

『データ解析におけるプライバシー保護』第1刷正誤表

この度は、標記書籍をお買い求めいただき誠にありがとうございました。
標記書籍に誤りがありました。訂正し、深くお詫び申し上げます。

ページ数	位置	誤	正
xiii	4 行目	8.3.4 ラプラスメカニズムの正確性	8.3.4 ラプラスメカニズムの有用性
	11 行目	8.5.2 指数メカニズムの正確性	8.5.2 指数メカニズムの有用性
xvi	下から 3 行目	bit 例 a, b の連結	bit 列 a, b の連結
	下から 2 行目	bit 例 a, b の排他的理論和	bit 列 a, b の排他的理論和
3	9 行目	データベースが記録の対象としている人間は全部で N 人であり、	データベースが記録の対象としている人間は全部でたとえば $n = 100$ 人であり、
7	9 行目	SNS のアカウント情報など	SNS のアカウント情報や履歴情報など
43	下から 5 行目	d_{Q_I} 個の属性を間接識別情報とします。 k 匿名性が仮定する	d_{Q_I} 個の属性を間接識別情報とします。 Q_I は間接識別情報 (quasi identifier) を表す添え字です。 k 匿名性が仮定する
47	下から 3 行目	母集団一意性は統計的に推定します。	母集団一意性は統計的に推定し、これを特定リスクの評価値として利用できます。
76	18 行目	$\mathcal{A}(x)$ は確率分布になります。	$\mathcal{A}(x)$ は確率変数になります。
77	9 行目	確率変数の取りうる値を Ω とします	確率変数の取りうる値の集合を Ω とします
	20 行目	出た値を 10 倍する関数を	たとえば、出た値を 10 倍する関数を
79	下から 2 行目	その出力は確率分布になります。	その出力はある確率分布に従います。
80	式 (6.2)	$\Pr_{z \leftarrow f(x)}(y = z) - \Pr_{z \leftarrow f(x')}(y = z) = 0 \quad (6.2)$	$\Pr_{z \leftarrow f(x)}(z = y) - \Pr_{z \leftarrow f(x')}(z = y) = 0 \quad (6.2)$
92	図 7.2 左下囲み	コントロール群 (疾患あり)	コントロール群 (疾患なし)
93	8 行目	個人の特定性は必ずしも失われない	個人の属性値が推測される
	下から 8 行目	X はレコードのドメインです。	X はレコードの定義域です。
94	下から 3 行目	出力を入力にとり、何らかの応答値を返す	出力 y を入力にとり、何らかの応答値 z を返す
97	下から 6 行目	このように平均値を応答するクエリが安全であるとはいえません。データベースに依存せず、応答そのものについて秘匿性を保証するには、	平均値を応答するクエリが常に安全であるとはいえません。あるクエリについて、データベースに依存せず、その応答について秘匿性を保証するには、
98	1 行目	「弱い秘匿性」は、どのような	「弱い秘匿性」は、あるクエリ q についてどのような
	6 行目	ここで、 c は 1 より大きいある正の定数です。	ここで、 c は 1 より大きいある有限の定数です。
104	定理 7.3	メカニズム m は (ϵ, δ) -差分プライバシーを満たすとして、このとき、少なくとも確率 $1 - \delta'$ で以下が成り立ちます。 $e^{-\epsilon'} \Pr(m(D') = y) \leq \Pr(m(D) = y) \leq e^{\epsilon'} \Pr(m(D') = y).$	メカニズム m はクエリ q について (ϵ, δ) -差分プライバシーを満たすとして、このとき、少なくとも確率 $1 - \delta'$ で以下が成り立ちます。 $e^{-\epsilon'} \Pr(m(q, D') = y) \leq \Pr(m(q, D) = y) \leq e^{\epsilon'} \Pr(m(q, D') = y).$
	下から 2 行目	$Z = \{y \Pr(m(D) = y) \geq e^{2\epsilon} \Pr(m(D') = y)\}$ とします。	$Z = \{y \Pr(m(q, D) = y) \geq e^{2\epsilon} \Pr(m(q, D') = y)\}$ とします。
105	式 (7.13)	$\Pr(m(D) \in Z) \geq e^{2\epsilon} \Pr(m(D') \in Z) \geq e^{\epsilon} (1 + \epsilon) \Pr(m(D') \in Z) \quad (7.13)$	$\Pr(m(q, D) \in Z) \geq e^{2\epsilon} \Pr(m(q, D') \in Z) \geq e^{\epsilon} (1 + \epsilon) \Pr(m(q, D') \in Z) \quad (7.13)$
	式 (7.14)	$e^{\epsilon} \Pr(m(D') \in Z) \leq \Pr(m(D) \in Z) - e^{\epsilon} \Pr(m(D') \in Z) \leq \delta \quad (7.14)$	$e^{\epsilon} \Pr(m(q, D') \in Z) \leq \Pr(m(q, D) \in Z) - e^{\epsilon} \Pr(m(q, D') \in Z) \leq \delta \quad (7.14)$

