سوال ۱:

a) مسئله‌ی gamblers' ruin مربوط به یک قمارباز است. فرض کنید پول قمارباز m باشد. این قمارباز شرط‌بندی‌های متوالی انجام می‌دهد.

قمارباز در هر شرط ← با احتمال q پیروز می‌گردد و ۱ امتیاز دریافت می‌کند. / با احتمال $p=1-q$ شکست می‌خورد و ۱ امتیاز از دست می‌دهد.

(امتیاز و پول یکی‌اند. ۱ امتیاز $\equiv$ ۱ پول)

حال اگر قمارباز تعداد پولش m شود ← پیروز می‌گردد و اگر پولش تمام شود، بازنده می‌شود. در این مثال به دنبال احتمال پیروزی قمارباز هستیم. (موفقیت با پول اولیه‌ی i)

$$prob(i) = q\,prob(i+1) + p\,prob(i-1)$$

$$p = 1-q \Rightarrow prob(i) = q\,prob(i) + p\,prob(i)$$

$$q\big(prob(i+1) - prob(i)\big) = p\big(prob(i) - prob(i-1)\big)$$

$$\Rightarrow prob(i+1) - prob(i) = \frac{p}{q}\big(prob(i) - prob(i-1)\big)$$

استقرایی

$$prob(i+1) - prob(i) = \underbrace{\left(\frac{p}{q}\right)\left(\frac{p}{q}\right)\cdots\left(\frac{p}{q}\right)}_{i\text{ بار}}\big(prob(1) - \overset{0}{prob(0)}\big)$$

$$= \left(\frac{p}{q}\right)^i prob(1)$$

یادآوری تلسکوپی: $prob(i+1) - prob(1) = prob(i+1) - \cancel{prob(i)} + \cancel{prob(i)} - \cancel{prob(i-1)} + \cdots - prob(1)$

$$= \left(\frac{p}{q}\right)^i prob(1) + \left(\frac{p}{q}\right)^{i-1} prob(1) + \cdots + \left(\frac{p}{q}\right) prob(1)$$

$$\begin{cases} = prob(1)\left(\dfrac{1-\left(\frac{p}{q}\right)^{i+1}}{1-\left(\frac{p}{q}\right)}\right) & \text{if (note } p \neq q) \quad \text{= تصاعد هندسی} \\ = prob(1)(i+1) & \text{if } p = q \quad \text{= تصاعد حسابی یا همان هندسی با قدر نسبت 1.} \end{cases}$$

Subject:
Date

از آنجا که هنگامی که به مبلغ N رسیدیم پیروز می‌شویم داریم $prob(N)=1$

consider $i+1=N$

$$prob(N)=\begin{cases} prob(1)\,\dfrac{1-(p/q)^N}{1-(p/q)} & p\neq q \\ prob(1)\,(N) & p=q \end{cases}$$

$$\Rightarrow prob(1)=\begin{cases} \dfrac{1-p/q}{1-(p/q)^N} & \text{if } p\neq q \\ 1/N & \text{if } p=q \end{cases}$$

$$\Rightarrow prob(i)=\begin{cases} \dfrac{\cancel{1-p/q}}{1-(p/q)^N}\times\dfrac{1-(p/q)^i}{\cancel{1-p/q}} & p\neq q \\ i/N & p=q \end{cases}$$

$$prob(i)=\begin{cases} \dfrac{1-(p/q)^i}{1-(p/q)^N} & p\neq q \\ i/N & p=q=1-p=1/2 \end{cases}$$

حال در صفحه بعد به بیان ارتباط این مسئله با بیت کوین می‌پردازیم.

