强化学习基本原理及编程实现: TRPO

郭宪

2019.11.16

人工智能学院 College of Artificial Intelligence









策略梯度的缺点

1. 很难在整个优化过程选择一个时间步长, 特别是由于状态和回报在改变统计特性。

2. 策略经常会过早地收敛到一个次优的几乎确定的策略。

步长的重要性!

当步长不合适时,所学到的策略是一个坏的策略,由坏的策略所采集到的数据也是不好的数据,学习很可能会崩溃

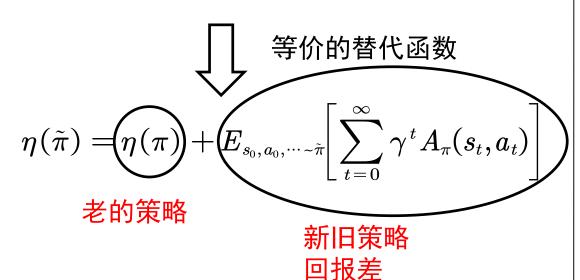




用 τ 表示一组状态-行为序列 s_0,u_0,\cdots,s_H,u_H

目标函数为:

$$\eta(ilde{\pi}) = E_{ au| ilde{\pi}} iggl[\sum_{t=0}^{\infty} \gamma^t(r(s_t)) iggr]$$



优势函数的定义:

$$A_{\pi}(s,a) = Q_{\pi}(s,a) - V_{\pi}(s)$$

$$=E_{s'\sim P(s'|s,a)}[r(s)+\gamma V^{\pi}(s')-V^{\pi}(s)]$$

证明:

$$E_{ au| ilde{\pi}}\!\!\left[\sum_{t=0}^{\infty}\gamma^{\,t}A_{\pi}\!\left(s_{t},a_{t}
ight)
ight]$$

$$= E_{ au| ilde{\pi}} iggl[\sum_{t=0}^{\infty} \gamma^t ig(r(s) + \gamma V^{\pi}(s_{t+1}) - V^{\pi}(s_t) ig) iggr]$$

$$= E_{ au| ilde{\pi}} iggl[\sum_{t=0}^{\infty} \gamma^{\,t}(r(s_t)) + \sum_{t=0}^{\infty} \gamma^{\,t}(\gamma V^{\pi}(s_{t+1}) - V^{\,\pi}(s_t)) iggr]$$

$$= E_{ au| ilde{\pi}} iggl[\sum_{t=0}^{\infty} \gamma^t(r(s_t)) iggr] + E_{s_0} [-V^{\pi}(s_0)]$$

$$= \eta(\tilde{\pi}) - \eta(\pi)$$

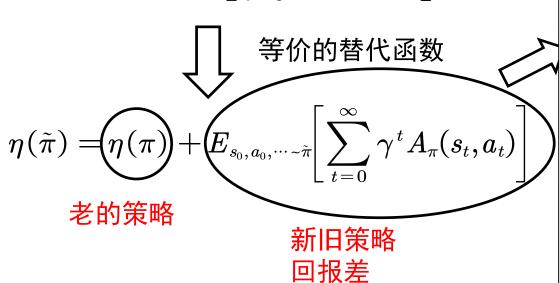




用 τ 表示一组状态-行为序列 s_0,u_0,\cdots,s_H,u_H

目标函数为:

$$\eta(ilde{\pi}) = E_{ au| ilde{\pi}} iggl[\sum_{t=0}^{\infty} \gamma^t(r(s_t)) iggr]$$



定义:

$$\rho_{\pi}(s) = P(s_0 = s) + \gamma P(s_1 = s) + \gamma^2 P(s_2 = s) + \cdots$$

第t步出现s的概率 状态s处动作进行 加和 $\eta(\widetilde{\pi}) = \eta(\pi) + \sum_{t=0}^{\infty} \sum_{s} P(s_t = s | \widetilde{\pi}) \sum_{a} \widetilde{\pi}(a | s) \gamma^t A_{\pi}(s, a)$ $= \eta(\pi) + \sum_{s} \rho_{\widetilde{\pi}}(s) \sum_{a} \widetilde{\pi}(a | s) A^{\pi}(s, a)$

