Vorlesungsskriptum zu

Statistisches Schätzen unter ‘differential privacy’

von Lukas Steinberger

11. Februar 2019

Inhaltsverzeichnis

Vorwort

Dieses Skriptum entsteht begleitend zur Vorlesung ‘Statistical estimation under differential privacy’ vom Sommersemester 2018 an der Albert-Ludwigs-Universität Freiburg. Es werden nur Vorkenntnisse aus Wahrscheinlichkeitstheorie und etwas Funktionalanalysis vorausgesetzt. Die nötigen Begriffe der mathematischen Statistik werden kurz wiederholt. Ein Grundverständnis der mathematischen Statistik, insbesondere der asymptotischen Minimax-Schätzung, ist aber jedenfalls sehr hilfreich.

Freiburg, 11. Februar 2019

Kapitel 1

Grundbegriffe

1.1 Motivation

Wir betrachten eine Situation in der eine gegebene Anzahl von n Individuen sensible Daten (z.B. medizinische Daten, Smartphone-Nutzerdaten, etc.) besitzen. Die Daten des i-ten Individuums bezeichnen wir mit $x_i \in \mathbb{R}^d$. Die Gesellschaft möchte nun die in diesen Daten enthaltene Information verwenden (z.B. Forschung, Technik, öffentlicher Verkehr, etc.). Andererseits möchten die Individuen ihre Privatsphäre schützen und sind nicht bereit ihre Daten ohne weiteres zu veröffentlichen.

Daten	Individuen	Alter	Geschlecht	...	Diabetes (ja/nein)
$x_1 =$	Alice	34	w	...	0
$x_2 =$	Bob	34	m	...	1
$\vdots$					$\vdots$
$x_n =$	Zoey	28	w	...	0

Tabelle 1.1: Beispiel einer typischen Datenmatrix x.

Es lassen sich jetzt grundsätzlich zwei Szenarien unterscheiden.

1. Es gibt einen vertrauenswürdigen Datenbankbetreiber (trusted curator). Die Individuen geben ihre Originaldaten x_i an den Datenbankbetreiber weiter und dieser garantiert im Gegenzug, dass die Daten nur in geeignet privatisierter Form an Dritte weitergegeben werden (siehe Tabelle 1.2).
2. Die Individuen vertrauen niemandem (no trusted curator). Anstelle der Originaldaten sind sie lediglich bereit eine geeignet verschleierte Version z_i ihrer Daten zu veröffentlichen (siehe Tabelle 1.3).

Im ersten Fall (trusted curator) scheint das Problem der Privatisierung eine einfache und wohlbekannte Lösung zu haben. Wir entfernen einfach sämtliche Informationen aus der Datenbank, die ein Individuum eindeutig identifizieren (z.B. Name, Steuernummer, etc.). Wir bezeichnen diesen Vorgang im Folgenden auch als Anonymisierung. Anstelle von x wie in Tabelle 1.1 veröffentlichen wir also

$$z = \begin{pmatrix} 34 & w & \dots & 0 \\ 34 & m & \dots & 1 \\ \vdots & & & \vdots \\ 28 & w & \dots & 0 \end{pmatrix}.$$

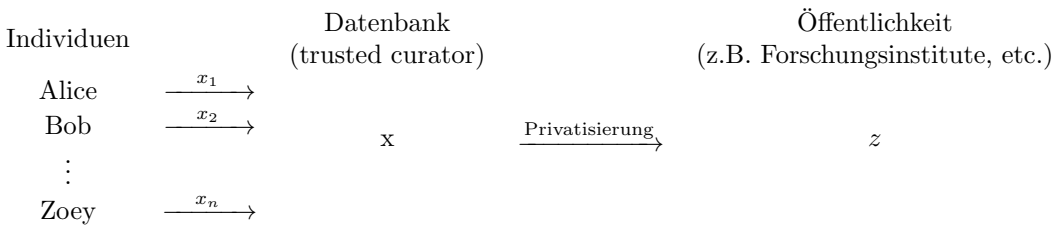


Tabelle 1.2: Die Individuen vertrauen ihre Daten einem Datenbankbetreiber an, welcher die Daten nur in 'privatisierter' Form weiter gibt.

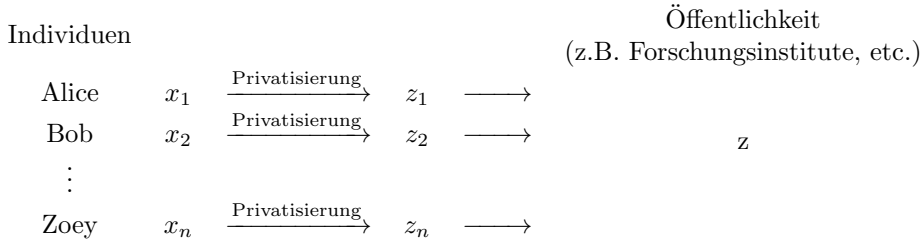


Tabelle 1.3: Die Individuen vertrauen niemandem und geben nur bereits privatisierte Daten z_i weiter.

Dies ist aber keine zufriedenstellende Lösung des Privatisierungsproblems. Denn wenn wir wissen, dass Bob 34 Jahre alt ist und er zufälligerweise der einzige Mann in der Datenbank mit diesem Alter ist, so wissen wir bereits, dass er Diabetes hat. Die Chance ein Individuum in der Datenbank eindeutig identifizieren zu können wird natürlich entsprechend höher, wenn man mehr als nur zwei Merkmale verwendet, wie das folgende reale Beispiel zeigt.

Beispiel (Netflix-Preis)**.** *Das obige Beispiel dient natürlich nur der Illustration. Ein praxisnahes Beispiel ist etwa der Fall des sogenannten Netflix-Preises (siehe Narayanan and Shmatikov, 2006). Im Jahr 2006 wollte der bekannte Videoverleih Netflix sein internes Empfehlungssystem verbessern um seinen Kunden basierend auf deren Filmbewertungen (1 bis 5 Sterne) sinnvolle Vorschläge für weitere noch nicht gesehene Filme machen zu können. Dazu veröffentlichte das Unternehmen einen Teil seiner echten Bewertungsdatenbank, natürlich ohne Kundennamen, und schrieb ein Preisgeld für den Algorithmus aus, der die beste Prognose für die Kundenbewertungen errechnet. Die Wettbewerbsteilnehmer konnten also die anonymisierten Bewertungen von knapp 500.000 Netflix Kunden einsehen, um daraus deren Präferenzen zu lernen. Einige Bewertungen wurden von Netflix einbehalten. An diesen sollten die von den Teilnehmern entwickelten Algorithmen dann getestet werden um einen Sieger zu ermitteln. Den Autoren Narayanan and Shmatikov (2006) gelang es nun, mit Hilfe von öffentlich zugänglichen Filmbewertungen auf IMDB, den Netflix Datensatz weitestgehend zu Deanonymisieren. Insbesondere konnten sie zeigen, dass man mit nur acht Filmbewertungen 99% aller Einträge in der Netflix-Datenbank eindeutig identifizieren kann. Nun scheint die Tragweite dieses Problems auf den ersten Blick relativ beschränkt zu sein, da Filmbewertungen keine sensiblen Informationen darstellen. Allerdings lassen sich aufgrund von hunderten Filmbewertungen einer Person durchaus gewisse Schlüsse über, zum Beispiel, deren politische Gesinnung oder sexuelle Orientierung ziehen, was etwa einen potentiellen Arbeitgeber beeinflussen könnte.*

Wir haben also gesehen, dass es keineswegs genügt einfach die Personenkennungen aus der Datenbank zu entfernen, da unter Verwendung von geeigneter Zusatzinformation die Individuen dennoch identifiziert werden können. Es dürfen also auch die anonymisierten Originaldaten nicht veröffentlicht werden.

Idee: Veröffentliche eine geeignet manipulierte bzw. verrauschte Version der Originaldaten, so dass die Identifikation von Individuen erschwert wird aber ein gewisser Informationsgehalt erhalten bleibt.

1.2 Differentielle und lokal differentielle Privatisierung

Es seien $(\mathcal{X}, \mathcal{F})$ und $(\mathcal{Z}, \mathcal{G})$ messbare Räume, $x_1, \dots, x_n \in \mathcal{X}$ und $x = (x_1, \dots, x_n)^t \in \mathcal{X}^n$ die Originaldaten. Für $x, x' \in \mathcal{X}^n$, schreiben wir $d_0(x, x') := \#\{i : x_i \neq x'_i\}$ für die Anzahl der nicht übereinstimmenden Komponenten der beiden n-Tupel x und x'. Mit $(\mathcal{X}^n, \mathcal{F}^{\otimes n})$ bezeichnen wir den n-fachen Produktraum von $(\mathcal{X}, \mathcal{F})$ und mit $\mathcal{B}([0,1])$ die Borelmengen von $[0,1]$. Weiter sei $Q : \mathcal{G} \times \mathcal{X}^n \to [0,1]$ ein Markov-Kern. Wir bezeichnen Q auch als **Kanal**, als **Privatisierungsmechanismus** oder als **channel distribution**. Zur Erinnerung, ein Markov-Kern ist definiert durch die folgenden Eigenschaften:

- $x \mapsto Q(A|x)$ ist $\mathcal{F}^{\otimes n} - \mathcal{B}([0,1])$-messbar für alle $A \in \mathcal{G}$.
- $A \mapsto Q(A|x)$ ist ein W-Maß auf $(\mathcal{Z}, \mathcal{G})$ für alle $x \in \mathcal{X}^n$.

Idee: Gegeben die Daten $x \in \mathcal{X}^n$, lassen sich aus dem W-Maß $Q(dz|x)$ privatisierte/randomisierte Daten $z \in \mathcal{Z}$ generieren.

1.2.1 Differentielle Privatisierung

Wir benötigen zunächst eine formale Definition dafür was es heißt, dass ein Privatisierungsmechanismus Q die Privatsphäre der Individuen schützt.

Definition 1.1 (Dwork et al. (2006); Evfimievski et al. (2003))**.** *Sei $\alpha \in (0, \infty)$. Ein Kanal $Q : \mathcal{G} \times \mathcal{X}^n \to [0,1]$ ist α-**differentiell privat** (α-**DP**), falls für alle $x, x' \in \mathcal{X}^n$ mit $d_0(x, x') = 1$ und alle $A \in \mathcal{G}$ gilt, dass*

$$Q(A|x) \;\leq\; e^{\alpha}\, Q(A|x').$$

Idee: Die Verteilung der privatisierten (veröffentlichten) Daten z hängt nicht zu stark von den Daten eines einzelnen Individuums ab.

Korollar 1.2. *Sei $f : (\mathcal{Z}, \mathcal{G}) \to (\mathbb{R}^m, \mathcal{B}(\mathbb{R}^m))$ eine messbare Funktion und $Q : \mathcal{G} \times \mathcal{X}^n \to [0,1]$ α-DP. Dann ist auch die Verteilung von f unter Q α-DP, d.h.,*

$$Q(\{z : f(z) \in A\}|x) \;\leq\; e^{\alpha}\, Q(\{z : f(z) \in A\}|x'),$$

für alle $A \in \mathcal{B}(\mathbb{R}^m)$ und für alle $x, x' \in \mathcal{X}^n$ mit $d_0(x, x') = 1$.

Beweis. Trivial, da $\{z : f(z) \in A\} = f^{-1}(A) \in \mathcal{G}$. □

Bemerkung 1.3.

a) Klarerweise gilt in Definition 1.1, je kleiner $\alpha > 0$, desto strenger ist der Schutz der Privatsphäre. Im Grenzfall $\alpha = 0$ hat die Verteilung der privatisierten Daten z nichts mehr mit den Originaldaten x zu tun.

b) Im Allgemeinen kann unter Definition 1.1 die Verteilung der privatisierten Daten $z \in \mathcal{Z}$ von allen $x_1, \dots, x_n \in \mathcal{X}$ abhängen. Dies lässt sich praktisch nur dann realisieren, wenn es einen 'trusted curator' gibt.

c) Korollar 1.2 zeigt, dass auch jede Berechnung die auf α-differentiell privatisierten Daten z beruht selbst wieder α-DP ist, die Verteilung des Ergebnisses also wiederum kaum von den Originaldaten eines einzelnen Individuums abhängt.

1.2.2 Lokal differentielle Privatisierung

Definition 1.4. *Ein Kanal $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ ist **nicht-interaktiv (NI)** falls es Kanäle $Q_i : \mathcal{G} \times \mathcal{X} \to [0,1]$, $i = 1, \dots, n$, gibt, mit*

$$Q(A_1 \times \cdots \times A_n | x_1, \dots, x_n) = \prod_{i=1}^{n} Q_i(A_i | x_i), \qquad \text{für alle } A_i \in \mathcal{G}, x_i \in \mathcal{X} \text{ und } i = 1, \dots, n.$$

Korollar 1.5. *Sei $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ nicht-interaktiv. Dann ist Q α-DP, genau dann wenn für alle $i = 1, \dots, n$, $Q_i : \mathcal{G} \times \mathcal{X}^1 \to [0,1]$ α-DP ist.*

Beweis. Sei Q α-DP, $i \in \{1, \dots, n\}$, $x_1, \dots, x_n \in \mathcal{X}$ und $A_i \in \mathcal{G}$. Da Q NI ist, gilt $Q_i(A_i|x_i) = Q(\mathcal{Z} \times \cdots \times A_i \times \cdots \times \mathcal{Z} | x_1, \dots, x_n)$ und somit sofort auch, dass Q_i α-DP ist. Für die Umkehrung, fixiere $x, x' \in \mathcal{X}^n$ mit $x_i \neq x_i'$, $d_0(x, x') = 1$ und $A \in \mathcal{G}^{\otimes n}$, und verwende die NI Eigenschaft von Q gemeinsam mit dem Satz von Tonelli um

$$\begin{aligned}
Q(A|x) &= \int_{\mathcal{Z}} \cdots \int_{\mathcal{Z}} \mathbb{1}_A(z_1, \dots, z_n) \bigotimes_{j=1}^{n} Q(dz_j | x_j) \\
&= \int_{\mathcal{Z}} \cdots \int_{\mathcal{Z}} Q_i(A(z_1, \dots, z_{i-1}, z_{i+1}, \dots, z_n) | x_i) \bigotimes_{j \neq i} Q(dz_j | x_j) \\
&\leq \int_{\mathcal{Z}} \cdots \int_{\mathcal{Z}} e^{\alpha} Q_i(A(z_1, \dots, z_{i-1}, z_{i+1}, \dots, z_n) | x_i') \bigotimes_{j \neq i} Q(dz_j | x_j) \\
&= e^{\alpha} Q(A|x'),
\end{aligned}$$

zu erhalten, wobei für $(z_1, \dots, z_{i-1}, z_{i+1}, \dots, z_n) \in \mathcal{Z}^{n-1}$, die Menge $A(z_1, \dots, z_{i-1}, z_{i+1}, \dots, z_n)$ gegeben ist durch $\{z_i \in \mathcal{Z} : (z_1, \dots, z_n) \in A\}$. Somit ist Q also α-DP. □

Bemerkung 1.6.

a) Nicht-interaktive Privatisierungsmechanismen sind besonders dann von Interesse, wenn die Individuen niemandem ihre Originaldaten anvertrauen wollen (no trusted curator). In diesem Fall kann das i-te Individuum seine Daten x_i (lokal, z.B. auf dem eigenen Rechner/Smartphone etc.) selbst mittels $Q_i(dz_i|x_i)$ privatisieren und nur das Ergebnis z_i weitergeben. Wir sprechen auch von 'lokal differentieller Privatisierung' ('local differential privacy').

b) Der Begriff der interaktiven, bzw. nicht-interaktiven Privatisierungsmechanismen ist nicht zu verwechseln mit dem Begriff eines interaktiven Veröffentlichungsprotokolls, bei dem ein Analyst wiederholte Abfragen an eine Datenbank stellen kann (vgl. Dwork, 2008). Hier betrachten wir ausschließlich 'nicht-interaktive Protokolle', in dem Sinne, dass die Daten nur ein einziges Mal privatisiert und veröffentlicht werden.

Beispiel 1.7.

a) Sei P ein W-Maß auf $(\mathcal{Z}, \mathcal{G})$. Dann ist für $A \in \mathcal{G}$ und $x \in \mathcal{X}^n$, der Kanal $Q(A|x) := P(A)$ α-DP für jedes $\alpha \in (0, \infty)$, aber ein uninformativer (trivialer) Mechanismus.

b) Sei $\alpha \in (0, \infty)$, $\mathcal{Z} = \mathcal{X} = \mathbb{R}$, $\mathcal{G} = \mathcal{B}(\mathbb{R})$, $z_0 = \frac{e^{\alpha}+1}{e^{\alpha}-1}$ und für $x \in \mathbb{R}$, definiere $T(x) = \min(\max(x, -1), 1) \in [-1, 1]$. Betrachte einen nicht-interaktiven Kanal $Q : \mathcal{B}(\mathbb{R}^n) \times \mathbb{R}^n \to [0,1]$ mit identischen Marginalen $Q_i = Q_1$ gegeben durch

$$\begin{aligned}
Q_1(\{z_0\}|x) &:= \frac{1}{2}\left(1 + \frac{T(x)}{z_0}\right), \\
Q_1(\{-z_0\}|x) &:= \frac{1}{2}\left(1 - \frac{T(x)}{z_0}\right).
\end{aligned}$$

Dann gilt für $x, x' \in \mathbb{R}$ und $A \in \mathcal{B}(\mathbb{R})$,

$$\frac{Q_1(A|x)}{Q_1(A|x')} = \begin{cases} \frac{0}{0} = 1, & \{-z_0, z_0\} \cap A = \varnothing, \\ \frac{1}{1} = 1, & \{-z_0, z_0\} \subseteq A, \\ \frac{1+\frac{T(x)}{z_0}}{1+\frac{T(x')}{z_0}}, & z_0 \in A, -z_0 \notin A, \\ \frac{1-\frac{T(x)}{z_0}}{1-\frac{T(x')}{z_0}}, & z_0 \notin A, -z_0 \in A. \end{cases}$$

Weiters sieht man leicht, dass

$$\frac{1+\frac{T(x)}{z_0}}{1+\frac{T(x')}{z_0}} \leq \frac{1+\frac{e^\alpha-1}{e^\alpha+1}}{1-\frac{e^\alpha-1}{e^\alpha+1}} = \frac{\frac{2e^\alpha}{e^\alpha+1}}{\frac{2}{e^\alpha+1}} = e^\alpha,$$

und analog

$$\frac{1-\frac{T(x)}{z_0}}{1-\frac{T(x')}{z_0}} \leq e^\alpha,$$

Somit ist Q nach Korollar 1.5 α-DP. Außerdem gilt, dass für $x_i \in \mathbb{R}$,

$$\mathbb{E}_{Q_{(x)}}[Z_i] := \int_{\mathbb{R}^n} \pi_i(z)\, Q(dz|x) = \int_{\mathbb{R}} z_i\, Q_i(dz_i|x_i) = T(x_i),$$

wobei $\pi_i(z) = z_i$ die i-te Koordinatenprojektion ist und $Q_{(x)}(dz) = Q(dz|x)$. Die Verteilung der privatisierten Daten des i-ten Individuums trägt also noch eine gewisse Information über die Originaldaten x_i.