بررسی ارتباط مسئله gambler & بیت کوین:

① gambler as adversary

consider: ② $q \rightarrow$ adversary's block mining possibility

③ $N = i + k$ متخاصم به اندازه‌ی k مرحله (پول) از Honest جلو بیوفتند؟

④ $i \rightsquigarrow \infty$ دارایی قمارباز (متخاصم) در شروع خیلی زیاد باشد.

$$P\left(\begin{array}{c}\text{پیشی گرفتن قمارباز (متخاصم)}\\ \text{به اندازه‌ی } k \text{ امتیاز (مرحله یا پول)}\\ \text{از اینست مطلق است}\end{array}\right) = \underset{\substack{i \to \infty \\ N = i+k}}{prob(i)} = \lim_{i \to \infty} \frac{1-(p/q)^{i}}{1-(p/q)^{i+k}}$$

⇓

(یعنی متخاصم k واحد عقب باشد و بخواهد از صادق، پیشی بگیرد.)

$$= \begin{cases} 1 & p<q \\ (q/p)^{k} & p>q \end{cases}$$

نسبت به صادق

اگر متخاصم احتمال پیروزی اش بیشتر باشد ⟸ احتمال پیشی گرفتن با فرض داشتن پول کافی قطعی است.

اگر " " کمتر باشد ⟸ " " با سرعت نمایی نسبت به k به صفر می‌گراید.

مشابه با بیت کوین ← اگر $\lambda_a > \lambda_h$ ← پیشی گرفتن با احتمال ۱ اتفاق می‌افتد (حالت ۱)

" " ← $\lambda_a < \lambda_h$ ← احتمال پیشی گرفتن به صورت نمایی با k افت می‌کند (حالت ۲)

b) ابتدا نود صادق، k بلوک منتظر می‌ماند، اگر در این هنگام متخاصم k' بلوک تولید کند نیاز است تا $k-k'$ بلوک دیگر از زنجیره‌ی (زنجیره‌ی) صادق‌ها جلو بیوفتد (پیشی بگیرد) لذا داریم: ←

k' دارای توزیع پواسون با میانگین λ است:

$$\lambda = k\left(\frac{q}{p}\right)$$

$$P(k\text{-depth error}) = \sum_{k'=0}^{\infty} \frac{\lambda^{k'} e^{-\lambda}}{k'!} = \begin{cases} \left(\frac{q}{p}\right)^{k-k'} & k' \leq k \\ 1 & k' > k \end{cases}$$

$$P(\text{error}) = 1 - \sum_{k'=0}^{k} \frac{\lambda^{k'} e^{-\lambda}}{k'!}\left(1 - \left(\frac{q}{p}\right)^{(k-k')}\right)$$

c) قطعاً این مدل کامل نیست مثلاً از جمله ایرادات آن می‌توان به موارد زیر اشاره کرد:

1. تأخیر شبکه در نظر گرفته نشده است.
2. امکان رخ داد natural fork در اثر وجود $\Delta \neq 0$ در شبکه واقعی
3. افت λ در صادق‌ها به علت رخ داد natural fork

و همانطور که ملاحظه می‌کنید موارد فوق در این مدل در نظر گرفته نشده است.

Subject:

Date

سوال ۲:

a) مهاجم در صورتی تغییر مسیر می‌دهد هنگام رسیدن به h_1 یا هیچ بلاکی تولید نکرده باشد یا ۱ بلاک تولید کرده باشد.

$$P_* = \int_0^\infty P\left(\text{مهاجم حداکثر ۱ بلاک در زمان } t \text{ تولید کرده باشد.}\right) P\left(\text{تولید کردن } h_1 \text{ به اندازه‌ی } t \text{ طول بکشد}\right) dt$$

$$= \int_0^\infty \Big(\underbrace{e^{-\lambda_a t}}_{\text{هیچ}} + \underbrace{e^{-\lambda_a t}\lambda_a t}_{\text{یک}}\Big)\left(\lambda_h e^{-\lambda_h t}\right) dt$$

$$= \lambda_a\lambda_h \underbrace{\int_0^\infty t e^{-\overbrace{(\lambda_a+\lambda_h)}^{\alpha}t} dt}_{\text{انتگرال معروف} \to \frac{1}{\alpha^2}} + \int_0^\infty \lambda_h \underbrace{e^{-\overbrace{(\lambda_a+\lambda_h)}^{\alpha}t} dt}_{\text{انتگرال معروف} \to \frac{1}{\alpha}}$$

