数据隐私HW1

范翔宇 PB18000006

A1

recursive(c,l)-diversity即r_1<c(r_l+r_{l+1}+...+r_m)，而其中概率r_k对应于数据s_k，且r_1>r_2>...>r_m。该式确保了概率较大的数据出现的概率如r_1不会过大，也确保了概率较小的数据出现的概率如r_m等也不会过小，达到了一个balance的目的。该式的实际意义将各数据分为s_1，s_2，...，s_{l-1}和s_l+s_{l+1}...+s_m共l类，并且其中每类的概率之间也不会相差太大，那么这样攻击者在试图利用概率攻击时便会遇到阻碍。允许攻击者最多拥有l-2条类似"Bob does not have heart disease"的背景知识，是因为攻击者最多依靠这些背景知识从s_1，s_2，...，s_{l-1}和s_l+s_{l+1}...+s_m中排除(l-2)类数据，即最少也会剩下两种概率相差不大的数据让攻击者难以抉择。因此，recursive(c,l)-diversity可以防范最多有l-2条类似"Bob does not have heart disease"的背景知识的攻击者。

A2

分类讨论：

①将Race泛化到R_0，ZipCode泛化到Z_0，即都不泛化(泛化到$R_0, Z0$意义下同)，题目已经讨论论过，在这不赘述，不符合题意。

②将Race泛化到R_1，ZipCode泛化到Z_0，则得下表

Race:R_1	**ZipCode:**Z_0
person	**94138**
person	**94138**
person	**94138**
person	**94138**
person	*94142*
person	*94142*
person	*94142*

其中为达到2匿名，要suppress ZipCode = 94141的记录，MaxSup = 1，符合题意。

③将Race泛化到 R_0，ZipCode泛化到Z_1，得到下表

Race: R_0	ZipCode: Z_1
asian	**9413***
asian	**9413***
asian	*9414**
asian	*9414**
black	**9414***
black	**9414***

其中为达到2匿名，要suppress Race = white的记录和Race = black同时ZipCode = 94138的记录，MaxSup = 2，不符合题意。

④将Race泛化到R_1，ZipCode泛化到Z_1，得到下表(version_1)

Race: R_1	ZipCode: Z_1
person	**9413***
person	**9413***
person	**9413***
person	**9413***
person	*9414**
person	*9414**
person	*9414**
person	*9414**

其中为达到2匿名，不需要Suppress，符合题意。那么也就意味着可以多Suppress一条记录，来达到更多的可能性。

⑤将Race泛化到R_1，ZipCode泛化到Z_1，得到下表(version_2)

Race:R_1	ZipCode:Z_1
person	**9413***
person	**9413***
person	**9413***
person	**9413***
person	*9414**
person	*9414**
person	*9414**

其实与④类似，但是其中为达到2匿名，Suppress了一条ZipCode = 9414*的记录，MaxSup = 1，符合题意。

⑥将Race泛化到R_1，ZipCode泛化到Z_1，得到下表(verison_3)

Race:R_1	ZipCode:Z_1
person	**9413***
person	**9413***
person	**9413***
person	*9414**
person	*9414**
person	*9414**
person	*9414**

其实与④类似，但是其中为达到2匿名，Suppress了一条ZipCode = 9413*的记录，MaxSup = 1，符合题意。

⑦将Race泛化到R_0，ZipCode泛化到Z_2，得到下表

Race:R_0	**ZipCode:**Z_2
asian	**941****
asian	**941****
asian	**941****
asian	**941****
black	*941***
black	*941***
black	*941***

其中为达到2匿名，要suppress Race = white的记录，MaxSup = 1，符合题意。

⑧将Race泛化到R_1，ZipCode泛化到Z_2，得到下表(version_1)

Race:R_1	**ZipCode:**Z_2
person	**941****
person	**941****
person	**941****
person	**941****
person	**941****
person	**941****
person	**941****
person	**941****

其中为达到2匿名，不需要Suppress，符合题意。那么也就意味着可以多Suppress一条记录，来达到更多的可能性。

⑨将Race泛化到R_1，ZipCode泛化到Z_2，得到下表(version_2)

Race:R_1	**ZipCode:**Z_2
person	**941****
person	**941****
person	**941****
person	**941****
person	**941****
person	**941****
person	**941****