	6~10 行目	$\Pr(m(D') \in Z) < \frac{\delta}{e\epsilon^e}. \quad (7.15)$ 同様に、$Z' = \{y \Pr(m(D) = y) < e^{-2\epsilon} \Pr(m(D') = y)\}$ とすると、 $\Pr(m(D') \in Z') < \frac{\delta}{e\epsilon^e}. \quad (7.16)$ これより $\Pr(m(D') \in Z \cup Z') < \frac{2\delta}{e\epsilon^e}$ を得ます。このことは、 $e^{-2\epsilon} \Pr(m(D') = y) \leq \Pr(m(D) = y) \leq e^{2\epsilon} \Pr(m(D') = y) \quad (7.17)$	$\Pr(m(q, D') \in Z) < \frac{\delta}{e\epsilon^e}. \quad (7.15)$ 同様に、$Z' = \{y \Pr(m(q, D) = y) < e^{-2\epsilon} \Pr(m(q, D') = y)\}$ とすると、 $\Pr(m(q, D') \in Z') < \frac{\delta}{e\epsilon^e}. \quad (7.16)$ これより $\Pr(m(q, D') \in Z \cup Z') < \frac{2\delta}{e\epsilon^e}$ を得ます。このことは、 $e^{-2\epsilon} \Pr(m(q, D') = y) \leq \Pr(m(q, D) = y) \leq e^{2\epsilon} \Pr(m(q, D') = y) \quad (7.17)$
106	7 行目	10.7.4 節を参照	7.10.5 節を参照
107	式 (7.18)	$b(D y) = \frac{\Pr(m(D, q) = y)b(D)}{\sum_{Z \in \mathcal{D}} \Pr(m(Z, q) = y)b(Z)} \quad (7.18)$	$b(D y) = \frac{\Pr(m(q, D) = y)b(D)}{\sum_{Z \in \mathcal{D}} \Pr(m(q, Z) = y)b(Z)} \quad (7.18)$
108	定義 7.4	X と Y を確率変数とする 2 つの確率分布分布 d_X , d_Y を考えます。	X と Y を確率変数とする 2 つの確率分布 d_X , d_Y を考えます。
	式 (7.20)	$b_i(D y) = \frac{\Pr(m(D_{-i}, q) = y)b(D)}{\sum_{Z \in \mathcal{D}} \Pr(m(Z_{-i}, q) = y)b(Z)} \quad (7.20)$	$b_i(D y) = \frac{\Pr(m(q, D_{-i}) = y)b(D)}{\sum_{Z \in \mathcal{D}} \Pr(m(q, Z_{-i}) = y)b(Z)} \quad (7.20)$
109	定義 7.5	任意のメカニズム m の出力 $y \in Y$,	メカニズム m の任意の出力 $y \in Y$,
	9 行目	定義 7.6	定理 7.6
	式 (7.22)	$e^{-\epsilon/2} \Pr(m(D_{-i}, q) = y) \leq \Pr(m(D, q) = y) \leq e^{\epsilon/2} \Pr(m(D_{-i}, q) = y) \quad (7.22)$	$e^{-\epsilon/2} \Pr(m(q, D_{-i}) = y) \leq \Pr(m(q, D) = y) \leq e^{\epsilon/2} \Pr(m(q, D_{-i}) = y) \quad (7.22)$
	下から 1 行目	$\frac{b(D y)}{b_i(D y)} = \frac{\Pr(m(D, q) = y)}{\Pr(m(D_{-i}, q) = y)} \frac{\sum_{Z \in \mathcal{D}} \Pr(m(Z_{-i}, q) = y)b(Z)}{\sum_{Z \in \mathcal{D}} \Pr(m(Z, q) = y)b(Z)}$	$\frac{b(D y)}{b_i(D y)} = \frac{\Pr(m(q, D) = y)}{\Pr(m(q, D_{-i}) = y)} \frac{\sum_{Z \in \mathcal{D}} \Pr(m(q, Z_{-i}) = y)b(Z)}{\sum_{Z \in \mathcal{D}} \Pr(m(q, Z) = y)b(Z)}$
110	1 行目	$\leq e^{\epsilon/2} \cdot \frac{\sum_{Z \in \mathcal{D}} e^{\epsilon/2} \Pr(m(Z, q) = y)b(Z)}{\sum_{Z \in \mathcal{D}} \Pr(m(Z, q) = y)b(Z)} = e^{\epsilon}.$	$\leq e^{\epsilon/2} \cdot \frac{\sum_{Z \in \mathcal{D}} e^{\epsilon/2} \Pr(m(q, Z) = y)b(Z)}{\sum_{Z \in \mathcal{D}} \Pr(m(q, Z) = y)b(Z)} = e^{\epsilon}.$