$$= \frac{\lambda_a\lambda_h}{(\lambda_a+\lambda_h)^2} + \frac{\lambda_h}{(\lambda_a+\lambda_h)} = \frac{2\lambda_a\lambda_h + \lambda_h^2}{(\lambda_a+\lambda_h)^2} = 2\Big(\overbrace{\frac{\lambda_a}{\lambda_a+\lambda_h}}^{\rho}\Big)\Big(\overbrace{\frac{\lambda_h}{\lambda_a+\lambda_h}}^{1-\rho}\Big)$$

$$+ \underbrace{\left(\frac{\lambda_h}{\lambda_a+\lambda_h}\right)^2}_{(1-\rho)^2} = 2\rho(1-\rho) + (1-\rho)^2 = (1-\rho)(1+\rho)$$

$$= 1-\rho^2$$

$\rho < 0.5$ داریم $\Rightarrow \rho^2 < 0.25$

$$\Downarrow$$

$$P_* > 0.75 \quad //$$

بنابراین احتمال تغییر مسیر مهاجم در لحظه رسیدن به h_1 برابر حداقل 0.75 است ($= 1-\rho^2$)

حال می‌خواهیم عمق متخاصم را در هنگامی که به h_1 می‌رسد بگیریم:

$$\text{expected Depth} = \int_0^{\infty} E\left(\begin{matrix}\text{تعداد بلوک‌های}\\ \text{mine شده توسط}\\ \text{adversary}\end{matrix} \;\middle|\; \begin{matrix}h_1 \text{ در زمان } t\\ \text{اعلام شود}\end{matrix}\right) \cdot P\left(\begin{matrix}h_1 \text{ در زمان } t\\ \text{اعلام شود}\end{matrix}\right) dt$$

قانون احتمال کل

$$= \int_0^{\infty} (\lambda_a t)(\lambda_h e^{-\lambda_h t})\, dt$$

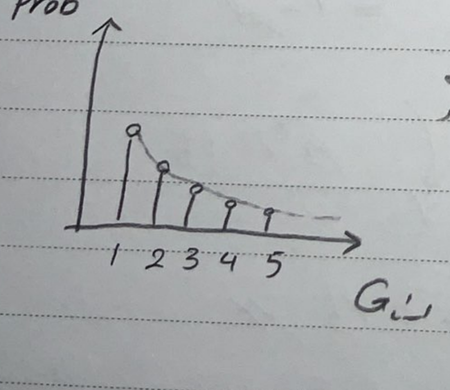
$$= \lambda_a \lambda_h \underbrace{\int_0^{\infty} t e^{-\overset{\alpha}{\lambda_h} t} dt}_{\text{انتگرال معروف} = \frac{1}{\alpha^2}} = \lambda_a \lambda_h \left(\frac{1}{\lambda_h^2}\right) = \frac{\lambda_a}{\lambda_h}$$

$$\frac{\lambda_a}{\lambda_h} < 1 \longleftarrow \text{چون داریم } \beta < 0.5$$

$$\beta = \frac{\lambda_a}{\lambda_a + \lambda_h} < 0.5$$

لذا داریم که میانگین تعداد بلوک‌های mine شده توسط متخاصم کمتر از ۱ است.

b) همانند مفاهیم درس و بحث‌های concentration inequality داریم که با افزایش i توزیع G_i به نمایی میل می‌کند و احتمال بزرگ شدن آن به صورت نمایی افت می‌کند.



توجه کنید که متخاصم هیچ وقت از chain اصلی عقب می‌افتد و در ارتفاع بزرگتر باید آن کار را می‌کند.

c) واقعاً داریم که اگر G_{i-1} برابر صفر باشد، این حمله با حمله‌ی private double spending یکسان خواهد بود اما اگر G_{i-1} مقداری مثبت باشد داریم که حمله‌کننده می‌تواند G_{i-1} عدد بلاک کمتر از حمله‌ی private double spend تولید کند و همچنان پیروز باشد و لذا احتمال موفقیت حمله افزایش می‌یابد.

همانطور که مشاهده کردیم احتمال ناصفر بودن G_{i-1} مثبت بوده و مهاجم می‌تواند از یک حلقه زودتری شروع به ساختن private chain حمله کند.