c) Sei wiederum $\alpha \in (0, \infty)$ und $\mathcal{Z} = \mathcal{X} = \mathbb{R}$, $\mathcal{G} = \mathcal{B}(\mathbb{R})$ und für $x, z \in \mathbb{R}$, betrachte die Dichte einer Laplace-Verteilung mit Mittelwert x und Skalenparameter $\alpha/2$,

$$q(z|x) := \frac{\alpha/2}{2} \exp\left(-\frac{\alpha}{2}|z-x|\right).$$

Konstruiere nun den nicht-interaktiven Kanal Q mit identischen Marginalen $Q_i = Q_1$ durch

$$Q_1(A|x) := \int_A q(z|x)\, dz.$$

Anders ausgedrückt randomisiert der so konstruierte Kanal den Wert von x_i durch Addition einer Zufallszahl mit Laplace($\alpha/2$)-Verteilung. Die privatisierten Daten von Individuum i werden also generiert als $Z_i = x_i + W_i$, mit $W_i \sim \mathit{Laplace}(\alpha/2)$. Wir berechnen jetzt für $x \in \mathbb{R}$,

$$Q_1((-\infty, 0]|x) = \frac{\alpha}{4} \int_{-\infty}^{0} \exp(-(\alpha/2)|z-x|)\, dz = \frac{\alpha}{4} \int_{-\infty}^{-x} \exp(-(\alpha/2)|u|)\, du \xrightarrow{x\to\infty} 0,$$

wegen dem Satz der monotonen Konvergenz, und

$$Q_1((-\infty, 0]|0) = 1/2.$$

Somit ist also

$$Q_1((-\infty, 0]|0) \leq e^\alpha Q_1((-\infty, 0]|x)$$

nicht für jedes $x \neq 0$ erfüllt und Q ist nicht α-DP. Dies lässt sich allerdings beheben wenn man die x-Abhängigkeit der Dichte q geeignet anpasst. Verwendet man nämlich die Trunkationsabbildung T wie in Beispiel 1.7.(b), und setzt $\tilde{Q}_1(A|x) = \int_A q(z|T(x))\, dz$, so ergibt sich für $z, x, x' \in \mathbb{R}$ aus der umgekehrten Dreiecksungleichung,

$$\frac{q(z|T(x))}{q(z|T(x'))} = \exp\left(\frac{\alpha}{2}\left[|z-T(x')| - |z-T(x)|\right]\right) \leq \exp\left(\frac{\alpha}{2}|T(x')-T(x)|\right) \leq e^\alpha,$$

und somit für $A \in \mathcal{B}(\mathbb{R})$,

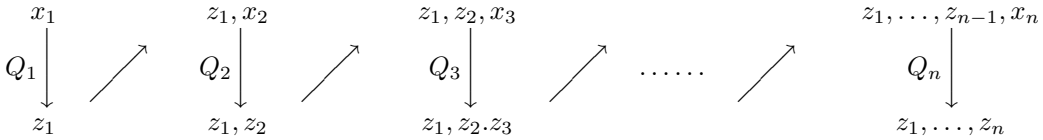
$$\frac{\tilde{Q}_1(A|x)}{\tilde{Q}_1(A|x')} = \frac{\int_A \frac{q(z|T(x))}{q(z|T(x'))} q(z|T(x'))\,dz}{\int_A q(z|T(x'))\,dz} \leq e^\alpha.$$

d) Schließlich betrachten wir noch ein Beispiel für einen interaktiven Mechanismus (Situation eines 'trusted curator'). Angenommen wir wollen die Anzahl der Individuen in der Datenbank $x \in \mathcal{X}^n = \mathbb{R}^{n\times d}$ ermitteln die eine Eigenschaft E besitzen. Wir können $E \subseteq \mathbb{R}^d$ als eine Teilmenge von $\mathbb{R}^d$ auffassen und die Abfrage der Anzahl der Individuen mit Eigenschaft E formalisieren durch $\kappa(x) = \sum_{i=1}^n \mathbb{1}_E(x_i)$. Natürlich darf der Wert von $\kappa(x)$ nicht direkt weitergegeben werden wenn wir α-differentielle Privatheit sicherstellen wollen. Dagegen können wir den folgenden Laplace-Mechanismus verwenden. Für $\alpha \in (0,\infty)$, $z \in \mathbb{R}$ und $x \in \mathcal{X}^n$, sei $q(z|x) = \frac{\alpha}{2}\exp(-\alpha|z-\kappa(x)|)$ wie in Beispiel 1.7.(c). Somit gilt für $z \in \mathbb{R}$ und $x, x' \in \mathcal{X}^n$ mit $d_0(x,x') = 1$, dass $|\kappa(x) - \kappa(x')| \leq 1$, und

$$\frac{q(z|\kappa(x))}{q(z|\kappa(x'))} \leq \exp(\alpha|\kappa(x') - \kappa(x)|) \leq e^\alpha.$$

Der zugehörige Kanal $Q(A|x) = \int_A q(z|\kappa(x))\,dz$, für $A \in \mathcal{B}(\mathbb{R})$, $x \in \mathcal{X}^n$, ist also α-DP aber **nicht NI**.

Bemerkung 1.8. Auch das folgende Privatisierungsprotokoll ist 'lokal' realisierbar (no trusted curator) (vgl. Duchi et al., 2014).



Dabei privatisiert das erste Individuum seine Daten x_1 mit Q_1 und erzeugt z_1. Diesen Wert z_1 gibt es an das zweite Individuum weiter welches jetzt aus z_1 und x_2 mit Hilfe des Kanals Q_2 den privatisierten Wert z_2 erzeugt und (z_1, z_2) an das dritte Individuum weitergibt, usw. Ein solcher 'sequentieller' Mechanismus ist klarer weise nicht NI, da die Verteilung von z_i nicht nur von x_i alleine abhängt. Warum genügt es uns aber nicht im lokalen Fall einfach nur NI Mechanismen zu betrachten? Die Hoffnung ist, dass kompliziertere Mechanismen in der Lage sind mehr Information aus den Originaldaten zu bewahren aber dennoch α-differentielle Privatheit sicherzustellen. In Kapitel 3 werden wir sehen, dass diese Hoffnung zumindest in bestimmten Fällen nicht erfüllt wird und nicht-interaktive Kanäle in einem gewissen Sinne genauso effizient sind wie sequentielle. Damit ist die Nützlichkeit von sequentiellen Mechanismen für lokale Probleme aber im Allgemeinen noch nicht widerlegt.

Definition 1.9. *Ein Kanal $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ heißt **sequentiell-interaktiv (SI)** falls es Kanäle $Q_1 : \mathcal{G} \times \mathcal{X} \to [0,1]$ und $Q_i : \mathcal{G} \times (\mathcal{X} \times \mathcal{Z}^{i-1}) \to [0,1]$, $i = 2, \ldots, n$, gibt, so dass für $A_1, \ldots, A_n \in \mathcal{G}$ und $x_1, \ldots, x_n \in \mathcal{X}$, gilt*

$$\begin{aligned} &Q(A_1 \times \cdots \times A_n | x_1, \ldots, x_n) \\ &\quad = \int_{A_1} \cdots \int_{A_{n-1}} \int_{A_n} Q_n(dz_n | x_n, z_1, \ldots, z_{n-1}) Q_{n-1}(dz_{n-1} | x_{n-1}, z_1, \ldots, z_{n-2}) \ldots Q_1(dz_1|x_1). \end{aligned}$$

Für $i \geq 2$ schreiben wir auch $Q_i^{(z_{i-1},\ldots,z_1)}(dz_i|x_i) := Q_i(dz_i|x_i, z_1, \ldots, z_{i-1})$, so dass bei festen $(z_1, \ldots, z_{i-1}) \in \mathcal{Z}^{i-1}$, $Q_i^{(z_1,\ldots,z_{i-1})} : \mathcal{G} \times \mathcal{X}^1 \to [0,1]$.

Korollar 1.10. *Sei $\alpha \in (0,\infty)$ und $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ sequentiell-interaktiv. Definiere für $i = 2, \ldots, n$, $x_1, \ldots, x_{i-1} \in \mathcal{X}$ die W-Maße*

$$R_{i-1}^{(x_1,\ldots,x_{i-1})}(dz_1 \ldots dz_{i-1}) := Q_{i-1}(dz_{i-1}|x_{i-1}, z_1, \ldots, z_{i-2}) \ldots Q_1(dz_1|x_1),$$

auf $(\mathcal{Z}^{i-1}, \mathcal{G}^{\otimes i-1})$. Dann sind die folgenden Aussagen äquivalent.

- *Q ist α-DP.*
- *$Q_1 : \mathcal{G} \times \mathcal{X}^1 \to [0,1]$ ist α-DP und für alle $i = 2, \dots, n$, alle $x_1, \dots, x_{i-1} \in \mathcal{X}$ und für $R_{i-1}^{(x_1,\dots,x_{i-1})}$-fast alle $(z_1, \dots, z_{i-1}) \in \mathcal{Z}^{i-1}$, ist auch $Q_i^{(z_1,\dots,z_{i-1})} : \mathcal{G} \times \mathcal{X}^1 \to [0,1]$ α-DP.*

Fehler!!! Definiere SI als α-SIDP wie im paper!

Beweis. Angenommen Q ist α-DP. Dass Q_1 α-DP ist, folgt sofort mit $A = A_1 \times \mathcal{Z}^{n-1}$. Seien also $i \geq 2$ und $x_1, \dots x_{i-1} \in \mathcal{X}$. Dann gilt für $A_i \in \mathcal{G}$, $B_i \in \mathcal{G}^{\otimes i-1}$ und $x_i', x_i, x_{i+1} \dots, x_n \in \mathcal{X}$, dass

$$\begin{aligned}
\int_{B_i} Q_i^{(z_1,\dots,z_{i-1})}(A_i|x_i) R_{i-1}^{(x_1,\dots,x_{i-1})}(dz_1, \dots, dz_{i-1}) &= Q(B_i \times A_i \times \mathcal{Z}^{n-i}|x_1, \dots, x_n) \\
&\leq e^\alpha Q(B_i \times A_i \times \mathcal{Z}^{n-i}|x_1, \dots, x_i', \dots, x_n) \\
&= \int_{B_i} e^\alpha Q_i^{(z_1,\dots,z_{i-1})}(A_i|x_i') R_{i-1}^{(x_1,\dots x_{i-1})}(dz_1, \dots, dz_{i-1}).
\end{aligned}$$

Da $B_i \in \mathcal{G}^{\otimes i-1}$ beliebig war, folgt aus einem bekannten Satz der W-Theorie, dass

$$Q_i^{(z_1,\dots,z_{i-1})}(A_i|x_i) \leq e^\alpha Q_i^{(z_1,\dots,z_{i-1})}(A_i|x_i'),$$

für $R_{i-1}^{(x_1,\dots,x_{i-1})}$-fast alle $(z_1, \dots, z_{i-1}) \in \mathcal{Z}^{i-1}$. Für die Umkehrung, beachte, dass für $i = 1, \dots, n$, $x_i, x_i' \in \mathcal{X}$ und für jede messbare Funktion $S : \mathcal{Z}^i \to [0, \infty)$, durch Approximation mittels einfacher Funktionen, gilt

$$\int_{\mathcal{Z}} S(z_1, \dots, z_i) Q_i^{(z_1,\dots,z_{i-1})}(dz_i|x_i) \leq e^\alpha \int_{\mathcal{Z}} S(z_1, \dots, z_i) Q_i^{(z_1,\dots,z_{i-1})}(dz_i|x_i'),$$

für $R_{i-1}^{(x_1,\dots,x_{i-1})}$-fast alle $(z_1, \dots, z_{i-1}) \in \mathcal{Z}^{i-1}$. Somit erhalten wir für $A \in \mathcal{G}^{\otimes n}$ und $x, x' \in \mathcal{X}^n$, mit $d_0(x, x') = 1$, $x_i \neq x_i'$, und

$$S^{(x_{i+1},\dots,x_n)}(z_1, \dots, z_i) := \int_{\mathcal{Z}} \cdots \int_{\mathcal{Z}} \mathbb{1}_A(z_1, \dots, z_n) Q_n^{(z_1,\dots,z_{n-1})}(dz_n|x_n) \dots Q_{i+1}^{(z_1,\dots,z_i)}(dz_{i+1}|x_{i+1}),$$

dass

$$\begin{aligned}
Q(A|x) &= \int_{\mathcal{Z}} \cdots \int_{\mathcal{Z}} \mathbb{1}_A(z_1, \dots, z_n) Q_n^{(z_1,\dots,z_{n-1})}(dz_n|x_n) \dots Q_1(dz_1|x_1) \\
&= \int_{\mathcal{Z}^{i-1}} \int_{\mathcal{Z}} S^{(x_{i+1},\dots,x_n)}(z_1, \dots, z_i) Q_i^{(z_1,\dots,z_{i-1})}(dz_i|x_i) R_{i-1}^{(x_1,\dots,x_{i-1})}(dz_1, \dots, dz_{i-1}) \\
&\leq e^\alpha \int_{\mathcal{Z}^{i-1}} \int_{\mathcal{Z}} S^{(x_{i+1},\dots,x_n)}(z_1, \dots, z_i) Q_i^{(z_1,\dots,z_{i-1})}(dz_i|x_i') R_{i-1}^{(x_1,\dots,x_{i-1})}(dz_1, \dots, dz_{i-1}) \\
&= e^\alpha Q(A|x').
\end{aligned}$$

□

Bemerkung 1.11. Jeder nicht-interaktive Kanal $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ ist auch sequentiell-interaktiv, mit $Q_i(A_i|x_i, z_1, \dots, z_{i-1}) = Q_i(A_i|x_i)$.

Satz 1.12. *Sei $(\mathcal{Z}, \mathcal{G}) = (\mathbb{R}^m, \mathcal{B}(\mathbb{R}^m))$. Dann sind die folgenden Aussagen äquivalent.*

- *Der Kanal $Q : \mathcal{G} \times \mathcal{X}^1 \to [0,1]$ ist α-DP.*
- *Es existiert ein σ-endliches Maß μ auf $(\mathcal{Z}, \mathcal{G})$ und für jedes $x \in \mathcal{X}^1$ eine μ-Dichte $z \mapsto q(z|x)$ von $Q(dz|x)$, derart, dass für jedes $x' \in \mathcal{X}^1$ gilt*

$$q(z|x) \;\leq\; e^\alpha \, q(z|x'), \qquad \forall z \in \mathcal{Z}.$$

Beweis. Sei Q α-DP und $x^* \in \mathcal{X}^1$. Dann ist $\mu(dz) := Q(dz|x^*)$ ein σ-endliches Maß auf $(\mathcal{Z}, \mathcal{G})$ (sogar ein W-Maß), und nach Definition 1.1 gilt $Q(dz|x) \ll \mu(dz)$, für alle $x \in \mathcal{X}^1$. Sei nun für $x \in \mathcal{X}^1$, $z \mapsto q(z|x)$ eine μ-Dichte von $Q(dz|x)$ und für $r \in (0, \infty)$, $z \in \mathcal{Z}$, definiere die abgeschlossene Kugel $K_r(z) := \{y \in \mathcal{Z} : \|y - z\|_2 \leq r\}$. Nach dem Differentiationssatz von Lebesgue-Besicovitch (vgl. Mattila, 1995, Corollary 2.14) gilt

$$q(z|x) \;=\; \lim_{r \downarrow 0} \frac{1}{\mu(K_r(z))} \int_{K_r(z)} q(u|x)\, \mu(du) \;=\; \lim_{r \downarrow 0} \frac{Q(K_r(z)|x)}{Q(K_r(z)|x^*)},$$

für alle $z \in N_x^c$ und eine μ-Nullmenge $N_x \in \mathcal{G}$. Außerdem sind die Quotienten auf der rechten Seite laut Voraussetzung alle Element von $[e^{-\alpha}, e^{\alpha}]$, und somit auch $e^{-\alpha} \leq q(z|x) \leq e^{\alpha}$, für alle $x \in \mathcal{X}^1$ und $z \in N_x^c$. Wir ändern nun die Dichte $z \mapsto q(z|x)$ auf der μ-Nullmenge N_x ab, so dass $q(z|x) = 1$ für alle $z \in N_x$. Dies ändert nichts daran, dass $z \mapsto q(z|x)$ eine μ-Dichte von $Q(dz|x)$ ist. Für $x, x' \in \mathcal{X}^1$ unterscheiden wir nun vier Fälle. Falls $z \in N_x \cap N_{x'}$, dann gilt $q(z|x) = 1 \leq e^{\alpha} = e^{\alpha} q(z|x')$. Für $z \in N_x \cap N_{x'}^c$, gilt $q(z|x) = 1$ und $q(z|x')e^{\alpha} \geq 1$, also $q(z|x) \leq e^{\alpha} q(z|x')$. Für $z \in N_x^c \cap N_{x'}^c$ verfährt man analog. Für $z \in N_x^c \cap N_{x'}^c$ gilt

$$\frac{q(z|x)}{q(z|x')} = \lim_{r \downarrow 0} \frac{\frac{Q(K_r(z)|x)}{Q(K_r(z)|x^*)}}{\frac{Q(K_r(z)|x')}{Q(K_r(z)|x^*)}} = \lim_{r \downarrow 0} \frac{Q(K_r(z)|x)}{Q(K_r(z)|x')} \leq \lim_{r \downarrow 0} \frac{e^{\alpha} Q(K_r(z)|x')}{Q(K_r(z)|x')} = e^{\alpha}.$$

Für die Umkehrung, wähle $A \in \mathcal{G}$ und $x, x' \in \mathcal{X}^1$ und beachte, dass $Q(A|x) = \int_A q(z|x)\, \mu(dz) \leq \int_A e^{\alpha} q(z|x')\, \mu(dz) = e^{\alpha} Q(A|x')$. □

1.3 Übungsaufgaben

Aufgabe 1.1. Es sei $\kappa : \mathcal{X}^n \to \mathbb{R}^m$ eine Abbildung und ihre **Sensitivität** sei definiert durch

$$\mathcal{S}(\kappa) := \sup_{\substack{x, x' \in \mathcal{X}^n \\ d_0(x, x') = 1}} \|\kappa(x) - \kappa(x')\|_1.$$

Finden Sie analog zu Beispiel 1.7.(d) einen Privatisierungsmechanismus der die Datenbankabfrage $\kappa(x)$ α-differentiell privatisiert falls $\mathcal{S}(\kappa) < \infty$. (vgl. Dwork et al., 2006) (2P)

Aufgabe 1.2. Unternehmen Sie eine Literaturrecherche. Erstellen Sie eine kleine Sammlung alternativer aber formal definierter 'privacy'-Begriffe aus der Literatur und erläutern Sie jeden davon kurz. (*)

Aufgabe 1.3. Betrachten Sie den folgenden Privatisierungsmechanismus. Individuum i generiert seine privaten Daten unabhängig von den anderen Individuen durch Projektion von x_i auf $[-1, 1]$ und Addition einer $\mathcal{N}(0, \sigma^2)$-verteilten Zufallszahl, also $Z_i = T(x_i) + U_i$, $U_i \sim \mathcal{N}(0, \sigma^2)$. Gibt es ein $\sigma = \sigma(\alpha)$, so dass dieser Mechanismus α-DP ist? (2P)