111	5~9 行目	することもできます。2 つの確率変数 $x, y \in R$ の間の max divergence は以下のように与えられます。 $d_{\max}(x y) = \max_{S \subseteq R} \ln \frac{\Pr(x \in S)}{\Pr(y \in S)}$ 同様に、δ 近似 max divergence は以下のように与えられます。 $d_{\max}^{\delta}(x y) = \max_{S \subseteq R: \Pr(y \in S) \geq \delta} \ln \frac{\Pr(x \in S) - \delta}{\Pr(y \in S)}$	することもできます。2 つの確率変数 $x, y \in \Omega$ の間の max divergence は以下のように与えられます。 $d_{\max}(x y) = \max_{S \subseteq \Omega} \ln \frac{\Pr(x \in S)}{\Pr(y \in S)}$ 同様に、δ 近似 max divergence は以下のように与えられます。 $d_{\max}^{\delta}(x y) = \max_{S \subseteq \Omega: \Pr(y \in S) \geq \delta} \ln \frac{\Pr(x \in S) - \delta}{\Pr(y \in S)}$
	11~13 行目	$d_{\max}(m(D, q) m(D', q)) \leq \epsilon$ であることは等価です。 また、メカニズム m が (ϵ, δ) 差分プライバシーであることと、 $d_{\max}^{\delta}(m(D, q) m(D', q)) \leq \epsilon$ であることは等価です。	$d_{\max}(m(q, D) m(q, D')) \leq \epsilon$ であることは等価です。 また、メカニズム m が (ϵ, δ) 差分プライバシーであることと、 $d_{\max}^{\delta}(m(q, D) m(q, D')) \leq \epsilon$ であることは等価です。
117	12 行目	また D' の各レコードを D	また D' の各レコードを D'
118	9 行目	$= \max_{x_n, x'_n \in [0, 1]} \left \max_i x_i - \max_i x'_i \right = 1 - 0 = 1$	$= \max_{x_n, x'_n \in [0, 1]} x_n - x'_n = 1 - 0 = 1$
119	5 行目	クエリ q の l_1 感度を	クエリ q の ℓ_1 感度を
	8 行目	出力を $m_{\text{Lap}}(D, q)$ と書きます。	出力を $m_{\text{Lap}}(q, D)$ と書きます。
	下から 2 行目	$m_{\text{Lap}}(D, q)$ と書くことにします。	$m_{\text{Lap}}(q, D)$ と書くことにします。
120	式 (8.4)	$p(m_{\text{Lap}}(D, q) = y)$	$p(m_{\text{Lap}}(q, D) = y)$
	式 (8.5)	$\left \ln \frac{p(m_{\text{Lap}}(D, q) = y)}{p(m_{\text{Lap}}(D', q) = y)} \right = \left \ln \frac{\exp\left(-\frac{\epsilon y-q(D) }{\Delta_{1,q}}\right)}{\exp\left(-\frac{\epsilon y-q(D') }{\Delta_{1,q}}\right)} \right $	$\left \ln \frac{p(m_{\text{Lap}}(q, D) = y)}{p(m_{\text{Lap}}(q, D') = y)} \right = \left \ln \frac{\exp\left(-\frac{\epsilon y-q(D) }{\Delta_{1,q}}\right)}{\exp\left(-\frac{\epsilon y-q(D') }{\Delta_{1,q}}\right)} \right $
	1 行目		
	14~15 行目	8.3.4 ラプラスメカニズムの正確性 ラプラスメカニズムの正確性については	8.3.4 ラプラスメカニズムの有用性 ラプラスメカニズムの有用性については
	定理 8.3	定理 8.3 (ラプラスメカニズムの正確性) $y = m_{\text{Lap}}(D, q)$ とします。	定理 8.3 (ラプラスメカニズムの有用性) $y = m_{\text{Lap}}(q, D)$ とします。
	下から 2 行目	ラプラスメカニズムの正確性を示しましょう。	ラプラスメカニズムの有用性を示しましょう。
124	16 行目	真の主力 $q(D)$ に近いほど、	真の出力 $q(D)$ に近いほど、