G_{i-1} احتمال ناصفر بودن $= \sum_{K=1}^{\infty} pr(G_{i-1} = K) > 0$

✓✓ بنابراین این حمله با احتمال بالا از حمله‌ی private double spending قدرتمندتر است.

سوال ۳)

a) می‌دانیم که تعداد بلاک‌های mine شده در بازه‌ی زمانی t از توزیع پواسون با میانگین λt پیروی می‌کند لذا داریم که فاصله‌ی زمانی بین دو بلاک از توزیع نمایی پیروی می‌کند.

تجمعی

می‌دانیم $F(t) = P($مدت زمان بین دو بلاک $> t)$

توزیع پواسون بدون حافظه memoryless است.

$\Rightarrow 1-F(t) = P($مدت زمان بین دو بلاک $> t) =$ no block during t $= e^{-\lambda t} \quad t \geq 0$

$\Rightarrow F(t) = 1 - e^{-\lambda t} \quad t \geq 0 \Rightarrow f(t) = \frac{d}{dt} F(t) = \lambda e^{-\lambda t} \quad t \geq 0$

چگالی توزیع

$$\begin{cases} \text{Expected} = \frac{1}{\lambda} \\ \text{Variance} = \frac{1}{\lambda^2} \end{cases}$$

✓✓ توزیع T (بازه‌ی زمانی بین تولید بلاک‌ها) یک توزیع نمایی خواهد بود.

$T = exp(\lambda)$

Subject:

Date

$\star$ $\begin{cases} \text{consider } T_i' \text{ as time interval for adversary blocks.} \\ \text{consider } T_i \text{ as time interal for honest blocks.} \end{cases}$

b) مثل مطالب درس داریم:

$$P(E_k) = P\left(\sum_{i=1}^{k} T_i > \sum_{i=1}^{k} T_i'\right)$$

// ضرب در $1/k$ تاثیری در علامت ندارد.

$$= P\left(\frac{1}{k}\sum_{i=1}^{k} T_i - \frac{1}{k}\sum_{i=1}^{k} T_i' > 0\right)$$

$$= P\Big(\underbrace{\frac{1}{k}\sum_{i=1}^{k} T_i}_{\approx 1/\lambda_h} - \underbrace{\frac{1}{k}\sum T_i'}_{\approx 1/\lambda_a} > 0\Big) \overset{k\to\infty}{=} P\left(\frac{1}{\lambda_h} - \frac{1}{\lambda_a} > 0\right)$$

$(k \to \infty)$ قانون اعداد بزرگ

$\approx 1/\lambda_h$

$(k \to \infty)$ قانون اعداد بزرگ

$\approx 1/\lambda_a$

if $\lambda_a > \lambda_h \Rightarrow P(E_k) \overset{k\to\infty}{=} 1$ ✓✓

if $\lambda_a < \lambda_h \Rightarrow P(E_k) \underset{k\to\infty}{=} 0$ ✓✓

c)

$$P(E_k) = P\left(\sum_{i=1}^{k}(T_i - T_i') > 0\right)$$

$$= P\left(e^{s\sum_{i=1}^{k}(T_i - T_i')} > 1\right) \quad s>0 \text{ داریم}$$

chernoff $\Rightarrow P(E_k) < \dfrac{E\left(e^{s\sum_{i=1}^{k} T_i - T_i'}\right)}{1}$

استقلال T_i ها و T_i' ها

$$\Rightarrow P(E_k) < E\left(e^{s\sum_{i=1}^{k} T_i}\right) E\left(e^{-s\sum_{i=1}^{k} T_i'}\right)$$

استقلال جزء T_i ها و

استقلال T_i' ها

$$\Rightarrow P(E_k) < \prod_{i=1}^{k} E\left(e^{sT_i}\right) E\left(e^{-sT_i'}\right)$$

$$\Rightarrow P(E_k) < \left[\left(\frac{\lambda_h}{\lambda_h - s}\right)\left(\frac{\lambda_a}{\lambda_a + s}\right)\right]^k = \left[\frac{\lambda_a \lambda_h}{(\lambda_h - s)(\lambda_a + s)}\right]^k$$

