2 MOTIVATION

Vulnerability of Time-relevant Scoring compared with Non-time-relevant Scoring: Consider a simple time-varying scoring with only one factor, say "deploy factor". Here we wish the user to deploy quota q ($q > 0$) as much as possible. Then we can score the user via his past T deployments like $s(T) = \frac{1}{T}\sum_{t=1}^{T} q_t \cdot e^{-\gamma(T-t)}$ where γ controls the effect of time decay. Intuitively, if the next deployment q_{T+1} is larger than the last one q_T, the credit score should be higher. However, we can justify that $q_{T+1} > q_T$, $s(T+1) < s(T)$ holds if the following conditions are satisfied:

$$\begin{aligned} &q_T < \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} \\ &T > e^{\lambda} \end{aligned} \tag{1}$$

Proof:
Let $q_{T+1} = q_T + \delta$ where $\delta > 0$, then:

$$\begin{aligned} &S(T+1) < S(T) \\ \Leftrightarrow &\frac{1}{T+1}\sum_{t=1}^{T+1} q_t \cdot e^{-\lambda(T+1-t)} < \frac{1}{T}\sum_{t=1}^{T} q_t \cdot e^{-\lambda(T-t)} \\ \Leftrightarrow &\frac{q_T+\delta}{T+1} + \underbrace{\frac{1}{T+1}\sum_{t=1}^{T} q_t \cdot e^{-\lambda(T+1-t)}}_{\text{align the summation range}} < \frac{1}{T}\sum_{t=1}^{T} q_t \cdot e^{-\lambda(T-t)} \\ \Leftrightarrow &0 < \frac{T+1}{T}\sum_{t=1}^{T} q_t \cdot e^{-\lambda(T-t)} - q_T - \delta - \sum_{t=1}^{T} q_t \cdot e^{-\lambda(T+1-t)} \\ \Leftrightarrow &0 < (\frac{1}{T} - e^{-\lambda})q_T - \delta + \underbrace{\frac{1+T}{T}\sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} - e^{-\lambda}\sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)}}_{\text{align the exponent}} \\ \Leftrightarrow &0 < \underbrace{(e^{\lambda} - T)}_{<0} q_T - \delta + (Te^{\lambda} + e^{\lambda} - T)\sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} \\ \Leftrightarrow &q_T < \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} - \delta \end{aligned}$$

Since $\delta > 0$, we have:

$$\begin{aligned} q_T &< \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} - \delta \\ &< \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} \end{aligned}$$

Therefore, we have

$$S(T+1) < S(T) \Rightarrow q_T < \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)}$$

On the other hand, if $q_T < \frac{(T+1)e^{\lambda}-T}{T-e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)}$, there always exists a small vale $\delta > 0$, making the following relation hold:

$$q_T < \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} - \delta$$

The we have

$$q_T < \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)} \Rightarrow S(T+1) < S(T)$$

Therefore,

$$S(T+1) < S(T) \Leftrightarrow q_T < \frac{(T+1)e^{\lambda} - T}{T - e^{\lambda}} \sum_{t=1}^{T-1} q_t \cdot e^{-\lambda(T-t)}$$

The above claim suggests that we can always generate counter cases by generating successive action pair (q_{T+1}, q_T) according to existing history $\{q_1, \cdots, q_{T-1}\}$. Once we generate a counter case (q_{T+1}, q_T), we can still generate another counter cases (q_{T+3}, q_{T+2}), (q_{T+5}, q_{T+4}), $\cdots$ Also note that, the condition (1) needs $T > e^{\lambda}$. A larger λ means faster time decay on the history and focusing more on the current action. When $\lambda \to \infty_+$ the scoring function degenerates into a non-time-relevant scoring system, and the condition is not satisfied anymore ($T \to \infty_+$), so the counter case is harder to find. In practice, the scoring system usually has multiple factors, which can be tangled in a complex manner, in which case S_T relies on multiple factors, and one action can simultaneously influence multiple factors. In such situations, the attacking policy can be much more complex, which motivates us to use adversarial learning to defend possible attacking policies.