=1}^{n} e^{(e^t-1)p_i}}{e^{t(1+\delta)\mu}} = \frac{e^{(e^t-1)\sum_{i=1}^{n} p_i}}{e^{t(1+\delta)\mu}} = \frac{e^{(e^t-1)\mu}}{e^{t(1+\delta)\mu}}$$

定理1 证明（续）

由于对于所有的$\boldsymbol{t>0}$，下式都成立

$$\mathbf{Pr}[\boldsymbol{X}>(\mathbf{1}+\boldsymbol{\delta})\boldsymbol{\mu}]<\frac{\boldsymbol{e}^{(e^t-1)\mu}}{\boldsymbol{e}^{t(1+\delta)\mu}}$$

对右式关于$\boldsymbol{t}$求导得

$$\left(\frac{\boldsymbol{e}^{(e^t-1)\mu}}{\boldsymbol{e}^{t(1+\delta)\mu}}\right)'=\left(\boldsymbol{e}^{\left((e^t-1)-t(1+\delta)\right)\mu}\right)'$$

$$=\left(\boldsymbol{e}^{\left((e^t-1)-t(1+\delta)\right)\mu}\right)\boldsymbol{\mu}\left(\boldsymbol{e}^t-(\mathbf{1}+\boldsymbol{\delta})\right)$$

令求导式等于 $\mathbf{0}$ 求得

$$\boldsymbol{e}^t-(\mathbf{1}+\boldsymbol{\delta})=\mathbf{0}\Rightarrow\boldsymbol{t}=\ln(\mathbf{1}+\boldsymbol{\delta})$$

时，求得最紧的界。

切诺夫（Chernoff）界

定理 2 令$X_1, \ldots, X_n$为独立 Poisson 试验，即对于$1 \le i \le n$，有$\Pr[X_i = 1] = p_i$，其中$0 < p_i < 1$。对于$X = \sum_{i=1}^{n} X_i$，$\mu = \mathrm{E}[X] = \sum_{i=1}^{n} p_i$，以及$\forall \delta, 0 < \delta \le 1$，

$$\Pr[X < (1-\delta)\mu] < \left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}\right)^{\mu} < e^{-\frac{\delta^2}{2}\mu}$$

定理2 证明

证明：对于任意的正实数$\boldsymbol{t}$,

$$\mathbf{Pr}[\boldsymbol{X} < (\mathbf{1}-\boldsymbol{\delta})\boldsymbol{\mu}] = \mathbf{Pr}\left[\boldsymbol{e}^{-\boldsymbol{tX}} > \boldsymbol{e}^{-\boldsymbol{t}(\mathbf{1}-\boldsymbol{\delta})\boldsymbol{\mu}}\right] < \frac{\mathbf{E}[\boldsymbol{e}^{-\boldsymbol{tX}}]}{\boldsymbol{e}^{-\boldsymbol{t}(\mathbf{1}-\boldsymbol{\delta})\boldsymbol{\mu}}} < \frac{\boldsymbol{e}^{(\boldsymbol{e}^{-\boldsymbol{t}}-\mathbf{1})\boldsymbol{u}}}{\boldsymbol{e}^{-\boldsymbol{t}(\mathbf{1}-\boldsymbol{\delta})\boldsymbol{\mu}}}$$

令$\boldsymbol{t} = \ln\left(\frac{\mathbf{1}}{\mathbf{1}-\boldsymbol{\delta}}\right)$，得

$$\mathbf{Pr}[\boldsymbol{X} < (\mathbf{1}-\boldsymbol{\delta})\boldsymbol{\mu}] < \left[\frac{\boldsymbol{e}^{-\boldsymbol{\delta}}}{(\mathbf{1}-\boldsymbol{\delta})^{(\mathbf{1}-\boldsymbol{\delta})}}\right]^{\boldsymbol{\mu}}$$