$= \dfrac{-\lambda_a}{-\lambda_a - s}$

PAPCO

(ادامه در صفحه بعد)

Subject:
Date

$$\Rightarrow p(E_k) \leq \left[\left(\frac{\lambda_h}{\lambda_h - s}\right)\left(\frac{\lambda_a}{\lambda_a + s}\right)\right]^k$$

$$\left(\text{consider } s = \frac{\lambda_h - \lambda_a}{2} \right) \Big\} \Rightarrow p(E_k) \leq \left[\frac{4\lambda_a \lambda_h}{(\lambda_a + \lambda_h)}\right]^k$$

$$\leq e^{-ck}$$

$$\text{simply } c \triangleq \ln \frac{(\lambda_a + \lambda_h)^2}{4\lambda_a \lambda_h}$$

(d

$$p(k\text{-depthError}) = p\left(\bigcup_{t=k}^{\infty} E_t\right) \leq \sum_{t=k}^{\infty} p(E_t) = \sum_{t=k}^{\infty} e^{-ct}$$

$$= \frac{e^{-ck}}{1 - e^{-ck}}$$

$$\Rightarrow p(k\text{-depthError}) = \frac{e^{-ck}}{1 - e^{-ck}}$$

سوال ۴)

(a

$$p(N_a > N_h) = \sum_{k=1}^{\infty} p(N_a = k)\, p(N_h < k) \qquad N_h = 0, 1, 2, \ldots, k-1$$

$$= \sum_{k=1}^{\infty} e^{-\lambda_a t} \frac{(\lambda_a t)^k}{k!} \sum_{i=0}^{k-1} e^{-\lambda_h t} \frac{(\lambda_h t)^i}{i!}$$

$$= \sum_{k=1}^{\infty} \sum_{i=0}^{k-1} e^{-(\lambda_a + \lambda_h)t} \frac{(\lambda_a t)^k (\lambda_h t)^i}{k!\, i!}$$

Subject:
Date

b) داریم $p(N_a > N_h) = p(N_a - N_h > 0) = p(e^{s(N_a - N_h)} > 1)$ (باید $s>0$)

در نظر بگیرید: $(s=1)$ ✓

$$\text{chernoff}: \; p(N_a > N_h) < \frac{E(e^{N_a - N_h})}{1}$$

استقلال

$$\Rightarrow p(N_a > N_h) < \frac{E(e^{N_a})}{E(e^{N_h})}$$

داریم:

$$N_a \sim poiss(\lambda_a t)$$
$$N_h \sim poiss(\lambda_h t)$$

(نکته: $E(e^{sX}) = M_X(s)$)

$$p(N_a < N_h) < \frac{E(e^{N_a})}{E(e^{N_h})} = \frac{M_{\lambda_a}(1)}{M_{\lambda_h}(1)} = \frac{e^{\lambda_a t(e-1)}}{e^{\lambda_h t(e-1)}}$$

به کمک نکته $M_\lambda(\gamma) = exp(\lambda(e^{\gamma} - 1))$

$$\Rightarrow p(N_a < N_h) < e^{\lambda_a t e - \lambda_a t - \lambda_h t e + \lambda_h t}$$

$$= e^{-(\lambda_h - \lambda_a)(e-1)t}$$

همانطور که مشاهده می‌کنید این احتمال به صورت نمایی با افزایش t کاهش می‌یابد.

(ادامه در صفحه بعد)

PAPCO

Subject:
Date

c) متوسط زمان طول می‌کشد تا بلوک iام پس از بلوک i-1ام، mine شود، T_i در نظر بگیرید.

$$\text{latency of } k\text{-depth} = \sum_{i=1}^{k} T_i$$

$$\Rightarrow \text{Expected (latency } k\text{-depth)} = E\left(\sum_{i=1}^{k} T_i\right) = \sum_{i=1}^{k} E(T_i) = \frac{k}{\lambda}$$

$$\underline{\underline{k\text{-depth}:}}\ p(\text{error}) < e^{-\ln\left(\frac{\lambda_a+\lambda_h}{4\lambda_a\lambda_h}\right)^2 \frac{\lambda_h t}{k}}$$

$$\underline{\underline{t\text{-confirm}:}}\ p(\text{error}) < e^{-(\lambda_h-\lambda_a)(e-1)t}$$

۱) احتمال خطا در confirm در هر دو روش با سرعت‌ها نسبت به t کاهش می‌یابد.

