Cheat Sheet

1 Probabilities

Notations. Let $\mathcal{B}_p$ denote the Bernouilli distribution with probability p. $\mathrm{SD}(X,Y)$ denotes the statistical distance between random variables (X,Y) over a set S, defined as

$$\begin{aligned}\mathrm{SD}(X,Y) &= \frac{1}{2}\cdot\sum_{x\in S}|\Pr[X=x]-\Pr[Y=x]| \\ &= \max_{f:S\mapsto\{0,1\}}|\Pr[f(X)=1]-\Pr[f(Y)=1]| \\ &= \max_{Z\subseteq S}|\Pr[X\in Z]-\Pr[Y\in Z]|.\end{aligned}$$

1.1 Basics Probabilities

Union Bound, Bayes' Rule.

$$\Pr[A\cup B]\le\Pr[A]+\Pr[B],\quad \Pr[A|B]=\frac{\Pr[B|A]\cdot\Pr[A]}{\Pr[B]}.$$

Others.

$$\min\{\Pr[A],\Pr[B]\}\le\Pr[A\cap B]\le\Pr[A]+\Pr[B]-1$$
$$\Pr[A\cap B]\le\Pr[A|B]$$

1.2 Expectations

$|\mathbb{E}[XY]|\le\mathbb{E}[|XY|]\le\sqrt{\mathbb{E}[|X|^2]\,\mathbb{E}[|Y|^2]}$ **(Cauchy-Schwarz)**
For ϕ convex, $\phi(\mathbb{E}[X])\le\mathbb{E}[\phi(X)]$ **(Jensen)**

1.3 Concentration Bounds

Lemma 1.1 (Markov Inequality). *Let X be a positive random variable with finite expected value μ. Then for any $k>0$,*

$$\Pr[X\ge k]\le\frac{\mu}{k}.$$

Lemma 1.2 (Bienaymé-Chebyshev Inequality). *Let X be a random variable with finite expected value μ and finite nonzero variance σ^2. Then for any $k>0$,*

$$\Pr[|X-\mu|\le k\sigma]\le\frac{1}{k^2}.$$

Lemma 1.3 (Chernoff Inequality). *Let $n\in\mathbb{N}$ and let $(X_1,\cdots,X_n)$ be independent random variables taking values in $\{0,1\}$. Let X denote their sum and $\mu\leftarrow\mathbb{E}[X]$. Then for any $\delta\in[0,1]$,*

$$\Pr[X\ge(1+\delta)\mu]\le\exp\left(-\frac{\delta^2\mu}{3}\right)$$
$$\Pr[X\le(1-\delta)\mu]\le\exp\left(-\frac{\delta^2\mu}{2}\right).$$

Furthermore, for any $\delta\ge 0$,

$$\Pr[X\ge(1+\delta)\mu]\le\exp\left(-\frac{\delta^2\mu}{2+\delta}\right).$$

Lemma 1.4 (Generalized Chernoff Inequality [5]). *Let $n\in\mathbb{N}$ be an integer and let $(X_1,\cdots,X_n)$ be boolean random variables such that, for some $\delta\in[0,1]$, it holds that for every subset $S\subset[n]$, $\Pr[\wedge_{i\in S}X_i]\le\delta^{|S|}$. Then for any $\gamma\in[\delta,1]$,*

$$\Pr\left[\sum_{i=1}^n X_i\ge\gamma n\right]\le\exp\left(-nD(\gamma||\delta)\right),$$

where $D(\gamma||\delta)$ denotes the relative entropy function, satisfying $D(\gamma||\delta)\ge 2(\gamma-\delta)^2$.

For more discussions and a constructive proof of the generalized Chernoff bound, see Impagliazzo and Kabanets [3].