126	5~6 行目	8.5.2 指数メカニズムの正確性 続いて、指数メカニズムが応答する値の正確性	8.5.2 指数メカニズムの有用性 続いて、指数メカニズムが応答する値の有用性

	定理 8.7	定理 8.7 (指数メカニズムの正確性)	定理 8.7 (指数メカニズムの有用性)
129	定理 8.8 下から 2 行目	$\{m_i(D)\}_{i=1}^k$ を出力する	$\{m_i(q_i, D)\}_{i=1}^k$ を出力する
130	2~5 行目	$\frac{\Pr(m_i(D, q_i) = y)}{\Pr(m_i(D', q_i) = y)} \leq e^{\epsilon_i}$ このとき, $\frac{\Pr(m(D, q) = (y_1, \dots, y_k))}{\Pr(m(D', q) = (y_1, \dots, y_k))} = \frac{\prod_{i=1}^k \Pr(m_i(D, q_i) = y_i)}{\prod_{i=1}^k \Pr(m_i(D', q_i) = y_i)} = \prod_{i=1}^k \left(\frac{\Pr(m_i(D, q_i) = y_i)}{\Pr(m_i(D', q_i) = y_i)} \right)$	$\frac{\Pr(m_i(q_i, D) = y)}{\Pr(m_i(q_i, D') = y)} \leq e^{\epsilon_i}$ このとき, $\frac{\Pr(m(q, D) = (y_1, \dots, y_k))}{\Pr(m(q, D') = (y_1, \dots, y_k))} = \frac{\prod_{i=1}^k \Pr(m_i(q_i, D) = y_i)}{\prod_{i=1}^k \Pr(m_i(q_i, D') = y_i)} = \prod_{i=1}^k \left(\frac{\Pr(m_i(q_i, D) = y_i)}{\Pr(m_i(q_i, D') = y_i)} \right)$
131	1 行目	定義 8.9	定理 8.9
137	定義 8.10 5~7 行目	$q_i \geq \theta - \alpha$ が成り立ち, また $y_i = \text{false}$ となるような q_i については $q_i \leq \theta + \alpha$	$q_i(D) \geq \theta - \alpha$ が成り立ち, また $y_i = \text{false}$ となるような q_i については $q_i(D) \leq \theta + \alpha$
144	式 (9.8)	$h(\alpha x + (1 - \alpha)) \leq \alpha h(x) +$	$h(\alpha x + (1 - \alpha)y) \leq \alpha h(x) +$
146	9 行目	$= \frac{1}{n} \ell(y_n) \{ \ell(y_n, \hat{y}_n) - \ell(y'_n, \hat{y}'_n) \}$	$= \frac{1}{n} \{ \ell(y_n, \hat{y}_n) - \ell(y'_n, \hat{y}'_n) \}$
149	定理 9.3 2 行目	モデルの経験損失と期待損失の差は	モデルの経験損失と真の経験損失の差は
151	式 (9.23)	$\frac{\Pr(\tilde{w}^* D)}{\Pr(\tilde{w}^* D')} = \frac{\nu(\mathbf{b})}{\nu(\mathbf{b}')} \frac{ \det(\mathbf{H}(\mathbf{w} \rightarrow \mathbf{b} D)) ^{-1}}{ \det(\mathbf{H}(\mathbf{w} \rightarrow \mathbf{b}' D')) ^{-1}} \leq \exp(\epsilon) \quad (9.23)$	$\frac{\Pr(\tilde{w}^* D)}{\Pr(\tilde{w}^* D')} = \frac{\nu(\mathbf{b})}{\nu(\mathbf{b}')} \frac{ \det(\mathbf{H}(\mathbf{w} \rightarrow \mathbf{b} D)) ^{-1}}{ \det(\mathbf{H}(\mathbf{w} \rightarrow \mathbf{b}' D')) ^{-1}} \leq \exp(\epsilon) \quad (9.23)$
169~170	下から 1 行目~1 行目	ここで 田 は要素ごとの排他的論理和です. 平文と同じ長さの鍵を用いて, 平文をランダム化します.	ここで 田 は要素ごとの排他的論理和です.
202	下から 1 行目	計算すれば, $(u_1, \dots, u_m)$ は	計算すれば, $(u'_1, \dots, u'_m)$ は
206	下から 6 行目	10 万次元のベクトルの内積計算に約 0.55 秒, 1 万次元のベクトルの内積計算に約 0.15 秒, 10 万次元のベクトルの内積計算に約 0.55 秒, 1 万要素の数値の比較に約 25 秒, 10 万要素の数値の比較に 275 秒を要しています.	10 万次元のベクトルの内積計算に約 0.55 秒, 1 万要素の数値の比較に約 25 秒, 10 万要素の数値の比較に約 275 秒を要しています.