۲) نرخ افت خطا confirm در روش t-confirm ~~بیشتر~~ است. (ضریب نما بیشتر بوده است).

جمع‌بندی: نرخ افت روش t-con از روش k-depth بیشتر است ولی هر دو نمایی نزول می‌یابند.

سوال ۵:

a) سناریوی زیر را در نظر بگیرید:

leader یک microblock تولید می‌کند، و tx مربوط را درون آن قرار داده است، حال این را منتشر نمی‌کند و تلاش می‌کند تا keyblock بعدی را mine کند و تا ۱۰۰٪ fee را دریافت می‌کند. اما اگر قبل از اینکه keyblock بعدی را بسازد شخصی موفق گردید صبر می‌کند تا tx در micro ای قرار گیرد و سپس از ادامه‌ی آن شاخه، تولید keyblock می‌کند.

باید پارامترها را به طریقی تعیین کنیم که در آمدها کمتر شود: $\beta + (1-\beta)\beta(1-r_{leader}) < r_{leader}$

$$(r_{leader}=0.4) \Longleftrightarrow \beta + (1-\beta)\beta(0.6) < 0.4$$

$$\Rightarrow -0.6\beta^2 + 1.6\beta - 0.4 < 0 \Rightarrow \beta < 0.28$$

Subject:
Date

ادامه سوال ۵ : داریم که $\beta^* > 0.28$ و $\beta^* \approx 0.25$ و این مقدار نصف توان تهاجم در اجماع ناکاماتو

است یعنی توان تهاجم حدوداً حداکثر نصف توان (حداکثر) تهاجم (در حالتی که خودشان نزنند) می‌توانند باشند تا این

حمله صرفه نباشد.

b) باید پارامترها به میزانی باشند که درآمد به صورت (نسبی) $1-r_{leader}$ از T_H نسبت به متوسط

درآمد در سناریوی صورت سوال بیشتر باشد تا چنین کاری بکنند.

$$\underbrace{r_{leader}}_{\text{(درآمد leader)}} + \beta(1-r_{leader}) < 1-r_{leader}$$

$$\Downarrow \quad r_{leader} = 0.4$$

$$0.4 + \beta(0.6) < 0.6 \Rightarrow \beta < 1/3 .$$

همانطور که مشاهده می‌کنید، به دلیل نسبت به حملات نوع (b) مقاوم‌تر است تا حمله اول، چرا که در حمله دوم تا $1/3 \times$ توان کل = توان تهاجم را می‌تواند تحمل کند و همچنان خراب نشود

اما در حالت اول تا ۲۸٪ (33٪) توان کل شبکه = توان تهاجم را می‌تواند تحمل کند و در عین حال امن باشد.

Subject:
Date

سوال ۶:

a) بن جمله صادقی در رخ داد $D < \delta\lambda_c$ ، رخ داد زیر است:

$$\forall i \quad x_i \in \left(\mu - \frac{\delta\lambda_c}{2}, \mu + \frac{\delta\lambda_c}{2}\right) \equiv \forall i \; |x_i - \mu| < \frac{\delta\lambda_c}{2}$$

بیان دیگر

$\mu_i = E[x_i]$ ✓ $\quad$ (all x_i are iid $\Rightarrow \mu = \mu_i = E[x_i]$)

پس داریم: $P\left[\forall i \; |x_i - \mu_i| < \frac{\delta\lambda_c}{2}\right] \leq P[D < \delta\lambda_c]$

