《最优化算法》第一次作业

学号：4012014015　姓名：张浩枝

一、 开放问题

【参考文献】:

Optimization problem in quantum cryptography

1、问题描述：

研究者们在最近进行了一次完整的优化，通过量子密码学四状态协议中的一般酉纠缠探测器产生最大信息增益。发现比以前从不完全优化中知道的更大的一组最佳探头参数。并且详细比较了完全和不完全优化。 还为四态协议确定了一组新的最佳探头参数。

2、可能的求解算法

最大$\boldsymbol{Renyi}$信息增益由四态量子密钥分发协议中的一般幺正纠缠窃听探头获得的，而且最大$\boldsymbol{Renyi}$信息增益最近由表征由探头与信号相互作用影响的幺正变换的完整最佳探头参数确定$[\mathbf{1},\mathbf{2}]$。信号的非正交光子线性偏振态之间的角度被认为是任意的。优化的条件是在合法接收机中由探测器引起的固定误差率，并且通过以与信号状态相关的探测器状态的重叠表示$\boldsymbol{Renyi}$信息增益来实现，以误差率的条件和探头参数，并且在保持误差率固定的同时使$\boldsymbol{Renyi}$信息增益相对于探头参数最大化。

特别地，通过探针的最大$\boldsymbol{Renyi}$信息增益$\boldsymbol{I_{opt}^{R}}$:

$$\boldsymbol{maximum}:\quad \boldsymbol{I_{opt}^{R}=\log_2(2-Q^2)},$$

$$\boldsymbol{subject\ \ to}: \boldsymbol{Q} = \frac{\frac{\boldsymbol{1}}{\boldsymbol{2}}(\boldsymbol{q}-\boldsymbol{1})+\boldsymbol{E}}{\left[(\boldsymbol{1}-\boldsymbol{E})^{\boldsymbol{2}}-\frac{\boldsymbol{1}}{\boldsymbol{4}}\boldsymbol{c}^{\boldsymbol{2}}\boldsymbol{sin}^{\boldsymbol{2}}\boldsymbol{2\alpha}\right]^{\frac{\boldsymbol{1}}{\boldsymbol{2}}}}$$

因此可得当$\boldsymbol{Q}$最小时，$\boldsymbol{I}_{\boldsymbol{opt}}^{\boldsymbol{R}}$最大。

二、课后练习

Assignment：6.1

==========

【一阶必要条件】

多元实值函数f在约束集Ω上一阶连续可微，即$f\epsilon\ C^1$,约束集Ω是$\mathbb{R}^n$的子集。如果x^*是函数f在Ω上的局部极小点，则对于$\boldsymbol{x}^*$处的任意可行方向$\boldsymbol{d}$,都有

$$\boldsymbol{d}'\boldsymbol{\nabla f}(\boldsymbol{x}^*) \geq \boldsymbol{0},$$

成立。

a) 由于$\boldsymbol{x}^* = [\boldsymbol{1},\boldsymbol{2}]', \boldsymbol{\nabla f}(\boldsymbol{x}^*) = [\boldsymbol{1},\boldsymbol{1}]'$,因此由一阶必要条件可得$\boldsymbol{x}^*$绝对不是局部极小点。

b) 由于$\boldsymbol{x}^* = [\boldsymbol{1},\boldsymbol{2}]', \boldsymbol{\nabla f}(\boldsymbol{x}^*) = [\boldsymbol{1},\boldsymbol{0}]'$,因此由一阶必要条件可得$\boldsymbol{x}^*$绝对不是局部极小点。

【局部极小点的二阶充分条件】

多元实值函数f在约束集Ω上二阶连续可微，即$f\epsilon\ C^2$,约束集Ω是$\mathbb{R}^n$的子集。x^*是约束集的一个内点，如果同时满足：

1. $\boldsymbol{\nabla f}(\boldsymbol{x}^*) = \boldsymbol{0}$,
2. $\boldsymbol{F}(\boldsymbol{x}^*) > \boldsymbol{0}$.

则$\boldsymbol{x}^*$是函数f在Ω上的一个严格局部极小点。

c) 由于

$\boldsymbol{x^* = [1,2]', \Omega = \{x = \{x_1, x_2\}' : x_1 \geq 0, x_2 \geq 0\}, \nabla f(x^*) = [0,0]',}$

而且黑赛矩阵为$\boldsymbol{F(x^*) = I}$（单位矩阵）。

因此由二阶充分条件可得$\boldsymbol{x^*}$绝对是局部极小点。

d) 由于

$\boldsymbol{x^* = [1,2]', \Omega = \{x = \{x_1, x_2\}' : x_1 \geq 1, x_2 \geq 2\}, \nabla f(x^*) = [1,0]',}$

而且黑赛矩阵为$\boldsymbol{F(x^*) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}}$。

