Exercise 1 *15 points*
Let $\sum_{i=1}^{r}\sigma_i u_i v_i^T$ be the SVD of A, where $A \in \mathbb{R}^{n\times d}$. Show that $|u_1^T A| = \sigma_1$ and $|u_1^T A| = \max_{\|u\|=1}\|u^T A\|$ where $\|x\| = \sqrt{\sum_{i=1}^{d} x_i^2}$ for a vector $x \in \mathbb{R}^d$.

$$A = \sum_{i=1}^{r} \sigma_i u_i v_i^T$$

$$|u_1^T A| = |u_1^T \sum_{i=1}^{r} \sigma_i u_i v_i^T| = |\sigma_1 v_1^T| = \sigma_1$$

设 $u = \sum_{i=1}^{n} \alpha_i u_i$，其中 $\sqrt{\sum_{i=1}^{n} \alpha_i^2} = 1$

$$\|u^T A\| = \|\sum_{i=1}^{n} \alpha_i u_i^T \sum_{i=1}^{r} \sigma_i u_i v_i^T\| = \|\sum_{i=1}^{r} \alpha_i \sigma_i v_i^T\| = \sqrt{\sum_{i=1}^{r} \alpha_i^2 \sigma_i^2}$$

$$\le \sqrt{\sigma_1^2 \sum_{i=1}^{r} \alpha_i^2} = \sigma_1 = |u_1^T A|$$

当且仅当 $|\alpha_1| = 1$ 时等号成立，

$$\therefore \|u_1^T A\| = \max_{\|u\|=1} \|u^T A\|$$

Exercise 2 *25 points*
Let A be an $n \times d$ matrix with SVD such that $A = \sum_{i=1}^{r}\sigma_i u_i v_i^\top$. Let $x \in \mathbb{R}^d$ be a vector such that $\|x\|_2 = 1$ and $|x^\top v_1| \ge \delta$ for some $\delta > 0$. Suppose that $\sigma_2 < \frac{1}{2}\sigma_1$. Let w be the vector after $k = \log(1/\varepsilon\delta)$ iterations of the power method, namely,

$$w = \frac{(A^\top A)^k x}{\|(A^\top A)^k x\|_2}.$$

Prove that the length of the projection of w onto the line defined by the first singular vector v_1 is at least $1-\varepsilon$, i.e., $|w \top v_1| \ge 1 - \varepsilon$.

$$A = \sum_{i=1}^{r} \sigma_i u_i v_i^T$$

设 $B = A^T A = (\sum_{i=1}^{r} \sigma_i v_i u_i^T)(\sum_{i=1}^{r} \sigma_i u_i v_i^T) = \sum_{i=1}^{r} \sigma_i^2 v_i v_i^T$

则 $B^k = (A^T A)^k = \sum_{i=1}^{r} \sigma_i^{2k} v_i v_i^T$

$\because \|x\|_2 = 1$ $\therefore$ 可设 $x = \sum_{i=1}^{n} \alpha_i v_i$，其中 $\sqrt{\sum_{i=1}^{n} \alpha_i^2} = 1$

则 $B^k x = (\sum_{i=1}^{r} \sigma_i^{2k} v_i v_i^T)(\sum_{i=1}^{n} \alpha_i v_i) = \sum_{i=1}^{r} \sigma_i^{2k} \alpha_i v_i$

$$w = \frac{B^k x}{\|B^k x\|_2} = \frac{\sum_{i=1}^{r} \sigma_i^{2k} \alpha_i v_i}{\|B^k x\|_2} \qquad w^T = \frac{\sum_{i=1}^{r} \sigma_i^{2k} \alpha_i v_i^T}{\|B^k x\|_2}$$

$$|w^T v_1| = \frac{|\sum_{i=1}^{r} \sigma_i^{2k} \alpha_i v_i^T v_1|}{\|B^k x\|_2}$$

$$|\sum_{i=1}^{r} \sigma_i^{2k} \alpha_i v_i^T v_1| = |\sigma_1^{2k} \alpha_1|$$

$$\|B^k x\|_2^2 = (B^k x)^T (B^k x) = \sum_{i=1}^{r} \sigma_i^{4k} \alpha_i^2 = \sigma_1^{4k}\alpha_1^2 + \sum_{i=2}^{r} \sigma_i^{4k}\alpha_i^2$$

