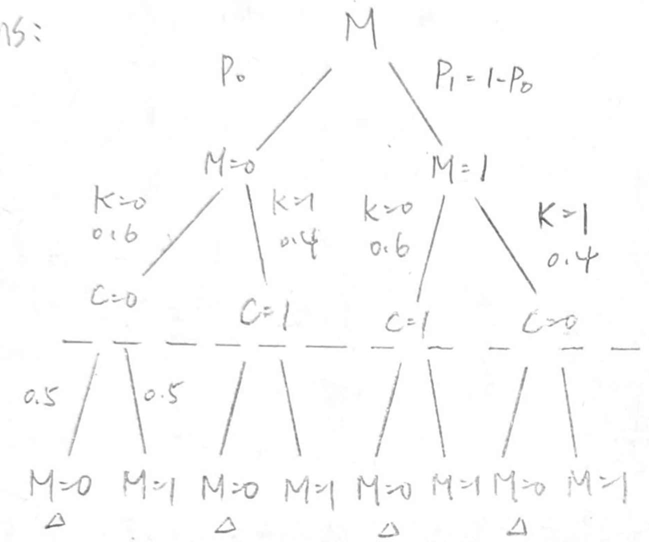
Homework 1

游鎮遠 111061548

1.(a) $Pr[M=b] = P_b$, $b \in [0,1]$, $Pr[K=0] = 0.6$, $Pr[K=1] = 0.4$

Ans:



$Pr[M=0]$

$= P_0 \times 0.6 \times 0.5 + P_0 \times 0.4 \times 0.5$
$+ (1-P_0) \times 0.6 \times 0.5 + (1-P_0) \times 0.4 \times 0.5$

$= 0.5P_0 \times \cancel{(0.6+0.4)}$
$+ 0.5(1-P_0) \times \cancel{(0.6+0.4)}$

$= 0.5(\cancel{P_0} + 1 - \cancel{P_0}) = 0.5$ #

1.(b)
Ans:

$$Pr[M=0 \mid C=0] = \frac{Pr[C=0 \mid M=0] \times Pr[M=0]}{Pr[C=0]}$$

$$= \frac{0.6P_0}{0.6P_0 + 0.4P_1}$$

$$Pr[M=0 \mid C=1] = \frac{0.4P_0}{0.4P_0 + 0.6P_1}$$

$$Pr[M=1 \mid C=0] = \frac{0.4P_1}{0.6P_0 + 0.4P_1}$$

$$Pr[M=1 \mid C=1] = \frac{0.6P_1}{0.4P_0 + 0.6P_1} .$$

When $C=0$, if $0.6P_0 > 0.4P_1$, A_2 guess $M=0$,
elif $0.6P_0 < 0.4P_1$, A_2 guess $M=1$,

When $C=1$, if $0.4P_0 > 0.6P_1$, A_2 guess $M=0$,
elif $0.4P_0 < 0.6P_1$, A_2 guess $M=1$

#

2.(a) Ans:

```
def gcd(a,b)
    if a==b:
        return a
    elif a>b:
        gcd(a-b,b)
    elif a<b:
        gcd(a,b-a)
```

---

or

```
def gcd(a,b)
    if a%b ==0
        return b
    else:
        gcd(b,a%b)
```

---

or

```
def gcd(a,b)
    while (b!=0):
        a = a mod b
        Swap(a,b)
    return a
```

$m = len(a) + len(b)$,

In each iteration, $a = a \bmod b$ will a least reduce one bit, so the worst case of while-loop is to take $len(a)+len(b)$ times of iterations,

and the computation time of $a = a \bmod b$ is $O((len(a)-len(b)+1) \times len(b))$, the swapping is $O(len(a)+len(b))$,

so the computation time of whole gcd algorithm is $(len(a)+len(b)) \times O((len(a)-len(b)+1) \times len(b) + len(a) + len(b))$

$= m \times O(m^2+m) = O(m^3+m^2) = O(m^3)$,

which is polynomial time of m.