其中为达到2匿名，可以Suppress一条ZipCode = 941**的记录，MaxSup = 1符合题意。

综上，为满足2匿名，有②④⑤⑥⑦⑧⑨共七种可能性。

A3

首先对于总体，有如下分布Q，其中Q(Salary = ik) = $\frac{1}{9}$，其中i = 3，4，5，6，7，8，9，10，11。

对于第一个等价类，分布为P_1(Salary = ak) = $\frac{1}{3}$，其中a = 3，5，9；

当然对于P_1(Salary = bk) = 0，其中b = 4，6，7，8，10，11。

根据公式ri = pi - qi(i = 1，2，...， m)，按顺序求得：

r1 = p1 - q1 = P_1(Salary = 3k) - Q(Salary = 3k) = $\frac{2}{9}$；

r2 = p2 - q2 = P_1(Salary = 4k) - Q(Salary = 4k) = -$\frac{1}{9}$；

r3 = p3 - q3 = P_1(Salary = 5k) - Q(Salary = 5k) = $\frac{2}{9}$；

r4 = p4 - q4 = P_1(Salary = 6k) - Q(Salary = 6k) = -$\frac{1}{9}$；

r5 = p5 - q5 = P_1(Salary = 7k) - Q(Salary = 7k) = -$\frac{1}{9}$；

r6 = p6 - q6 = P_1(Salary = 8k) - Q(Salary = 8k) = -$\frac{1}{9}$；

r7 = p7 - q7 = P_1(Salary = 9k) - Q(Salary = 9k) = $\frac{2}{9}$；

r8 = p8 - q8 = P_1(Salary = 10k) - Q(Salary = 10k) = -$\frac{1}{9}$；

r9 = p9 - q9 = P_1(Salary = 11k) - Q(Salary = 11k) = -$\frac{1}{9}$

而EMD的公式为D[P,Q] = $\frac{1}{m-1}\Sigma_{i=1}^{m}|\Sigma_{j=1}^{i}$rj|

代入即有D[P_1,Q] = $\frac{1}{8}${|$\frac{2}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$| + |$\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$|} = $\frac{1}{6}$

对于第二个等价类分析同上，不过P_2(Salary = ak) = $\frac{1}{3}$，其中的a变为6，8，11；其余概率为0。

代入之后求得{r1，r2，r3，r4，r5，r6，r7，r8，r9} = {-$\frac{1}{9}$，-$\frac{1}{9}$，-$\frac{1}{9}$，$\frac{2}{9}$，-$\frac{1}{9}$，$\frac{2}{9}$，-$\frac{1}{9}$，-$\frac{1}{9}$，$\frac{2}{9}$}

代入即有D[P_2,Q] = $\frac{1}{8}${|-$\frac{1}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$|} = $\frac{1}{6}$

对于第三个等价类分析同上，不过P_3(Salary = ak) = $\frac{1}{3}$，其中的a变为4，7，10；其余概率为0。

代入之后求得{r1，r2，r3，r4，r5，r6，r7，r8，r9} = {-$\frac{1}{9}$，$\frac{2}{9}$，-$\frac{1}{9}$，-$\frac{1}{9}$，$\frac{2}{9}$，-$\frac{1}{9}$，-$\frac{1}{9}$，$\frac{2}{9}$，-$\frac{1}{9}$}

代入即有D[P_3,Q] = $\frac{1}{8}${|-$\frac{1}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$| + |-$\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$ - $\frac{1}{9}$ + $\frac{2}{9}$ - $\frac{1}{9}$|} = $\frac{1}{12}$

