The Birthday Paradox

Want number of people t so that

$$P\left(\begin{array}{c}\text{At least 2 of the } t \text{ people} \\ \text{have the same birthday}\end{array}\right) > 0.5$$

$P(\text{no match among } 2) = 1 - \frac{1}{365}$

$P(\text{no match among } 3) = \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)$

$P(\text{no match among } 4) = \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\left(1 - \frac{3}{365}\right)$

$\vdots$

$P(\text{no match among } t)$

$$= \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\left(1 - \frac{3}{365}\right) \cdots \left(1 - \frac{t-1}{365}\right)$$

$P(\text{match among } t)$

$$= 1 - \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\left(1 - \frac{3}{365}\right) \cdots \left(1 - \frac{t-1}{365}\right)$$

If $t = 23$

$P(\text{match among } 23)$

$$= 1 - \left(1 - \frac{1}{365}\right)\left(1 - \frac{2}{365}\right)\left(1 - \frac{3}{365}\right) \cdots \left(1 - \frac{22}{365}\right)$$

$$\approx 0.507$$

"collision"

Want number of outputs t so that

$$P(\text{collision}) > 0.5$$

2^N outputs

$P(\text{no collision among } t)$

$$= \left(1 - \tfrac{1}{2^N}\right)\left(1 - \tfrac{2}{2^N}\right)\left(1 - \tfrac{3}{2^N}\right) \cdots \left(1 - \tfrac{t-1}{2^N}\right)$$

$$= \prod_{i=1}^{t-1} \left(1 - \tfrac{i}{2^N}\right)$$

recall

$$\underbrace{e^{-x} = 1 - x + \tfrac{x^2}{2} - \tfrac{x^3}{3!} + \tfrac{x^4}{4!} - \cdots}_{\text{approximation}}$$

$P(\text{no collision among } t)$

$$\approx \prod_{i=1}^{t-1} e^{-\frac{i}{2^N}}$$

$$= e^{-\left(\frac{1}{2^N} + \frac{2}{2^N} + \frac{3}{2^N} + \cdots + \frac{t-1}{2^N}\right)}$$

$$= e^{-\frac{1+2+3+\cdots+(t-1)}{2^N}}$$

recall

$$1 + 2 + 3 + \cdots + (t-1) = \frac{t(t-1)}{2}$$

$$P(\text{no collision among } t) \approx e^{-\frac{t(t-1)}{2 * 2^N}}$$

$$\lambda = P(\text{at least one collision among } t)$$

$$\approx 1 - e^{-\frac{t(t-1)}{2*2^n}}$$

$$1-\lambda \approx e^{-\frac{t(t-1)}{2*2^n}}$$

$$\ln(1-\lambda) \approx -\frac{t(t-1)}{2*2^n}$$

$$-\ln(1-\lambda) \approx \frac{t(t-1)}{2*2^n}$$

$$\ln\frac{1}{1-\lambda} \approx \frac{t(t-1)}{2*2^n}$$

$$2*2^n*\ln\frac{1}{1-\lambda} \approx t(t-1) = t^2 - t \approx t^2$$

$$t \approx \sqrt{2*2^n*\ln\frac{1}{1-\lambda}}$$

$$t \approx \sqrt{2^n}\sqrt{2}\sqrt{\ln\frac{1}{1-\lambda}}$$

$$t \approx 2^{n/2}\sqrt{2}\sqrt{\ln\frac{1}{1-\lambda}}$$

want $\lambda > \frac{1}{2}$

$$t \approx 2^{n/2}\sqrt{2}\sqrt{\ln\frac{1}{1/2}}$$

$$t \approx 2^{n/2}\underbrace{\sqrt{2}\sqrt{\ln 2}}_{1.177} \approx 2^{n/2}$$