即证 $\dfrac{|\sigma_1^{2k}\alpha_1|}{\sqrt{\sigma_1^{4k}\alpha_1^2 + \sum_{i=2}^{r}\sigma_i^{4k}\alpha_i^2}} \geq 1-\varepsilon$

$\because \sigma_1 > \frac{1}{2}\sigma_1 > \sigma_2 \geq \sigma_3 \geq \cdots \geq \sigma_r$

$\therefore$ 不等式左边 $\geq \dfrac{\sigma_1^{2k}|\alpha_1|}{\sqrt{\sigma_1^{4k}\alpha_1^2 + \sum_{i=2}^{r}(\frac{1}{2}\sigma_1)^{4k}\alpha_i^2}} = \dfrac{\sigma_1^{2k}|\alpha_1|}{\sigma_1^{2k}\sqrt{\alpha_1^2 + (\frac{1}{2})^{4k}\sum_{i=2}^{r}\alpha_i^2}}$

$\therefore$ 左边 $\geq \dfrac{|\alpha_1|}{\sqrt{\alpha_1^2 + (\frac{1}{2})^{4k}\sum_{i=2}^{r}\alpha_i^2}}$

将 $k = \log\frac{1}{\varepsilon\delta}$ 代入，则左边 $\geq \dfrac{|\alpha_1|}{\sqrt{\alpha_1^2 + (\varepsilon\delta)^4\sum_{i=2}^{r}\alpha_i^2}}$

又 $\because |x^T v_1| \geq \delta$，即 $\left|\sum_{i=1}^{n}\alpha_i v_i^T v_1\right| = |\alpha_1| \geq \delta$

$\therefore \sum_{i=2}^{r}\alpha_i^2 = 1-\alpha_1^2 \leq 1-\delta^2$

$\therefore$ 左边 $\geq \dfrac{|\alpha_1|}{\sqrt{\alpha_1^2 + (\varepsilon\delta)^4(1-\delta^2)}} = \dfrac{1}{\sqrt{1+\frac{(\varepsilon\delta)^4}{\alpha_1^2}(1-\delta^2)}} \geq \dfrac{1}{\sqrt{1+\frac{(\varepsilon\delta)^4}{\delta^2}(1-\delta^2)}}$

$$= \frac{1}{1+\varepsilon^4\delta^2(1-\delta^2)}$$

又 $\delta^2(1-\delta^2) \leq \dfrac{\delta^2+1-\delta^2}{2} = \dfrac{1}{2}$ 故 $\dfrac{1}{1+\varepsilon^4\delta^2(1-\delta^2)} \geq \dfrac{1}{1+\frac{1}{2}\varepsilon^4}$

即证 $\dfrac{1}{1+\frac{1}{2}\varepsilon^4} \geq 1-\varepsilon$

即 $1+\frac{1}{2}\varepsilon^4 - \varepsilon - \frac{1}{2}\varepsilon^5 \leq 1$

即 $\frac{1}{2}\varepsilon^3 - \frac{1}{2}\varepsilon^4 \leq 1$

即 $\frac{1}{2}\varepsilon^3(1-\varepsilon) \leq 1$

当 $\varepsilon \in (0,1)$ 时，$\frac{1}{2}\varepsilon^3 < 1$，$1-\varepsilon < 1$，故 $\frac{1}{2}\varepsilon^3(1-\varepsilon) \leq 1$

故不等式成立.

Exercise 3 *20 points*
Let $k < d$. Let $U \in \mathbb{R}^{d\times k}$ be a random matrix such that its (i,j)-th entry is denoted as u_{ij}, where $\{u_{ij}\}$ are independent random variables such that

$$u_{ij} = \begin{cases} 1 & \text{with probability } \frac{1}{2}, \\ -1 & \text{with probability } \frac{1}{2} \end{cases}$$

Now we use matrix B as a random projection matrix. That is, for a (row) vector $a \in \mathbb{R}^d$, we map it to

$$f(a) = \frac{1}{\sqrt{k}} aU$$

For each j such that $1 \le j \le k$, define $b_j = [f(a)]_j$, i.e., b_j is the j-th entry of $f(a)$.