利用$\boldsymbol{\delta} \in (\mathbf{0}, \mathbf{1}]$,

$$(\mathbf{1}-\boldsymbol{\delta})^{(\mathbf{1}-\boldsymbol{\delta})} > \boldsymbol{e}^{-\boldsymbol{\delta}+\frac{\boldsymbol{\delta}^2}{\mathbf{2}}}$$

得到

$$\mathbf{Pr}[\boldsymbol{X} < (\mathbf{1}-\boldsymbol{\delta})\boldsymbol{\mu}] < \boldsymbol{e}^{-\frac{\boldsymbol{\mu}\boldsymbol{\delta}^2}{\mathbf{2}}}$$

切诺夫（Chernoff）界

定理 3 令$X_1, \ldots, X_n$为独立 Poisson 试验，即对于$1 \le i \le n$，有$\Pr[X_i = 1] = p_i$，其中$0 < p_i < 1$。对于$X = \sum_{i=1}^{n} X_i$，$\mu = \mathrm{E}[X] = \sum_{i=1}^{n} p_i$，以及$\forall c > 0$，

$$\Pr[|X - \mu| > c\mu] < 2e^{-\min\left\{\frac{c^2}{4}, \frac{c}{2}\right\}\mu}$$

定理3 证明

证明：当$\mathbf{1 \geq c > 0}$时，$\mathbf{Pr[X < (1-c)\mu] \leq e^{-\frac{c^2}{2}\mu}}$

当$\mathbf{c > 1}$时，$\mathbf{Pr[X < (1-c)\mu < 0] = 0 \leq e^{-\frac{c^2}{2}\mu}}$，于是

$$\mathbf{Pr[\mu - X > c\mu] = Pr[X < (1-c)\mu] \leq e^{-\frac{c^2}{2}\mu} \leq e^{-\frac{c^2}{4}\mu}}$$

} $Pr[\mu - X > c\mu]$

当$\mathbf{c \geq 2}$时，$\left[\frac{e^c}{(1+c)^{(1+c)}}\right]^{\mu} \leq e^{-\frac{c}{2}\mu}$

当$\mathbf{c \leq 2}$时，$\left[\frac{e^c}{(1+c)^{(1+c)}}\right]^{\mu} \leq e^{-\frac{c^2}{4}\mu}$

} $Pr[X - \mu > c\mu]$

$$\mathbf{Pr[|X-\mu| > c\mu]}$$
$$\mathbf{= Pr[\mu - X > c\mu] + Pr[X - \mu > c\mu]}$$
$$\mathbf{\leq 2e^{-\min\left\{\frac{c^2}{4},\frac{c}{2}\right\}\mu}}$$

Load Balancing

- Load balancing. System in which m jobs arrive in a stream and need to be processed immediately on n identical processors. Find an assignment that balances the workload across processors.
- Centralized controller. Assign jobs in round-robin manner. Each processor receives at most $\lceil m/n \rceil$ jobs.
- Decentralized controller. Assign jobs to processors uniformly at random. How likely is it that some processor is assigned “too many” jobs?

Load Balancing: Analysis (m=n)

- Let X_i = number of jobs assigned to processor i
- Let $Y_{ij} = 1$ if job j assigned to processor i, and 0 otherwise
- We have $E[Y_{ij}] = 1/n$
- Thus, $X_i = \sum_j Y_{ij}$, and $\mu = E[X_i] = 1$
- Applying Chernoff bounds with $\delta = c - 1$ yields $Pr[X_i > c] < e^{c-1}/c^c$
- Let $\gamma(n)$ be number x such that $x^x = n$, and choose $c = e\gamma(n)$

$$Pr[X_i > c] < e^{c-1}/c^c < (e/c)^c = (1/\gamma(n))^{e\gamma(n)} < (1/\gamma(n))^{2\gamma(n)} = 1/n^2$$

- Union bound ⇒ with probability ≥ 1-1/n no processor receives more than $e\gamma(n) = \Theta(\log n/\log\log n)$ jobs