$\boxed{x_i \text{ها مستقل اند}}$

$$P\left[\forall i \; |x_i - \mu_i| < \frac{\delta\lambda_c}{2}\right] = \prod_{i=1}^{k} P\left[|x_i - \mu_i| < \frac{\delta\lambda_c}{2}\right]$$

$$\overset{\boxed{\text{iid بودن } x_i \text{ها}}}{=} \left(P\left[|x_i - \mu_i| < \frac{\delta\lambda_c}{2}\right]\right)^k$$

$$P\left[|x_i - \mu_i| < \frac{\delta\lambda_c}{2}\right] = 1 - \left\{P\left[x_i - \mu_i > \frac{\delta\lambda_c}{2}\right] + P\left[x_i - \mu_i < -\frac{\delta\lambda_c}{2}\right]\right\}$$

$$= 1 - \left\{P\left[x_i > \mu_i + \frac{\lambda_c\delta}{2}\right] + P\left[x_i < \mu_i - \frac{\delta\lambda_c}{2}\right]\right\}$$

$$= 1 - \left\{P\left[x_i > \mu_i\Big(1 + \underbrace{\frac{\lambda_c\delta}{2\mu_i}}_{A_i}\Big)\right] + P\left[x_i < \mu_i\Big(1 - \underbrace{\frac{\delta\lambda_c}{2\mu_i}}_{A_i}\Big)\right]\right\}$$

$$\underset{\text{نکات سوال}}{\geq} 1 - \left(e^{-\frac{A_i^2}{3}\mu_i} + e^{-\frac{A_i^2}{2}\mu_i}\right)$$

$$A_i = \frac{\delta\lambda_c}{2\mu_i} \longrightarrow P\left[|x_i - \mu_i| < \frac{\delta\lambda_c}{2}\right] \geq 1 - e^{-\frac{A_i^2}{3}\mu_i} - e^{-\frac{A_i^2}{2}\mu_i}$$

$$> 1 - 2e^{-A_i^2\mu_i/3}$$

(ادامه در صفحه بعد)

PAPCO

Subject:
Date

$$\left(A = A_i = \frac{\delta \lambda_c}{2\mu_i} \right)$$

داریم $P\left[\forall i : |X_i - \mu_i| < \frac{\delta\lambda_c}{2}\right] \geq \prod_{i=1}^{k}\left(1 - e^{-\frac{A_i^2}{3}\mu_i} - e^{-\frac{A_i^2}{2}\mu_i}\right)$

$$\geq \prod_{i=1}^{k}\left(1 - 2e^{-\frac{A_i^2}{3}\mu_i}\right) \overset{\text{iid بودن}}{=} \left(1 - 2e^{-\frac{A^2}{3}\mu}\right)^k$$

برنولی: $(1+u)^n \geq 1 + nu$, $|u| \leq 1$

(در هم: iid بودن X_iها)

$\left(\text{داریم } \mu_i = \mu_j,\ 1 \leq \forall i,j \leq k \right)$ $\geq \left(1 - 2ke^{-\frac{A^2}{3}\mu}\right)$

$$\Rightarrow Pr(D < \delta\lambda_c) \geq P\left[\forall i : |X_i - \mu| < \frac{\delta\lambda_c}{2}\right] \geq 1 - 2ke^{-\frac{A^2}{3}\mu}$$

$$\Rightarrow \left(P(D < \delta\lambda_c) \geq 1 - 2ke^{-\frac{A^2}{3}\mu} \qquad A = \frac{\delta\lambda_c}{2\mu} \right) \ *$$

b) اگر قرار بدهیم $\delta = \frac{\lambda a - 1}{2\lambda c}$ داریم:

$$A = \frac{\delta\lambda_c}{2\mu} = \frac{\lambda a - 1}{2\cancel{\lambda c}} \times \frac{\cancel{\lambda c}}{2\mu} = \frac{\lambda a - 1}{4\mu} \quad **$$

$\left(\delta\lambda c = \frac{\lambda a - 1}{2}\right)$

$$*, ** \Rightarrow P\left(D < \frac{\lambda a - 1}{2}\right) \geq 1 - 2k\exp\left(-\frac{(\lambda a - 1)^2}{3 \times 16\mu^{\cancel{2}}}\cancel{\mu}\right)$$

$$\Rightarrow P\left(D < \frac{\lambda a - 1}{2}\right) \geq 1 - 2ke^{-\frac{(\lambda a-1)^2}{48\mu}} = 1 - 2ke^{\frac{-(\lambda a - 1)^2}{48\mu}}$$

$$\Rightarrow \left(P\left(D < \frac{\lambda a - 1}{2}\right) \geq 1 - 2ke^{\frac{-(\lambda a-1)^2}{48\mu}} \right)$$

سود

که balancer ها $\leftarrow$ ذخیره است.