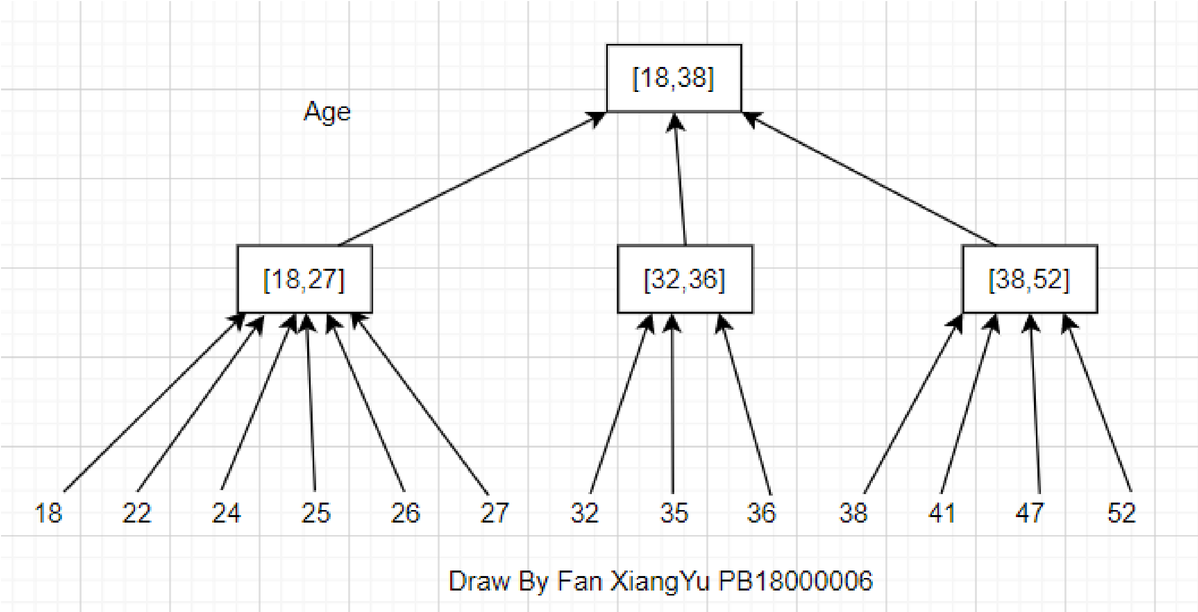
则t = max{D[P_1,Q]，D[P_2,Q]，D[P_3,Q]} = max{$\frac{1}{6}$，$\frac{1}{6}$，$\frac{1}{12}$} = $\frac{1}{6}$

A4

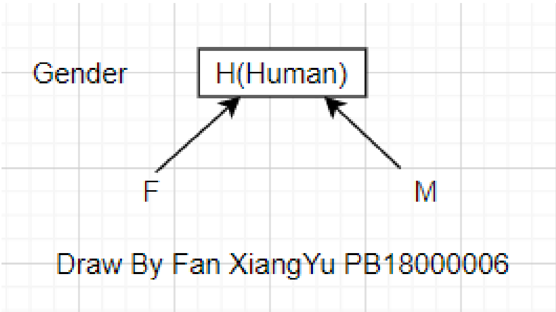
(a)Age，Gender，Nationality，Salary

(b)generalization hierarchies

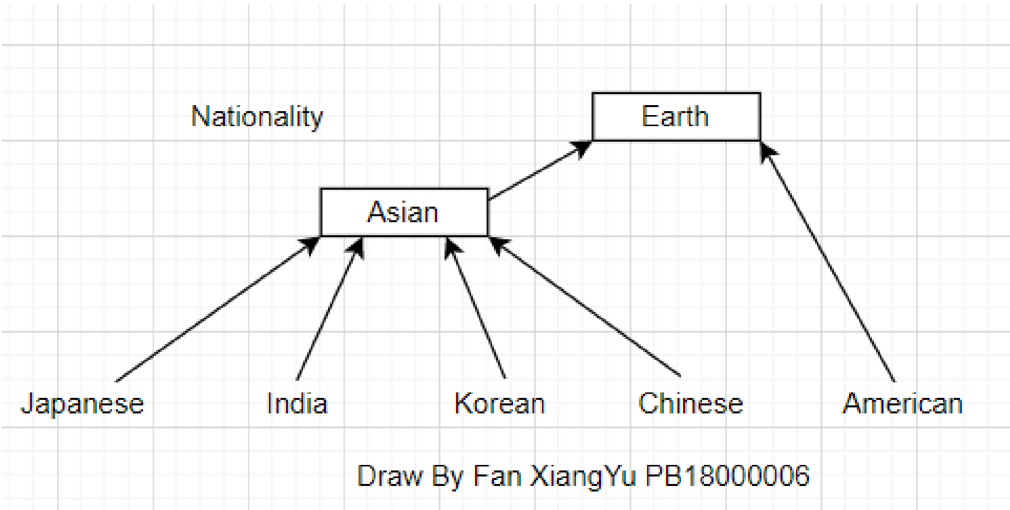
Age:



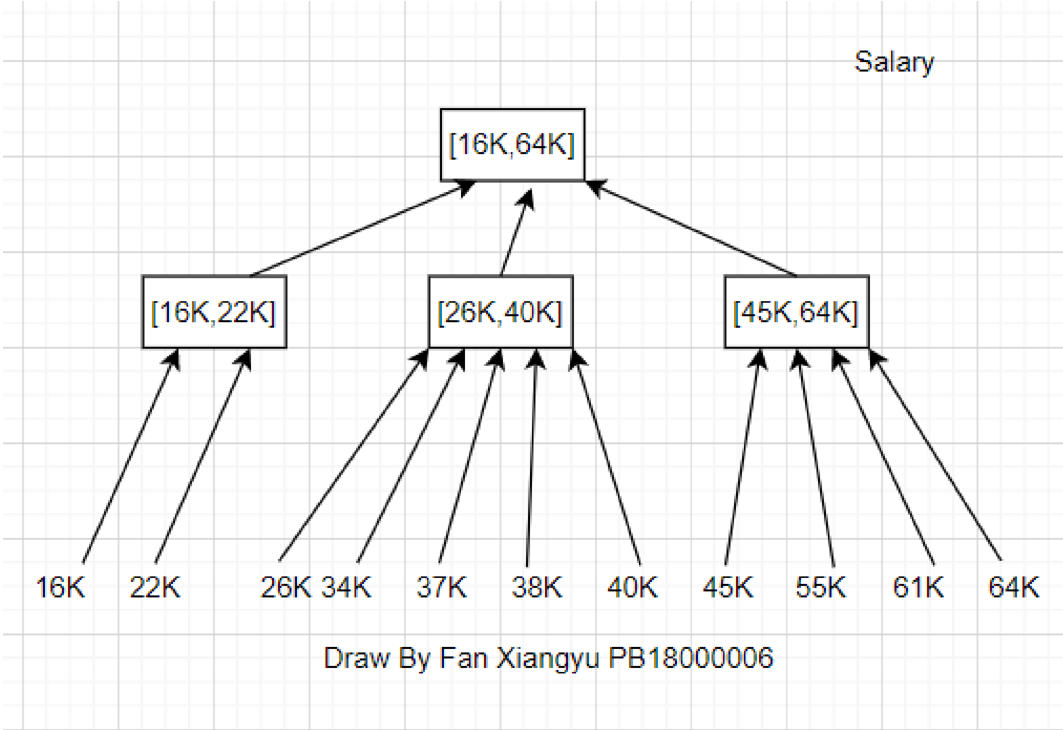
Gender:



Nationality:



Salary:



泛化后即得的最后结果即:

Age	Gender	Nationality	Salary
[18,27]	**H**	**American**	**[16K,22K]**
[18,27]	**H**	**American**	**[16K,22K]**
[18,27]	*H*	*American*	*[26K,40K]*
[18,27]	*H*	*American*	*[26K,40K]*
[18,27]	**H**	**Asian**	**[26K,40K]**
[18,27]	**H**	**Asian**	**[26K,40K]**
[32,36]	*H*	*Asian*	*[26K,40K]*
[32,36]	*H*	*Asian*	*[26K,40K]*
[32,36]	*H*	*Asian*	*[26K,40K]*
[38,52]	**H**	**Asian**	**[45K,64K]**
[38,52]	**H**	**Asian**	**[45K,64K]**
[38,52]	*H*	*American*	*[45K,64K]*
[38,52]	*H*	*American*	*[45K,64K]*

calculation of the loss metric:

Age: LM = $\frac{6\times(27-18)+3\times(36-32)+4\times(52-38)}{13\times(52-18)} = \frac{61}{221} \approx 0.276$;

Gender: LM = 1(F和M全部泛化为H);

Nationality:LM = $\frac{6\times0+7\times\frac{3}{4}}{13} = \frac{21}{52} \approx 0.404$;