Load Balancing: Many Jobs

- Theorem. Suppose the number of jobs $m = 16n\ln n$. Then on average, each of the n processors handles $\mu = 16\ln n$ jobs. With high probability, every processor will have between half and twice the average load.
- Proof.
  - Let X_i, Y_{ij} be as before.
  - Applying Chernoff bounds with δ = 1 yields
  - $Pr[X_i > 2\mu] < (e/4)^{16\ln n} < (1/e)^{\ln n} = 1/n^2$
  - $Pr[X_i < \frac{1}{2}\mu] < e^{-\frac{1}{2}(\frac{1}{2})^2 16\ln n} = 1/n^2$
  - Union bound ⇒ every processor has load between half and twice the average with probability ≥ 1-2/n

并行计算机的路由问题

- 考虑有 ***N*** 个处理器，标号从 **1** 到 ***N***， 并行处理器的网络抽象为一个图。
- 直接互联的处理器间可以直接通信；
- 不直接互联的处理器间的通信必须通过其他处理器转发。
- 假设每个处理器都可以在单个同步周期内向所有直接互联的处理器分别发送一个单位的消息。

- 考虑其中的排列路由问题
- 利用 **Chernoff** 界可证明：其随机算法比任何确定性算法都好

排列路由（Permutation Routing）问题

- 设开始时，每个处理器 i 均有一个消息包 v_i 将要发给处理器 $\pi(i)$。其中 $\pi(i)$（$1 \le i \le N$）构成 $\{1 \ldots N\}$ 的一个排列，即每个处理器恰好是一个消息包的目的地。
- 包的路由，即包从处理器 i 至处理器 $\pi(i)$ 所经过的节点或边的序列。
- 排列路由问题要为包确定一条路由。多个等待在同一条边上发送的消息包通过某种排队机制按顺序处理。

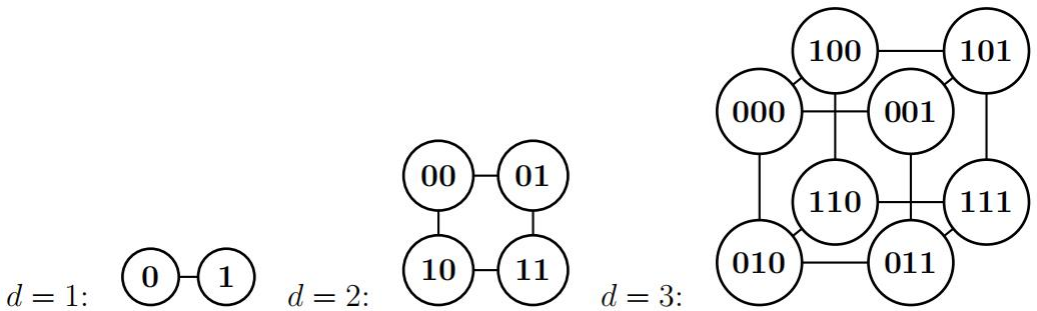
遗忘路由（Oblivous Routing）策略

- 遗忘路由：消息 v_i 采用的路由仅与它的目的地相关，而与其它任意消息的目的地无关。
  - [Val82] L. G. Valiant, “A Scheme for Fast Parallel Communication,” SIAM J. Comput., vol. 11, no. 2, pp. 350–361, May 1982.

- 定理：任意确定性遗忘排列路由算法，对于由出度为 $n = \log N$ 的 N 个结点构成的超立方体网络，总存在一个排列路由的实例至少需要 $\Omega(\sqrt{N}/n)$ 步
  - [KKT91] Christos Kaklamanis, Danny Krizanc, and Thanasis Tsantilas. Tight bounds for oblivious routing in the hypercube. Theory of Computing Systems, 24(1):223–232, 1991.