داریم که $P\left(D < \frac{\lambda a - 1}{2}\right)$ برابر است با احتمال کافی بودن توان متخاصم جهت balance نگه داشتن شبکه است.

در بالانس نگه داشتن شبکه

لذا داریم که برای احتمال موفقیت متخاصم یک کران پایین به دست آوردیم یعنی داریم :

*

احتمال موفقیت متخاصم در نگه داشتن balance زنجیره

$$> \underbrace{1-2k\, e}\,^{-\frac{1}{48}\frac{(\lambda_a-1)^2}{\mu}} = 1-2k\, e^{-\frac{1}{48}\frac{(\lambda_a-1)^2}{\lambda_c}}$$

$$\mu = E[x_i] = \lambda_c$$

احتمال خطای رخ داد پیشامد (*) به صورت نمایی با توان $-\frac{(\lambda_a-1)^2}{\lambda_c}$ است

کم می‌کند و به صفر میل کند.

لذا برای متوازن سازی زنجیره کافی است تا $(\lambda_a-1)^2$ در مقابل λ_c قابل توجه باشد و این یعنی λ_a در مقایسه با $\sqrt{\lambda_c}$ قابل توجه باشد لذا در اینجا کافی است جهت میل به هدف، λ_a را مقداری قابل توجه در مقابل $\sqrt{\lambda_c}$ در نظر بگیریم، لذا حکم قسمت b را ارضا کردیم.

Subject:
Date

سوال ۷ :

a: از لحظه $t=0$ اگر در هر زنجیره‌ای از voter ها بلاکی mine شود طبق پروتکل به این proposer رای خواهد داد.

می‌دانیم که تعداد بلاک‌های mine شده در بازه‌ی $t \approx$ توزیع پواسون : $\lambda = \frac{\lambda}{h}$

(λ = تعداد ... ۷۰٪ زنجیره‌ها، صادق بودن همه در prism)

می‌دانیم که احتمال اینکه هیچ بلاکی در بازه t mine نشود برابر است با $e^{-\lambda t}$

لذا احتمال mine شدن حداقل یک بلاک برابر است با: $1-e^{-\lambda t}$

لذا داریم که هر زنجیره از voter ها در بازه t با احتمال $1-e^{-\lambda t}$ به این proposal رای می‌دهند، حال اگر تعداد زنجیره‌ها (m) زیاد باشد داریم

$\underbrace{(1-e^{-\lambda t})}_{\text{کسر رای دهنده}} \times m$ عدد از زنجیره‌های voter به این proposal رای خواهند داد.

b)

$$(*) \quad P(\text{احتمال اینکه در یک زنجیره attack ایجاد شود تا } t) = e^{-\lambda t}\frac{(\lambda t)^{k+1}}{(k+1)!}$$

increasing m

$$E[\text{تعداد زنجیره‌هایی که نشانده در آن‌ها attack شده است}] = \underbrace{m}_{\text{تعداد زنجیره‌ها کل}} \times \frac{e^{-\lambda t}(\lambda t)^{k+1}}{(k+1)!}$$

Subject:
Date

برابر با نرخ عدم ثابت قدمی است
⟵ تعویض رأی

داریم q_k

c)

(حالا برسیم سر عمق k-depth ها)

$$H(t) = \sum_{k=0}^{\infty} \left(\underset{\text{با } k \text{ بار ثابت}}{\text{تعداد } k\text{-Deep}} \right) \times \underbrace{(1 - q_k)}_{\text{ثابت قدمی}}$$

تعداد رأی دهنده‌های k-deep و ثابت قدم در رأی

$$\overset{\text{part b}}{=} \sum_{k=0}^{\infty} \left(m \, \frac{e^{-\lambda_n t} (\lambda_n t)^{k+1}}{(k+1)!} \right) (1 - q_k)$$

✓✓

PAPCO