Aufgabe 1.4. Gibt es einen lokal realisierbaren ('no trusted curator') Privatisierungsmechanismus der nicht sequentiell-interaktiv ist? (*)

Kapitel 2

Mathematische Statistik und 'differential privacy'

2.1 Minimax Schätzung

In dieser Sektion wiederholen wir kurz einige Grundbegriffe der mathematischen Statistik die im Folgenden von Bedeutung sein werden. Wie bisher beginnen wir mit einem messbaren Raum $(\mathcal{X}, \mathcal{F})$, den wir auch als **Stichprobenraum** bezeichnen. In der Statistik verstehen wir unsere Daten $x \in \mathcal{X}^n$ üblicherweise als eine Realisierung eines zufälligen Prozesses. Dieser kann in der Praxis zum Beispiel in der zufälligen Auswahl von Personen aus einer (idealisierten) Grundgesamtheit, oder in mit (unvorhersehbaren) Messfehlern behafteten physikalischen Messungen bestehen. Mathematisch formulieren wir diesen zufälligen Datengenerierenden Prozess durch ein W-Maß P auf $(\mathcal{X}, \mathcal{F})$. In einer konkreten Anwendung wissen wir aber typischerweise nicht genau aus welchem W-Maß P unsere Daten generiert wurden. Man unterstellt also ein sogenanntes **statistisches Modell**, d.h. eine ganze Familie $\mathcal{P} = \mathcal{P}(\mathcal{X}, \mathcal{F})$ von W-Maßen auf $(\mathcal{X}, \mathcal{F})$ und nimmt an, dass die Daten aus einem der $P \in \mathcal{P}$ erzeugt wurden. Dabei gehen wir in dieser Vorlesung immer von unabhängig und identisch verteilten (iid) Beobachtungen aus, wir unterstellen also, dass $x \in \mathcal{X}^n$ eine Realisierung eines Produktmaßes P^n für ein $P \in \mathcal{P}$ ist. Sei nun $(\mathcal{Z}_m, \mathcal{G}_m) = (\mathbb{R}^m, \mathcal{B}(\mathbb{R}^m))$ und $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$ ein Kanal. Wir betrachten hier nur Fälle in denen der kanal Q (öffentlich) bekannt ist. Es geht also nicht darum Rückschlüsse auf Q zu ziehen. Wir definieren

$$QP^n(dz) := \int_{\mathcal{X}^n} Q(dz|x)\, P^n(dz).$$

Wurden die Originaldaten $x \in \mathcal{X}^n$ also aus P^n 'gezogen' und anschließend mit Q privatisiert, so folgen die privatisierten Daten $z \in \mathcal{Z}_m^n$ der Verteilung QP^n. Ziel der Statistik ist es nun:

- **klassische:** Aus den unter dem unbekannten W-Maß P^n (für ein $P \in \mathcal{P}$) generierten Daten $x \in \mathcal{X}^n$ Rückschlüsse auf P zu ziehen.
- **privat:** Aus den unter dem W-Maß QP^n (für ein $P \in \mathcal{P}$) generierten privaten Daten $z \in \mathcal{Z}_m^n$ Rückschlüsse auf P zu ziehen.

In dieser Vorlesung beschränken wir uns darauf nur gewisse Merkmale der wahren datengenerierenden Verteilung $P \in \mathcal{P}$ zu schätzen. Konkret interessieren wir uns für den Wert $\theta(P)$ eines **reellen Funktionals** $\theta : \mathcal{P} \to \mathbb{R}$. Dies kann zum Beispiel von der Form $\theta(P) := \mathbb{E}_P[f]$, für ein messbaren $f : \mathcal{X} \to \mathbb{R}$, sein. Für $f(x) = x$ ist $\theta(P)$ dann etwa der Erwartungswert von P und für $f(x) = x^k$, das k-te Moment von P. Obwohl wir uns auf ein reellwertiges Merkmal der Verteilung P konzentrieren, kann das Modell $\mathcal{P}$ aber trotzdem sehr groß sein und muss sich nicht unbedingt durch eine endlich-dimensionale Parametermenge indizieren lassen. Wir sprechen auch von einem **semi-parametrischen** Schätzproblem.

Minimax-Schätzung (klassisch)

Ein **Schätzer** ist eine messbare Abbildung $\hat{\theta}_n : \mathcal{X}^n \to \mathbb{R}$. Idealerweise sollte der Wert von $\hat{\theta}_n(x)$, in einem geeigneten Sinne, nahe bei $\theta(P)$ liegen, wenn $x \in \mathcal{X}^n$ unter P^n generiert wurde. Um das zu präzisieren wählt man zunächst eine **Verlustfunktion** $l : \mathbb{R}_+ \to \mathbb{R}_+$, wobei hier $\mathbb{R}_+ := [0, \infty)$, und definiert das **Risiko** des Schätzers $\hat{\theta}_n$ durch

$$\mathcal{R}_n(\hat{\theta}_n, P, \theta) := \mathbb{E}_{P^n}\left[l\left(\left|\hat{\theta}_n - \theta(P)\right|\right)\right] = \int_{\mathcal{X}^n} l\left(\left|\hat{\theta}_n(x) - \theta(P)\right|\right) P^n(dx).$$

Verschiedene Schätzer lassen sich jetzt anhand ihres Risikos vergleichen. Ein beliebter Ansatz um einen **Optimalitätsbegriff** zu definieren ist es nun, den ungünstigsten Fall zu betrachten. Ein Schätzer $\hat{\theta}_n^*$ heißt **minimax-optimal** falls sein ungünstigstes Risiko gleich dem sogenannten **Minimax-Risiko** $\mathcal{M}_n = \mathcal{M}_n(\mathcal{P}, \theta)$ ist, also falls

$$\sup_{P \in \mathcal{P}} \mathcal{R}_n(\hat{\theta}_n^*, P, \theta) = \inf_{\hat{\theta}_n : \mathcal{X}^n \to \mathbb{R}} \sup_{P \in \mathcal{P}} \mathcal{R}_n(\hat{\theta}_n, P, \theta) =: \mathcal{M}_n(\mathcal{P}, \theta),$$

wobei das Infimum hier über alle möglichen Schätzer $\hat{\theta}_n : \mathcal{X}^n \to \mathbb{R}$ läuft. In komplexeren Modellen $\mathcal{P}$ ist es oft ein zu ehrgeiziges Ziel einen solchen Minimax-Schätzer zu finden. Daher begnügt man sich oft damit einen Schätzer $\hat{\theta}_n^*$ zu finden, der die **Minimax-Rate** erreicht, das heißt, dass es Konstanten $C \geq 1$ und $n_0 \in \mathbb{N}$ gibt, mit

$$\sup_{P \in \mathcal{P}} \mathcal{R}_n(\hat{\theta}_n^*, P, \theta) \leq C \cdot \mathcal{M}_n(\mathcal{P}, \theta) \qquad \forall n \geq n_0.$$

Minimax-Schätzung (privat)

Im privaten Fall ist ein **Schätzer** nun eine messbare Abbildung $\hat{\theta}_n : \mathcal{Z}_m^n \to \mathbb{R}$. Ist der Kanal Q gegeben, so ist das **Q-Risiko** des Schätzers $\hat{\theta}_n$ definiert durch

$$\mathcal{R}_n(\hat{\theta}_n, Q, P, \theta) := \mathbb{E}_{QP^n}\left[l\left(\left|\hat{\theta}_n - \theta(P)\right|\right)\right] = \int_{\mathcal{Z}_m^n} l\left(\left|\hat{\theta}_n(z) - \theta(P)\right|\right) QP^n(dz).$$

Das α**-private Minimax-Risiko** $\mathcal{M}_{n,\alpha} = \mathcal{M}_{n,\alpha}(\mathcal{P}, \theta)$ ist jetzt gegeben durch

$$\mathcal{M}_{n,\alpha}(\mathcal{P}, \theta) := \inf_{m \in \mathbb{N}} \inf_{Q \in \mathcal{Q}_\alpha(m)} \inf_{\hat{\theta}_n : \mathcal{Z}_m^n \to \mathbb{R}} \sup_{P \in \mathcal{P}} \mathcal{R}_n(\hat{\theta}_n, Q, P, \theta),$$

wobei $\mathcal{Q}_\alpha(m)$ eine gewünschte Menge von α-DP Kanälen $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$ ist (z.B. alle NI oder SI Kanäle). Ein Tripple $(Q_{(n)}, \hat{\theta}_n, m_n)$, wobei $Q_{(n)} : \mathcal{G}_{m_n}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ und $\hat{\theta}_n : \mathcal{Z}_{m_n}^n \to \mathbb{R}$, erreicht die α**-private minimax-Rate** falls es Konstanten $C \geq 1$ und $n_0 \in \mathbb{N}$ gibt, mit

$$\sup_{P \in \mathcal{P}} \mathcal{R}_n(\hat{\theta}_n, Q_{(n)}, P, \theta) \leq C \cdot \mathcal{M}_{n,\alpha}(\mathcal{P}, \theta) \qquad \forall n \geq n_0.$$

Minimax-Rate und Stetigkeitsmodul

Die minimax Konvergenzrate bzw. die Konvergenzgeschwindigkeit von $\mathcal{M}_n(\mathcal{P}, \theta)$ (im klassischen Fall) beschreibt in gewisser Weise die 'Schwierigkeit' des Schätzproblems. Konvergiert $\mathcal{M}_n(\mathcal{P}, \theta)$ sehr schnell, so lässt sich $\theta(P)$ über dem Modell $\mathcal{P}$ relativ 'leicht' schätzen, nämlich schon mit einer relativ kleinen Stichprobe der Größe n. Wohingegen bei langsam konvergierendem $\mathcal{M}_n(\mathcal{P}, \theta)$ eine sehr viel größere Stichprobengröße n notwendig ist um die selbe Genauigkeit zu erreichen. Intuitiv gesprochen sollte es dann besonders leicht sein $\theta(P)$ zu schätzen, wenn $\theta(P_0)$ und $\theta(P_1)$ sehr nahe aneinander liegen, selbst wenn die Verteilungen P_0 und P_1 sehr unterschiedlich sind. Im Extremfall ist $\theta : \mathcal{P} \to \mathbb{R}$ konstant, und dann kenne ich den Wert von $\theta(P)$ selbst ohne einen Blick auf die Daten geworfen zu haben. Im anderen Extremfall nimmt θ zwei völlig verschiedene

Werte $\theta(P_0)$ und $\theta(P_1)$ an, selbst wenn P_0 und P_1 beliebig nahe zu einander liegen. Unter P_0 und unter P_1 generierte Daten 'sehen also beinahe gleich aus', obwohl der zu schätzende Wert jeweils komplett unterschiedlich ist. Im letztgenannten Fall ist θ in einem gewissen Sinne unstetig. Die Schwierigkeit des Schätzproblems sollte also etwas mit der lokalen Variabilität des Funktionals $\theta : \mathcal{P} \to \mathbb{R}$ zu tun haben. Diese lässt sich etwa durch einen **Stetigkeitsmodul** quantifizieren.

Definition 2.1. *Sei $\theta : \mathcal{P} \to \mathbb{R}$ ein Funktional und $d : \mathcal{P} \times \mathcal{P} \to [0, \infty)$ eine Metrik. Dann definieren wir für $\varepsilon \in [0, \infty)$, den d-**Stetigkeitsmodul** von θ über $\mathcal{P}$ durch*

$$\omega_d(\varepsilon) := \omega_{d,\mathcal{P},\theta}(\varepsilon) := \sup\{|\theta(P_0) - \theta(P_1)| : d(P_0, P_1) \leq \varepsilon, P_0, P_1 \in \mathcal{P}\}.$$

Das Minimax-Risiko lässt sich tatsächlich durch einen geeigneten Stetigkeitsmodul charakterisieren. Im Folgenden bedeutet die Notation $a_n \asymp b_n$, für $n \to \infty$, dass es Konstanten $c_0, c_1 > 0$ und $n_0 \in \mathbb{N}$ gibt, mit $c_0 a_n \leq b_n \leq c_1 a_n$, für alle $n \geq n_0$. Mit $d_H : \mathcal{P} \times \mathcal{P} \to [0, \infty)$ bezeichne man die sogenannte Hellinger-Distanz (siehe Sektion 2.2).

Satz 2.2. *[Donoho and Liu (1991)] Angenommen $\mathcal{P}$ ist konvex und dominiert, $\theta : \mathcal{P} \to \mathbb{R}$ ist linear und beschränkt, und $l : \mathbb{R}_+ \to \mathbb{R}_+$ ist hinreichend regulär[1]. Falls es ein $r \in (0, 2]$ gibt, mit $\omega_{d_H}(\varepsilon) \asymp \varepsilon^r$, für $\varepsilon \to 0$, dann gilt*

$$\mathcal{M}_n(\mathcal{P}, \theta) \asymp l \circ \omega_{d_H}(n^{-1/2}) \qquad \text{für } n \to \infty.$$

Ein ähnliches Resultat hätten wir nun gerne auch im privaten Fall für $\mathcal{M}_{n,\alpha}(\mathcal{P}, \theta)$. Insbesondere ist natürlich die Frage ob und wie sich die Konvergenzraten im klassischen und im privaten Fall unterscheiden. Dies gibt uns eine Idee vom Preis (im Sinne einer langsameren Konvergenzgeschwindigkeit) den man für α-differentielle Privatisierung bezahlen muss. Zusätzlich hätten wir natürlich auch noch gerne ein allgemeines Rezept um optimale Kanäle Q und private Schätzer $\hat{\theta}_n$ zu konstruieren, die die α-private minimax-Rate erreichen. Diesem Programm widmen wir uns näher in Kapitel 3. Zunächst müssen wir einige technische Werkzeuge dafür entwickeln.

2.2 Tests und Wahrscheinlichkeitsmetriken

2.2.1 Statistische Tests

Sei $(\Omega, \mathcal{A})$ ein messbarer Raum und $\mathcal{P} = \mathcal{P}(\Omega, \mathcal{A})$ ein Modell. Ein **statistischer Test** wird dazu verwendet um von zwei möglichen **statistischen Hypothesen** zu entscheiden zu welcher die 'wahre' datengenerierende Verteilung gehört. Man bezeichnet die Hypothesen traditionell als die Nullhypothese H_0 und die Alternativhypothese H_1, und definiert formal $H_0, H_1 \subseteq \mathcal{P}$ als Teilmengen des Modells. Ein **(randomisierter) Test** ist eine messbare Abbildung $\phi : \Omega \to [0, 1]$. Dabei ist der Wert $\phi(\omega)$ als die Wahrscheinlichkeit zu verstehen, mit der man sich für H_1 entscheiden soll. Man zieht also eine gleichverteilte Zufallszahl und entscheidet sich für H_1 falls $Unif[0, 1] \leq \phi(\omega)$, und für H_0 andernfalls. Dabei sagt man, dass der Test ϕ einen **Fehler erster Art** begeht, wenn $P \in H_1$, aber die Testentscheidung für H_0 ausfällt, und, dass ϕ einen **Fehler zweiter Art** begeht, wenn $P \in H_0$, aber H_1 gewählt wird. Die Wahrscheinlichkeit, dass sich ein (randomisierter) Test für H_1 entscheidet, ist also gegeben durch

$$P \otimes U\Big((\omega, u) : u \leq \phi(\omega)\Big) = \mathbb{E}_P\left[\mathbb{E}_U\left[\mathbb{1}_{[0,\phi]}\right]\right] = \mathbb{E}_P[\phi],$$

wobei U das W-Maß der Gleichverteilung auf $[0, 1]$ bezeichnet. Analog ist die Wahrscheinlichkeit, dass er sich für H_0 entscheidet gegeben durch $\mathbb{E}_P[1 - \phi]$. Die maximalen Fehler erster und zweiter Art sind somit gegeben durch

$$\sup_{P \in H_0} \mathbb{E}_P[\phi] \quad \text{und} \quad \sup_{P \in H_1} \mathbb{E}_P[1 - \phi].$$

[1] Siehe Annahme (**??**) in Sektion 3.2.

Ein häufiges Vorgehen bei der Konstruktion von Tests ist es, sich ein sogenanntes **Signifikanzniveau** $\gamma \in (0,1)$, bzw. den Fehler erster Art, vorzugeben. Ist der Fehler erster Art eines Tests $\phi : \Omega \to [0,1]$ durch γ beschränkt, also $\sup_{P \in H_1} \mathbb{E}_P[\phi] \leq \gamma$, so nenne wir ihn auch einen Test zum Niveau γ. Oft sucht man unter allen Tests zu einem vorgegebenen Niveau γ denjenigen mit der größten Güte. Dabei ist die Güte eines Tests ϕ (bei einfacher Alternativhypothese $H_1 = \{P_1\}$) definiert als die Gegenwahrscheinlichkeit eines Fehlers zweiter Art, also $\mathbb{E}_{P_1}[\phi]$. Alternativ sucht man manchmal auch nach einem sogenannten **Minimax-Test für H_0 gegen H_1**, das heißt, nach einem Test $\phi^* : \Omega \to [0,1]$, derart, dass

$$\sup_{\substack{P_0 \in H_0 \\ P_1 \in H_1}} \mathbb{E}_{P_0}[\phi^*] + \mathbb{E}_{P_1}[1-\phi^*] = \inf_{\phi:\Omega\to[0,1]} \sup_{\substack{P_0 \in H_0 \\ P_1 \in H_1}} \mathbb{E}_{P_0}[\phi] + \mathbb{E}_{P_1}[1-\phi].$$

Unter Verwendung der 'schwachen' Folgenkompaktheit der Testfunktionen lässt sich leicht zeigen, dass minimax Tests zumindest für dominierte Modelle immer existieren (siehe Aufgabe 2.1). In Kapitel 3 werden wir dann sehen, wie man für gewisse Probleme aus minimax Tests auch Schätzer konstruieren kann, die die minimax-Rate erreichen.

2.2.2 Wahrscheinlichkeitsmetriken

In dieser Sektion sei $(\Omega, \mathcal{A})$ ein abstrakter messbarer Raum und $\mathcal{P}$ die Menge aller W-Maße auf $(\Omega, \mathcal{A})$. Wir definieren die folgenden Distanzbegriffe und Affinitäten auf $\mathcal{P}$.

Definition 2.3.

a) Kullback-Leibler-Divergenz:

$$D_{KL}(P_0|P_1) = \begin{cases} \int_\Omega \log \frac{dP_0}{dP_1}(\omega)\, P_0(d\omega), & \text{falls } P_0 \ll P_1, \\ +\infty, & \text{sonst.} \end{cases}$$

b) Totalvariationsdistanz:

$$d_{TV}(P_0, P_1) = \sup_{A \in \mathcal{A}} |P_0(A) - P_1(A)|.$$

c) Hellinger-Distanz:

$$d_H(P_0, P_1) = \left(\int_\Omega \left(\sqrt{p_0(\omega)} - \sqrt{p_1(\omega)} \right)^2 \mu(d\omega) \right)^{1/2},$$

für Dichten p_0 und p_1 von P_0 und P_1 bezüglich eines beliebigen Maßes μ (z.B. $\mu = P_0 + P_1$).

d) Hellinger-Affinität:

$$\rho_H(P_0, P_1) = \int_\Omega \sqrt{p_0(\omega) p_1(\omega)}\, \mu(d\omega),$$

für Dichten p_0 und p_1 von P_0 und P_1 bezüglich eines beliebigen dominierenden Maßes μ.

e) Test-Affinität:

$$\rho_T(P_0, P_1) := \inf_\phi \Big(\mathbb{E}_{P_0}[\phi] + \mathbb{E}_{P_1}[1-\phi] \Big),$$

wobei das Infimum über alle randomisierten Tests $\phi : \Omega \to [0,1]$ läuft.

