Some Thoughts and Solutions

金之涵

1 Problem (Sunrise Problem) Consider we know nothing about sunrise but the fact that the sun has risen once a day for N days, what is the probability of the sun also rising tomorrow? Because we have no idea the probability p of the sun rising on any given day, we only the situation with p uniformly distributed in $[0, 1]$.

Solution Let A be the event that the sun rises tomorrow and B be the event that the sun has risen once a day during the past N days. Similar to Bayes' law in discrete form, we have the following equation, where dp is the distribution of p.

$$
\begin{aligned}
P(A|B) &= \frac{P(A \cap B)}{P(B)} \\
&= \frac{\int\limits_0^1 p^{N+1} dp}{\int\limits_0^1 p^N dp} \\
&= \frac{N+1}{N+2}
\end{aligned}
$$

2 Problem (Matrix Test) Assume matrix A, B, C are uniformly distributed in $\mathbb{F}_2^{n\times n}$ independently, which means each element in A, B, C is uniformly distributed in $\mathbb{F}_2$ independently. Consider a method to test if $AB = C$ that we generate a random vector r $\in \mathbb{F}_2^{n\times 1}$ and determine the result by calculating $(AB - C)r$. Although this new method is more efficient, we want to know its precision.

Solution Let P be the event that $AB = C$, Q be the event that $ABr = Cr$. Due to the fact that $ABr = Cr$ always holds when $AB = C$, we only care about the situation when $AB \neq C$, which is $P(Q|P^c)$.

$$P(Q|P^c) = \frac{P(Q\cap P^c)}{P(P^c)} = \frac{\sum_{i=1}^{n} P(r(AB-C)=i)\cdot P(Q|r(AB-C)=i)}{P(P^c)}$$

Randomly generating A, B and C in order, we can find that the distribution of $AB - C$ is the same as that of C. So we can replace $AB - C$ with C.

$$P(P^c) = P(C \neq 0) = 1 - 2^{-n^2}$$
$$P(r(AB-C)=i) = P(r(C)=i)$$

We then consider the kernel of C.

$$Cr = 0 \iff r \in Ker(C)$$

So $P(Q|r(AB - C) = i) = 2^{-i}$. We now have the following equation.

$$P(Q|P^c) = \frac{1}{1-2^{-n^2}} \cdot \sum_{i=1}^{n} P(r(C)=i)\cdot 2^{-i}$$

A rough estimate can be obtained as following using $2^{-i} \leq 2^{-1}$. The test can be considered reliable after testing several times with different r.

$$P(Q|P^c) \leq \frac{1}{2} \tag{1}$$

We will next use a lemma to acquire a estimate close to the actual situation.

Lemma Let $B_{n,k}$ be the number of ordered k-basis of a subspace of $\mathbb{F}_2^n$.[1]

$$B_{n,k} = \prod_{i=0}^{k-1}(2^n - 2^i)$$

Proof Every linear space has its basis. There are $(2^n - 2^0)$ vectors to choose from for the first element, $(2^n - 2^1)$ to choose from for the second element, $\cdots$ $(2^n - 2^{k-1})$ vectors to choose from for the kth element.

$\blacksquare$

Let $f_{n,k}$ be the number of matrices($\in \mathbb{F}_2^{n\times n}$) whose rank is k. We will next count $f_{n,k}$ by two steps.

First, count the number of linear spaces of matrix $M \in \mathbb{F}_2^{n\times n}$ whose rank is k. A linear space is determined by a ordered basis $v_1, v_2, \cdots, v_k$, which has $B_{n,k}$ cases. However each space is counted $B_{k,k}$ times. So the number of linear spaces of M is $\dfrac{B_{n,k}}{B_{k,k}}$.

