マルコフ限界 (Markov Bound) とチェルノフ限界 (Chernoff Bound) Part. 1

清家大嗣

2021 年 6 月 6 日

1　マルコフ限界 (Markov bound) について

与えられた正の確率変数 X に対して, 任意の正数 a が与えられた場合, 下の不等式が成立することをマルコフ限界は主張する.

$$\Pr(X \geq a) \leq \frac{\mathrm{E}[X]}{a} \tag{1}$$

上式の理解は, 確率変数の期待値が与えられる場合, その期待値よりも遥かに大きな値を確率変数が持つ確率は小さくなるということである. 証明は, 確率変数が a よりも大きな値を取る場合を全て $X = a$ とすることで, 期待値の下限を計算する. その値は $a \cdot \Pr(X \geq a)$ となり, (1) 式が導かれる.

2　チェルノフ限界 (Chernoff bound) について

マルコフ限界を用いることで, 指数関数の単調性を利用することで, 不等式に指数関数を含んだチェルノフの不等式を導出できる. 不等式の内部にマルコフの不等式が含まれていることに注意する.

$$\Pr(X \geq a) = \Pr(e^{tX} \geq e^{ta}) \geq \frac{\mathrm{E}[e^{tX}]}{e^{ta}} \tag{2}$$

また, 同様にして次式も導出できる.

$$\Pr(X \leq a) = \Pr(e^{-tX} \geq e^{-ta}) \geq \frac{\mathrm{E}[e^{-tX}]}{e^{-ta}} \tag{3}$$

その 2 において, チェルノフの不等式を変形したものについて説明する. その変形された不等式は, 共通プレフィックス定理 (Common-Prefix Theorem) といったブロックチェーンの安全性を示す定理の証明に用いられている.

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