超立方体网络

- n 维超立方体网络有 $N=2^n$ 个结点
- 想象正方形（2维）或正方体（3维）的n维版本



超立方体网络

- 考虑一个布尔超立方体并行处理器网络 $G = (V, E)$：

$$V = \{i \in \mathbb{N} \mid 0 \le i < N, N = 2^n\}$$

设$(i_0, i_1, \dots, i_{n-1}) \in \{0, 1\}^n$为$i$的二进制表示，即

$$i = \sum_{k=0}^{n-1} i_k 2^k$$

$$E = \{(i, j) \mid \exists k, \forall t \neq k, i_t = j_t, i_k \neq j_k\}$$

边只存在于结点编号二进制表示仅有一位不同的结点间

超立方体网络的 Bit-Fixing 路由（一种遗忘路由）

- 从 i 发送消息 v_i 到结点 $\pi(i)$ 的路由算法为：
  - 从左到右扫描 $\pi(i)$ 的二进制位，与 v_i 当前所在结点 j 的地址比较
  - 找到当前地址与 $\pi(i)$ 不同的最左边的二进制位对应的边 $e(j, \pi(i))$
  - 从 $e(j, \pi(i))$ 将消息 v_i 转发出结点 j 。
- 若 i = 1011、$\pi(i)$ = (0000)，则 v_i 所经历的结点序列为：
  - 第1次转发 1011 → 0011 ： e(j=1011, π(i)=0000)
    第2次转发 0011 → 0001 ： e(j=0011, π(i)=0000)
    第3次转发 0001 → 0000 ： e(j=0001, π(i)=0000)
- 最坏情况步数的下界是 $\Omega(\sqrt{N}/n)$

（提示：对于 σ(ab)=ba 形式的排列，考虑 xx 形式结点的消息传递步数）

两阶段的随机遗忘路由算法

对于每条消息 v_i，独立的执行下面两个阶段。

- 阶段1：从 $\{1, \ldots, N\}$ 中随机选择中间目标 $\sigma(i)$，将 v_i 传输到结点 $\sigma(i)$。
- 阶段2：等待至第 $7n$ 步开始，将 v_i 从 $\sigma(i)$ 传输到目标结点 $\pi(i)$。

（阶段1和阶段2均采用 Bit-Fixing 路由算法）

（拥塞结点的排队规则：不同时相遇，先进先出；同时相遇，可以任意顺序转发）

定理：上述随机路由算法以至少 $1-(1/N)$ 的概率，使每个包在 $14n$ 或更少的步数内达到它的目标。

（两阶段是对称的，只需证明任一阶段大概率在 $7n$ 步内完成）

随机遗忘路由算法的运行时间分析

- 即分析每个 v_i 到达目的结点需要花费的步数。
- 先分析 v_i 在“阶段1”中的路由过程。
  所需步数由两部分构成：
  - 路线 ρ_i 的长度（至多为 n）；
  - 在路线 ρ_i 的中间结点排队（延迟）的步数（至多为 $|S_i|$，定义见下一页）。

阶段1中消息包的延迟

- 关于延迟上界的引理
  - 令消息 v_i 的路由路线为有向边的序列 $\rho_i = \{e_1, e_2, \ldots, e_k\}$ 。
  - 令 S_i 为除 v_i 外、经过 ρ_i 任意边的消息集合（即消息的路由路线至少经过 $\{e_1, e_2, \ldots, e_k\}$ 中的一个：$S_i = \{v_j \mid v_j \neq v_i \text{ and } \rho_j \cap \rho_i \neq \Phi\}$）。
  - 那么，消息 v_i 的延迟至多为 $|S_i|$ 。

- 证明：如果某时刻 v_j 导致 v_i 等待，v_i 给 v_j 发放一枚 token；如果某时刻 v_k ($k \neq i$) 导致带 token 的 v_j 等待，v_j 将 token 转移至 v_k。可证明 $|S_i|$ 的每条消息在任意时刻至多携带一枚 token，也即导致 v_i 等待的次数最多 $|S_i|$ 次。