Lemma 1.5 (Bernstein Inequality). *Let $X_1,\cdots,X_m$ be independent zero-mean random variables, and let M be a bound such that $|X_i|\le M$ almost surely for $i=1$ to m. Let X denote the random variable $\sum_{i=1}^m X_i$. It holds that*

$$\Pr[X>B]\le\exp\left(-\frac{B^2}{2\sum_{i=1}^m\mathsf{Enc}[X_i^2]+\frac{2}{3}MB}\right).$$

Bounded Difference Inequality. First proved by McDiarmid in [4], in a more general form than below. Special case of Azuma inequality [1]. Let $(n,m)\in\mathbb{N}^2$ be two integers. We say that a function $\Phi:[n]^m\mapsto\mathbb{R}$ satisfies the *Lipschitz property with constant d* if for every $\vec{x},\vec{x}'\in[n]^m$ which differ in a single coordinate, it holds that

$$|\Phi(\vec{x})-\Phi(\vec{x}')|\le d.$$

Lemma 1.6 (Bounded Difference Inequality). *Let $\Phi:[n]^m\mapsto\mathbb{R}$ be a function satisfying the Lipschitz property with constant d, and let $(X_1,\cdots,X_m)$ be independent random variables over $[n]$. Then*

$$\Pr[\Phi(X_1,\cdots,X_m)<\mathbb{E}[\Phi(X_1,\cdots,X_m)]-t]\le\exp\left(-\frac{2t^2}{m\cdot d^2}\right).$$

1.4 Entropy Notions

Let $\mathbf{H}(x)=x\log(1/x)+(1-x)\log(1/(1-x))$ be the binary entropy function. We let $\mathbf{H}_1(X)$ and $\mathbf{H}_\infty(X)$ denote respectively the Shannon entropy, min-entropy, average min-entropy conditioned on Z, and ε-smooth min-entropy of a random variable X, defined as

$$\begin{aligned}\mathbf{H}_1(X) &= -\sum_{x\in\mathsf{Supp}(X)}\Pr[X=x]\cdot\log\Pr[X=x] \\ \mathbf{H}_\infty(X) &= \min_{x\in\mathsf{Supp}(X)}\log(1/\Pr[X=x]) \\ \tilde{\mathbf{H}}_\infty(X|Z) &= -\log\mathop{\mathbb{E}}_{z\leftarrow Z}[2^{-\mathbf{H}_\infty(X|Z=z)}] \\ \mathbf{H}_\infty^\varepsilon(X) &= \max_{\mathsf{SD}(X,Y)\le\varepsilon}\mathbf{H}_\infty(Y).\end{aligned}$$

Note that $\mathbf{H}_1(\mathcal{B}_p)=\mathbf{H}(p)$.

Lemma 1.7 ([2], Lemma 2.2a). *For any $\delta > 0$, $\mathrm{H}_\infty(X|Z = z)$ is at least $\tilde{\mathrm{H}}_\infty(X|Z) - \log(1/\delta)$ with probability at least $1 - \delta$ over the choice of z.*

Lemma 1.8 ([2], Lemma 2.2b). *Conditioning on Z that has b bits of information reduces the entropy of X by at most b:* $\tilde{\mathrm{H}}_\infty(X|Z_1, Z_2) \geq \mathrm{H}_\infty(X, Z_1|Z_2) - \log|\mathrm{Supp}(Z_1)|$.

1.5 Binomial Coefficients

- For any $0 < \mu < 1/2$ and $m \in \mathbb{N}$,
$$\sum_{i=0}^{\mu m} \binom{m}{i} = 2^{m\mathrm{H}(\mu) - \frac{\log m}{2} + O(1)}.$$
- For $k = o(n)$, $\log \binom{n}{k} = (1 + o(1))k \log \frac{n}{k}$.
- For any (k, n), $\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \frac{n^k}{k!} < \left(\frac{ne}{k}\right)^k$.

1.6 Useful Inequalities

- $\forall x > 0$, $\exp(-x) > 1 - x$.
- $\forall\ 0 < x < \frac{2-\sqrt{2}}{2}$, $1 - x > 2^{-\frac{2+\sqrt{2}}{2}x}$.
- $\forall n \geq 1$, $\left(1 - \frac{1}{n}\right)^n \leq \exp(-1)$ and $\exp(-1) \leq \left(1 - \frac{1}{n}\right)^{n-1}$.
- $\forall \delta > 0$, $\frac{2\delta}{2+\delta} \leq \log(1 + \delta)$.