Second, count the number of matrices that forms a identical subspace of $\mathbb{F}_2^n$. Let U be a fixed subspace and R be a fixed $k \times n$ matrix whose row vectors form a basis of U. Let A be any matrix that forms U. Since each row vector of A can be expressed uniquely as a linear combination of rows of R, there exists a unique $n \times k$ matrix M such that $A = MR$. Obviously rank(A) is k. On the other hand, for any $A_{n\times n}$ with rank k forming U, A can be factorized as $A_{n\times n} = M_{n\times k}R_{k\times n}$, where rank$(M)$ is k. So A is only determined by R, the number of valid As is $B_{n,k}$.

$$f_{n,k} = \frac{B_{n,k}^2}{B_{k,k}}$$

It is easy to see

$$\begin{aligned}
\frac{\dfrac{f_{n+1,k+1}\cdot 2^{-(k+1)}}{2^{(n+1)^2-1}}}{\dfrac{f_{n,k}\cdot 2^{-k}}{2^{n^2-1}}} &= \frac{1}{2}\cdot\frac{2^{n^2}-1}{2^{(n+1)^2}-1}\cdot\frac{\left(2^{n+1}-1\right)^2\cdot 2^k}{2^{k+1}-1} \\
&< \frac{1}{2}\cdot\frac{1}{2^{(n+1)^2-n^2}}\cdot\frac{1}{2}\cdot 2^{2n+2} \\
&< \frac{1}{2}
\end{aligned}$$

The probability of dimention n can be expressed as

$$P_n(Q|P^c) = \frac{1}{2^{n^2}-1}\cdot\sum_{i=1}^{n} f_{n,i}\cdot 2^{-i}$$

$$
\begin{aligned}
\frac{P_{n+1}(Q|P^c)}{P_n(Q|P^c)} &= \frac{\dfrac{1}{2^{(n+1)^2}-1} \cdot \sum\limits_{i=1}^{n+1} f_{n+1,i} \cdot 2^{-i}}{\dfrac{1}{2^{n^2}-1} \cdot \sum\limits_{i=1}^{n} f_{n,i} \cdot 2^{-i}} \\
&<= \frac{2^{n^2}-1}{2^{(n+1)^2}-1} \cdot \frac{f_{n+1,1} \cdot \dfrac{1}{2}}{\sum\limits_{i=1}^{n} f_{n,i} \cdot 2^{-i}} + \max_{k=1}^{n} \frac{\dfrac{f_{n+1,k+1} \cdot 2^{-(k+1)}}{2^{(n+1)^2-1}}}{\dfrac{f_{n,k} \cdot 2^{-k}}{2^{n^2-1}}} ?? \\
&< \frac{1}{2^{2n+2}} \cdot \frac{(2^{n+1}-1)^2}{2^{-n} \cdot \sum\limits_{i=1}^{n} f_{n,i}} + \frac{1}{2} \\
&< \frac{1}{2^{2n+2}} \cdot \frac{2^{n+1}-1}{2^{-n}} \cdot \frac{2^{n+1}-1}{2^{n^2}-1} + \frac{1}{2} \\
&< \frac{1}{2^{2n+2}} \cdot \frac{2^{n+1}}{2^{-n}} \cdot \frac{2^{n+1}}{2^{n^2}} + \frac{1}{2} \\
&< \frac{1}{2} + \epsilon
\end{aligned}
$$

where $\lim\limits_{n \to \infty} \epsilon = 0$. So $P_n(Q|P^c)$ can be expressed as a geometric sequence form, which decreases fast as the increasing of n.

$$
P_n(Q|P^c) < C \cdot c^n, 0 < c < 1 \tag{2}
$$

After running a code, we have the following data.

n	1	2	3	4	5	6	7	8
$P_n(Q\|P^c)$	0.5	0.4	0.23288	0.12108	0.06152	0.03101	0.01556	0.00780
$\frac{P_{n+1}(Q\|P^c)}{P_n(Q\|P^c)}$	0.8	0.5822	0.51993	0.50812	0.50397	0.50197	0.50098	0.50049

The actual trend of the P_n is close to a geometry sequence with common ratio 0.5, when $n > 2$. So the test is reliable when n is large, even if testing only one time.

Reference

[1] Frank R. Kschischang. Gaussian coefficients. December 2008.