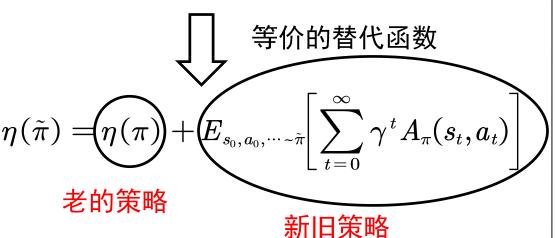




用 au 表示一组状态-行为序列 s_0,u_0,\cdots,s_H,u_H

目标函数为:

$$\eta(ilde{\pi}) = E_{ au| ilde{\pi}} \!\! \left[\sum_{t=0}^{\infty} \gamma^t \! \left(r(s_t)
ight)
ight]$$



回报差

$$=\eta(\pi)+\sum_s
ho_{\widetilde{\pi}}(s)\sum_a \widetilde{\pi}(a|s)A^\pi(s,a)$$

策略改善理论

$$\begin{split} & v_{\pi}(s) \leqslant q_{\pi}(s, \pi'(s)) \\ &= \mathbb{E} \big[R_{t+1} + \gamma v_{\pi}(s_{t+1}) | s_{t} = s, \ a_{t} = \pi'(s) \big] \\ &= \mathbb{E}_{\pi'} \big[R_{t+1} + \gamma v_{\pi}(s_{t+1}) | s_{t} = s \big] \\ &\leqslant \mathbb{E}_{\pi'} \big[R_{t+1} + \gamma q_{\pi}(s_{t+1}, \pi'(s_{t+1})) | s_{t} = s \big] \\ &= \mathbb{E}_{\pi'} \big[R_{t+1} + \gamma \mathbb{E}_{\pi'} \big[R_{t+2} + \gamma v_{\pi}(s_{t+1}) | s_{t+1}, a_{t+1} = \pi'(s_{t+1}) \big] | s_{t} = s \big] \\ &= \mathbb{E}_{\pi'} \big[R_{t+1} + \gamma R_{t+2} + \gamma^{2} v_{\pi}(s_{t+2}) | s_{t} = s \big] \\ &\leqslant \mathbb{E}_{\pi'} \big[R_{t+1} + \gamma R_{t+2} + \gamma^{2} R_{t+3} + \gamma^{3} v_{\pi}(s_{t+2}) | s_{t} = s \big] \\ &\vdots \\ &\leqslant \mathbb{E}_{\pi'} \big[R_{t+1} + \gamma R_{t+2} + \gamma^{2} R_{t+3} + \gamma^{3} R_{t+4} + \cdots | s_{t} = s \big] \\ &= v_{\pi'}(s) \end{split}$$

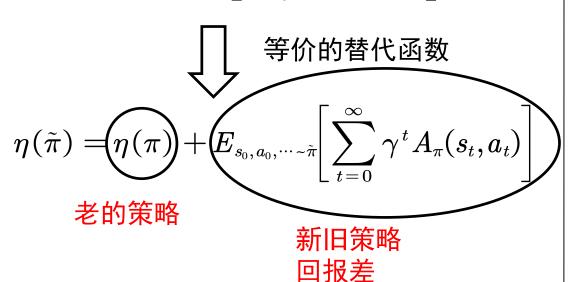




用 au 表示一组状态-行为序列 s_0,u_0,\cdots,s_H,u_H

目标函数为:

$$\eta(ilde{\pi}) = E_{ au| ilde{\pi}} \!\! \left[\sum_{t=0}^{\infty} \gamma^t (r(s_t))
ight]$$



$$=\eta(\pi)+\sum_{s}
ho_{\widetilde{\pi}}(s)\sum_{a}\widetilde{\pi}(a|s)A^{\pi}(s,a)$$

策略改善理论

一个更好的策略应该满足:

在每个状态s处:

$$\sum_{a} \tilde{\pi}(a \mid s) A^{\pi}(s, a) \ge 0$$

然而, 在函数逼近的情况下:

存在估计和逼近误差,因此导致在一些状态处

$$\sum_{\sigma} \tilde{\pi}(a \mid s) A^{\pi}(s, a) < 0$$

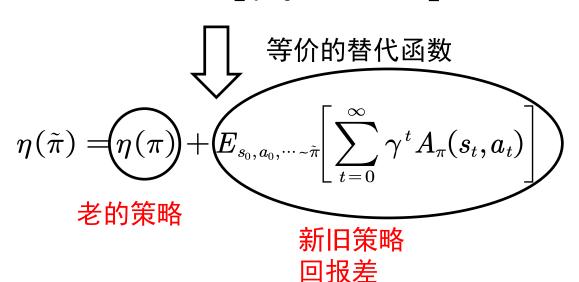




用 au 表示一组状态-行为序列 s_0,u_0,\cdots,s_H,u_H

目标函数为:

$$\eta(ilde{\pi}) = E_{ au| ilde{\pi}} \!\! \left[\sum_{t=0}^{\infty} \gamma^t(r(s_t))
ight]$$



$$\eta(\widetilde{\pi}) = \eta(\pi) + \underbrace{\sum_{s} \rho_{\widetilde{\pi}}(s)}_{a} \underbrace{\widetilde{\pi}(a|s)}_{a} A^{\pi}(s,a)$$

注意: 这时状态分布由新的策略产生,对新的策略严重依赖

第一个技巧:对状态分布的处理,忽略状态分布的变化,依然用旧的策略所对应的状态分布

$$L_{\pi}(\widetilde{\pi}) = \eta(\pi) + \sum_{s} oldsymbol{
ho}_{\pi}(s) \left[\sum_{a} \widetilde{\pi}(a|s) A^{\pi}(s,a)
ight]$$

第二个技巧:对动作分布的处理,重要性采样

$$\sum_{a} ilde{\pi}_{ heta}(a|s_n)A_{ heta_{old}}(s_n,a) = E_{a ilde{-}q}igg[rac{ ilde{\pi}_{ heta}(a|s_n)}{q(a|s_n)}A_{ heta_{old}}(s_n,a)igg]$$

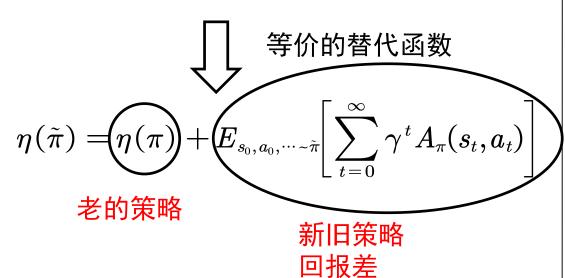




用 au 表示一组状态-行为序列 s_0,u_0,\cdots,s_H,u_H

目标函数为:

$$\eta(ilde{\pi}) = E_{ au| ilde{\pi}} iggl[\sum_{t=0}^{\infty} \gamma^t(r(s_t)) iggr]$$



$$L_{\pi}(\widetilde{\pi}) = \eta(\pi) + \sum_{s} oldsymbol{
ho}_{\pi}(s) \sum_{a} \widetilde{\pi}(a|s) A^{\pi}(s,a)$$

$$\sum_{a} ilde{\pi}_{ heta}(a|s_n)A_{ heta_{old}}(s_n,a) = E_{a ext{-}q}igg[rac{ ilde{\pi}_{ heta}(a|s_n)}{q(a|s_n)}A_{ heta_{old}}(s_n,a)igg]$$

$$oxed{rac{1}{1-\gamma}E_{s\sim
ho_{ heta_{old}}}[\cdots]}$$
 代替 $\sum_{s}
ho_{ heta_{old}}(s)\left[\cdots
ight]$

$$ig|\, q(a|s_n) = \pi_{ heta_{\scriptscriptstyle old}}(a|s_n)$$

$$L_{\pi}(\widetilde{\pi}) = \eta(\pi) + E_{s \sim
ho_{ heta_{old}}, a \sim \pi_{ heta_{old}}} iggl[rac{ ilde{\pi}_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a) iggr]$$





原回报函数与替代回报函数比较

原回报函数:

$$\eta(\widetilde{\pi}) = \eta(\pi) + \sum_{s}
ho_{\widetilde{\pi}}(s) \sum_{a} \widetilde{\pi}(a|s) A^{\pi}(s,a)$$

替代回报函数:

$$L_{\pi_{\theta_{old}}}(\pi_{\theta}) = \eta(\pi_{\theta_{old}}) + E_{s \sim \rho_{\theta_{old}}, a \sim \pi_{\theta_{old}}} \left[\frac{\tilde{\pi}_{\theta}(a \mid s)}{\pi_{\theta_{old}}(a \mid s)} A_{\theta_{old}}(s, a) \right]$$