Im Folgenden schreiben wir für Modelle $\mathcal{P}_0$ und $\mathcal{P}_1$ auf $(\Omega, \mathcal{A})$ auch

$$\rho_H(\mathcal{P}_0, \mathcal{P}_1) := \sup_{\substack{P_0 \in \mathcal{P}_0 \\ P_1 \in \mathcal{P}_1}} \rho_H(P_0, P_1), \quad \rho_T(\mathcal{P}_0, \mathcal{P}_1) := \sup_{\substack{P_0 \in \mathcal{P}_0 \\ P_1 \in \mathcal{P}_1}} \rho_T(P_0, P_1), \quad \text{etc.}$$

Weiter bezeichnen wir mit $\text{conv}(\mathcal{P}_0)$ die konvexe Hülle der Menge $\mathcal{P}_0$, also

$$\text{conv}(\mathcal{P}_0) := \left\{ \sum_{i=1}^{k} \lambda_i P_i : k \in \mathbb{N}, \lambda_i \geq 0, \sum_{i=1}^{k} \lambda_i = 1, P_i \in \mathcal{P}_0 \right\}.$$

Es gelten die folgenden Beziehungen.

Satz 2.4.

1) Pinsker-Ungleichung: $d_{TV} \leq \sqrt{\frac{1}{2} D_{KL}}$.

2) $d_H^2 = 2(1 - \rho_H)$.

3) $\rho_H(P_0^n, P_1^n) = \rho_H(P_0, P_1)^n$.

4) $\frac{1}{2} d_H^2 \leq d_{TV} \leq d_H$.

5) $\rho_T = 1 - d_{TV}$.

6) $\rho_T \leq \rho_H \leq \sqrt{\rho_T(2 - \rho_T)}$.

7) $d_H \leq \sqrt{D_{KL}}$.

Beweis. Zum Beweis der Pinsker-Ungleichung siehe Lemma 2.5 in Tsybakov (2009). Die Gleichungen (2) und (3) sind trivial. Für (4), verwende Aufgabe 2.3 und die Cauchy-Schwarz Ungleichung um die folgenden Abschätzungen zu erhalten,

$$\begin{aligned}
d_{\mathrm{H}}^2 &= \int (\sqrt{p_0} - \sqrt{p_1})^2 = \int |\sqrt{p_0} - \sqrt{p_1}||\sqrt{p_0} - \sqrt{p_1}| \\
&\leq \int |\sqrt{p_0} - \sqrt{p_1}||\sqrt{p_0} + \sqrt{p_1}| = \int |p_0 - p_1| = 2 d_{\mathrm{TV}} \\
&\leq \sqrt{\int (\sqrt{p_0} - \sqrt{p_1})^2} \sqrt{\int (\sqrt{p_0} + \sqrt{p_1})^2} = \sqrt{\int (\sqrt{p_0} - \sqrt{p_1})^2} \sqrt{\int (p_0 + 2\sqrt{p_0 p_1} + p_1)} \\
&\leq d_{\mathrm{H}} \sqrt{2 + 2 \int \sqrt{p_0 p_1}} \leq d_{\mathrm{H}} \sqrt{2 + 2 \sqrt{\int p_0 \int p_1}} = 2 d_{\mathrm{H}}.
\end{aligned}$$

Für (5), beachte zunächst, dass wegen Aufgabe 2.3, gilt $d_{\mathrm{TV}} = \int [p_0 - p_1]_+$. Sei nun $\phi : \Omega \to [0, 1]$ ein Test. Dann gilt

$$\int \phi [p_0 - p_1] = \int \phi [p_0 - p_1]_+ - \int \phi [p_0 - p_1]_- \leq \int \phi [p_0 - p_1]_+ \leq \int [p_0 - p_1]_+ = d_{\mathrm{TV}}.$$

Außerdem gilt mit $\phi_0 = \mathbb{1}_{\{p_0 \geq p_1\}}$, dass $\int \phi_0 [p_0 - p_1] = \int [p_0 - p_1]_+ = d_{\mathrm{TV}}$. Somit haben wir also gezeigt, dass $\sup_\phi \int \phi [p_0 - p_1] = d_{\mathrm{TV}}$. Schließlich erhalten wir also $1 - d_{\mathrm{TV}} = \inf_\phi (1 - \int \phi [p_0 - p_1]) = \inf_\phi \mathbb{E}_{P_1}[\phi] + \mathbb{E}_{P_0}[1 - \phi] = \rho_T$. Für (6), verwende zunächst (5), (4) und (2) um

$$\rho_T = 1 - d_{\mathrm{TV}} \leq 1 - \frac{1}{2} d_{\mathrm{H}}^2 = 1 - \frac{1}{2} 2(1 - \rho_H) = \rho_H$$

zu erhalten. Nun verwende das selbe Argument wie im Beweis von (4) zusammen mit (2), um zu zeigen, dass

$$2 d_{\mathrm{TV}} \leq \sqrt{d_{\mathrm{H}}^2 2(1 + \rho_H)} = \sqrt{4(1 - \rho_H)(1 + \rho_H)} = 2\sqrt{1 - \rho_H^2}.$$

Somit folgt mit (5), dass $\rho_T = 1 - d_{\mathrm{TV}} \geq 1 - \sqrt{1 - \rho_H^2}$ und weiter $\rho_H^2 \leq 1 - (1 - \rho_T)^2 = 2\rho_T - \rho_T^2 = \rho_T(2 - \rho_T)$. Für den Beweis von (7) betrachten wir schließlich ohne Beschränkung

der Allgemeinheit nur den Fall $D_{KL}(P_0|P_1) < \infty$, was $P_0 \ll P_1$ impliziert. Es sei nun p_0 eine zugehörige P_1-Dichte. Da $\log(1+x) \leq x$, für alle $x > -1$, erhalten wir

$$\begin{aligned} D_{KL}(P_0|P_1) &= \int_{0<p_0<\infty} \log p_0 \, dP_0 = -2 \int_{0<p_0<\infty} \log\left(1 + \frac{1}{\sqrt{p_0}} - 1\right) dP_0 \\ &\geq 2\left(1 - \int_{0<p_0<\infty} \frac{1}{\sqrt{p_0}} p_0 \, dP_1\right) = 2\left(1 - \int \sqrt{p_0 \cdot 1}\, dP_1\right) = d_{\mathrm{H}}(P_0, P_1)^2, \end{aligned}$$

wegen (2). □

Satz 2.5 (LeCam (1986), p. 477)**.** *Seien $\mathcal{P}_0$ und $\mathcal{P}_1$ Modelle auf $(\Omega, \mathcal{A})$ und $\mathcal{P}_0'$, $\mathcal{P}_1'$ Modelle auf $(\Omega', \mathcal{A}')$. Mit $\mathcal{P}_0 \otimes \mathcal{P}_0'$ bezeichnen wir die Menge aller Maße $P_0 \otimes P_0'$ auf $(\Omega \times \Omega', \mathcal{A} \otimes \mathcal{A}')$, mit $P_0 \in \mathcal{P}_0$ und $P_1 \in \mathcal{P}_1$, und analog für $\mathcal{P}_1 \otimes \mathcal{P}_1'$. Dann gilt*

$$\rho_H(conv(\mathcal{P}_0 \otimes \mathcal{P}_0'), conv(\mathcal{P}_1 \otimes \mathcal{P}_1')) \;\leq\; \rho_H\left(conv(\mathcal{P}_0), conv(\mathcal{P}_1)\right) \cdot \rho_H\left(conv(\mathcal{P}_0'), conv(\mathcal{P}_1')\right).$$

Beweis. Ein beliebiges Element $M_0 \in \mathrm{conv}(\mathcal{P}_0 \otimes \mathcal{P}_0')$ lässt sich darstellen als $M_0(d\omega, d\omega') = \int_{\mathbb{R}} P_{0,s}(d\omega) P_{0,s}'(d\omega')\, \mu(ds)$, wobei μ ein W-Maß mit endlicher Trägermenge $S \subseteq \mathbb{R}$ ist, $P_{0,s} \in \mathcal{P}_0$ und $P_{0,s}' \in \mathcal{P}_0'$, für $s \in S$. Betrachte nun das W-Maß $P_{0,s}(d\omega)\mu(ds)$ auf $(\Omega \times \mathbb{R}, \mathcal{A} \otimes \mathcal{B}(\mathbb{R}))$. Wegen Theorem 8.28 in Klenke (2008) gibt es eine bedingte Verteilung (einen Markov-Kern) $\mu(ds|\omega) : \mathcal{B}(\mathbb{R}) \times \Omega \to [0,1]$, so dass $P_{0,s}(d\omega)\mu(ds) = \mu(ds|\omega)\bar{P}_0(d\omega)$, wobei $\bar{P}_0(d\omega) := \int_{\mathbb{R}} P_{0,s}(d\omega)\mu(ds)$ die Ω-Randverteilung von $P_{0,s}(d\omega)\mu(ds)$ ist. Definiere jetzt die bedingte Verteilung $\bar{R}_0'(d\omega'|\omega) := \int_{\mathbb{R}} P_{0,s}'(d\omega')\, \mu(ds|\omega)$. Somit ergibt sich

$$\bar{R}_0'(d\omega'|\omega)\bar{P}_0(d\omega) = \int_{\mathbb{R}} P_{0,s}'(d\omega')\, \mu(ds|\omega)\bar{P}_0(d\omega) \int_{\mathbb{R}} P_{0,s}'(d\omega') P_{0,s}(d\omega)\, \mu(ds) = M_0(d\omega, d\omega').$$

Völlig analog schreiben wir für $M_1 \in \mathrm{conv}(\mathcal{P}_1 \otimes \mathcal{P}_1')$ auch $M_1(d\omega, d\omega') = \bar{R}_1'(d\omega'|\omega)\bar{P}_1(d\omega)$. Setze nun $\bar{P}_0'(d\omega) = \int_{\mathbb{R}} P_{0,s}'(d\omega)\mu(ds)$ und $\bar{P}_1'(d\omega) = \int_{\mathbb{R}} P_{1,s}'(d\omega)\mu(ds)$ und beachte, dass für $\bar{P}_0$-fast alle $\omega \in \Omega$ gilt $\bar{R}_0'(d\omega'|\omega) \ll \bar{P}_0'(d\omega') \ll \bar{P}_0'(d\omega') + \bar{P}_1'(d\omega') =: \nu'(d\omega')$, und für $\bar{P}_1$-fast alle $\omega \in \Omega$ gilt $\bar{R}_1'(d\omega'|\omega) \ll \bar{P}_1'(d\omega') \ll \bar{P}_0'(d\omega') + \bar{P}_1'(d\omega') = \nu'(d\omega')$. Seien $\bar{r}_0'(\omega'|\omega)$ und $\bar{r}_1'(\omega'|\omega)$ zugehörige ν'-Dichten. Setze $\nu := \bar{P}_0 + \bar{P}_1$ und bezeichne mit $\bar{p}_0$ und $\bar{p}_1$ ν-Dichten von $\bar{P}_0$ und $\bar{P}_1$. Somit zeigt sich, dass

$$\begin{aligned} \bar{r}_0'(\omega'|\omega)\bar{p}_0(\omega)\, \nu \otimes \nu'(d\omega, d\omega') &= \bar{r}_0'(\omega'|\omega)\nu'(d\omega')\, \bar{p}_0(\omega)\nu(d\omega) \\ &= \bar{R}_0'(d\omega'|\omega)\bar{P}_0(d\omega) = M_0(d\omega, d\omega'), \end{aligned}$$

$\bar{r}_0'(\omega'|\omega)\bar{p}_0(\omega)$ also eine $\nu \otimes \nu'$-Dichte von M_0 ist. Analog zeigt man, dass $\bar{r}_1'(\omega'|\omega)\bar{p}_1(\omega)$ eine $\nu \otimes \nu'$-Dichte von M_1 ist. Wir erhalten also

$$\begin{aligned} \rho_H(M_0, M_1) &= \int_{\Omega \times \Omega'} \sqrt{\bar{r}_0'(\omega'|\omega)\bar{p}_0(\omega)\bar{r}_1'(\omega'|\omega)\bar{p}_1(\omega)}\, \nu \otimes \nu'(d\omega, d\omega') \\ &= \int_{\Omega} \int_{\Omega'} \sqrt{\bar{r}_0'(\omega'|\omega)\bar{r}_1'(\omega'|\omega)}\, \nu'(d\omega') \sqrt{\bar{p}_0(\omega)\bar{p}_1(\omega)}\, \nu(d\omega) \\ &\leq \int_{\Omega} \sqrt{\bar{p}_0(\omega)\bar{p}_1(\omega)}\, \nu(d\omega) \sup_{\omega \in \Omega} \int_{\Omega'} \sqrt{\bar{r}_0'(\omega'|\omega)\bar{r}_1'(\omega'|\omega)}\, \nu'(d\omega') \\ &= \rho_H\left(\bar{P}_0, \bar{P}_1\right) \sup_{\omega \in \Omega} \rho_H\left(\bar{R}_0'(\cdot|\omega), \bar{R}_1'(\cdot|\omega)\right). \end{aligned}$$

Es gilt aber $\bar{P}_0 \in \mathrm{conv}(\mathcal{P}_0)$, $\bar{P}_1 \in \mathrm{conv}(\mathcal{P}_1)$, und für jedes $\omega \in \Omega$, auch $\bar{R}_0'(d\omega'|\omega) \in \mathrm{conv}(\mathcal{P}_0')$ und $\bar{R}_1'(d\omega'|\omega) \in \mathrm{conv}(\mathcal{P}_1')$. Somit ist die gewünschte Ungleichung gezeigt. □

2.2.3 Eine Minimax-Identität für Tests

Auch wenn sich in der Definition des Minimax-Risikos

$$\mathcal{M}_n(\mathcal{P},\theta) := \inf_{\hat{\theta}_n} \sup_{P\in\mathcal{P}} \mathcal{R}_n(\hat{\theta}_n, P, \theta)$$

das Infimum und das Supremum natürlich nicht vertauschen lassen, so ist für dessen Analyse oft eine Sattelpunkt-Identität der Form

$$\inf_{x\in A}\sup_{y\in B} f(x,y) = \sup_{y\in B}\inf_{x\in A} f(x,y)$$

nützlich. Allgemeine Identitäten dieser Form wurden etwa von Sion (1958) bewiesen. Das allgemeine Prinzip hinter solchen Identitäten ist immer, dass eine Art Sattelpunkt vorliegt. Dies bedeutet zunächst, dass die Funktion f im ersten Argument eine gewisse Konvexität und im zweiten Argument eine gewisse Konkavität aufweist (Abschwächungen der konventionellen Definition von Konvexität und Konkavität sind möglich). Weiters benötigt man für ein solches Resultat gewöhnlich, dass die Mengen A und B konvex sind, und, dass zumindest eine der beiden Mengen kompakt ist. Schließlich wird zumindest eine gewisse Halbstetigkeit in jedem einzelnen Argument gefordert, wobei sich hier die Stetigkeit in derjenigen Variable die über der kompakten Menge optimiert wird auf die selbe Topologie bezieht in der die Menge eben kompakt ist.

Satz 2.6. *Betrachte Konstanten $-\infty < a \le b < \infty$. Sei $\mathbb{S}$ eine konvexe Menge von endlichen signierten Maßen auf einem messbaren Raum $(\Omega,\mathcal{A})$ welche durch ein σ-endliches Maß dominiert ist. Weiter sei $\mathbb{T}$ die Menge aller $\mathcal{A}-\mathcal{B}(\mathbb{R})$-messbaren Funktionen $\phi:\Omega\to[a,b]$. Dann gilt*

$$\sup_{\phi\in\mathbb{T}}\inf_{\sigma\in\mathbb{S}} \int_\Omega \phi\, d\sigma \quad = \quad \inf_{\sigma\in\mathbb{S}}\sup_{\phi\in\mathbb{T}} \int_\Omega \phi\, d\sigma.$$

Beweis. Das Resultat folgt aus einem allgemeinen Minimax-Theorem von Sion (1958, Corollary 3.3) und dem Satz von Banach-Alaoglu (vgl. Rudin, 1973, Section 3.15) um die schwach*-Kompaktheit von $\mathbb{T}$ nachzuweisen. □

Korollar 2.7. *Seien $\mathcal{P}_0$ und $\mathcal{P}_1$ zwei Modelle auf einem messbaren Raum $(\Omega,\mathcal{A})$, so dass $\mathcal{P}_0\cup\mathcal{P}_1$ durch ein σ-endliches Maß dominiert ist. Dann gilt*

$$\begin{aligned}\inf_{Tests\ \phi}\sup_{\substack{P_0\in\mathcal{P}_0\\P_1\in\mathcal{P}_1}} \mathbb{E}_{P_0}[\phi]+\mathbb{E}_{P_1}[1-\phi] &= \sup_{\substack{P_0\in conv(\mathcal{P}_0)\\P_1\in conv(\mathcal{P}_1)}}\inf_{Tests\ \phi} \mathbb{E}_{P_0}[\phi]+\mathbb{E}_{P_1}[1-\phi] \\ &= \rho_T\left(conv(\mathcal{P}_0), conv(\mathcal{P}_1)\right),\end{aligned} \tag{2.2.1}$$

wobei das Infimum über alle (randomisierten) Tests $\phi:\Omega\to[0,1]$ läuft.

