マルコフ限界 (Markov Bound) とチェルノフ限界 (Chernoff Bound) Part. 3

清家大嗣

2021 年 6 月 9 日

1　チェルノフ限界 (Markov bound) について (続 3)

その 2 において, 以下のような不等式を導出した (X は 0 か 1 の値を取る確率変数 X_k の総和). これをより見やすい不等式へと変形する.

$$\begin{cases} \Pr(X \geq (1+\delta)\mathrm{E}[X]) \leq \left(\dfrac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{\mathrm{E}[X]} = \exp\Big(\delta\mathrm{E}[X] - (1+\delta)\mathrm{E}[X]\log(1+\delta)\Big) \\ \Pr(X \geq (1-\delta)\mathrm{E}[X]) \leq \left(\dfrac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{\mathrm{E}[X]} = \exp\Big(-\delta\mathrm{E}[X] - (1-\delta)\mathrm{E}[X]\log(1-\delta)\Big) \end{cases} \tag{1}$$

その過程で, 次の 3 つの不等式を用いる (これらの不等式は微分を用いて, 増減を確認すれば簡単に証明できる).

$$\log(1+\delta) \geq \frac{\delta}{1+\delta/2} \qquad (0 \leq \delta) \tag{2}$$

$$\log(1-\delta) \geq \frac{-\delta}{\sqrt{1-\delta}} \qquad (0 \leq \delta < 1) \tag{3}$$

$$\sqrt{1-\delta} \leq 1 - \frac{\delta}{2} \qquad (0 \leq \delta < 1) \tag{4}$$

(2) 式を (1) の上の式に用いることで, 次のように不等式を拡張できる.

$$\begin{aligned} \Pr(X \geq (1+\delta)\mathrm{E}[X]) &\leq \exp\Big(\delta\mathrm{E}[X] - (1+\delta)\mathrm{E}[X]\cdot\log(1+\delta)\Big) \\ &\leq \exp\left(\delta\mathrm{E}[X] - (1+\delta)\mathrm{E}[X]\cdot\frac{\delta}{1+\delta/2}\right) \\ &\leq \exp\left(\delta\mathrm{E}[X] - (1+\delta)\mathrm{E}[X]\cdot\frac{\delta}{1+\delta/2}\right) \\ &= \exp\left(-\frac{\delta^2}{2+\delta}\mathrm{E}[X]\right) \end{aligned} \tag{5}$$

同様に (3), (4) 式を (1) の下の式に用いることで, 次のような不等式を得ることができる.

$$\begin{aligned} \Pr(X \geq (1-\delta)\mathrm{E}[X]) &\leq \exp\Big(-\delta\mathrm{E}[X] - (1-\delta)\mathrm{E}[X]\log(1-\delta)\Big) \\ &\leq \exp\left(-\delta\mathrm{E}[X] - (1-\delta)\mathrm{E}[X]\cdot\frac{-\delta}{\sqrt{1-\delta}}\right) \\ &\leq \exp\left(-\delta\mathrm{E}[X] + (1-\frac{\delta}{2})\cdot\delta\mathrm{E}[X]\right) \\ &= \exp\left(-\frac{\delta^2}{2}\mathrm{E}[X]\right) \end{aligned} \tag{6}$$

これらは, マイニングが成功した場合に確率変数 X_k が 1 となり, 失敗した場合に X_k が 0 となると考えれば, 十分に長い試行回数を行えば, その成功回数が期待値の周辺に高確率で収束していくことを意味する. つまり, 僅かでも攻撃者のノードより正統なノードが多ければ, いずれチェーンは正統なノードが伸ばしていくチェーンへと収束していく ([2] を参考).

参考文献

[1] Chernoff の不等式（Chernoff 限界）の導出, https://whyitsso.net/math/statistics/Chernoff_bound.html

[2] 鈴木涼一監修, ブロックチェーン 3.0 - 国内外特許からユースケースまで NTS