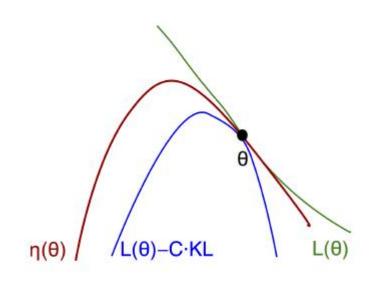
在 θ_{old} 处一阶近似:

$$L_{\pi_{ heta_{old}}}\!(\pi_{ heta_{old}}) = \eta(\pi_{ heta_{old}})$$

$$|
abla_{ heta}L_{\pi_{ heta_{old}}}\!(\pi_{ heta})|_{ heta=\, heta_{old}}\!=\!
abla_{ heta}\eta(\pi_{ heta})|_{ heta=\, heta_{old}}$$

在 θ_{old} 附近, 能改善L的策略也能改善

原回报函数。问题是步长多大呢?







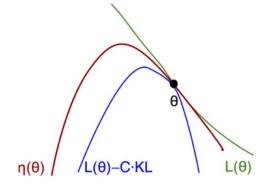
原回报函数与替代回报函数比较

定理1:

令
$$\alpha = D_{TV}^{max}(\pi_{old}, \pi_{new})$$
 , 则存在下面的界:

$$\eta(\pi_{new}) \ge L_{\pi_{old}}(\pi_{new}) - \frac{4\varepsilon}{(1-\gamma)^2} \alpha^2$$

Where: $\varepsilon = \max_{s,a} |A_{\pi}(s,a)|$



Algorithm 1 Policy iteration algorithm guaranteeing non-decreasing expected return η

Initialize π_0 .

for $i=0,1,2,\ldots$ until convergence do Compute all advantage values $A_{\pi_i}(s,a)$. Solve the constrained optimization problem

$$\pi_{i+1} = \underset{\pi}{\operatorname{arg\,max}} \left[L_{\pi_i}(\pi) - CD_{\mathrm{KL}}^{\mathrm{max}}(\pi_i, \pi) \right]$$
where $C = 4\epsilon \gamma/(1 - \gamma)^2$
and $L_{\pi_i}(\pi) = \eta(\pi_i) + \sum_s \rho_{\pi_i}(s) \sum_a \pi(a|s) A_{\pi_i}(s, a)$

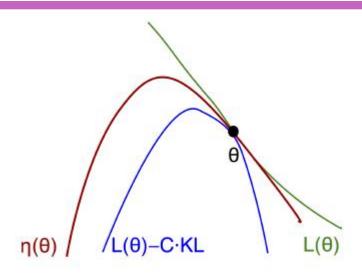
end for

策略迭代算法





单调改进策略



$$\eta(ilde{\pi}) \geqslant L_{\pi}(ilde{\pi}) - CD_{KL}^{\max}(\pi, ilde{\pi})$$
 ,

where
$$C = \frac{2\varepsilon\gamma}{(1-\gamma)^2}$$

令:
$$M_i(\pi) = L_{\pi_i}(\pi) - CD_{KL}^{\max}(\pi_i,\pi)$$

则:
$$\eta(\pi_{i+1}) \geqslant M_i(\pi_{i+1})$$

又因为:
$$\eta(\pi_i) = M_i(\pi_i)$$

所以:
$$\eta(\pi_{i+1}) - \eta(\pi_i) \ge M_i(\pi_{i+1}) - M(\pi_i)$$

所以每次最大化 M_i 能够保证策略非递减。

如何利用理论来得到最优的策略 π_{i+1} ?

参数化策略!