Beweis. Beachte, dass sich die linke Seite von (2.2.1) nicht verändert, wenn wir für $j=0,1$, $\mathcal{P}_j$ durch seine konvexe Hülle $\mathrm{conv}(\mathcal{P}_j)$ ersetzen, da für $P_{0,s}\in\mathcal{P}_0$, $P_{1,t}\in\mathcal{P}_1$ gilt, dass

$$\begin{aligned}\mathbb{E}_{\sum_{s=1}^k \alpha_s P_{0,s}}[\phi]+\mathbb{E}_{\sum_{t=1}^l \beta_t P_{1,t}}[1-\phi] &= \sum_{s,t}\alpha_s\beta_t\left(\mathbb{E}_{P_{0,s}}[\phi]+\mathbb{E}_{P_{1,t}}[1-\phi]\right)\\ &\le \sup_{\substack{P_0\in\mathcal{P}_0\\P_1\in\mathcal{P}_1}} \mathbb{E}_{P_0}[\phi]+\mathbb{E}_{P_1}[1-\phi],\\ &\le \sup_{\substack{P_0\in\mathrm{conv}(\mathcal{P}_0)\\P_1\in\mathrm{conv}(\mathcal{P}_1)}} \mathbb{E}_{P_0}[\phi]+\mathbb{E}_{P_1}[1-\phi],\end{aligned}$$

wobei α_s und β_t nicht-negative Koeffizienten mit $\sum_{s=1}^k\alpha_s = 1 = \sum_{t=1}^l\beta_t$ sind. Wende jetzt Satz 2.6 mit $\mathbb{S}=\{P_0-P_1 : P_j\in\mathrm{conv}(\mathcal{P}_j), j=0,1\}$ und $a=0$, $b=1$, an. □

2.3 Kontraktionseigenschaften von Markov-Kernen

Es seien $(\Omega, \mathcal{A})$ und $(\Omega', \mathcal{A}')$ messbare Räume, $\mathcal{P}$ und $\mathcal{P}'$ jeweils die Menge aller W-Maße auf $(\Omega, \mathcal{A})$, beziehungsweise auf $(\Omega', \mathcal{A}')$ und $Q : \mathcal{A}' \times \Omega \to [0,1]$ ein Markov-Kern. Wie oben definieren wir für $P \in \mathcal{P}$ die Verknüpfung $QP(d\omega') := \int_\Omega Q(d\omega'|\omega)\, P(d\omega)$. Man kann also $P \mapsto QP$ als eine Abbildung von $\mathcal{P}$ nach $\mathcal{P}'$ auffassen. Der nächste Satz zeigt, dass diese Abbildung in der Hellinger-Distanz Lipschitz-stetig ist mit Konstante 1.

Satz 2.8 (Del Moral et al. (2003))**.** *Für $P_0, P_1 \in \mathcal{P}$ gilt, $d_H(QP_0, QP_1) \leq d_H(P_0, P_1)$ und $\rho_H(P_0, P_1) \leq \rho_H(QP_0, QP_1)$.*

Beweis. Wegen Satz 2.4.(2) genügt es die Ungleichung für die Hellinger-Affinität zu beweisen. Sei $Q_0 = QP_0$, $Q_1 = QP_1$, $\mu = P_0 + P_1$, $\nu = Q_0 + Q_1$, und wähle entsprechende Dichten p_0, p_1 und q_0, q_1. Betrachte nun die Lebesgue-Zerlegung (cf. Klenke, 2008, Theorem 7.33) von P_0 bezüglich P_1, also

$$P_0 \;=\; P_0^a + P_0^\perp,$$

wobei $P_0^a \ll P_1$ und $P_0^\perp \perp P_1$. Klarerweise sind P_0^a und $P_0^\perp$ absolut stetig bezüglich μ und wir schreiben p_0^a und $p_0^\perp$ für zugehörige μ-Dichten, so dass $p_0 = p_0^a + p_0^\perp$ erfüllt ist. Definiere $Q_0^a(d\omega') := \int_\Omega Q(d\omega'|\omega)\, P_0^a(d\omega)$ und $Q_0^\perp(d\omega') := \int_\Omega Q(d\omega'|\omega)\, P_0^\perp(d\omega)$ und beachte, dass $Q_0 = Q_0^a + Q_0^\perp$, so dass Q_0^a und $Q_0^\perp$ absolut stetig bezüglich ν sind. Mit q_0^a und $q_0^\perp$ bezeichnen wir wiederum ν-Dichten, so dass $q_0 = q_0^a + q_0^\perp$. Wegen Orthogonalität von $P_0^\perp$ und P_1, gibt es eine Menge $S \in \mathcal{A}$, so dass $p_0^\perp$ auf S μ-fast überall gleich Null ist und p_1 auf S^c, μ-fast-überall gleich null ist. Somit erhalten wir

$$\begin{aligned}\rho_H(P_0, P_1) &= \int_\Omega \sqrt{p_0 p_1}\, d\mu = \int_S \sqrt{p_0^a p_1 + p_0^\perp p_1}\, d\mu + \int_{S^c} \sqrt{p_0^a p_1 + p_0^\perp p_1}\, d\mu \\ &= \int_S \sqrt{p_0^a p_1}\, d\mu \leq \int_\Omega \sqrt{p_0^a p_1}\, d\mu = \rho_H(P_0^a, P_1).\end{aligned}$$

Andererseits gilt aber auch

$$\rho_H(Q_0, Q_1) = \int_{\Omega'} \sqrt{q_0 q_1}\, d\nu \geq \int_{\Omega'} \sqrt{q_0^a q_1}\, d\nu = \rho_H(Q_0^a, Q_1).$$

Es bleibt also zu zeigen, dass $\rho_H(P_0^a, P_1) \leq \rho_H(Q_0^a, Q_1)$. Betrachte dazu eine P_1-Dichte $\tilde{p}_0$ von P_0^a. Natürlich ist $\tilde{p}_1 \equiv 1$ eine P_1-Dichte von P_1. Somit erhalten wir $\rho_H(P_0^a, P_1) = \int_\Omega \sqrt{\tilde{p}_0}\, dP_1$ und $Q_0^a(d\omega') = \int_\Omega Q(d\omega'|\omega)\tilde{p}_0(\omega)\, P_1(d\omega)$, $Q_1(d\omega') = \int_\Omega Q(d\omega'|\omega)\, P_1(d\omega)$, so dass $Q_0^a \ll Q_1$, und wir bezeichnen mit $\tilde{q}_0$ eine zugehörige Q_1-Dichte von Q_0^a. Wir müssen also zeigen, dass

$$\int_\Omega \sqrt{\tilde{p}_0}\, dP_1 \;\leq\; \int_{\Omega'} \sqrt{\tilde{q}_0}\, dQ_1.$$

Wir zeigen stattdessen die folgende, etwas stärkere Aussage.

Behauptung. *Sei P_1 ein W-Maß auf $(\Omega, \mathcal{A})$, $p \in \mathcal{L}_1(\Omega, \mathcal{A}, P_1)$ nicht-negativ, $Q : \mathcal{A}' \times \Omega \to [0,1]$ ein Kanal, $Q_1 = QP_1$ und $Q^a(d\omega') = \int_\Omega Q(d\omega'|\omega)p(\omega)\, P_1(d\omega)$. Klarerweise gilt $Q^a \ll Q_1$ und Q^a ist ein endliches Maß. Wir bezeichnen mit $q : \Omega' \to [0, \infty)$ eine zugehörige Q_1-Dichte von Q^a. Dann gilt*

$$\int_\Omega \sqrt{p}\, dP_1 \;\leq\; \int_{\Omega'} \sqrt{q}\, dQ_1. \tag{2.3.1}$$

Wir beweisen die Behauptung zunächst für einfache Funktionen $p = \sum_{i=1}^n \alpha_i \mathbb{1}_{A_i}$, wobei $\alpha_i \in (0, \infty)$ und $A_1, \ldots, A_n \in \mathcal{A}$ paarweise disjunkt sind. Wegen Disjunktheit sieht man leicht, dass

$$\int_\Omega \sqrt{p}\, dP_1 = \int_\Omega \sqrt{\sum_{i=1}^n \alpha_i \mathbb{1}_{A_i}}\, dP_1 = \sum_{i=1}^n \sqrt{\alpha_i} P_1(A_i). \tag{2.3.2}$$

Als nächstes definieren wir uns endliche Maße $Q_i^a(d\omega') := \int_{A_i} Q(d\omega'|\omega)\, P_1(d\omega)$ und betrachten für $A' \in \mathcal{A}'$,

$$\int_{A'} q\, dQ_1 = Q^a(A') = \int_\Omega Q(A'|\omega)p(\omega)\, P_1(d\omega) = \sum_{i=1}^n \alpha_i \int_{A_i} Q(A'|\omega)\, P_1(d\omega) = \sum_{i=1}^n \alpha_i Q_i^a(A').$$

Da $\alpha_i > 0$, gilt $Q_i^a \ll Q^a \ll Q_1$, und wir bezeichnen die zugehörigen Q_1-Dichten mit q_i, so dass $q = \sum_{i=1}^n \alpha_i q_i$, Q_1-fast sicher. Für $\omega' \in \Omega'$ setze jetzt $r(\omega') := \sum_{i=1}^n q_i(\omega')$ und $R := r^{-1}((0,\infty))$, und beachte, dass für alle $A' \in \Omega'$,

$$\begin{aligned}\int_{A'} 1\, dQ_1 = Q_1(A') = \int_\Omega Q(A'|\omega)\, P_1(d\omega) &\geq \sum_{i=1}^n \int_{A_i} Q(A'|\omega)\, P_1(d\omega) = \sum_{i=1}^n Q_i^a(A') \\ &= \sum_{i=1}^n \int_{A'} q_i\, dQ_1 = \int_{A'} r\, dQ_1,\end{aligned}$$

wegen Disjunktheit der A_i, so dass $r \leq 1$, Q_1-fast sicher. Somit folgt aus der Jensen-Ungleichung, dass

$$\begin{aligned}\int_{\Omega'} \sqrt{q}\, dQ_1 &\geq \int_R \sqrt{\sum_{i=1}^n \alpha_i q_i}\, dQ_1 = \int_R \sqrt{r}\sqrt{\sum_{i=1}^n \alpha_i \frac{q_i}{r}}\, dQ_1 \\ &\geq \int_R \sqrt{r} \sum_{i=1}^n \sqrt{\alpha_i}\frac{q_i}{r}\, dQ_1 \geq \int_R \sum_{i=1}^n \sqrt{\alpha_i} q_i\, dQ_1 = \sum_{i=1}^n \sqrt{\alpha_i} Q_i^a(R).\end{aligned}$$

Aber es gilt natürlich $Q_i^a(R) = Q_i^a(\Omega') - Q_i^a(R^c) = Q_i^a(\Omega') = P_1(A_i)$. Unter Verwendung von (2.3.2) haben wir somit (2.3.1) für einfaches p gezeigt. Für allgemeines $p \geq 0$, sei nun $(p^{(n)})_{n\in\mathbb{N}}$ eine Folge von einfachen Funktionen, so dass $p^{(n)}(\omega) \uparrow p(\omega)$. Wenn $q^{(n)}$ eine Q_1-Dichte von $\int_\Omega Q(d\omega'|\omega)p^{(n)}(\omega)\, P_1(d\omega)$ ist, dann sieht man leicht, dass $q^{(n)} \leq q$, Q_1-fast sicher. Somit folgt aus (2.3.1) für einfache Funktionen, dass

$$\int_\Omega \sqrt{p^{(n)}}\, dP_1 \leq \int_{\Omega'} \sqrt{q^{(n)}}\, dQ_1 \leq \int_{\Omega'} \sqrt{q}\, dQ_1.$$

Die allgemeine Relation (2.3.1) folgt jetzt aus dem Satz der monotonen Konvergenz. □

Bemerkung. Die Aussage von Satz 2.8 sollte uns nicht besonders überraschen. Natürlich sollte es schwieriger sein die privatisierten Verteilungen QP_0 und QP_1 zu unterscheiden als die nicht-privatisierten P_0 und P_1. Das ist gewissermaßen gerade die Idee beim Privatisieren mittels eines Kanals Q. Etwas überraschend ist es dafür aber vielleicht, dass der Beweis aufwendiger ist als man auf den ersten Blick vermuten würde. Dies kommt aber nur von der Wurzel in der Definition der Hellinger-Distanz. Für die Totalvariationsdistanz ist der Beweis des analogen Satzes ein Einzeiler (vgl. Aufgabe 2.5).

2.3.1 Die Duchi-Jordan-Wainwright Ungleichungen

Wie zu beginn dieses Kapitels sei jetzt wieder $(\mathcal{X}, \mathcal{F})$ unser Stichprobenraum und $\mathcal{P}$ ein statistisches Modell auf $(\mathcal{X}, \mathcal{F})$.

Satz 2.9 (Duchi et al. (2014))**.** *Sei $\alpha \in (0,\infty)$ und $(\mathcal{Z}, \mathcal{G}) = (\mathbb{R}^m, \mathcal{B}(\mathbb{R}^m))$. Weiter sei der Kanal $Q : \mathcal{G} \times \mathcal{X}^1 \to [0,1]$ α-DP und $P_0, P_1 \in \mathcal{P}$. Dann gilt*

$$D_{KL}(QP_0|QP_1) + D_{KL}(QP_1|QP_0) \;\leq\; \min(4, e^{2\alpha})(e^\alpha - 1)^2 d_{TV}(P_0, P_1)^2.$$

Bemerkung. Auf den ersten Blick scheint Satz 2.9 recht unverdächtig zu sein. Tatsächlich ist er aber gemeinsam mit Korollar 2.10 eines der fundamentalsten Resultate für die Statistik unter 'local differential privacy', insbesondere wenn es darum geht die private Minimax-Optimalität von Schätzern nachzuweisen (siehe Kapitel 3). Außerdem ist das Resultat insofern etwas überraschend, als man natürlich für beliebige W-Maße P_0 und P_1 ohne Privatisierung niemals eine Ungleichung der Art $D_{KL}(P_0|P_1) \leq C d_{\mathrm{TV}}(P_0, P_1)^r$ erhalten kann, da ja $D_{KL}(P_0|P_1)$ nicht unbedingt endlich sein muss, wohingegen $d_{\mathrm{TV}}(P_0, P_1) \leq 1$ gilt.

Beweis von Satz 2.9. Für $x \in \mathcal{X}^1$ sei $q(z|x)$ wie in Satz 1.12 eine Dichte von $Q(dz|x)$ bezüglich eines dominierenden Maßes μ. Wegen Aufgabe 2.4 ist dann $m_j(z) = \int_{\mathcal{X}} q(z|x)\, P_j(dx)$ eine μ-Dichte von QP_j, für $j = 0, 1$, und m_0 und m_1 besitzen gemeinsamen Träger. Tatsächlich folgt aus Satz 1.12 sogar, dass alle $z \mapsto q(z|x)$ für $x \in \mathcal{X}$ einen gemeinsamen Träger haben. Somit ergibt sich

$$\begin{aligned} D_{KL}(QP_0|QP_1) + D_{KL}(QP_1|QP_0) &= \int_{\mathcal{Z}} m_0(z) \log \frac{m_0(z)}{m_1(z)} \mu(dz) + \int_{\mathcal{Z}} m_1(z) \log \frac{m_1(z)}{m_0(z)} \mu(dz) \\ &\leq \int_{\mathcal{Z}} |m_0(z) - m_1(z)| \left| \log \frac{m_0(z)}{m_1(z)} \right| \mu(dz). \end{aligned}$$

Am Ende des Beweises werden wir zeigen, dass

$$|m_0(z) - m_1(z)| \leq \min(2, e^\alpha) \inf_{x \in \mathcal{X}} q(z|x)(e^\alpha - 1) d_{\mathrm{TV}}(P_0, P_1), \qquad \forall z \in \mathcal{Z}. \tag{2.3.3}$$

Es folgt nun aus Aufgabe 2.6, dass für $z \in \mathcal{Z}$ mit $m_0(z) \neq 0$, $m_1(z) \neq 0$, gilt

$$\begin{aligned} \left| \log \frac{m_0(z)}{m_1(z)} \right| &\leq \frac{|m_0(z) - m_1(z)|}{\min(m_0(z), m_1(z))} \\ &\leq \frac{\min(2, e^\alpha) \inf_{x \in \mathcal{X}} q(z|x)(e^\alpha - 1) d_{\mathrm{TV}}(P_0, P_1)}{\inf_{x \in \mathcal{X}} q(z|x)} \\ &= \min(2, e^\alpha)(e^\alpha - 1) d_{\mathrm{TV}}(P_0, P_1). \end{aligned}$$

Neuerliche Anwendung von (2.3.3) liefert also

$$\begin{aligned} D_{KL}(QP_0|QP_1) + D_{KL}(QP_1|QP_0) &\leq \min(4, e^{2\alpha})(e^\alpha - 1)^2 d_{\mathrm{TV}}(P_0, P_1)^2 \int_{\mathcal{Z}} \inf_{x \in \mathcal{X}} q(z|x)\, \mu(dz) \\ &\leq \min(4, e^{2\alpha})(e^\alpha - 1)^2 d_{\mathrm{TV}}(P_0, P_1)^2 \int_{\mathcal{Z}} q(z|x)\, \mu(dz) \\ &= \min(4, e^{2\alpha})(e^\alpha - 1)^2 d_{\mathrm{TV}}(P_0, P_1)^2. \end{aligned}$$

Es bleibt die Ungleichung in (2.3.3) zu zeigen. Seien p_0 und p_1 Dichten von P_0 und P_1 bezüglich $\nu := P_0 + P_1$. Somit gilt

$$\begin{aligned} m_0(z) - m_1(z) &= \int_{\mathcal{X}} q(z|x)[p_0(x) - p_1(x)]\, \nu(dx) \\ &= \int_{\mathcal{X}} q(z|x)[p_0(x) - p_1(x)]_+ \nu(dx) - \int_{\mathcal{X}} q(z|x)[p_0(x) - p_1(x)]_- \nu(dx) \\ &\leq \sup_{x \in \mathcal{X}} q(z|x) \int_{\mathcal{X}} [p_0(x) - p_1(x)]_+ \nu(dx) - \inf_{x \in \mathcal{X}} q(z|x) \int_{\mathcal{X}} [p_0(x) - p_1(x)]_- \nu(dx) \\ &= \left[\sup_{x \in \mathcal{X}} q(z|x) - \inf_{x \in \mathcal{X}} q(z|x) \right] d_{\mathrm{TV}}(P_0, P_1), \end{aligned}$$

mit Aufgabe 2.3. Es folgt

$$|m_0(z) - m_1(z)| \leq \sup_{x, x' \in \mathcal{X}} |q(z|x) - q(z|x')| d_{\mathrm{TV}}(P_0, P_1). \tag{2.3.4}$$

Als nächstes betrachten wir

$$\begin{aligned}\sup_{x,x'\in\mathcal{X}} |q(z|x) - q(z|x')| &\leq \inf_{x^*\in\mathcal{X}} \sup_{x,x'\in\mathcal{X}} |q(z|x) - q(z|x^*) + q(z|x^*) - q(z|x')| \\ &\leq 2 \inf_{x^*\in\mathcal{X}} \sup_{x\in\mathcal{X}} |q(z|x) - q(z|x^*)| \\ &= 2 \inf_{x^*\in\mathcal{X}} q(z|x^*) \sup_{x\in\mathcal{X}} \left| \frac{q(z|x)}{q(z|x^*)} - 1 \right| \\ &\leq 2 \inf_{x^*\in\mathcal{X}} q(z|x^*)(e^\alpha - 1).\end{aligned}$$

Analog erhalten wir

$$\begin{aligned}|q(z|x) - q(z|x')| &\leq q(z|x') \left| \frac{q(z|x)}{q(z|x')} - 1 \right| \\ &= \inf_{x^*\in\mathcal{X}} \frac{q(z|x')}{q(z|x^*)} q(z|x^*) \left| \frac{q(z|x)}{q(z|x')} - 1 \right| \\ &\leq e^\alpha \inf_{x^*\in\mathcal{X}} q(z|x^*)(e^\alpha - 1).\end{aligned}$$

Somit folgt

$$\sup_{x,x'\in\mathcal{X}} |q(z|x) - q(z|x')| \leq \min(2, e^\alpha) \inf_{x^*\in\mathcal{X}} q(z|x^*)(e^\alpha - 1).$$

Zusammen mit (2.3.4) ist (2.3.3) gezeigt. □

Korollar 2.10 (Duchi et al. (2014))**.** *Es sei $\alpha \in (0,\infty)$, $(\mathcal{Z},\mathcal{G}) = (\mathbb{R}^m, \mathcal{B}(\mathbb{R}^m))$ und $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ sequentiell-interaktiv und α-DP. Weiter seien für $i = 1,\dots,n$, $P_{0,i}, P_{1,i} \in \mathcal{P}$. Definiere die Produktmaße $P_0 = \bigotimes_{i=1}^n P_{0,i}$ und $P_1 = \bigotimes_{i=1}^n P_{1,i}$. Dann gilt*

$$D_{KL}(QP_0|QP_1) + D_{KL}(QP_1|QP_0) \;\leq\; 2\min(4, e^{2\alpha})(e^\alpha - 1)^2 \sum_{i=1}^n d_{TV}(P_{0,i}, P_{1,i})^2.$$

Bemerkung 2.11. Korollar 2.10 scheint ebenfalls zunächst unverdächtig. Allerdings ist zu beachten, dass dieses Korollar, unter Verwendung von Pinskers Ungleichung (Satz 2.4.(1)) und unter der Annahme, dass $P_{0,i} = P_{0,n}$ und $P_{1,i} = P_{1,n}$, für alle $i = 1,\dots,n$, die folgende Implikation hat

$$d_{\mathrm{TV}}(QP_{0,n}^n, QP_{1,n}^n) \leq \min(\sqrt{2}, e^\alpha/\sqrt{2})(e^\alpha - 1)\sqrt{n} \cdot d_{\mathrm{TV}}(P_{0,n}, P_{1,n}). \tag{2.3.5}$$

In dieser Ungleichung ist die Abhängigkeit von n zu beachten. Vergleicht man dies nämlich mit der scharfen Abschätzung ohne Privatisierung (vgl. Aufgabe 2.8)

$$d_{\mathrm{TV}}(P_{0,n}^n, P_{1,n}^n) \leq n \cdot d_{\mathrm{TV}}(P_{0,n}, P_{1,n}),$$

so erkennt man, dass die Privatisierung einen entscheidenden Einfluss auf die Ordnung (in n) hat, mit der sich Produktmaße einander annähern. Sequentiell privatisierte Produktmaße sind also um Größenordnungen schwerer zu unterscheiden, als ihre nicht-privaten Versionen. Dies ist der treibende Mechanismus der zu den unterschiedlichen Konvergenzraten in Kapitel 3 führt.