- What is the expectation $\mathrm{E}[b_j]$?
- What is $\mathrm{E}[b_j^2]$?
- What is $\mathrm{E}[\|f(a)\|^2]$?

(1) $b_j = \frac{1}{\sqrt{K}} a \cdot u_j = \frac{1}{\sqrt{K}} \sum_{i=1}^{d} a_i u_{ij}$

$\because u_{ij} = \begin{cases} 1, & w.p. \frac{1}{2} \\ -1, & w.p. \frac{1}{2} \end{cases}$

$\therefore E[a_i u_{ij}] = \frac{1}{2}\cdot 1 \cdot a_i - \frac{1}{2}\cdot 1 \cdot a_i = 0 \quad , 1\le i \le d$

$E[b_j] = \frac{1}{\sqrt{K}} \sum_{i=1}^{d} E[a_i u_{ij}] = 0$

(2) $b_j^2 = \frac{1}{K} a^2 u_j^2 = \frac{1}{K} \sum_{i=1}^{d} a_i^2 u_{ij}^2$

$E[a_i^2 u_{ij}^2] = \frac{1}{2}\cdot 1^2 \cdot a_i^2 + \frac{1}{2}\cdot (-1)^2 \cdot a_i^2 = a_i^2$

$E[b_j^2] = \frac{1}{K} \sum_{i=1}^{d} E[a_i^2 u_{ij}^2] = \frac{1}{K} \sum_{i=1}^{d} a_i^2 = \frac{1}{K} \|a\|^2$

(3) $\|f(a)\|^2 = \sum_{i=1}^{K} b_j^2$

$E[\|f(a)\|^2] = \sum_{i=1}^{K} E[b_j^2] = K \cdot \frac{1}{K} \cdot \|a\|^2 = \|a\|^2$

Exercise 4 *20 points*

In the class, we have seen an algorithm, denoted by $\mathcal{A}$, for the (c,r)-ANN problem with success probability at least 0.6. That is, upon a queried vertex x such that there exists a point a^* in the set $\mathcal{P}$ with $d(x,a^*) \le r$, the algorithm $\mathcal{A}$ outputs some $a \in \mathcal{P}$ with $d(x,a) \le c \cdot r$ with probability at least 0.6.

Let $\delta \in (0,1)$. Using the above $\mathcal{A}$ as a subroutine, give a new algorithm $\mathcal{B}$ with success probability at least $1-\delta$. That is, for the above query vertex x, the algorithm $\mathcal{B}$ outputs some $a \in \mathcal{P}$ with $d(x,a) \le c \cdot r$ with probability at least $1-\delta$. Your algorithm should use as little query time as possible. Explain the correctness of your algorithm and state its query time, assuming the query time of $\mathcal{A}$ is $T_{\mathcal{A}}$.

算法 $\mathcal{B}$:

$$k = \left\lceil \frac{\log \delta}{\log 0.4} \right\rceil$$

```
for i = 1 to k:
    a = A(x)
    if d(x, a) ≤ cr:
        return a
return FAIL
```

(3) $\|f(a)\|^2 = \sum_{j=1}^{k} b_j^2$

$E\|f(a)\|^2 = \sum_{j=1}^{k} E[b_j^2] = k \cdot \frac{1}{k} \cdot \|a\|^2 = \|a\|^2$

证明:

$P(\mathcal{B}$失败$) = P(k$次$\mathcal{A}$均失败$)$

故 $P(\mathcal{B}$成功$) = 1 - [P(\mathcal{A}$失败$)]^k \geqslant 1 - (1-0.6)^k$

将 $k = \dfrac{\log \delta}{\log 0.4}$ 代入, $P(\mathcal{B}$成功$) \geqslant 1 - 0.4 \geqslant 1 - 0.4^{\log_{0.4} \delta} = 1 - \delta$