TRP0实用算法: 优化参数化的策略

问题形式化为:

如果利用惩罚因子C则每次迭代步长很小, 因此问题可转化为:

$$\max_{ heta} imize E_{s \sim
ho_{ heta_{old}}, \, a \sim \pi_{ heta_{old}}} \!\! \left[rac{\pi_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a)
ight] \!\!
brace$$

 $subject \ to \ \ D_{\mathit{KL}}^{\max}(heta_{\mathit{old}}, heta) \leqslant \delta$

无穷多个状态, 无穷多约束

第三个技巧:利用平均KL散度:

$$subject \,\, to \,\, ar{D}^{\,
ho_{ heta_{old}}}_{\mathit{KL}}(heta_{old}, heta) \leqslant \delta$$

第四个技巧: 利用当前策略状态空间分布

$$s extsf{\sim}
ho_{ heta_{old}} o s extsf{\sim}\pi_{ heta_{old}}$$

TRPO的问题形式化为:

$$egin{aligned} \max_{ heta} & imize E_{s \sim \pi_{ heta_{old}}, \, a \sim \pi_{ heta_{old}}} igg[rac{\pi_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a) igg] \end{aligned}$$

$$subject \; to \; E_{s \sim \pi_{ heta_{old}}} igl[D_{\mathit{KL}} igl(\pi_{ heta_{old}}(\cdot|s) || \pi_{ heta}(\cdot|s) igr) igr] \leqslant \delta$$







第三个技巧:利用平均KL散度:

 $subject \,\, to \,\, \overline{D}_{\mathit{KL}}^{\,
ho_{ heta_{old}}}(heta_{old}, heta) \leqslant \delta$

第四个技巧: 利用当前策略状态空间分布

$$s extsf{\sim}
ho_{ heta_{old}} o s extsf{\sim}\pi_{ heta_{old}}$$

TRPO的问题形式化为:

$$egin{aligned} \max_{ heta} & imize E_{s \sim \pi_{ heta_{old}}, \, a \sim \pi_{ heta_{old}}} igg[rac{\pi_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a) \, igg] \end{aligned}$$

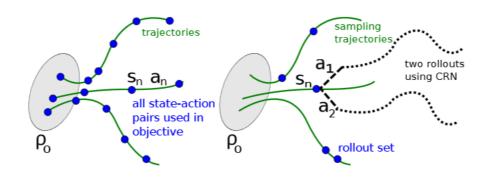
$$\left| subject \,\, to \,\, E_{s \sim \pi_{ heta_{old}}} igl[D_{\mathit{KL}} igl(\pi_{ heta_{old}} (\cdot | s) || \pi_{ heta} (\cdot | s) igr) igr] \leqslant \delta
ight|$$

如何得到目标函数和约束条件?

基于采样的方法对目标函数和约束进行估计

利用蒙特卡洛方法估计:

利用样本的平均值来代替期望



Single path

Vine **Nankai University**





TRP0实用算法

第三个技巧:利用平均KL散度:

$$subject \,\, to \,\, \overline{D}_{\mathit{KL}}^{\,
ho_{ heta_{old}}}(heta_{old}, heta) \leqslant \delta$$

第四个技巧:利用当前策略状态空间分布

$$s extsf{\sim}
ho_{ heta_{old}} o s extsf{\sim}\pi_{ heta_{old}}$$

TRPO的问题形式化为:

$$egin{aligned} \max_{ heta} & imize E_{s \sim \pi_{ heta_{old}}, \, a \sim \pi_{ heta_{old}}} igg[rac{\pi_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a) \, igg] \end{aligned}$$

$$egin{aligned} subject \ to \ E_{s \sim \pi_{ heta_{old}}} igl[D_{\mathit{KL}} igl(\pi_{ heta_{old}}(\cdot|s) || \pi_{ heta}(\cdot|s) igr) igr] \leqslant \delta igr] \end{aligned}$$

TRP0算法流程:

For 迭代 1,2, ... do

运行当前策略T步或N条轨迹

利用所有时间步数据估计优势函数

利用共轭梯度法和线性搜索计算参数更新

End for





共轭梯度法搜索可行方向

$$egin{aligned} \max_{ heta} & imize E_{s \sim \pi_{ heta_{old}}, a \sim \pi_{ heta_{old}}} igg[rac{\pi_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a) \, igg] \end{aligned}$$

$$egin{aligned} subject \ to \ E_{s \sim \pi_{ heta_{old}}} igl[D_{\mathit{KL}} igl(\pi_{ heta_{old}}(\cdot|s) || \pi_{ heta}(\cdot|s) igr) igr] \leqslant \delta iggr] \end{aligned}$$

将目标进行线性化逼近,将约束进行二次逼近后优化问题为:

$$subject \ to \ \left. rac{1}{2} \left(heta_{old} - heta
ight) {}^{\scriptscriptstyle T} A(heta_{old}) \left(heta_{old} - heta
ight) \leqslant \delta
ight|$$

