Mechanisms as statistical experiments

October 23, 2014

1 Statistical Experiment and Blackwell's Theorem

We focus on the context with finite discrete states. The follows could be easily extended to the general setting.

Let $\Omega = \{\omega_1, \ldots, \omega_n\}$ be a finite set of states. Let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be a finite set of experimental outcomes.

Definition 1. *An experiment is a probability measure from Ω to Γ. It is represented by an $n \times m$ Markov matrix $[P_{ij}]_{i\in[n];\, j\in[m]}$, such that $\Sigma_{j=1}^{m} P_{ij} = 1$ for all $i \in [n]$. P_{ij} is the probability of observing outcome γ_j in state ω_i.*

A decision maker conducts experiments to solve decision problem in which the loss that the decision maker suffers depends on the current state. Let $A \in \mathbb{R}^n$ denote the set of decisions. Suppose $a \in A$, a_i denote the loss of the decision maker if she chooses action a in state ω_i.

Assume the decision maker first observes the outcome of the experiment P and then choose an action from A. A decision rule maps outcomes of P to elements in A. We describe such action decision by a $m \times n$ matrix D, where each row of D is an element of A.

Consider the $n \times n$ matrix PD. The diagonal elements of it describes the expected loss in each state ω_i. Let $diag(PD)$ denote the vector of diagonal of PD, which is called "risk vector" in literature. As D varies over all possible decision rules, we define "risk region" of experiment P with actions A as

$$B(P, A) = \bigcup_{D} diag(PD)$$

Definition 2. *Let P and Q be two experiments. Then P is more informative than Q, written as $P \supset Q$ if $B(Q, A) \subset B(P, A)$ for all closed, bounded and convex subsets $A \in \mathbb{R}^n$*

Definition 3. *Let P and Q be two $n \times m1$ and $n \times m2$ Markov matrices corresponding to two experiments. P is sufficient for Q, denoted as $P \prec Q$, if there is an $m1 \times m2$ Markov matrix T such that $PT = Q$.*

Theorem 1 (Blackwell's)**.** *Let P and Q be two experiments with the same set of actions. Then, $P \supset Q$ iff $P \prec Q$.*

2 Mechanisms as statistical experiments

2.1 Case of DP

For an arbitrary set S and two databases x_0, x_1, define $P_{FA}(x_0, x_1, M, S) = P(M(x_0) \in S)$ and $P_{MD}(x_0, x_1, M, S) = P(M(x_1) \in \bar{S})$. It is easy to see the following is an equivalent definition of DP.

Theorem 2. *For any $\epsilon \geq 0$ and $\delta \in [0, 1]$, a database mechanism M is (ϵ, δ)-differentially private if and only if the following conditions are satisfied for all pairs of neighboring databases x_0 and x_1, and all region $S \subseteq \mathcal{Y}$:*

$$P_{FA}(x_0, x_1, M, S) + e^{\epsilon} P_{MD}(x_0, x_1, M, S) \geq 1 - \delta, \quad \textit{and}$$

$$e^{\epsilon} P_{FA}(x_0, x_1, M, S) + P_{MD}(x_0, x_1, M, S) \geq 1 - \delta.$$

This gives a graphical representation (region) of DP:

$$R(\epsilon, \delta) = \{(P_{MD}, P + FA) \,|\, P_{FA} + e^{\epsilon} P_{MD} \geq 1 - \delta, e^{\epsilon} P_{FA} + P_{MD} \geq 1 - \delta\}.$$

For any two databases x_0 and x_1, define

$$R(M, x_0, x_1) = conv\{(P_{MD}(x_0, x_1, M, S), P_{FA}(x_0, x_1, M, S)) \,|\, \text{for all } S \subseteq \mathcal{Y}\}$$

Define $R(M) = \bigcup_{(x_0, x_1)} R(M, x_0, x_1)$, where (x_0, x_1) is a pair of neighboring databases. It should not hard to see the following theorem.

Theorem 3. *M is (ϵ, δ)-differentially private iff $R(M) \subseteq R(\epsilon, \delta)$.*

Now, consider mechanism M as a statistical experiment defined in section 1.