即算法 $\mathcal{B}$ 将会以至少 $1-\delta$ 的概率成功.

$$T_{\mathcal{B}} = O(k \times T_A) = O\left(T_A \cdot \frac{\log \delta}{\log 0.4}\right)$$

Exercise 5 *20 points*
Let $\alpha \in (0,1]$. Suppose we change the (basic) Morris algorithm to the following:

(a) Initialize $X \leftarrow 0$

(b) For each update, increment X by 1 with probability $\frac{1}{(1+\alpha)^X}$

(c) For a query, output $\tilde{n} = \frac{(1+\alpha)^X - 1}{\alpha}$.

Let X_n denote X in the above algorithm after n updates.

- Calculate $\mathrm{E}[\tilde{n}]$ and upper bound $\mathrm{Var}[\tilde{n}]$.
- Let $\epsilon, \delta \in (0,1)$. Based upon the above algorithm, give a new algorithm such that with probability at least $1-\delta$, it outputs an estimator $\tilde{n}$ such that $|\tilde{n} - n| \le \epsilon n$. Explain the correctness and the space complexity (i.e., the number of bits) of your algorithm. It suffices to give an algorithm with space complexity that is a polynomial function of $1/\delta$.

(1) ① $E[\tilde{n}] = E\left[\frac{(1+\alpha)^{X_n}-1}{\alpha}\right] = \frac{1}{\alpha} E(1+\alpha)^{X_n} - \frac{1}{\alpha}$

下证：$E(1+\alpha)^{X_n} = \alpha n + 1$，$n \in N$

当 $n=0$ 时，$X_0=0$，$E(1+\alpha)^{X_0} = 1$ 成立

设当 $n=k$ 时有 $E(1+\alpha)^{X_k} = \alpha k + 1$，则当 $n=k+1$ 时，有

$$E(1+\alpha)^{X_{k+1}} = \sum_{i=1}^{k} P(X_k = i)\, E[(1+\alpha)^{X_{k+1}} \mid X_k = i]$$

$$= \sum_{i=1}^{k} P(X_k=i)\left[\frac{1}{(1+\alpha)^i}\cdot(1+\alpha)^{i+1} + \left(1-\frac{1}{(1+\alpha)^i}\right)\cdot(1+\alpha)^i\right]$$

$$= \sum_{i=1}^{k} P(X_k=i)\left[(1+\alpha) + (1+\alpha)^i - 1\right]$$

$$= \alpha \sum_{i=1}^{k} P(X_k=i) + \sum_{i=1}^{k}(1+\alpha)^i P(X_k=i)$$

$$= \alpha\cdot 1 + E(1+\alpha)^{X_k}$$

$$= \alpha + \alpha k + 1$$

$$= \alpha(k+1) + 1$$

由数学归纳法，$E(1+\alpha)^{X_n} = \alpha n + 1$，$n \in N$

$\therefore\ E[\tilde{n}] = \frac{1}{\alpha}\cdot(\alpha n + 1) - \frac{1}{\alpha} = n$

② $Var(\tilde{n}) = E[\tilde{n}^2] - (E[\tilde{n}])^2$

$$E[\tilde{n}^2] = E\left[\frac{(1+\alpha)^{X_n}-1}{\alpha}\right]^2 = \frac{1}{\alpha^2} E\left[(1+\alpha)^{2X_n} - 2(1+\alpha)^{X_n} + 1\right]$$

下证：$E(1+\alpha)^{2X_n} = (\frac{1}{2}\alpha^3 + \alpha^2)n^2 + (-\frac{1}{2}\alpha^3 + 2\alpha)n + 1$

