R08323019 呂旻峰

Bayesian Privacy

- What is the question?
  Second Best Contract (Monopolistic Screening) 問題中，適當條件之下，最適機制的結果是設計者事後會完全知道買家的私有資訊，買家因而損失自己所有的隱私。作者們想要討論，假如額外設定買家在機制中隱私損失的上限，那麼會如何改變最適機制的結果。為了處理這個議題，作者們定義如何衡量隱私損失，刻畫出新的最適機制結果並回答了幾個問題，包含：買家的私有資訊揭露至何種程度？不同私有資訊的買家其揭露程度相同嗎？對設計者收益、買家剩餘和總福利的影響？

- Why should we care about this?
  資訊科技的進展使得大型企業有能力獲取並分析個人的大量資料。群眾開始擔憂隱私損失和其帶來的危害，因此認為政府應該管制企業收集和使用個人資料。假如政府真的這麼做，那麼這篇文章的分析可以讓我們明白這個政策經濟上的影響，同時最適機制的結果也提供政府一個簡單的方法檢查企業是否違反管制措施。

- How did you get there?
  從 Second Best Contract (Monopolistic Screening) 出發。在這個模型中，設計者可以透過設計機制 $\mathbb{M} = \langle M, p, q \rangle$ 販售她的產品，其中 M 代表設計者允許買家可以釋放的訊息 m 的集合，$p: M \to R^+$ 和 $q: M \to R^+$ 是設計者制定的遊戲規則。當買家釋放出訊息 m ，設計者承諾以價格 $p(m)$ 販售品質 $q(m)$ 的商品。買家的私有資訊是 $\theta \in [\underline{\theta}, \overline{\theta}]$，代表對每單位品質 q 的願付價格。

  與原本模型不同的地方是，除了 IC 和 IR 限制式以外，作者額外增加了隱私限制式 (Privacy Constraint, P) 設定買家在機制中隱私損失的上限 κ。作者藉由類似 revelation principle 的技巧簡化問題，進而刻劃在適當條件下的最適機制。透過分析這個結果，作者們得到前二個問題的答案，也得知上限 κ 對設計者收益、買家剩餘和總福利的影響。

- What is the answer?
  作者將設計者對 θ 的後驗機率與先驗機率的相對差異定義為隱私損失的大小 (Kullback-Leibler Divergence)。新的最適機制結果是，$[\underline{\theta}, \overline{\theta}]$ 會被分割成不同的區間 (interval) 。私有資訊 θ 落在同一區間的買家會釋放出一樣的訊息，而區間的個數上下限和隱私損失的上限 κ 有關。隱私損失的限制愈嚴格 (κ 愈低)，個數上下限愈低。

  第二個結論是 $\underline{\theta}$ 對應到的區間裡的買家數量最少(或最多)，接著區間裡的買家數量隨著 θ 上升而增加(或減少)；亦即設計者收集到的資訊精確度對 θ 呈現單調性，她會更加清楚低(或高) θ 買家的資訊。

  設計者收益隨著 κ 上升而增加；適當條件下，買家剩餘在 $\kappa = 0$ 時最大，$\kappa = \infty$ 時最小；θ 的密度函數如果是遞增(或遞減)，則總福利在 $\kappa = 0$ 時最大(或最小)，$\kappa = \infty$ 時最小(或最大)。

- Real-world example

  這個議題本身即是由現實生活中的例子簡化而來。當大型網路電商例如 Amazon，被要求限制取得個人消費者的資訊時，這篇文章揭示如何設計機制才能在滿足隱私限制時，取得最大的利益。

- List of notation

  - $F(\theta), f(\theta)$ 設計者對 θ 的先驗機率，$f(\theta)$ 是密度函數
  - σ^* 均衡策略
  - $D_{KL}(F(\cdot\,|m,\sigma^*)\,\|\,F)$ Kullback-Leibler Divergence
  - $I(\mathbb{M},\sigma^*)$ 事後隱私損失 (Ex-post loss of privacy)，σ^* 可以省略
  - $I(\mathbb{M}) \le \kappa$ 隱私限制式 (Privacy Constraint)