Salary: LM = $\frac{2\times(22K-16K)+7\times(40K-26K)+4\times(64K-45K)}{13\times(64K-16K)} = \frac{31}{104} \approx 0.298$;

ALL: LM = Σ(part LM) = 0.276 + 1 + 0.404 + 0.298 = 1.978

(c)可以像第二题一样对generalization hierarchies 穷举并且计算对应的LM，找出在满足条件的同时LM最优的情况。也可以基于LM的大小像实验那样结合generalization hierarchies 进行二分查找。

A5

(a)先验概率：P(X=0) = 0.01，P(X∈[200,800]) = (800-200+1) × 0.00099 = 0.59499。

后验概率:

对于x = 0的情况

method(a)，结合贝叶斯公式: P(R_1(X) = 0 | X = 0) = 0.2，P(R_1(x) = 0 | X $\neq$ 0) = 0.8×0.001 = 0.0008；

P(X = 0 | R_1(X) = 0) = $\frac{P(X=0,R_1(X)=0)}{P(R_1(X)=0)}$ = $\frac{P(R_1(X)=0|X=0)P(X=0)}{P(R_1(X)=0)}$

= $\frac{P(R_1(X)=0|X=0)P(X=0)}{P(R_1(X)=0|X=0)P(X=0)+P(R_1(X)=0|X\neq 0)P(X\neq 0)}$

=$\frac{0.2\times 0.01}{0.2\times 0.01+0.0008\times(1-0.01)}$

= 0.716

method(b)： P(R_2(X) = 0 | X $\in$ [0,100] $\cup$ [901,1000]) = $\frac{1}{(100-0+1)+(1000-901+1)}$ = 0.00498；

P(R_2(X) = 0 | X∈[101,900]) = 0；

P(X = 0 | R_2(X)=0) = $\frac{P(X=0,R_2(X)=0)}{P(R_2(X)=0)}$ =

$$\frac{P(R_2(X)=0|X=0)P(X=0)}{P(R_2(X)=0|X=0)P(X=0)+P(R_2(X)=0|X\in[1,100]\cup[901,1000])P(X\in[1,100]\cup[901,1000])+P(R_2(X)=0|X\in[101,900])P(X\in[101,900])}$$

= $\frac{0.00498\times 0.01}{0.00498\times 0.01+0.00498\times 0.00099\times 200+0}$

= 0.048

method(c): 令"a uniformly random number in {0; · · · ; 1000}"为C。

则

P($R_3(X)$ = 0 | X $\in$ [0,100] $\cup$ [901,1000]) = P(R_3(X) $\rightarrow$ R_2(X), R_2(X)=0 | X $\in$ [0,100] $\cup$ [901,1000])

+P(R_3(X) $\rightarrow$ C, C = 0 | X $\in$ [0,100] $\cup$ [901,1000]) = 0.5 × 0.00498 + 0.5 × $\frac{1}{1000-0+1}$ = 0.00299

P($R_3(X)$ = 0 | X $\in$ [101,900]) = P(R_3(X) $\rightarrow$ R_2(X), R_2(X)=0 | X $\in$ [101,900])

+P(R_3(X) $\rightarrow$ C, C = 0 | X $\in$ [101,900]) = 0.5 × 0 + 0.5 × $\frac{1}{1000-0+1}$ = 0.0004995

P(X = 0 | R_3(X) = 0) = $\frac{P(X=0,R_3(X)=0)}{P(R_3(X)=0)}$ =

$$\frac{P(R_3(X)=0|X=0)P(X=0)}{P(R_3(X)=0|X=0)P(X=0)+P(R_3(X)=0|X\in[1,100]\cup[901,1000])P(X\in[1,100]\cup[901,1000])+P(R_3(X)=0|X\in[101,900])P(X\in[101,900])}$$

= $\frac{0.00299\times 0.01}{0.0029\times 0.01+0.00299\times 0.00099\times 200+0.0004995\times 0.00099\times 800}$