当 $n=0$ 时，$X_0=0$，$E(1+\alpha)^{2X_0} = 1$ 成立

设当 $n=k$ 时有 $E(1+\alpha)^{2X_k} = (\frac{1}{2}\alpha^3+\alpha^2)k^2 + (-\frac{1}{2}\alpha^3 + 2\alpha)k + 1$，则当 $n=k+1$ 时，有

$$E(1+\alpha)^{2X_{k+1}} = \sum_{i=0}^{k} P(X_k=i)\, E[(1+\alpha)^{2X_{k+1}} \mid P(X_k=i)]$$

$$= \sum_{i=0}^{k} P(X_k=i)\left[\frac{1}{(1+\alpha)^i}\cdot(1+\alpha)^{2i+2} + \left(1-\frac{1}{(1+\alpha)^i}\right)(1+\alpha)^{2i}\right]$$

$$= \sum_{i=0}^{k} P(X_k=i)\left[(1+\alpha)^{i+2} + (1+\alpha)^i\left((1+\alpha)^i-1\right)\right]$$

$$= \sum_{i=0}^{k} P(X_k=i)\left[(1+\alpha)^{2i} + (1+\alpha)^i(1+2\alpha+\alpha^2-1)\right]$$

$$= \sum_{i=0}^{k}(1+\alpha)^{2i}P(X_k=i) + (\alpha^2+2\alpha)\sum_{i=0}^{k}(1+\alpha)^i P(X_k=i)$$

$$= E(1+\alpha)^{2X_k} + (\alpha^2+2\alpha)E(1+\alpha)^{X_k}$$

$$= (\tfrac{1}{2}\alpha^3+\alpha^2)k^2 + (-\tfrac{1}{2}\alpha^3+2\alpha)k + 1 + (\alpha^2+2\alpha)(\alpha k+1)$$

$$= (\tfrac{1}{2}\alpha^3+\alpha^2)k^2 + (\tfrac{1}{2}\alpha^3+\alpha^2)\cdot 2k + (\tfrac{1}{2}\alpha^3+\alpha^2) + (-\tfrac{1}{2}\alpha^3+2\alpha)k$$
$$+ (-\tfrac{1}{2}\alpha^3+2\alpha) + 1$$

$$= (\tfrac{1}{2}\alpha^3+\alpha^2)(k+1)^2 + (-\tfrac{1}{2}\alpha^3+\alpha^2)(k+1) + 1$$

由数学归纳法，$E(1+\alpha)^{2X_n} = (\frac{1}{2}\alpha^3+\alpha^2)n^2 + (-\frac{1}{2}\alpha^3+2\alpha)n + 1$，$n\in N$

$$\therefore\ E[\hat{n}^2] = \frac{1}{\alpha^2}\cdot E(1+\alpha)^{2X_n} - \frac{2}{\alpha^2}E(1+\alpha)^{X_n} + \frac{1}{\alpha^2}$$

$$= (\tfrac{1}{2}\alpha+1)n^2 + (-\tfrac{1}{2}\alpha+\tfrac{2}{\alpha})n + \frac{1}{\alpha^2} - \frac{2n}{\alpha} - \frac{2}{\alpha^2} + \frac{1}{\alpha^2} = \tfrac{1}{2}\alpha n^2 + n^2 - \tfrac{1}{2}\alpha n$$

$$\therefore\ Var(\hat{n}) = E[\hat{n}^2] - (E[\hat{n}])^2 = \tfrac{1}{2}\alpha n^2 + n^2 - \tfrac{1}{2}\alpha n - n^2$$

$$= \tfrac{1}{2}\alpha n^2 - \tfrac{1}{2}\alpha n = \tfrac{1}{2}\alpha(n^2-n) < \tfrac{1}{2}\alpha n^2 = O(n^2)$$

(2)

新算法：

1. 独立运行 s 次上述算法，设这 s 个输出分别为 $\hat{n}_1, \hat{n}_2, \cdots, \hat{n}_s$
2. 输出 $\hat{n} = \frac{1}{s}\sum_{i=1}^{s}\hat{n}_i$

正确性：

$$E[\hat{n}] = E\left[\frac{1}{s}\sum_{i=1}^{s}\hat{n}_i\right] = \frac{1}{s}\cdot\sum_{i=1}^{s}E\hat{n}_i = \frac{1}{s}\cdot ns = n$$

$$Var[\hat{n}] = Var\left[\frac{1}{s}\sum_{i=1}^{s}\hat{n}_i\right] = \frac{1}{s^2}\cdot\sum_{i=1}^{s}Var[\hat{n}_i] < \frac{1}{s^2}\cdot s\cdot\frac{1}{2}\alpha n^2 = \frac{\alpha n^2}{2s}$$