A为Fisher信息矩阵:

$$A_{ij} = \frac{\partial}{\partial \theta_i} \frac{\partial}{\partial \theta_j} \overline{D}_{KL}(\theta_{old}, \theta)$$

$$\underbrace{\frac{\partial \mu_{\alpha}(x)}{\partial \theta_{i}} \, k l_{\alpha b}''(\mu_{\theta}(x), \mu_{old}(x)) \frac{\partial \mu_{b}(x)}{\partial \theta_{j}}}_{J^{\mathsf{T}} M J} + \underbrace{\frac{\partial^{2} \mu_{\alpha}(x)}{\partial \theta_{i} \partial \theta_{j}} \, k l_{\alpha}'(\mu_{\theta}(x), \mu_{old}(x))}_{=0 \text{ at } \mu_{\theta} = \mu_{old}}$$





共轭梯度法搜索可行方向

$$egin{aligned} \max_{ heta} & imize E_{s \sim \pi_{ heta_{old}}, \, a \sim \pi_{ heta_{old}}} igg[rac{\pi_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a) \, igg] \end{aligned}$$

$$ig| subject \; to \; E_{s \sim \pi_{ heta_{old}}} ig[D_{ extit{KL}} ig(\pi_{ heta_{old}} (\cdot | s) || \pi_{ heta} (\cdot | s) ig) ig] \leqslant \delta ig|$$

将目标进行线性化逼近,将约束进行二次 逼近后优化问题为:

$$subject \ to \ \frac{1}{2} (\theta_{old} - \theta)^{T} A(\theta_{old}) (\theta_{old} - \theta) \leqslant \delta$$

令
$$d = \theta - \theta_{old}$$
 为搜索方向,则搜索方向

应该满足:
$$A(heta_{old})d =
abla_{ heta}L_{ heta_{old}}(heta)|_{ heta= heta_{old}}$$

利用共轭梯度方法求解线性方程组AX = b的解方法: \sqrt{a}

构造目标函数 $f(x)=rac{1}{2}x^TAx-bx$,则x是目标函数的最小值。arphi

Step1: 给定初试迭代点 $x^{(1)}$,令k=1

Step2:计算梯度 $g_k = \nabla f(x^{(k)}) = Ax^{(k)} - b$, 若 $\|g_k\| = 0$ 则停止计算,并令 $x^* = x^{(k)}$,否则转下一步。

Step3:构造搜索方向,首先计算步长 $\beta_{k-1} = \frac{(d^{(k-1)})^T A g_k}{(d^{(k-1)})^T A d^{(k)}}$,若 $k = 1, \beta_{k-1} = 0$ 。

搜索方向为:
$$d^k = -g_k + \beta_{k-1} d^{k-1}$$

Step4: 计算搜索步长
$$\lambda_k = -\frac{g_k^T d^{(k)}}{(d^{(k)})^T A d^{(k)}}$$
,更新数据点 $x^{(k+1)} = x^{(k)} + \lambda_k d^{(k)}$ 。

此处:
$$b = \nabla_{\theta} L_{\theta_{old}}(\theta)|_{\theta = \theta_{old}}$$





线性搜索得到步长

第二步,利用线性搜索方法计算步长 β : φ

将第一步求得的搜索方向 d 乘以步长,带入约束方程得到:

$$\delta pprox rac{1}{2} (eta d)^{\mathrm{\scriptscriptstyle T}} A (eta d) = rac{1}{2} eta^2 d^{\mathrm{\scriptscriptstyle T}} A d$$
 ,

从而得到步长为:
$$\beta = \sqrt{\frac{2\delta}{d^T A d}}$$

将 β 带入目标函数 $L_{\theta_{old}}(\theta) - \mathcal{X}\left[\bar{D}_{KL}(\theta_{old},\theta) \leq \delta\right]$, 其中 $\mathcal{X}\left[\bar{D}_{KL}(\theta_{old},\theta) \leq \delta\right]$ 表示当满足不等式时为零,当不满足不等式时为无穷大。收缩步长 β ,直到目标函数得到改善。 θ

$$heta_{new} = heta_{old} + eta d$$





近端策略优化算法(PPO)

策略梯度的目标函数:

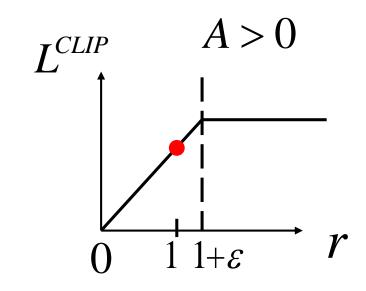
$$L^{PG}(\theta) = E_t \left[\log \pi_{\theta}(a_t \mid s_t) \hat{A}_t \right]$$

TRPO目标函数:

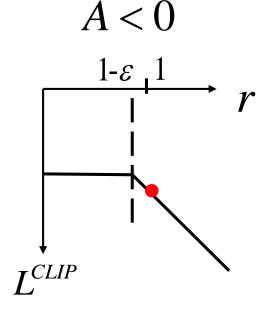
$$egin{aligned} ext{maximize} & E_{s \sim \pi_{ heta_{old}}, a \sim \pi_{ heta_{old}}} iggl[rac{\pi_{ heta}(a|s)}{\pi_{ heta_{old}}(a|s)} A_{ heta_{old}}(s,a) iggr] \ & subject \ to \ & E_{s \sim \pi_{ heta_{old}}} igl[D_{ ext{KL}}(\pi_{ heta_{old}}(\cdot|s) || \pi_{ heta}(\cdot|s)) igr] \leqslant \delta \end{aligned}$$

CLIP目标函数:

$$L^{CLIP}(\theta) = E_t[\min(r_t(\theta)\hat{A}_t, clip(r_t(\theta), 1-\varepsilon, 1+\varepsilon)\hat{A}_t)]$$











近端策略优化算法 (PPO)

PP0目标函数:

$$L_t^{CLIP+VF+S}(\theta) = \hat{E}_t[L_t^{CLIP}(\theta) - c_1 L_t^{VF}(\theta) + c_2 S[\pi_{\theta}](s_t)]$$

其中: V_t^{VF} 为值函数损失函数,S为熵。

为减小方差,优势函数可写为:

$$\hat{A}_{t} = \delta_{t} + (\gamma \lambda) \delta_{t+1} + \dots + (\gamma \lambda)^{T-t+1} \delta_{T-1}$$

其中:
$$\delta_t = r_t + \gamma V(s_{t+1}) - V(s_t)$$





近端策略优化算法(PPO)

```
Algorithm 1 PPO, Actor-Critic Style
```

```
for iteration=1,2,... do

for actor=1,2,..., N do

Run policy \pi_{\theta_{\text{old}}} in environment for T timesteps

Compute advantage estimates \hat{A}_1, \ldots, \hat{A}_T

end for

Optimize surrogate L wrt \theta, with K epochs and minibatch size M \leq NT

\theta_{\text{old}} \leftarrow \theta

end for
```

PP0伪代码





TRP0用到的信息论

熵的概念: 熵是信息多少的度量

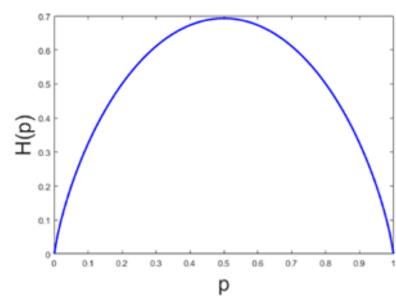
离散系统:
$$H(X) = -\sum_{i} p_{i} \log p_{i}$$

连续系统:
$$H(x) = E_{x\sim P}[I(x)] = -E_{x\sim P}[\log P(x)]$$

熵是不确定性的度量:不确定度越大,熵越大

二值熵定义:

$$H = -p \log(p) - (1-p) \log(1-p)$$







TRP0用到的信息论

交叉熵:

$$H(P,\ Q) = -E_{P(x)}Q(x) = -\int P(x)\log Q(x)dx$$

交叉熵用来衡量编码方案不一定完美时,平均编码的长度

KL散度: 衡量两个概率分布之间的距离

$$D_{\mathit{KL}}(P||Q) = E_{x \sim P} \bigg[\log \frac{P(x)}{Q(x)} \bigg] = \int P(x) \log P(x) dx - \int P(x) \log Q(x) dx$$





第七次作业

- 1. 阅读 Trust Region Policy Optimization 和 Proximal Policy Optimization Algorithms
- 2. 阅读代码