= 0.0294

对于x∈[200,800]，进行同上的分析，但是这里分母的概率P(R_n(X) = 0)为了简便都沿用x=0的计算。

method(a): P(X $\in$ [200,800] | R_1(X) = 0) = $\frac{P(X\in[200,800],R_1(x)=0)}{P(R_1(X)=0)}$ =

$$\frac{P(R_1(X)=0|X\in[200,800])P(X\in[200,800])}{P(R_1(X=0))}$$

= $\frac{P(R_1(X)=0|X\in[200,800])P(X\in[200,800])}{P(R_1(X)=0|X=0)P(X=0)+P(R_1(X)=0|X\neq 0)P(X\neq 0)}$

= $\frac{(0.8\times0.001)\times0.59499}{0.2\times0.01+0.0008\times(1-0.01)}$

= 0.171

method(b): P(X∈[200,800] | R_2(X) = 0) = $\frac{P(X\in[200,800],R_2(X)=0)}{P(R_2(X)=0)}$ =

$$\frac{P(R_2(X)=0|X\in[200,800])P(X\in[200,800])}{P(R_2(X)=0|X=0)P(X=0)+P(R_2(X)=0|X\in[1,100]\cup[901,1000])P(X\in[1,100]\cup[901,1000])+P(R_2(X)=0|X\in[101,900])P(X\in[101,900])}$$

= $\frac{0\times0.59499}{0.00498\times0.01+0.00498\times0.00099\times200+0}$

= 0

method(c): P(X ∈ [200,800] | R_3(X) = 0) = $\frac{P(X\in[200,800],R_3(X)=0)}{P(R_3(X)=0)}$ =

$$\frac{P(R_3(X)=0|X\in[200,800])P(X\in[200,800])}{P(R_3(X)=0|X=0)P(X=0)+P(R_3(X)=0|X\in[1,100]\cup[901,1000])P(X\in[1,100]\cup[901,1000])+P(R_3(X)=0|X\in[101,900])P(X\in[101,900])}$$

= $\frac{0.0004995\times0.59499}{0.0029\times0.01+0.00299\times0.00099\times200+0.0004995\times0.00099\times800}$

= 0.292

(b)评价method的Information Gain = P(X | R_i(X)-P(X))，算得方案c的最小，即method c最好。

A6

(a)当$P_f(\Phi(U)) \le \alpha$时

$P_f(\Phi(U)|R(U)=v)$ = $\Sigma_{u\in\Phi^{-1}} P_f(U=u|R(U)=v)$ = $\Sigma_{u\in\Phi^{-1}} \frac{P_f(U=u,R(U)=v))}{P_f(R(U)=v)}$ = $\Sigma_{u\in\Phi^{-1}} \frac{P_f(R(U)=v|U=u)P_f(U=u)}{P_f(R(U)=v)}$

= $\Sigma_{u\in\Phi^{-1}} \frac{P(R(u)=v)P_f(U=u)}{P_f(R(U)=v)}$ = $\frac{1}{P_f(R(U)=v)}$ $\Sigma_{u\in\Phi^{-1}} P(R(u)=v)P_f(U=u)$

取$u_1 = arg\, max_{u\in\Phi^{-1}} P(R(u)=v)$，那么即有

$P_f(\Phi(U)|R(U)=v) \le \frac{P(R(u_1)=v)}{P_f(R(U)=v)}\Sigma_{u\in\Phi} P_f(U=u)$ = $\frac{P(R(u_1)=v)}{P_f(R(U)=v)} P_f(\Phi(U))$，记为式a。

同理可得

取$u_2 = arg\, min_{u\in\Phi^{-1}} P(R(u)=v)$

$P_f(\overline{\Phi}(U)|R(U)=v) \ge \frac{P(R(u_2)=v)}{P_f(R(U)=v)} P_f(\overline{\Phi}(U))$，记为式b。

进一步得

$\frac{式a}{式b} = \frac{P_f(\Phi(U)|R(U)=v)}{1-P_f(\Phi(U)|R(U)=v)} \le \frac{P(R(u_1)=v)P_f(\Phi(U))}{P(R(u_2)=v)P_f(\overline{\Phi}(U))} \le \gamma\frac{\alpha}{1-\alpha}$

可以推得

$P_f(\Phi(U)|R(U)=v) \le \frac{\alpha\gamma}{\alpha\gamma+(1-\alpha)} = \beta$

即不存在upward(α,β)-privacy breach。

同理，当$P_f(\Phi(U)) \ge \beta$时，也不存在downwar(α,β)-privacy breach。