由 chebyshev's 不等式，$P[|\hat{n}-n| > \varepsilon n] \le \frac{Var[\hat{n}]}{\varepsilon^2 n^2} < \frac{\frac{\alpha n^2}{2s}}{\varepsilon^2 n^2} = \frac{\alpha}{2s\varepsilon^2}$

只要 $\frac{\alpha}{2s\varepsilon^2} \le \delta$，即 $s \ge \frac{\alpha}{2\delta\varepsilon^2}$，则新算法以至少 $1-\delta$ 的概率输出 $\hat{n}$ s.t. $|\hat{n}-n| \le \varepsilon n$.

空间复杂度：

当相对误差超过 ε 的概率不足 δ 时，新算法调用了 $s = \Theta(\frac{1}{\delta\varepsilon^2})$ 次悬浮算法，

假设悬浮算法在过程中达到了 $X = \log_{(1+\alpha)}(\frac{sn}{\delta'})$，那么它再增加一次的概率是 $\frac{1}{(1+\alpha)^X} \le \frac{\delta'}{sn}$

$\because$ X总共只有 n 次机会增加，$\therefore$ X在算法结束时至多 $\frac{n}{(1+\alpha)^X} \le \frac{\delta'}{s}$ 的概率增加。

总共有 s 个悬浮算法，至多有 s 个数达到了 $\log_{(1+\alpha)}(\frac{sn}{\delta'})$ 随时准备突破。

$\therefore$ 在算法结束时有至多 δ' 的概率某个悬浮算法的 X 超过 $\log_{(1+\alpha)}(\frac{sn}{\delta'})$ 了，

这就表明有至少 $1-\delta'$ 的概率所有达到过临界值 $\log_{(1+\alpha)}(\frac{sn}{\delta'})$ 的 X 都不会再增长了。

也就表明有至少 $1-\delta'$ 的概率所有悬浮算法中的 X 都不超过 $\log_{(1+\alpha)}(\frac{sn}{\delta'})$

则新算法以至少 $1-\delta'$ 的概率空间复杂度为 $O(s \log\log_{(1+\alpha)}(\frac{sn}{\delta'}))$

$$= O\left(\frac{1}{\delta\varepsilon^2} \log\log_{(1+\alpha)}\left(\frac{n}{\delta\varepsilon^2\delta'}\right)\right)$$

Exercise 6 *Bonus 10 points*

Recall that in the class (see Lecture note 7), we have seen one algorithm based on dimension reduction for solving (c, r)-ANN problem.

Let $0 < p \le \frac{1}{2}$. Prove that for any $x, y \in \{0,1\}^d$, it holds that

$$\Pr[(Ux)_i \neq (Uy)_i] = \frac{1}{2}\left(1 - (1-2p)^{\mathrm{Ham}(x,y)}\right),$$

where U is a $k \times d$ random matrix such that the entries are independently and identically distributed (i.i.d.) as follows:

$$u_{ij} = \begin{cases} 1 & \text{with probability } p, \\ 0 & \text{with probability } 1-p, \end{cases}$$

and all the calculations are in the finite field $GF(2)$ (i.e., addition and multiplication are always modulo 2).

Hint: You may consider to use the following fact: Let $w \in \{0,1\}^d$ be a random vector such that all entries w_i's are i.i.d. and $\Pr[w_i = 1] = \Pr[w_i = 0] = \frac{1}{2}$ for each $i \le d$. Then $\Pr[w^\top x \neq w^\top y] = \frac{1}{2}$.

$$(Ux)_i = \left(\sum_{j=1}^{d} u_{ij} x_j\right) \bmod 2$$

$$(Uy)_i = \left(\sum_{j=1}^{d} u_{ij} y_j\right) \bmod 2$$

对 x,y 中从 $j=1,\cdots d$ $\mathrm{Ham}(x,y)$ 改变的位置进行归纳，

当 $\mathrm{Ham}(x,y)=1$ 时，$\Pr[(Ux)_i \neq (Uy)_i] = p = \frac{1}{2}(1-(1-2p)^1)$

