1 Tail Bound

The tail of a random variable is the probability that the random variable exceeds some value

$$\mathbb{P}(X > \xi)$$

Tail bounds are important in providing guarantees on the probability of some bad outcome.

In cryptography, it is often necessary to estimate the probability of "bad events" in order to assess the power of an adversary and to place meaningful bounds on their capabilities. Many cryptographic constructions involve random processes, and it is crucial to have effective tools to bound this randomness. In this seminar, I will introduce the main tail bounds, with an emphasis on the techniques one should use to apply them. In the final part, I will explore specific applications of these bounds in greater detail, focusing in particular on their use with the binomial distribution.

Markov's Inequality [6]

Let X be a non-negative random variable (i.e. $\mathbb{P}(X \geq 0) = 1$) with finite expectation $\mathbb{E}([)X]$ (i.e. $\mathbb{E}(X) < \infty$). Then for any $\xi > 0$,

$$\mathbb{P}(X \geq \xi) \leq \frac{\mathbb{E}(X)}{\xi} \tag{M1}$$

$$\mathbb{P}(X \geq \xi \cdot \mathbb{E}(X)) \leq \frac{1}{\xi} \tag{M2}$$

$$\mathbb{P}(X \geq \xi) \leq \frac{\mathbb{E}(\varphi(X))}{\varphi(\xi)} \tag{M3}$$

where φ is a nondecreasing non negative function.

Chebyshev's Inequality [2]

Let X be an integrable random variable with $\mathbb{V}ar(X) \neq 0$ with finite expectation $\mathbb{E}(X)$ (i.e. $\mathbb{E}(X) < \infty$). Then for any $\xi > 0$,

$$\mathbb{P}\left(|X - \mathbb{E}(X)| \geq \xi \cdot \sqrt{\mathbb{V}ar(X)}\right) \leq \frac{1}{\xi^2} \tag{Chb1}$$

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \xi) \leq \frac{\mathbb{V}ar(X)}{\xi^2} \tag{Chb2}$$

Chernoff Bounds [3]

Let X be a random variable. Then for any $\xi \in \mathbb{R}$,
for $\forall t > 0$

$$\mathbb{P}(X \geq \xi) \leq e^{-\xi t} \cdot M_X(t) \tag{Chff1}$$

for $\forall t < 0$

$$\mathbb{P}(X \leq \xi) \leq e^{-\xi t} \cdot M_X(t) \tag{Chff2}$$

where $M_X(t) := \mathbb{E}\left(e^{tX}\right)$ is the moment generating function.

Hoeffding's Inequality [5] [3]

Let $X_1, X_2, \ldots, X_n$ be indipendent random variables such that $\forall i = 1, 2, \ldots, n$,

$$a_i \leq X_i \leq b_i$$

almost surely (i.e. $\mathbb{P}(a_i \leq X_i \leq b_i) = 1$). Let $S_n := \sum X_i$. Then for any $\xi \in \mathbb{R}$,

$$\mathbb{P}(S_n - \mathbb{E}(S_n) \geq \xi) \leq e^{-\frac{2\xi^2}{\sum (b_i - a_i)^2}} \tag{Hoef1}$$

Bennett's Inequality [1]

Let $X_1, X_2, \ldots, X_n$ be indipendent random variables such that $\forall i = 1, 2, \ldots, n$

1. $\mathbb{V}ar(X_i)$ exists finite
2. $|X_i - \mathbb{E}(X_i)| \leq M_i$ almost surely (i.e. $\mathbb{P}(|X_i - \mathbb{E}(X_i)| \leq M_i) = 1$)

Let $S_n := \sum X_i$m $M := \max\{M_i\}$. Then for any $\xi \geq 0$,

$$\mathbb{P}\left(S_n - \mathbb{E}\left(S_n\right) \geq \xi\right) \leq e^{-\frac{\mathbb{V}ar(S_n)}{M^2} \cdot L\left(\frac{M\xi}{\mathbb{V}ar(S_n)}\right)} \tag{Ben1}$$

where $L(u) := (1+u) \cdot \log(1+u) - u$

Bernstein's Inequality [1]