Beweis von Korollar 2.10. Für $j = 0,1$, $i = 1,\dots,n$ und $A_i \in \mathcal{G}^{\otimes i}$, definiere

$$M_{j,i}(A_i) := QP_j(A_i \times \mathcal{Z}^{n-i}) = \int_{\mathcal{X}^i} R_i^{(x_1,\dots,x_i)}(A_i) \bigotimes_{k=1}^i P_{j,k}(dx_k),$$

wobei $R_i^{(x_1,\dots,x_i)}$ wie in Korollar 1.10 definiert ist. Aus Aufgabe 2.7, Korollar 1.10 und Satz 2.9 folgt nun, dass

$$\begin{aligned}
D_{KL}(QP_0|QP_1) &= D_{KL}(Q_1P_{0,1}|Q_1P_{1,1}) \\
&\quad + \sum_{i=2}^{n} \int_{\mathcal{Z}^{i-1}} D_{KL}\left(Q_i^{(z_1,\dots,z_{i-1})}P_{0,i}\middle|Q_i^{(z_1,\dots,z_{i-1})}P_{1,i}\right) M_{0,i-1}(dz_1,\dots,dz_{i-1}) \\
&\leq \min(4,e^{2\alpha})(e^\alpha-1)^2 d_{\mathrm{TV}}(P_{0,1},P_{1,1})^2 \\
&\quad + \sum_{i=2}^{n} \int_{\mathcal{X}^{i-1}} \int_{\mathcal{Z}^{i-1}} \\
&\qquad D_{KL}\left(Q_i^{(z_1,\dots,z_{i-1})}P_{0,i}|Q_i^{(z_1,\dots,z_{i-1})}P_{1,i}\right) R_{i-1}^{(x_1,\dots,x_{i-1})}(dz_1,\dots,dz_{i-1}) \bigotimes_{k=1}^{i-1} P_{0,k}(dx_k) \\
&\leq \min(4,e^{2\alpha})(e^\alpha-1)^2 \sum_{i=1}^{n} d_{\mathrm{TV}}(P_{0,i},P_{1,i})^2.
\end{aligned}$$

□

2.4 Übungsaufgaben

Aufgabe 2.1. Sei $\mathcal{P}$ ein statistisches Modell auf einem messbaren Raum $(\Omega,\mathcal{A})$ das durch ein σ-endliches Maß μ dominiert ist, d.h. $P \ll \mu$ für alle $P \in \mathcal{P}$. Zeigen Sie, dass dann für beliebige Hypothesen $H_0, H_1 \subseteq \mathcal{P}$ ein minimax-Test $\phi^* : \Omega \to [0,1]$ existiert. (4P)

Hinweis: Verwenden Sie die folgende 'schwache Folgenkompaktheit' der Testfunktionen aus Nöle and Plachky (1967).

Satz. *Zu jeder Folge (ϕ_k) von randomisierten Tests $\phi_k : \Omega \to [0,1]$, gibt es eine Teilfolge (ϕ_{k_j}) und einen Test ϕ^* mit*

$$\int_\Omega \phi_{k_j} f\, d\mu \xrightarrow[j\to\infty]{} \int_\Omega \phi^* f\, d\mu, \qquad \text{für jedes } f \in \mathcal{L}_1(\Omega,\mathcal{A},\mu).$$

Aufgabe 2.2. Es sei $(\mathcal{Z},\mathcal{G})$ ein messbarer Raum und $Q : \mathcal{G} \times \mathcal{X}^n \to [0,1]$ α-DP. Durch $\mathcal{P} = \{P_x : x \in \mathcal{X}^n\}$, $P_x(dz) := Q(dz|x)$, ist ein statistisches Modell auf $(\mathcal{Z},\mathcal{G})$ gegeben. Zeigen Sie, dass für $x_0, x_1 \in \mathcal{X}^n$ mit $d_0(x_0,x_1) = 1$, jeder Test für $H_0 : x = x_0$ gegen $H_1 : x = x_1$ zum Niveau $\gamma \in (0,1)$, höchstens eine Güte von γe^α besitzen kann. (2P)

Aufgabe 2.3. Es seien P_0 und P_1 zwei W-Maße auf einem gemeinsamen W-Raum $(\Omega,\mathcal{A})$ und p_0 und p_1 Dichten von P_0 und P_1 bezüglich eines beliebigen dominierenden Maßes ν. Zeigen Sie, dass

$$d_{\mathrm{TV}}(P_0,P_1) = \int_\Omega [p_0(\omega)-p_1(\omega)]_+ \nu(d\omega) = \int_\Omega [p_0(\omega)-p_1(\omega)]_- \nu(d\omega) = \frac{1}{2}\int_\Omega |p_0(\omega)-p_1(\omega)|\nu(d\omega).$$

(2P)

Aufgabe 2.4. Für $\alpha \in (0,\infty)$ sei $Q : \mathcal{G} \times \mathcal{X}^1 \to [0,1]$ α-DP und $P_0, P_1 \in \mathcal{P} = \mathcal{P}(\mathcal{X},\mathcal{B}(\mathcal{X}))$. Weiter sei μ und $q(z|x)$ wie in Satz 1.12. Zeigen Sie, dass dann QP_0 und QP_1 bezüglich einander absolut stetig sind und μ-Dichten $m_j(z) = \int_\mathcal{X} q(z|x)\, P_j(dx)$, $j = 0,1$, besitzen welche gemeinsamen Träger haben. Zeigen Sie weiter, dass dieser gemeinsame Träger auch derselbe ist wie der von $z \mapsto q(z|x)$, unabhängig von $x \in \mathcal{X}$. (2P)

Aufgabe 2.5. Beweisen Sie das Analogon von Satz 2.8 für die Totalvariationsdistanz. (2P)

Aufgabe 2.6. Für $a,b \in (0,\infty)$, gilt $|\log \frac{a}{b}| \leq \frac{|a-b|}{\min(a,b)}$. (2P)

Aufgabe 2.7. Es sei $(\mathcal{Z}, \mathcal{G})$ ein messbarer Raum und P, R zwei W-Maße auf dem Produktraum $(\mathcal{Z}^n, \mathcal{G}^{\otimes n})$. Definiere die marginalen Verteilungen $P_i = P\pi_i^{-1}$, $R_i = R\pi_i^{-1}$, $P_{1:i} = P\pi_{1:i}^{-1}$ und $R_{1:i} = R\pi_{1:i}^{-1}$, wobei $\pi_i : \mathcal{Z}^n \to \mathcal{Z}$, $\pi_i(z_1, \dots, z_n) = z_i$ und $\pi_{1:i} : \mathcal{Z}^n \to \mathcal{Z}^i$, $\pi_{1:i}(z_1, \dots, z_n) = (z_1, \dots, z_i)$. Es gilt also z.B. $P_{1:1} = P_1$ und $P_{1:n} = P$. Angenommen für $i = 2, \dots, n$ existieren bedingte Verteilungen (Markov-Kerne) $P^{(i)} : \mathcal{G} \times \mathcal{Z}^{i-1} \to [0, 1]$ und $R^{(i)} : \mathcal{G} \times \mathcal{Z}^{i-1} \to [0, 1]$, so dass

$$\begin{aligned} P_{1:i}(dz_1, \dots, dz_i) &= P^{(i)}(dz_i | z_1, \dots, z_{i-1})\, P_{1:i-1}(dz_1, \dots, dz_{i-1}), \qquad \text{und} \\ R_{1:i}(dz_1, \dots, dz_i) &= R^{(i)}(dz_i | z_1, \dots, z_{i-1})\, R_{1:i-1}(dz_1, \dots, dz_{i-1}). \end{aligned}$$

Schreibe $P^{(z_1,\dots,z_{i-1})}(dz_i) = P^{(i)}(dz_i | z_1, \dots, z_{i-1})$ und $R^{(z_1,\dots,z_{i-1})}(dz_i) = R^{(i)}(dz_i | z_1, \dots, z_{i-1})$. Falls $P \ll R$, dann gilt

$$D_{KL}(P|R) = D_{KL}(P_1|R_1) + \sum_{i=2}^{n} \int_{\mathcal{Z}^{i-1}} D_{KL}\left(P^{(z_1,\dots,z_{i-1})} | R^{(z_1,\dots,z_{i-1})}\right) P_{1:i-1}(dz_1, \dots, dz_{i-1}).$$

(4P)

Aufgabe 2.8. Es seien P_0 und P_1 W-Maße auf einem messbaren Raum $(\Omega, \mathcal{A})$. Zeigen Sie

$$d_{\mathrm{TV}}(P_0^n, P_1^n) \leq n \cdot d_{\mathrm{TV}}(P_0, P_1).$$

Finden Sie weiter zwei Folgen $P_{0,n}$ und $P_{1,n}$ sowie eine Konstante $C > 0$, so dass

$$n \cdot d_{\mathrm{TV}}(P_{0,n}, P_{1,n}) \leq C d_{\mathrm{TV}}(P_{0,n}^n, P_{1,n}^n),$$

zumindest für alle großen n. (4P)

Aufgabe 2.9. Es sei $(\Omega, \mathcal{A})$ ein messbarer Raum, $\mathcal{P} = \mathcal{P}(\Omega, \mathcal{A}) \neq \varnothing$ ein Modell und $\theta : \mathcal{P} \to \mathbb{R}$ ein Funktional. Schreibe $\omega_{d_{\mathrm{TV}}} = \omega_{d_{\mathrm{TV}},\mathcal{P},\theta}$. Unter welchen (möglichst allgemeinen) Annahmen an $(\Omega, \mathcal{A})$, $\mathcal{P}$ und/oder θ sind die folgenden beiden Aussagen äquivalent?

- $\frac{\omega_{d_{\mathrm{TV}}}(\varepsilon)}{\varepsilon} \to 0$, für $\varepsilon \to 0$.
- $\theta : \mathcal{P} \to \mathbb{R}$ ist konstant.

(*)

Hinweis: Ein Beweis unter der Annahme, dass $\mathcal{P}$ konvex ist, ist mir bekannt und $(2P)$ wert. Lässt sich die Konvexität (möglicherweise unter zusätzlichen, "nicht-trivialen" Annahmen an $(\Omega, \mathcal{A})$ und θ abschwächen?

Aufgabe 2.10. Wie Aufgabe 2.9 nur für die Äquivalenz der Aussagen

- $\frac{\omega_{d_{\mathrm{H}}}(\varepsilon)}{\varepsilon^2} \to 0$, für $\varepsilon \to 0$.
- $\theta : \mathcal{P} \to \mathbb{R}$ ist konstant.

(*)

Kapitel 3

Schätzung reeller Funktionale unter α-SIDP

Wir kehren jetzt zu dem am Beginn von Kapitel 2 skizzierten Problem der Charakterisierung des privaten Minimax-Risikos zurück. Wir betrachten also wieder einen abstrakten Stichprobenraum $(\mathcal{X}, \mathcal{F})$ mit einem statistischen Modell $\mathcal{P} = \mathcal{P}(\mathcal{X}, \mathcal{F})$. Die Originaldaten sind also $x \in \mathcal{X}^n$ welche unter einem Produktmaß P^n, mit einem unbekannten $P \in \mathcal{P}$, erzeugt wurden. Wir beschränken uns wie bisher auf Privatisierungsmechanismen welche private Beobachtungen $z \in \mathcal{Z}^n$ erzeugen, wobei $\mathcal{Z} = \mathcal{Z}_m = \mathbb{R}^m$, für ein $m \in \mathbb{N}$. Ein Privatisierungsmechanismus oder Kanal ist also wie bisher ein Markov-Kern $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$, wobei $\mathcal{G}_m = \mathcal{B}(\mathcal{Z}_m) = \mathcal{B}(\mathbb{R}^m)$ die Borel'sche σ-Algebra auf $\mathcal{Z}_m = \mathbb{R}^m$ bezeichnet. Das statistische Problem besteht nun darin den Wert $\theta(P)$ des Funktionals $\theta : \mathcal{P} \to \mathbb{R}$ basierend auf den privatisierten Daten $z \in \mathcal{Z}^n$ zu schätzen. Wir konzentrieren uns dafür auf die Klasse der sequentiell interaktiven α-differentiell privaten Mechanismen (vgl. Definition 1.9 und Korollar 1.10) die Daten in $\mathcal{Z}_m^n$ generieren, also auf

$$\mathcal{Q}_\alpha(m) := \left\{ Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1] \;\middle|\; Q \text{ ist } \alpha\text{-SIDP} \right\}.$$

Das zugehörige α-private Minimax-Risiko ist also gegeben durch

$$\mathcal{M}_{n,\alpha}(\mathcal{P}, \theta) := \inf_{m \in \mathbb{N}} \inf_{Q \in \mathcal{Q}_\alpha(m)} \inf_{\hat{\theta}_n : \mathcal{Z}_m^n \to \mathbb{R}} \sup_{P \in \mathcal{P}} \mathbb{E}_{QP^n} \left[l\left(\left| \hat{\theta}_n - \theta(P) \right| \right) \right],$$

wobei $l : \mathbb{R}_+ \to \mathbb{R}_+$ eine nicht-fallende Verlustfunktion ist. Bezeichne mit

$$\omega_{d_{\mathrm{TV}}}(\varepsilon) := \omega_{d_{\mathrm{TV}}, \mathcal{P}, \theta}(\varepsilon) := \sup\{ |\theta(P_0) - \theta(P_1)| : d_{\mathrm{TV}}(P_0, P_1) \leq \varepsilon, P_0, P_1 \in \mathcal{P} \}$$

den d_{TV}-Stetigkeitsmodul von θ über $\mathcal{P}$. Unser erstes Ziel in diesem Kapitel ist es, für festes $\alpha \in (0, \infty)$, und unter geeigneten Annahmen, ein Resultat der Form

$$\mathcal{M}_{n,\alpha}(\mathcal{P}, \theta) \quad \asymp \quad l \circ \omega_{d_{\mathrm{TV}}} \left(\left[n(e^\alpha - 1)^2 \right]^{-1/2} \right),$$

für $n \to \infty$, zu beweisen. Dies sollte mit der Aussage von Satz 2.2 verglichen werden. Tatsächlich werden wir das Resultat von Satz 2.2 sogar als Nebenprodukt unserer Überlegungen erhalten. Wir beginnen zunächst mit einer Reihe von Definitionen. Die Resultate in diesem Kapitel stamme alle aus Rohde and Steinberger (2018).