1.7 Useful Lemmas

Splitting Lemma. Let $A \subset X \times Y$ such that $\Pr[(x, y) \in A] \leq \varepsilon$. For any $\varepsilon' < \varepsilon$, defining B as $B = \{(x, y) \in X \times Y \mid \Pr_{y' \leftarrow_r Y}[(x, y') \in A] \geq \varepsilon - \varepsilon'\}$, it holds that

$$\Pr[B] \geq \varepsilon' \quad \forall (x, y) \in B, \Pr_{y'}[(x, y') \in A] \geq \varepsilon - \varepsilon' \quad \Pr[B|A] \geq \varepsilon'/\varepsilon.$$

Forking Lemma. For any $q \geq 1$, any set H with $|H| \geq 2$, and randomized PPT algorithm $\mathcal{A}$ which, on input $(x, h_1, \cdots, h_q)$ returns a pair $(J, \sigma) \in [q] \times \{0, 1\}^*$, and input distribution $\mathcal{D}$, let

$$\begin{aligned} \mathrm{acc} \stackrel{\text{def}}{=} \Pr[x \leftarrow_r \mathcal{D}, &(h_1, \cdots, h_q) \leftarrow_r H, \\ &(J, \sigma) \leftarrow_r \mathcal{A}(x, h_1, \cdots, h_q) : J \geq 1]. \end{aligned}$$

Then define the following algorithm $\mathsf{F}_\mathcal{A}$: on input $x \in \mathrm{Supp}(\mathcal{D})$, $\mathsf{F}_\mathcal{A}(x)$ picks coins r, $(h_1, \cdots, h_q) \leftarrow_r H$, and runs $(I, \sigma) \leftarrow \mathcal{A}(x, h_1, \cdots, h_q; r)$. If $I = 0$, it returns $(0, \varepsilon, \varepsilon)$. Else, it picks $(h'_1, \cdots, h'_q) \leftarrow_r H$, and runs $(I', \sigma') \leftarrow \mathcal{A}(x, h_1, \cdots, h_{I-1}, h'_I, \cdots, h'_q; r)$. If $I = I'$ and $h_I \neq h_{I'}$, it returns $(1, \sigma, \sigma')$; else, it returns $(0, \varepsilon, \varepsilon)$. Let

$$\mathsf{frk} \stackrel{\text{def}}{=} \Pr[x \leftarrow_r \mathcal{D}, (b, \sigma, \sigma') \leftarrow_r \mathsf{F}_\mathcal{A}(x) : b = 1].$$

Then
$$\mathrm{acc} \leq \frac{q}{h} + \sqrt{q \cdot \mathsf{frk}}.$$

Leftover Hash Lemma.

Piling-Up Lemma. For $0 < \mu < 1/2$ and random variables $(X_1, \cdots, X_t)$ i.i.d. to $\mathcal{B}_\mu$, it holds that

$$\Pr\left[\bigoplus_{i=1}^t X_i = 0\right] = \frac{1}{2} \cdot \left(1 + (1 - 2\mu)^t\right) = \frac{1}{2} + 2^{-c_\mu t - 1},$$

where $c_\mu = \log \frac{1}{1-2\mu}$. In other terms, for any $0 < \mu \leq \mu' < 1/2$, it holds that

$$\mathcal{B}_\mu \oplus \mathcal{B}_{\frac{\mu' - \mu}{1-2\mu}} \approx \mathcal{B}_{\mu'}.$$

1.8 Hashing

Universal, pairwise independent

References

[1] Kazuoki Azuma. 1967. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal, Second Series* 19, 3 (1967), 357–367.

[2] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. 2004. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *EUROCRYPT 2004 (LNCS, Vol. 3027)*, Christian Cachin and Jan Camenisch (Eds.). Springer, Heidelberg, 523–540. https://doi.org/10.1007/978-3-540-24676-3_31

[3] Russell Impagliazzo and Valentine Kabanets. 2010. Constructive proofs of concentration bounds. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 617–631.

[4] Colin McDiarmid. 1989. On the method of bounded differences, in "Survey in Combinatorics,"(J. Simons, Ed.) London Mathematical Society Lecture Notes, Vol. 141.

[5] Alessandro Panconesi and Aravind Srinivasan. 1997. Randomized Distributed Edge Coloring via an Extension of the Chernoff–Hoeffding Bounds. *SIAM J. Comput.* 26, 2 (1997), 350–368.