设当 $\mathrm{Ham}(x,y)=k$ 时，有 $\Pr[(Ux)_i \neq (Uy)_i] = \frac{1}{2}(1-(1-2p)^k)$

则当 $\mathrm{Ham}(x,y)=k+1$ 时，

$\Pr[(\sum_{j=1}^{k+1} u_{ij} x_j) \bmod 2 \neq (\sum_{j=1}^{k+1} u_{ij} y_j) \bmod 2]$

$$= \Pr[x_{k+1} \neq y_{k+1}] \Pr[(\sum_{j=1}^{k+1} u_{ij} x_j) \bmod 2 \neq (\sum_{j=1}^{k+1} u_{ij} y_j) \bmod 2 \mid x_{k+1} \neq y_{k+1}]$$

$$+ \Pr[x_{k+1} \neq y_{k+1}] \Pr[(\sum_{j=1}^{k+1} u_{ij} x_j) \bmod 2 = (\sum_{j=1}^{k+1} u_{ij} y_j) \bmod 2 \mid x_{k+1} \neq y_{k+1}]$$

$$= \frac{1}{2}(1 - (1-2p)^k)(1-p) + \left(1 - \frac{1}{2}(1-(1-2p)^k)\right) p$$

$$= \frac{1}{2}(1-p) - \frac{1}{2}(1-2p)^k(1-p) + p - \frac{1}{2}p + \frac{1}{2}(1-2p)^k p$$

$$= \frac{1}{2} - \frac{1}{2}(1-2p)^k(1-p-p)$$

$$= \frac{1}{2}(1 - (1-2p)^{k+1})$$

则 $\Pr[(Ux)_i \neq (Uy)_i] = \frac{1}{2}(1-(1-2p)^{Ham(x,y)})$ 成立.

$= \frac{1}{2}\left[\frac{1}{2}(1-(1-2p)^k)\cdot\frac{1}{2}\right.$

对 x, y 从 $j=1,\cdots,d$ 进行数学归纳法

$j=1$: 若 $x_1 = y_1$, 则 $u_{i1}x_1 \neq u_{i1}y_1 = \frac{1}{2}\cdot p(1-p)$

若 $x_1 \neq y_1$, 则 $u_{i1}x_1 \neq u_{i1}y_1 = p = \frac{1}{2}(1-(1-2p)^1)$

$= \frac{1}{2}\cdot\Big[P[(\sum_{j=1}^{k} u_{ij}x_j) \bmod 2 = (\sum_{j=1}^{k} u_{ij}x_j) \bmod 2]\cdot(1-p)$

$P[(\sum_{j=1}^{k} u_{ij}x_j) \bmod 2 \neq (\sum_{j=1}^{k} u_{ij}x_j) \bmod 2]\cdot p\Big]$

不相等 k+1 相同 相等 k+1 不同

$\frac{1}{2}(1-(1-2p)^k)$

1 0 0

0 1 1

为1的 必 乘 0 $1-p$

$(1-p)^2+p^2$

k+1 同 $\frac{1}{2}$ (为1 的 次 乘 1^k) $p(1-p)$

$p(1-p)$

k+1 不同 $\left[1-\frac{1}{2}(1-(1-2p)^k)\right]\cdot p\ ]$

$\frac{1}{2}(1-p) - \frac{1}{2}(1-2p)^k(1-p)$

$+\ p - \frac{1}{2}p + \frac{1}{2}(1-2p)^k p$

$\frac{1}{2} - \cancel{\frac{1}{2}p} - \frac{1}{2}(1-2p)^k(1-2p)\ \cancel{+p-\frac{1}{2}p}$

前K位	K+1位	前K+1位不同需乘上
同	不同	p
同	同	$p(1-p)$
不同	不同	$1-p$
不同	同	$p^2+(1-p)^2$