Notation

Für einen beliebigen (nicht notwendigerweise α-privaten) Kanal $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$, setze

$$\mathcal{M}_{n,m}(Q, \mathcal{P}, \theta) := \inf_{\hat{\theta}_n : \mathcal{Z}_m^n \to \mathbb{R}} \sup_{P \in \mathcal{P}} \mathbb{E}_{QP^n} \left[l\left(\left| \hat{\theta}_n - \theta(P) \right| \right) \right].$$

Beachte, dass wir für $(\mathcal{X},\mathcal{F}) = (\mathcal{Z}_m,\mathcal{G}_m) = (\mathbb{R}^m,\mathcal{B}(\mathbb{R}^m))$ und falls $Q(dz|x) := \delta_x(dz)$ Punktmasse bei $x \in \mathcal{X}^n$ ist, die Gleichheit

$$\mathcal{M}_{n,m}(Q,\mathcal{P},\theta) = \inf_{\hat{\theta}_n:\mathcal{X}^n\to\mathbb{R}} \sup_{P\in\mathcal{P}} \mathbb{E}_{P^n}\left[l\left(\left|\hat{\theta}_n - \theta(P)\right|\right)\right]$$

erhalten, also das klassische, nicht-private Minimax-Risiko. Weiter definiere für $s,t \in \mathbb{R}$, $\mathcal{P}_{\leq t} := \{P \in \mathcal{P} : \theta(P) \leq t\}$, $\mathcal{P}_{\geq s} := \{P \in \mathcal{P} : \theta(P) \geq s\}$, $\mathcal{P}^n := \{P^n : P \in \mathcal{P}\}$ und $Q\mathcal{P}^n := \{QP^n : P \in \mathcal{P}\}$. Für $\Delta \in [0,\infty)$, sei

$$\eta_A^{(n)}(Q,\Delta) \;:=\; \sup_{t\in\mathbb{R}} \rho_T\left(\mathrm{conv}\left(Q\mathcal{P}^n_{\leq t}\right), \mathrm{conv}\left(Q\mathcal{P}^n_{\geq t+\Delta}\right)\right).$$

Zur Erinnerung, $\rho_T(P_0,P_1) = \inf_{\text{Tests }\phi}\left(\mathbb{E}_{P_0}[\phi] + \mathbb{E}_{P_1}[1-\phi]\right)$ ist die Test-Affinität und misst die Schwierigkeit des Testproblems $H_0 : P_0$ gegen $H_1 : P_1$ im Sinne der Summe aus Fehler erster und zweiter Art. Die Größe $\eta_A^{(n)}(Q,\Delta)$ bezeichnet also in gewisser Weise die maximale Schwierigkeit des Testproblems $H_0 : QP_0^n$ gegen $H_1 : QP_1^n$ wobei $|\theta(P_0) - \theta(P_1)| \geq \Delta$. Weiter definieren wir für $\eta \in [0,1)$ die verallgemeinerte Inverse von $\Delta \mapsto \eta_A^{(n)}(Q,\Delta)$ durch

$$\Delta_A^{(n)}(Q,\eta) := \sup\{\Delta \geq 0 : \eta_A^{(n)}(Q,\Delta) > \eta\}.$$

Wird Δ, also der Mindestabstand zwischen $\theta(P_0)$ und $\theta(P_1)$ größer, so wird es natürlicher höchstens leichter $H_0 : QP_0^n$ von $H_1 : QP_1^n$ zu unterscheiden. Die Größe $\Delta_A^{(n)}(Q,\eta)$ bezeichnet also die maximale Entfernung die $\theta(P_0)$ und $\theta(P_1)$ haben dürfen, so dass das ungünstigste der oben erwähnten Testprobleme schwerer ist als η. Für eine nicht-fallende Funktion $f : \mathbb{R}_+ \to \mathbb{R}_+ \cup \{\infty\}$ schreiben wir auch $l(y^-) := \lim_{x\uparrow y} l(x)$, für $y \in \mathbb{R}_+ \cup \{\infty\}$, und $l(0^-) := l(0)$. Beachte, dass gilt:

- $\eta_A^{(n)}(Q,0) = 1$.
- $\{\Delta \geq 0 : \eta_A^{(n)}(Q,\Delta) > \eta\} \neq \varnothing$, für $\eta \in [0,1)$, und somit $\Delta_A^{(n)}(Q,\eta) \geq 0$.
- $\Delta \mapsto \eta_A^{(n)}(Q,\Delta)$ ist monoton nicht-wachsend, da für $\Delta_0 \leq \Delta_1$ gilt, $\mathrm{conv}\left(Q\mathcal{P}^n_{\geq t+\Delta_0}\right) \supseteq \mathrm{conv}\left(Q\mathcal{P}^n_{\geq t+\Delta_1}\right)$.

3.1 Eine untere Schranke für das private Minimax-Risiko

Satz 3.1. *Sei $\eta \in (0,1)$, $n,m \in \mathbb{N}$, $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$ ein Kanal und $l : \mathbb{R}_+ \to \mathbb{R}_+$ eine nicht-fallende Funktion. Falls $Q\mathcal{P}^n$ dominiert ist, so gilt*

$$\mathcal{M}_{n,m}(Q,\mathcal{P},\theta) \;\geq\; l\left(\left[\frac{1}{2}\Delta_A^{(n)}(Q,\eta)\right]^-\right)\frac{\eta}{2}.$$

Beweis. Wir zeigen zunächst, dass für $\Delta \in [0,\infty)$ und einen beliebigen Schätzer $\hat{\theta}_n : \mathcal{Z}_m^n \to \mathbb{R}$, gilt

$$\sup_{P\in\mathcal{P}} QP^n\left(|\hat{\theta}_n - \theta(P)| \geq \Delta\right) \;\geq\; \frac{1}{2}\eta_A^{(n)}(Q,2\Delta). \tag{3.1.1}$$

Dafür definieren wir die Ereignisse $S := \{z \in \mathcal{Z}_m^n : |\hat{\theta}_n(z) - \theta(P)| \geq \Delta\}$, $S_1 := \{z \in \mathcal{Z}_m^n : \hat{\theta}_n(z) \geq t+\Delta, \theta(P) \leq t\}$, und $S_2 := \{z \in \mathcal{Z}_m^n : \hat{\theta}_n(z) < t+\Delta, \theta(P) \geq t+2\Delta\}$, welche $S_1 \subseteq S$ und $S_2 \subseteq S$ erfüllen. Verwendet man diese Mengeninklusionen, die Tatsache, dass $\max(a,b) \geq (a+b)/2$ ist

und Korollar 2.7, so erhält man für beliebiges $t \in \mathbb{R}$, dass

$$\begin{aligned}
\sup_{P\in\mathcal{P}} QP^n(S) &\geq \sup_{P\in\mathcal{P}} \max\{QP^n(S_1), QP^n(S_2)\} \\
&\geq \max\left\{ \sup_{P\in\mathcal{P}_{\leq t}} QP^n(\hat{\theta}_n \geq t+\Delta), \sup_{P\in\mathcal{P}_{\geq t+2\Delta}} QP^n(\hat{\theta}_n < t+\Delta) \right\} \\
&\geq \frac{1}{2} \sup_{\substack{P_0\in\mathcal{P}_{\leq t} \\ P_1\in\mathcal{P}_{\geq t+2\Delta}}} \left[QP_0^n(\hat{\theta}_n \geq t+\Delta) + QP_1^n(\hat{\theta}_n < t+\Delta) \right] \\
&\geq \frac{1}{2} \inf_{\text{Tests } \phi} \sup_{\substack{P_0\in\mathcal{P}_{\leq t} \\ P_1\in\mathcal{P}_{\geq t+2\Delta}}} \left(\mathbb{E}_{QP_0^n}[\phi] + \mathbb{E}_{QP_1^n}[1-\phi] \right) \\
&= \frac{1}{2} \inf_{\text{Tests } \phi} \sup_{\substack{Q_0\in Q\mathcal{P}^n_{\leq t} \\ Q_1\in Q\mathcal{P}^n_{\geq t+2\Delta}}} \left(\mathbb{E}_{Q_0}[\phi] + \mathbb{E}_{Q_1}[1-\phi] \right) \\
&= \frac{1}{2} \rho_T \left(\operatorname{conv}\left(Q\mathcal{P}^n_{\leq t}\right), \operatorname{conv}\left(Q\mathcal{P}^n_{\geq t+2\Delta}\right) \right).
\end{aligned}$$

Da $t \in \mathbb{R}$ beliebig war können wir auch das Supremum über $t \in \mathbb{R}$ vor die untere Schranke schreiben und erhalten somit (3.1.1). Wir betrachten nun als erstes den Fall $\Delta_A^{(n)}(Q,\eta) = 0$. Wegen der Monotonie von l gilt

$$\mathcal{M}_{n,m}(Q,\mathcal{P},\theta) = \inf_{\hat{\theta}_n} \sup_{P\in\mathcal{P}} \mathbb{E}_{QP^n}\left[l\left(|\hat{\theta}_n - \theta(P)| \right) \right] \geq l(0) \geq l(0)\frac{\eta}{2} = l\left(\left[\frac{1}{2}\Delta_A^{(n)}(Q,\eta) \right]^- \right) \frac{\eta}{2}.$$

Falls $\Delta_A^{(n)}(Q,\eta) = \infty$, dann gilt nach Definition von $\Delta_A^{(n)}(Q,\eta) = \sup\{\Delta \geq 0 : \eta_A^{(n)}(Q,\Delta) > \eta\}$, dass $\eta_A^{(n)}(Q,\Delta) > \eta$, für alle $\Delta \in \mathbb{R}_+ = [0,\infty)$. Somit folgt mit der Markov-Ungleichung, wegen der Monotonie von l und wegen (3.1.1), dass

$$\begin{aligned}
\mathcal{M}_{n,m}(Q,\mathcal{P},\theta) &\geq \inf_{\hat{\theta}_n} \sup_{P\in\mathcal{P}} QP^n(l(|\hat{\theta}_n - \theta(P)|) \geq l(\Delta)) l(\Delta) \\
&\geq \inf_{\hat{\theta}_n} \sup_{P\in\mathcal{P}} QP^n(|\hat{\theta}_n - \theta(P)| \geq \Delta) l(\Delta) \\
&\geq \frac{\eta_A^{(n)}(Q,2\Delta)}{2} l(\Delta) \\
&\geq l(\Delta)\frac{\eta}{2},
\end{aligned}$$

für jedes $\Delta \in \mathbb{R}_+$. Die gewünschte Ungleichung folgt also für $\Delta \uparrow \infty$. Schließlich betrachten wir den Fall $\Delta_A^{(n)}(Q,\eta) \in (0,\infty)$. Wähle $\varepsilon \in (0, \Delta_A^{(n)}(Q,\eta))$, setze $\Delta_0 := \frac{1}{2}[\Delta_A^{(n)}(Q,\eta) - \varepsilon] \in (0, \Delta_A^{(n)}(Q,\eta)/2)$ und $D := \{\Delta \geq 0 : \eta_A^{(n)}(Q,\Delta) > \eta\}$. Wegen Monotonie von $\Delta \mapsto \eta_A^{(n)}(Q,\Delta)$, gilt $D \supseteq [0, \sup D) = [0, \Delta_A^{(n)}(Q,\eta))$, und somit, $2\Delta_0 \in D$. Es folgt also, dass $\eta_A^{(n)}(Q,2\Delta_0) > \eta$. Das selbe Argument wie zuvor, mit der Markov-Ungleichung, Monotonie von l und (3.1.1), ergibt also

$$\mathcal{M}_{n,m}(Q,\mathcal{P},\theta) \geq \frac{\eta_A^{(n)}(Q,2\Delta_0)}{2} l(\Delta_0) \geq l\left(\frac{1}{2}[\Delta_A^{(n)}(Q,\eta) - \varepsilon] \right) \frac{\eta}{2}.$$

Für $\varepsilon \downarrow 0$ ist der Beweis also erbracht. □

Bemerkung.
- In Satz 3.1 wurden keine Annahmen an den Kanal $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$ gemacht. Er gilt also auch für den klassischen nicht-privaten Fall $(\mathcal{X},\mathcal{F}) = (\mathcal{Z}_m, \mathcal{G}_m)$ und $Q(dz|x) = \delta_x(dz)$.

- Die Größe $\Delta_A^{(n)}(Q,\eta)$ in der unteren Schranke in Satz 3.1 ist leider in den meisten Schätzproblemen immer noch nicht besonders einfach zu berechnen, auch wenn sie die Konvergenzrate des Minimax-Risikos tatsächlich allgemein charakterisiert. Darum konzentrieren wir uns hier auf eine alternative, kleinere Schranke, die die Minimax-Rate zwar nicht mehr in voller Allgemeinheit charakterisiert (da sie manchmal zu klein ist), aber eine solche Charakterisierung immer noch in vielen interessanten Fällen erlaubt.

Analog zu $\Delta_A^{(n)}(Q,\eta)$ definieren wir nun

$$\Delta_2^{(n)}(Q,\eta) := \sup\{\Delta \geq 0 : \eta_2^{(n)}(Q,\Delta) > \eta\},$$

wobei

$$\eta_2^{(n)}(Q,\eta) := \sup_{t\in\mathbb{R}} \rho_T\left(Q\mathcal{P}^n_{\leq t}, Q\mathcal{P}^n_{\geq t+\Delta}\right).$$

Klarerweise gilt $\eta_2^{(n)}(Q,\Delta) \leq \eta_A^{(n)}(Q,\Delta)$, und somit auch $\Delta_2^{(n)}(Q,\eta) \leq \Delta_A^{(n)}(Q,\eta)$. Wir können also $\Delta_A^{(n)}(Q,\eta)$ in Satz 3.1 sofort durch $\Delta_2^{(n)}(Q,\eta)$ ersetzen und erhalten eine kleinere untere Schranke an das Minimax-Risiko. Um diese Größer wiederum nach unten abzuschätzen kommt jetzt der Stetigkeitsmodul des Funktionals θ über dem Modell $\mathcal{P}$ ins Spiel (siehe Definition 2.1).

Lemma 3.2. *Sei $\eta \in (0,1)$, $n,m \in \mathbb{N}$, $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$ ein Kanal und $d : \mathcal{P}\times\mathcal{P} \to \mathbb{R}_+$ eine Metrik. Dann gilt*

$$\omega_{d,\mathcal{P},\theta}\left(g_{d,\mathcal{P}}(Q,\eta)^-\right) \;\leq\; \Delta_2^{(n)}(Q,\eta),$$

wobei $g_{d,\mathcal{P}}(Q,\eta) := \inf\{d(P_0,P_1) : \rho_T(QP_0^n, QP_1^n) \leq \eta, P_0,P_1 \in \mathcal{P}\}$.

Beweis. Der Einfachheit halber schreiben wir $\omega = \omega_{d,\mathcal{P},\theta}$ und $g = g_{d,\mathcal{P}}$. Für $\delta > 0$, setze $C := \{|\theta(P_0) - \theta(P_1)| : d(\mathcal{P}_0,P_1) \leq g(Q,\eta) - \delta, P_0,P_1 \in \mathcal{P}\}$. Es gilt also $\sup C = \omega(g(Q,\eta)-\delta)$. Schreiben wir $D := \{\Delta \geq 0 : \eta_2^{(n)}(Q,\Delta) > \eta\}$, so gilt $\sup D = \Delta_2^{(n)}(Q,\eta)$ und es bleibt die Inklusion $C \subseteq D$ zu zeigen und $\delta \downarrow 0$ zu betrachten. Falls $C = \varnothing$, so ist die gewünschte Ungleichung trivial. Wir wählen also $\Delta \in C$ beliebig. Nach Definition von C gibt es also $P_0,P_1 \in \mathcal{P}$, so dass $\Delta = |\theta(P_0) - \theta(P_1)|$ und $d(P_0,P_1) \leq g(Q,\eta) - \delta$. Es gilt also $\rho_T(QP_0^n, QP_1^n) > \eta$, da andernfalls, nach Definition von g, der Widerspruch $d(P_0,P_1) \geq g(Q,\eta) > g(Q,\eta) - \delta \geq d(P_0,P_1)$ folgt. Ohne Beschränkung der Allgemeinheit sei nun $t_0 := \theta(P_0) \leq \theta(P_1)$. Somit gilt $P_0 \in \mathcal{P}_{\leq t_0}$ und $P_1 \in \mathcal{P}_{\geq t_0+\Delta}$, was zur Folge hat, dass

$$\eta_2^{(n)}(Q,\Delta) \geq \rho_T(Q\mathcal{P}^n_{\leq t_0}, Q\mathcal{P}^n_{\geq t_0+\Delta}) \geq \rho_T(QP_0^n, QP_1^n) > \eta.$$

Damit ist aber $\Delta \in D$, und, da $\Delta \in C$ beliebig war, auch $C \subseteq D$. □

Satz 3.3. *Sei $\eta \in (0,1)$, $n,m \in \mathbb{N}$, $\alpha \in (0,\infty)$, $g_{d,\mathcal{P}}$ wie in Lemma 3.2 und $Q : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$ ein Kanal. Dann gilt mit $\eta_0 := \eta(2-\eta)$, dass*

$$g_{d_H,\mathcal{P}}(Q,\eta) \;\geq\; \sqrt{\frac{\eta_0|\log\eta_0|}{n}}.$$

Falls Q auch α-SI ist, so gilt ausserdem

$$g_{d_{TV},\mathcal{P}}(Q,\eta) \;\geq\; \frac{1-\eta}{\sqrt{2n(e^\alpha-1)^2}}.$$

Beweis. Beachte zunächst, dass für $P_0,P_1 \in \mathcal{P}$ gilt

$$\begin{aligned} d_{\mathrm{H}}^2(P_0,P_1) &\overset{Satz\ 2.4.(2)}{=} 2(1-\rho_H(P_0,P_1)) \overset{Satz\ 2.4.(4)}{=} 2\left(1-\rho_H(P_0^n,P_1^n)^{\frac{1}{n}}\right) \\ &\overset{Satz\ 2.8}{\geq} 2\left(1-\rho_H(QP_0^n,QP_1^n)^{\frac{1}{n}}\right) \\ &\overset{Satz\ 2.4.(6)}{\geq} 2\left(1-\left[\rho_T(QP_0^n,QP_1^n)\left(2-\rho_T(QP_0^n,QP_1^n)\right)\right]^{\frac{1}{2n}}\right). \end{aligned}$$

Ist also $\rho_T(QP_0^n, QP_1^n) \leq \eta$, so folgt wegen Monotonie von $x \mapsto x(2-x)$ auf $[0,1]$, dass

$$d_{\mathrm{H}}(P_0, P_1) \geq \sqrt{2\left(1 - [\eta(2-\eta)]^{\frac{1}{2n}}\right)},$$

und somit auch

$$g_{d_{\mathrm{H}},\mathcal{P}}(Q,\eta) = \inf\{d_{\mathrm{H}}(P_0,P_1) : \rho_T(QP_0^n, QP_1^n) \leq \eta, P_0, P_1 \in \mathcal{P}\} \geq \sqrt{2\left(1-\eta_0^{\frac{1}{2n}}\right)}.$$

Der erste Teil des Satzes folgt dann aus der folgenden Behauptung. Für $x, y \in (0,1)$ gilt

$$1 - y^x \;\geq\; y|\log y|x.$$

Dies sieht man aber leicht, da die Ableitung von $f(x) := 1 - y^x = 1 - \exp(x \log y)$ in dem interessierenden Wertebereich gegeben ist durch $f'(x) = -y^x \log y \geq y|\log y|$. Mit dem Mittelwertsatz der Differentialrechnung folgt also

$$\frac{f(x) - f(0)}{x} = f'(\zeta) \geq y|\log y|,$$

für ein $\zeta \in [0,x]$ und somit die Behauptung, da $f(0) = 0$.

Für den zweiten Teil erinnern wir uns an das Korollar 2.10, beziehungsweise an die Ungleichung (2.3.5). Es gilt also

$$d_{\mathrm{TV}}(QP_0^n, QP_1^n) \leq \sqrt{2n}(e^\alpha - 1) d_{\mathrm{TV}}(P_0, P_1),$$

für $P_0, P_1 \in \mathcal{P}$. Mit Satz 2.4.(5) folgt

$$d_{\mathrm{TV}}(P_0,P_1) \geq \frac{d_{\mathrm{TV}}(QP_0^n, QP_1^n)}{\sqrt{2n}(e^\alpha - 1)} = \frac{1 - \rho_T(QP_0^n, QP_1^n)}{\sqrt{2n(e^\alpha-1)^2}},$$

und somit

$$g_{d_{\mathrm{TV}},\mathcal{P}}(Q,\eta) = \inf\{d_{\mathrm{TV}}(P_0,P_1) : \rho_T(QP_0^n, QP_1^n) \leq \eta, P_0, P_1 \in \mathcal{P}\} \geq \frac{1-\eta}{\sqrt{2n(e^\alpha-1)^2}}.$$

□

Setzen wir alles zusammen, so erhalten wir das folgende Resultat.