关于延迟的期望 和 界

- 定义随机变量 H_{ij} $$H_{ij} = \begin{cases} 1 & \text{if } \rho_i \cap \rho_j \neq \Phi \\ 0 & \text{else} \end{cases}$$
- 则消息 v_i 的总延迟至多为 $$|S_i| \leq \sum_{j=1}^{N} H_{ij}$$
- H_{ij} ($i \neq j$) 是独立的 Poisson 试验，可以用 Chernoff 界估计
- 但首先考虑延迟的均值（或它的界） $$\mathbf{E}\left[\sum_{j=1}^{N} H_{ij}\right]$$

估计延迟期望的界

- 考虑随机变量 $T(e)$ 表示通过边 e 的路由线路的数目。
- 对于任意固定的路由线路 $\rho_i = \{e_1, e_2, \ldots, e_k\}$，有

$$\mathbf{E}\left[\sum_{j=1}^{N} H_{ij}\right] \leq \mathbf{E}\left[\sum_{l=1}^{k} T(e_l)\right] = \sum_{l=1}^{k} \mathbf{E}[T(e_l)]$$

- 由于超立方体的对称性：$\forall l, m, \mathbf{E}[T(e_l)] = \mathbf{E}[T(e_m)]$
- 路由线路 ρ_i 边数的期望为 n/2，总共 N 条路由线路，总共 N n 条有向边，每条边被通过的路由线路数目的期望：E[T(e)] = N * n/2 / (N n) = 1/2

延迟的 Chernoff 界

- 于是 $\mathbf{E}[T(e_l)] = \frac{1}{2} \Rightarrow \mathbf{E}\left[\sum_{j=1}^{N} H_{ij}\right] \leq \frac{k}{2} \leq \frac{n}{2}$
- 由定理1 可得：$\mathbf{Pr}[X \geq R] \leq 2^{-R}, \mathbf{for}\ R \geq 6E[X]$
  - 令 R = (1+δ) μ，

$$\begin{aligned}
\text{Prob}[X \geq (1+\delta)\cdot\mu] &\leq \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu} \\
&\leq \left(\frac{e}{1+\delta}\right)^{(1+\delta)\cdot\mu} \\
&\leq \left(\frac{e}{6}\right)^{R} \\
&\leq 2^{-R}.
\end{aligned}$$

延迟的 Chernoff 界

- 由 $\mathbf{Pr}[X \geq R] \leq 2^{-R}, \mathbf{for}\ R \geq 6E[X]$
  - 可证明单条消息延迟超过 $6n$ 的概率小于等于 2^{-6n}
  - 存在消息延迟超过 6n 的概率小于等于 $N \times 2^{-6n} = 2^n \times 2^{-6n} = 2^{-5n}$
- 定理：在阶段1中，以至少 $1-2^{-5n}$ 的概率，每个包在 $7n$ 或更少的步数内达到它的中间目标。
  - 步数 = 路由长度 + 延迟 超过 n + 6n = 7n 的概率小于 2^{-5n}
- 定理：随机路由算法以至少 1-(1/N) 的概率，每个包在 $14n$ 或更少的步数内达到它的目标。
- 对比：确定性算法步数的下界是 $\Omega(\sqrt{N}/n)$

本讲小结

- 切诺夫（Chernoff）界用于评估偏离均值的概率。
- 只能适用于独立Poisson试验。
- 可以根据期望的概率评估可能的偏离值。
- 随机算法很多时候比确定性算法性质更好。

- 本节内容主要出自
  - “13.10 Load Balancing,” in J. Kleinberg and E. Tardos, Algorithm Design. Pearson Education, 2006.
  - “4.2 Routing in a Parallel Computer,” in R. Motwani, P. Raghavan, “Randomized Algorithms”, Cambridge University Press, 1995.