Let $\mathcal{X}$ be the set of all databases. Let $\mathcal{Y}$ be the set of all out comes of mechanism M. M is a probability measure from $\mathcal{X}$ to $\mathcal{Y}$. For simplicity of analysis, assume $|\mathcal{X}| = n$ and $|\mathcal{Y}| = m$. Then, we have a corresponding $n \times m$ Markov matrix $P_M = [P_{M0}, \ldots, P_{M(n-1)}]^{\top}$.

First, we show $R(M) = B(M, A)$, where $A = [0, 1]^n$. It is sufficient to show $R(M, x_0, x_1) = B(M, A)$ in the case of $\mathcal{X} = \{x_0, x_1\}$. Consider $S = \{y_1, y_2\}$.

$$(P_{MD}(x_0, x_1, M, S), P_{FA}(x_0, x_1, M, S)) =$$

$$[P_{M0}, P_{M1}]^\top \cdot \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ \dots & \dots \\ 0 & 1 \end{bmatrix}$$

Pick $A = [0, 1]^2$, we have

$$R(M, x_0, x_1) =$$

$$conv\{(P_{MD}(x_0, x_1, M, S), P_{FA}(x_0, x_1, M, S)) \,|\, \text{for all } S \subseteq \mathcal{Y}\} = B(M, A).$$

Second, consider two mechanisms M_1, M_2 with the same database space $\mathcal{X}$. If we have $M_1 \prec M_2$, then we have the following Markov chain: $x - M_1(x) - M_2(x)$ for any $x \in \mathcal{X}$.

Theorem 4. *Let two mechanisms M_1, M_2 have the same database space $\mathcal{X}$. Then, $R(M_1) \supset R(M_2)$ iff $M_1 \prec M_2$.*

2.2 Case of CW-P

In the case of CW-P, we can define P_{FA} and P_{MD} as before. The difference is that now each X_i is a variable following some distribution D_i. For the simplicity of analysis, let's consider the case of DDP here. It follows that Theorem 2 and Theorem 3 still hold.

Similarly, we show $R(M, X_0, X_1) = B(M, A)$ in the case of $\mathcal{X} = \{x_0, x_1\}$. Let the pmf of X_0 and X_1 be f_0 and f_1, where f_i has the form $[p_{i0}, p_{i1}]$. Consider $S = \{y_1, y_2\}$.

$$(P_{MD}(X_0, X_1, M, S), P_{FA}(X_0, X_1, M, S)) =$$

$$[f_0, f_1]^\top \cdot [P_{M0}, P_{M1}]^\top \cdot \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ \dots & \dots \\ 0 & 1 \end{bmatrix}$$

Notice that we can construct a new mechanism M' with its corresponding Markov matrix being $[f_0, f_1]^\top \cdot [P_{M0}, P_{M1}]^\top$. M' has database space of size two, corresponding to X_0 and X_1. Pick $A = [0,1]^2$, we have $R(M) = B(M', A)$.

By definition, CW-P consider the case when databases come from a set of distributions $\mathcal{D} = \{D_0, \ldots, D_t\}$. Given mechanism M, it is easy to construct M' as above with a database space of $\{X_0, \ldots, X_t\}$. In fact, any two M_1' and M_2' w.r.t. mechanisms M_1 and M_2 will have the same database space, as long as M_1, M_2 consider the same set of database distribution $\mathcal{D}$.

Let $P_D = [f_t, \ldots, f_t]^\top$, where f_i denote the pmf of D_i. We can compute the Markov matrix of M' as follows.

$$[P_{M'}] = [P_D] \cdot [P_M]$$

Lemma 1. *Let two mechanisms M_1, M_2 have the same set of distributions on databases $\mathcal{D}$. Then, $M_1 \prec M_2$ iff $M_1' \prec M_2'$.*

Theorem 5. *Let two mechanisms M_1, M_2 have the same set of distributions on databases $\mathcal{D}$. Then, $R(M_1) \supset R(M_2)$ iff $M_1 \prec M_2$.*