Let $X_1, X_2, \ldots, X_n$ be indipendent random variables such that $\forall i = 1, 2, \ldots, n$

$$a_i \leq X_i \leq b_i$$

almost surely (i.e. $\mathbb{P}\left(a_i \leq X_i \leq b_i\right) = 1$). Let $S_n := \sum X_i$m $M := \max\{b_i\}$. Then for any $\xi \geq 0$,

$$\mathbb{P}\left(S_n - \mathbb{E}\left(S_n\right) \geq \xi\right) \leq e^{-\frac{\xi^2}{2} \cdot \frac{1}{\sum \mathbb{V}ar(X_i) + \frac{1}{3}M \cdot \xi}} \tag{Ber1}$$

Chernoff Bounds for Binomial [4]

Let X be a random variable, $X \sim Bin(n, p)$. Then for any $\xi > 0$,

$$\mathbb{P}\left(X - \mathbb{E}\left(X\right) \geq \xi\right) \leq e^{-\frac{2\xi^2}{n}} \tag{ChfBin1}$$

$$\mathbb{P}\left(X - \mathbb{E}\left(X\right) \leq -\xi\right) \leq e^{-\frac{2\xi^2}{n}} \tag{ChfBin2}$$

Stronger Chernoff Bounds for Binomial [4]

Let X be a random variable, $X \sim Bin(n, p)$. Then for any $\xi > 0$,

$$\mathbb{P}\left(X - \mathbb{E}\left(X\right) \geq \xi \cdot \mathbb{E}\left(X\right)\right) \leq \left(\frac{e^{\xi}}{(1+\xi)^{1+\xi}}\right)^{\mathbb{E}(X)} \tag{ChfBinS1}$$

Futhermore, when $0 < \xi < 1$

$$\mathbb{P}\left(X - \mathbb{E}\left(X\right) \leq -\xi \cdot \mathbb{E}\left(X\right)\right) \leq \left(\frac{e^{-\xi}}{(1-\xi)^{1-\xi}}\right)^{\mathbb{E}(X)} \tag{ChfBinS2}$$

I found the proofs of these bounds in various papers and summarized them in a handwritten file available on GitHub, in case anyone is interested. During the seminar, I will introduce these bounds and explain them with a few examples. Each bound is essentially a specific application of a previous one or a direct consequence of some calculus properties. For this reason, I believe that going through all the formal proofs is not particularly useful. Instead, I would prefer to focus on practical examples and provide some intuition on when a specific bound might be more suitable than another. To see a concrete application, we will prove the stronger version of the Chernoff bounds for the Binomial distribution ChfBinS1 and ChfBinS2,this is a nice example of how to apply Chernoff bounds in practical scenarios. If anyone is curious, we can also look at other proofs.

References

[1] *Bennett's and Bernstein's Inequality.* URL: https://mathweb.ucsd.edu/~xip024/Teaching/Math281C_Spring2020/lect4.pdf. (accessed: 01.09.2016).

[2] *Chebyshev's inequality.* URL: https://en.wikipedia.org/wiki/Chebyshev's_inequality. (accessed: 01.09.2016).

[3] *Chernoff Bounds and Hoeffding's Inequality.* URL: https://anr248.medium.com/statistical-learning-theory-hoeffdings-inequality-derivation-simulation-e3a97100d147. (accessed: 01.09.2016).

[4] Prof. Mor Harchol-Balter. *Introduction to Probability for Computing, Chapter 18.* 2024. URL: https://www.cs.cmu.edu/~harchol/Probability/book.html.

[5] *Hoeffding's Inequality.* URL: https://cs229.stanford.edu/extra-notes/hoeffding.pdf. (accessed: 01.09.2016).

[6] *Markov's inequality.* URL: https://en.wikipedia.org/wiki/Markov%27s_inequality. (accessed: 01.09.2016).