因此由二阶必要条件可得$\boldsymbol{x^*}$可能是局部极小点。

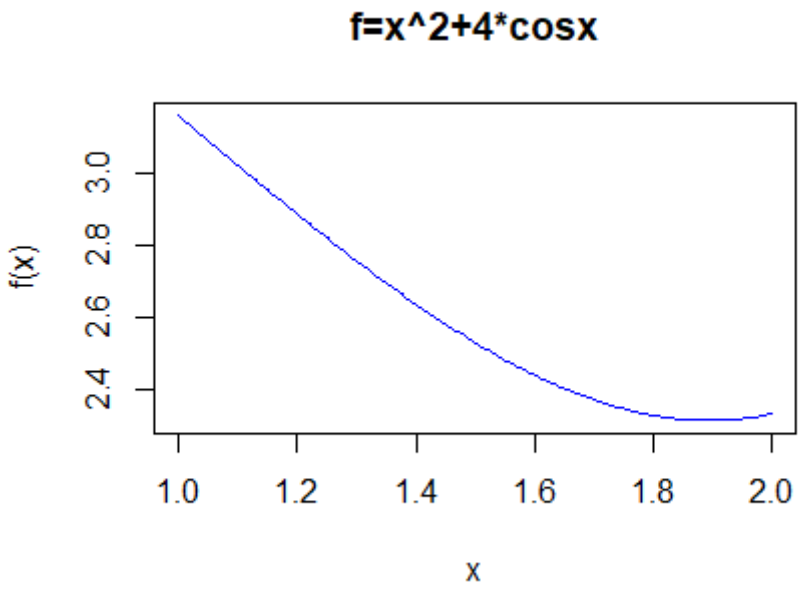
Assignment：6.15

==========

已知：$\boldsymbol{f(x) = 3x_1, \Omega = \{x = [x_1, x_2]' : x_1 + x_2^2 \geq 2\}}$.

1) 由于$\boldsymbol{x^* = [2,0]'}$，$\boldsymbol{\nabla f(x^*) = [3,0]',}$因此$\boldsymbol{x^*}$不满足一阶必要条件；
2) 由于$\boldsymbol{x^* = [2,0]'}$，$\boldsymbol{\nabla f(x^*) = [3,0]',}$$d$需要满足$\boldsymbol{d = [0, x_2]',}$又由于$\boldsymbol{F(x^*) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}$，因此$\boldsymbol{x^*}$满足二阶必要条件；
3) 由于$\boldsymbol{x^* = [2,0]'}$，$\boldsymbol{\nabla f(x^*) = [3,0]',}$$d$需要满足$\boldsymbol{d = [0, x_2]',}$又由于$\boldsymbol{F(x^*) = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}}$，因此$\boldsymbol{x^*}$满足二阶必要条件，但是$\boldsymbol{x^*}$不满足二阶充分条件，因此不是严格局部极小点，可能是局部极小点；

Assignment：7.2



由图像可以大致看出区间[1,2]内的极小点在区间[1.8,2]之内。

1) 如上图所示，为$\boldsymbol{f(x)=x^2+4cosx}$在区间[1,2]上的图像：

```
> f <- function(x) x^2+4*cos(x)
> curve(f,1,2,main="f=x^2+4*cosx",col="blue")
```

2) 利用黄金分割法：

step1. 利用$\boldsymbol{b_k-a_k=(1-\rho)^k(b_0-a_0)}$可知，经过$\boldsymbol{N}$步，区间[1,2]被压缩为原区间长度的$\boldsymbol{(0.61803)^N}$,因此可得：

$$\boldsymbol{(0.61803)^N \le 0.2/1}$$

```
> for(i in 1:200){
+   if(0.61803^i<=0.2){
+     print(i);
+     break;
+   }
+ }
[1] 4
```

可得$\boldsymbol{N=4}$，即经过 4 步压缩可以达到目的。

step2. 进行 4 次压缩，具体过程如下表所示：

第k次	a_k	b_k	$f(a_k)$	$f(b_k)$	新的区间
1	1.382	1.618	2.660631	2.429179	[1.382,2]
2	1.618076	1.763924	2.429122	2.34371	[1.618076,2]
3	1.763971	1.854105	2.343692	2.31957	[1.763971,2]
4	1.854134	1.909837	2.319566	2.317147	[1.854134,2]

由表中可得到此时区间的长度为$\mathbf{0.145857}$，以满足题目的 0.2 的要求。下面是软件使用黄金分割得到的结果：

```
> optimize(f,c(1,2))
$minimum
[1] 1.895496

$objective
[1] 2.316808
```

3) 利用斐波那契数列法：$\epsilon = 0.05$

step1. 确定迭代次数：

$$\frac{1+2\epsilon}{F_{N+1}} \leq \frac{0.2}{2-1}$$

可得：只需$N = 4$次迭代即可满足要求

step2. 迭代过程如表所示：

第k次	压缩比	a_k	b_k	$f(a_k)$	$f(b_k)$	新的区间
1	$\rho_1 = 3/8$	1.375	1.625	2.668816	2.423916	[1.375,2]
2	$\rho_2 = 2/5$	1.625	1.75	2.4239	2.3495	[1.625,2]
3	$\rho_3 = 1/3$	1.75	1.875	2.3495	2.3175	[1.75,2]
4	$\rho_4 = 1/2$	1.875	1.8875	2.3175	2.3169	[1.875,2]

由表可得，第 4 次迭代完成，区间的长度为$\mathbf{0.125}$，满足要求。

4) 利用牛顿法完成：初始值为$\boldsymbol{x^{(0)}=1,}$且迭代次数与黄金分割法相同：

step1. 计算$\boldsymbol{f(x)}$的一阶和二阶导数：

$$\boldsymbol{f(x)=x^2+4cosx,}$$

$$\boldsymbol{f'(x)=2x-4sinx,}$$

$$\boldsymbol{f''(x)=2-4cosx.}$$

step2. 利用：

$$\boldsymbol{x^{(k+1)}=x^{(k)}-\frac{2*x^{(k)}-4sinx^{(k)}}{2-4cosx^{(k)}}.}$$

可得：

$$\boldsymbol{x^{(1)}=-7.4727，\ x^{(2)}=14.4785，}$$

$$\boldsymbol{x^{(3)}=6.9351，\ x^{(4)}=16.6354.}$$