密码工程原理	2020 年 3 月 2 日
作业 2	
教师: 陈小明	*Due: Mar. 02, 2020*

Problem 1 (设) ( ) 分

随机向量 $\xi = (\xi_1, \cdots, \xi_n)$ 是 $\{0,1\}^n$ 上均匀分布的充要条件是 $\xi_1, \cdots, \xi_n$ 是 i.i.d.

Problem 2 (两两独立随机变量) () 分

3 维随机向量 $E = (E_1, E_2, E_3)$, 它在 $\{0,1\}^3$ 上的分布如下（表中 V4 以下向量的概率为 0）

E	E_1	E_2	E_3	P
v_1	0	0	0	1/4
v_2	0	1	1	1/4
v_3	1	0	1	1/4
v_4	1	1	0	1/4
v_5	X	X	X	0

回答下列问题:

1. E_1, E_2, E_3 是等概（均匀）分布吗?
2. E_1, E_2, E_3 是两两独立的吗?
3. E_1, E_2, E_3 是 i.i.d. 吗?
4. 修改该表使 E_1, E_3, E_3 为 i.i.d..

Problem 3 (变号点个数的概率分布) () 分

设 $\varepsilon = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_{n+1}$ 是 i.i.d., 定义 $\chi(\varepsilon_i) = \varepsilon_i \oplus \varepsilon_{i+1}$, 即 $\varepsilon_i = 1$ 表示在第 i 位置, 后面的比特发生反转 (与 ε 不一样). 设 $\xi = \Sigma_{i=1}^{n} \chi(\varepsilon_i)$.

1. ξ 是什么分布?

2. $\varepsilon = 1100100100001111110110101010001000100001011010001 1$
$000010001101001100010011000110011000101000101110 00,$
计算观察值和 P 值（借助 refc 函数的程序）。

3. 取 $\alpha = 0.01$, 拒绝还是接受"ε 是 i.i.d. 样本"？

Problem 4 (余差函数) () 分

设 $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$ 是标准正态分布的分布函数，定义余差函数 $refc(z) = \frac{2}{\sqrt{\pi}} \int_{z}^{\infty} e^{-u^2} du.$
证明 $\mathbb{P}(|x| > c) = \frac{1}{2} refc\left(\frac{c}{\sqrt{2}}\right)$

Problem 5 (不完全 Γ 函数) () 分

记 $\Gamma(a,z) = \int_{z}^{\infty} t^{a-1} e^{-t} dt, \Gamma(a) = \Gamma(a,0)$
$F(z) = \int_0^z \frac{1}{2^{n/2}\Gamma(\frac{n}{2})} x^{\frac{n}{2}-1} e^{-\frac{x}{2}} dx = \frac{1}{2^{n/2}\Gamma(\frac{n}{2})} \int_0^z x^{\frac{n}{2}-1} e^{-\frac{x}{2}} dx$ 是 χ^2 分布的分布函数，
不完全 Γ 函数定义为：$Q(a,y) = \frac{1}{\Gamma(a)} \int_{y}^{\infty} t^{a-1} e^{-t} dt.$
证明 $\mathbb{P}(x > c) = Q(n/2, z/2)$

Problem 6 (设计 χ^2 检验项目) () 分

1. 从 $0, 1, \cdots, 2^n - 1$ 中随机取一个数, 取完后放回. 独立重复这个过程 k 次, 求事件 A_m:"此 k 个数中最大的数是 m"的概率 $p_m(m \le 2^n - 1)$.(提示：$p_m = \frac{m^k - (m-1)^k}{(2^n-1)^k}$)

2. 根据上面的概率计算，设计一个随机性检验项目。要求：

   (a) 选定参数 n 和 k.

   (b) 写出检测算法过程，包括观察值的计算过程。

   (c) 说明确定 P 值的过程（借助不完全 Γ 函数）。

3. 选自己熟悉的语言和计算环境, 考虑编程实现所设计的检验项目, 为实验课做准备（返校后开始实验课）.