2. (b)

$r \times 128 + s \times 54 = 2. = \gcd(128, 54)$

Ans:

$$
\begin{aligned}
128 &= 2 \times 54 + 20 \\
54 &= 2 \times 20 + 14 \\
20 &= 1 \times 14 + 6 \\
14 &= 2 \times 6 + 2 \\
6 &= 3 \times 2 + 0
\end{aligned}
$$

$$
\begin{aligned}
2 &= 14 - 2 \times 6 \\
&= 14 - 2 \times (20 - 1 \times 14) \\
&= (54 - 2 \times 20) - 2 \times (20 - (54 - 2 \times 20)) \\
&= (54 - 2 \times (128 - 2 \times 54)) - 2 \times ((128 - 2 \times 54) - (54 - 2 \times (128 - 2 \times 54))) \\
&= 54 - 2 \times 128 + 4 \times 54 - 6 \times 128 + 14 \times 54 \\
&= 19 \times 54 - 8 \times 128
\end{aligned}
$$

$\therefore\ r = -8,\ s = 19$ #

3. $f(x) = x^{-1} \bmod x^8 + x^4 + x^3 + x + 1$,

$f(11110100l)$ is $x^7 + x^6 + x^5 + x^3 + 1$ under $GF(2^8)$

Ans: compute $\gcd(x^8 + x^4 + x^3 + x + 1,\ x^7 + x^6 + x^5 + x^3 + 1)$

$$
\begin{aligned}
x^8+x^4+x^3+x+1 &= (x^7+x^6+x^5+x^3+1) \times (x+1) &&+ x^5 \\
x^7+x^6+x^5+x^3+1 &= x^5 \times (x^2+x+1) &&+ x^3+1 \\
x^5 &= (x^3+1) \times x^2 &&+ x^2 \\
x^3+1 &= x^2 \times x &&+ 1
\end{aligned}
$$

---

let $x^8 + x^4 + x^3 + x + 1 = A$

$x^7 + x^6 + x^5 + x^3 + 1 = B$

$$
\begin{aligned}
1 &= (x^3+1) - (x^2 x) \\
&= (B - x^5(x^2+x+1)) - ((x^5 - (x^3+1)x^2)x) \\
&= (B - x^5(x^2+x+1)) - ((x^5 - (B - x^5(x^2+x+1))x^2)x)
\end{aligned}
$$

let $x^5 = C = A - B(x+1)$

$$
\begin{aligned}
&\Rightarrow (B - C(x^2+x+1)) - ((C - (B - \underline{C(x^2+x+1)})x^2)x) \\
&= B + Cx^2 + \cancel{Cx} + C + \cancel{Cx} + Bx^3 + Cx^5 + Cx^4 + Cx^3 \\
&= B(x^3+1) + C(x^5+x^4+x^3+x^2+1) \\
&= B(x^3+1) + (A - B(x+1))(x^5+x^4+x^3+x^2+1)
\end{aligned}
$$

$$1 = A(x^5+x^4+x^3+x^2+1) + B(x^6+x^3+x^2+x)$$

$\therefore f(11101001) = 01001110$

#

4. Chinese Remainder Theorem

$0 \leq x \leq 352$

$$\begin{cases} x \bmod 3 = 1 \\ x \bmod 11 = 3 \\ x \bmod 16 = 13 \end{cases}$$

Ans:

$(11 \times 16)^{-1} \bmod 3 = 2$

$(3 \times 16)^{-1} \bmod 11 = 3$

$(3 \times 11)^{-1} \bmod 16 = 1$

$$x = \Big(\underline{1 \times 11 \times 16 \times (11 \times 16)^{-1} \bmod 3}$$
$$+ \underline{3 \times 3 \times 16 \times (3 \times 16)^{-1} \bmod 3}$$
$$+ \underline{13 \times 3 \times 11 \times (3 \times 11)^{-1} \bmod 3} \Big) \bmod 528$$

$$= 1213 \bmod 528 = 157$$

#.