Korollar 3.4. *Sei $\eta \in (0,1)$, $\eta_0 := \eta(2-\eta)$, $n \in \mathbb{N}$, $\alpha \in (0,\infty)$ und $l : \mathbb{R}_+ \to \mathbb{R}_+$ nicht-fallend. Dann gilt*

$$\mathcal{M}_{n,\alpha}(\mathcal{P},\theta) \;\geq\; l\left(\left[\frac{1}{2}\left(\omega_{d_H}\left(\left[\sqrt{\frac{\eta_0|\log\eta_0|}{n}}\right]^-\right) \vee \omega_{d_{TV}}\left(\left[\frac{1-\eta}{\sqrt{2n(e^\alpha-1)^2}}\right]^-\right)\right)\right]^-\right)\frac{\eta}{2},$$

wobei $\omega_{d_{TV}} = \omega_{d_{TV},\mathcal{P},\theta}$ und $\omega_{d_H} = \omega_{d_H,\mathcal{P},\theta}$.

Bemerkung 3.5.

a) Die untere Schranke sollte mit Satz 2.2 verglichen werden.

b) Der Wert von η in Korollar 3.4 ist für die Konvergenzrate in n nicht von Bedeutung sondern beeinflusst lediglich die Größe der Konstanten in der unteren Schranke. Prinzipiell lässt sich die untere Schranke in $\eta \in (0,1)$ maximieren. Der optimale Wert hängt dann jedoch von den Stetigkeitsmodulen $\omega_{d_{\mathrm{TV}}}$ und $\omega_{d_{\mathrm{H}}}$ ab. Im Folgenden genügt es uns für η einfach einen beliebigen festen Wert, wie zum Beispiel $\eta = 1/2$, einzusetzen.

c) Wegen Satz 2.4.(4) gilt $\omega_{d_{\mathrm{H}}}(\varepsilon) \leq \omega_{d_{\mathrm{TV}}}(\varepsilon)$. Oft gilt $\omega_{d_{\mathrm{TV}}}(\varepsilon) \asymp \varepsilon^{r_0}$ und $\omega_{d_{\mathrm{H}}}(\varepsilon) \asymp \varepsilon^{r_1}$ (siehe unten). In diesem Fall ist die untere Schranke in Korollar 3.4 bei festem $\alpha \in (0,\infty)$ also von der Ordnung

$$l\left(\omega_{d_{\mathrm{TV}}}\left(n^{-1/2}\right)\right),$$

für $n \to \infty$.

d) Korollar 3.4 ist für beliebiges $n \in \mathbb{N}$ und $\alpha \in (0,\infty)$ formuliert. Wir können es also auch für eine Folge $\alpha = \alpha_n$ anwenden. Insbesondere sehen wir dann, dass für $\alpha_n \lesssim n^{-1/2}$ das α_n-privatisierte Minimax-Risiko $\mathcal{M}_{n,\alpha_n}(\mathcal{P},\theta)$ für $n \to \infty$ (ausser in trivialen Fällen) nicht mehr gegen 0 konvergiert. Andererseits sehen wir auch, dass für eine Folge $\alpha_n \to \infty$ die hinreichend schnell über alle Grenzen wächst, sich die untere Schranke auf die Schranke im nicht-privaten Fall reduziert (vgl. Satz 2.2), der $\omega_{d_{\mathrm{TV}}}$-Term also wegen dem Maximum für große n keinen Einfluss mehr hat. Dies war zu erwarten, da für großes α 'beinahe' keine Privatisierung vorliegt.

3.1.1 Beispiele

Beispiel 3.6 (Integralfunktionale)**.** Es sei $\mathcal{X} \subseteq \mathbb{R}^d$, $\mathcal{F} = \mathcal{B}(\mathcal{X})$, $f : \mathcal{X} \to \mathbb{R}$ messbar, $C \in (0,\infty)$ und $\kappa \in (1,\infty)$. Als unser Modell betrachten wir die Menge

$$\mathcal{P}_\kappa(C) := \{P : \mathbb{E}_P[|f|^\kappa] \leq C\}.$$

Für $P \in \mathcal{P}_\kappa(C)$, definiere $\theta(P) := \mathbb{E}_P[f]$. Um uns das Leben zu erleichtern und Trivialitäten zu vermeiden, nehmen wir an, dass es $x_0, x_1 \in \mathcal{X}$ gibt, so dass $f(x_0) \neq f(x_1)$, $|f(x_0)|^\kappa < C$ und $f(x_1)|^\kappa \leq C$. Mit dieser Konstruktion lassen sich also zum Beispiel insbesondere die folgenden Schätzprobleme Abbilden:

$d = 1$,	$f(x) = x^m$,	Momentenschätzung
$d = 2$,	$f(x,y) = xy$,	Kovarianzschätzung
$d \in \mathbb{N}$,	$f(z) = \mathbb{1}_A(z)$,	Schätzung der Wskt. von Ereignis $A \in \mathcal{B}(\mathcal{X})$.

Wir unterscheiden nun zwei Fälle in denen sich der Stetigkeitsmodul, und somit das Minimax-Risiko, qualitativ unterschiedlich verhält.

Behauptung.

A) Falls $\|f\|_\infty := \sup_{x\in\mathcal{X}} |f(x)| < \infty$*, so gilt,* $\exists \bar{A}_0 > 0 : \omega_{d_{TV}}(\varepsilon) \geq \bar{A}_0\varepsilon$, $\forall \varepsilon \in (0,1)$.

B) Falls $Im(|f|) := |f(\mathcal{X})| \supseteq (0,\infty)$*, so gilt,* $\omega_{d_{TV}}(\varepsilon) \geq \left(\frac{C}{2}\right)^{\frac{1}{\kappa}} \varepsilon^{\frac{\kappa-1}{\kappa}}$, $\forall \varepsilon \in (0,1)$.

Beweis. Im Fall A, seien $x_0, x_1 \in \mathcal{X}$, so dass $f(x_0) \neq f(x_1)$, $|f(x_0)|^\kappa < C$ und $f(x_1)|^\kappa \leq C$. Für $\varepsilon \in (0,1)$, definiere $\bar{P}_0 := \delta_{x_0}$ und $\bar{P}_1 := (1-\varepsilon)\delta_{x_0} + \varepsilon\delta_{x_1}$, wobei δ_x das Dirac-Maß bei $x \in \mathcal{X}$ bezeichnet. Somit gilt $\mathbb{E}_{\bar{P}_0}[|f|^\kappa] = |f(x_0)|^\kappa < C$ und $\mathbb{E}_{\bar{P}_1}[|f|^\kappa] = (1-\varepsilon)|f(x_0)|^\kappa + \varepsilon|f(x_1)|^\kappa < C$, also $\bar{P}_0, \bar{P}_1 \in \mathcal{P}_\kappa(C)$. Weiter berechnen wir

$$\begin{aligned} d_{\mathrm{TV}}(\bar{P}_0,\bar{P}_1) &= \sup_{A\in\mathcal{B}(\mathcal{X})} |\delta_{x_0}(A) - (1-\varepsilon)\delta_{x_0}(A) - \varepsilon\delta_{x_1}(A)| \\ &= \varepsilon \sup_{A\in\mathcal{B}(\mathcal{X})} |\delta_{x_0}(A) - \delta_{x_1}(A)| = \varepsilon, \end{aligned}$$

und $|\theta(\bar{P}_0) - \theta(\bar{P}_1)| = |f(x_0) - (1-\varepsilon)f(x_0) - \varepsilon f(x_1)| = \varepsilon|f(x_0) - f(x_1)| =: \varepsilon\bar{A}_0 > 0$. Es folgt also, dass $\omega_{d_{\mathrm{TV}}}(\varepsilon) = \sup\{|\theta(P_0) - \theta(P_1)| : d_{\mathrm{TV}}(P_0,P_1) \leq \varepsilon, P_0, P_1 \in \mathcal{P}\} \geq \bar{A}_0\varepsilon$.

Im Fall B, wähle $\varepsilon \in (0,1)$, $\delta \in (0,(C/2)^{\frac{1}{\kappa}}]$ beliebig. Laut Voraussetzung gibt es $x_0, x_1 \in \mathcal{X}$, so dass $|f(x_0)| = \delta$ und $|f(x_1)| = \left(\frac{C}{2\varepsilon}\right)^{\frac{1}{\kappa}}$. Wir wählen jetzt $\bar{P}_0$ und $\bar{P}_1$ wie im Fall A. Es ergibt sich also, dass $\mathbb{E}_{\bar{P}_0}[|f|^\kappa] = \delta^\kappa \leq C/2 < C$ und $\mathbb{E}_{\bar{P}_1}[|f|^\kappa] = (1-\varepsilon)\delta^\kappa + \varepsilon\frac{C}{2\varepsilon} \leq C/2 + C/2 = C$, und somit $\bar{P}_0, \bar{P}_1 \in \mathcal{P}_\kappa(C)$. Wie zuvor gilt $d_{\mathrm{TV}}(\bar{P}_0,\bar{P}_1) = \varepsilon$ und $|\theta(\bar{P}_0) - \theta(\bar{P}_1)| = \varepsilon|f(x_0) - f(x_1)| \to \varepsilon\left(\frac{C}{2\varepsilon}\right)^{\frac{1}{\kappa}} = (C/2)^{\frac{1}{\kappa}}\varepsilon^{\frac{\kappa-1}{\kappa}}$, für $\delta \to 0$. Es folgt die untere Schranke $\omega_{d_{\mathrm{TV}}}(\varepsilon) \geq (C/2)^{\frac{1}{\kappa}}\varepsilon^{\frac{\kappa-1}{\kappa}}$. □

Zuletzt betrachten wir noch den konkreten Fall $\mathcal{X} = \mathbb{R}$, $f(x) = x$, also Schätzung des Erwartungswertes, unter quadratischer Verlustfunktion $l(t) = t^2$ und $\kappa \geq 2$. Natürlich gilt hier für $\hat{\theta}_n(x_1, \ldots, x_n) := \frac{1}{n}\sum_{i=1}^n x_i$ und $P \in \mathcal{P}_\kappa(C)$, dass

$$\mathbb{E}_{P^n}[(\hat{\theta}_n - \theta(P))^2] = \frac{1}{n}\operatorname{Var}_P[f] \leq \frac{\mathbb{E}_P[f^2]}{n} \leq \frac{C^{\frac{2}{\kappa}}}{n}.$$

Die gewöhnliche, nicht-private, Minimax-Schätzrate ist also zumindest von der Ordnung $l(n^{-1/2}) = 1/n$. Im α-DPSI Fall gilt aber wegen Korollar 3.4 und der obigen Behauptung, dass

$$\begin{aligned}
\mathcal{M}_{n,\alpha}(\mathcal{P}_\kappa(C), \theta) &\geq \frac{\eta}{2} l\left(\frac{1}{2}\omega_{d_{\mathrm{TV}}}\left(\left[\frac{1-\eta}{\sqrt{2n(e^\alpha - 1)^2}}\right]^-\right)\right) \\
&\geq \frac{\eta}{8}(C/2)^{\frac{2}{\kappa}}\left(\frac{(1-\eta)^2}{2n(e^\alpha-1)^2}\right)^{\frac{\kappa-1}{\kappa}} \\
&=: \tilde{C}\left(\frac{1}{n(e^\alpha-1)^2}\right)^{\frac{\kappa-1}{\kappa}}.
\end{aligned}$$

Im privaten Fall kann also kein Schätzer eine bessere Rate als

$$l\left(\left(\frac{1}{\sqrt{n}(e^\alpha-1)}\right)^{\frac{\kappa-1}{\kappa}}\right) = \left(\frac{1}{n(e^\alpha-1)^2}\right)^{\frac{\kappa-1}{\kappa}}$$

erreichen, und diese ist deutlich langsamer als $1/n$, da $\frac{\kappa-1}{\kappa} < 1$.

Beispiel 3.7 (Gleichverteilung)**.** Es sei $M \in (1, \infty)$, $\mathcal{X} = [0, M]$, $\mathcal{F} = \mathcal{B}(\mathcal{X})$, $l(t) = t^2$, λ das Lebesgue maß auf $\mathbb{R}$,

$$\mathcal{P}_M := \left\{P_\vartheta : \frac{dP_\vartheta}{d\lambda} = \frac{1}{\vartheta}\mathbb{1}_{[0,\vartheta]}, \vartheta \in (0, M]\right\},$$

die Menge aller stetigen Gleichverteilungen auf $[0, \vartheta]$, und $\theta(P_\vartheta) := \vartheta = \mathbb{E}_{P_\vartheta}[f]$, wobei $f(x) = 2x$. Dieses Schätzproblem wird gerne als ein Beispiel für ein 'irreguläres Problem' herangezogen, in dem der Maximum-Likelihood-Schätzer nicht asymptotisch normalverteilt ist. Im direkten Problem ist wohl bekannt, dass $\hat{\theta}_n(x_1, \ldots, x_n) = \max(x_1, \ldots, x_n)$ die Minimax-Rate von $l(n^{-1}) = 1/n^2$ erreicht, also

$$\sup_{\vartheta \in (0,M]} \mathbb{E}_{P_\vartheta^n}[(\hat{\theta}_n - \theta(P))^2] = O\left(\frac{1}{n^2}\right).$$

Allerdings gilt für $\varepsilon \in (0, 1)$,

$$\begin{aligned}
d_{\mathrm{TV}}(P_1, P_{1-\varepsilon}) &= \frac{1}{2}\int_{\mathbb{R}} \left|\mathbb{1}_{[0,1]} - \frac{1}{1-\varepsilon}\mathbb{1}_{[0,1-\varepsilon]}\right| d\lambda \\
&= \frac{1}{2}\int_{\mathbb{R}} \frac{\varepsilon}{1-\varepsilon}\mathbb{1}_{[0,1-\varepsilon]} + \mathbb{1}_{(1-\varepsilon,1]}\, d\lambda \\
&= \varepsilon/2 + \varepsilon/2 = \varepsilon,
\end{aligned}$$

und $|\theta(P_1) - \theta(P_{1-\varepsilon})| = |1 - (1-\varepsilon)| = \varepsilon$. Somit folgt, dass $\omega_{d_{\mathrm{TV}}}(\varepsilon) \geq \varepsilon$, und

$$\mathcal{M}_{n,\alpha} \geq \frac{\tilde{C}}{n(e^\alpha - 1)^2}.$$

Im privaten Fall lässt sich also keine bessere Rate als $l(n^{-1/2}) = 1/n$ erreichen!

Beispiel 3.8 (Schätzung der Dichte und ihrer Ableitungen)**.** Sei $\mathcal{X} = \mathbb{R}$, $\mathcal{F} = \mathcal{B}(\mathbb{R})$, $x_0 \in \mathbb{R}$, $\beta > 0$, $C > 0$, $b := \lfloor \beta \rfloor$ der ganzzahlige Anteil von β, $m \in \mathbb{N}_0$, $m < \beta$ und $\mathcal{H}(\beta, C)$ die Hölder-Klasse aller Lebesgue-Dichten $p : \mathbb{R} \to [0, \infty)$, so dass p b-mal differentierbar ist und

$$\left| p^{(b)}(x) - p^{(b)}(y) \right| \ \leq \ C|x - y|^{\beta - b} \quad \forall x, y \in \mathbb{R}.$$

Für $p \in \mathcal{H}(\beta, C)$, betrachte $\theta(p) := p^{(m)}(x_0)$.

Behauptung. *Es gibt $\bar{A}_0 > 0$ und $\bar{\varepsilon}_0 > 0$, so dass*

$$\omega_{d_{TV}}(\varepsilon) \ \geq \ \bar{A}_0 \varepsilon^{\frac{\beta - m}{\beta + 1}} \quad \forall \varepsilon \in [0, \bar{\varepsilon}_0).$$

Zum Vergleich: Es gilt $\omega_{d_H}(\varepsilon) \asymp \varepsilon^{\frac{\beta - m}{\beta + 1/2}}$, für $\varepsilon \to 0$.

Bemerkung.

- *Hohe Ableitungen sind 'schwerer' zu schätzen.*
- *Sehr glatte Dichten sind 'leichter' zu schätzen.*
- *Bei sehr glatten Dichten wirkt sich die Privatisierung weniger dramatisch aus ($\beta \to \infty$).*

Beweis. Um die Behauptung zu beweisen beginnen wir mit der Funktion

$$\kappa_0(u) := \begin{cases} \exp\left(-\frac{1}{1-4u^2}\right), & u \in (-1/2, 1/2), \\ 0, & \text{sonst.} \end{cases}$$

Es ist wohl bekannt, dass $\kappa_0 : \mathbb{R} \to [0, e^{-1}]$ unendlich oft differentierbar ist, mit beschränkten Ableitungen $\|\kappa_0^{(k)}\|_\infty < \infty$, und so, dass alle Ableitungen den selben Träger $\operatorname{supp}(\kappa_0^{(k)}) = (-1/2, 1/2)$ haben. Als nächstes zeigen wir, dass κ_0 Hölder-stetig ist mit Exponenten $\beta - b$ und Konstante $\|\kappa_0^{(b+1)}\|_\infty$. Dafür verwenden wir zunächst den Mittelwertsatz der Differentialrechnung um für alle $x, y \in \mathbb{R}$ und für einen Zwischenwert $\zeta \in [x \wedge y, x \vee y]$,

$$\left| \frac{\kappa_0^{(b)}(x) - \kappa_0^{(b)}(y)}{x - y} \right| = |\kappa_0^{(b+1)}(\zeta)|,$$

zu erhalten. Da $0 \leq \beta - b \leq 1$, folgt für $x, y \in [-1/2, 1/2]$, dass

$$|\kappa_0^{(b)}(x) - \kappa_0^{(b)}(y)| \leq \|\kappa_0^{(b+1)}\|_\infty |x - y| \leq \|\kappa_0^{(b+1)}\|_\infty |x - y|^{\beta - b}.$$

Falls $x, y \in \mathbb{R} \setminus [-1/2, 1/2]$, so ist die obige Ungleichung trivial. Für $x \in [-1/2, 1/2]$, $y \in \mathbb{R} \setminus [-1/2, 1/2]$ und $T(y) := \min(\max(-1/2, y), 1/2)$, gilt

$$|\kappa_0^{(b)}(x) - \kappa_0^{(b)}(y)| = |\kappa_0^{(b)}(x) - \kappa_0^{(b)}(T(y))| \leq \|\kappa_0^{(b+1)}\|_\infty |x - T(y)|^{\beta - b} \leq \|\kappa_0^{(b+1)}\|_\infty |x - y|^{\beta - b}.$$

Die gewünschte Hölder-Stetigkeit von κ_0 ist also gezeigt. Als nächstes definieren wir $a_0 := (2\|\kappa_0^{(b+1)}\|_\infty)^{-1}$ und $\kappa(u) := a_0 \kappa_0(u)$. Wir sehen also sofort, dass

$$|\kappa^{(b)}(x) - \kappa^{(b)}(y)| \leq \frac{1}{2}|x - y|^{\beta - b} \quad \forall x, y \in \mathbb{R}.$$

Eine ähnliche Überlegung führt zur folgenden Behauptung.

Behauptung. *Es gibt $a_1, a_2, \delta_1, \delta_2 > 0$, so dass für $p_0(x) := a_1 \kappa_0\left(\frac{x - x_0}{a_2}\right)$ gilt, $p_0 \in \mathcal{H}(\beta, C/2)$ und $p_0(x) \geq \delta_2$, für alle $x \in (x_0 - \delta_1, x_0 + \delta_1)$.*

Damit p_0 eine Dichte ist, muss gelten, dass $1 = \int_{\mathbb{R}} p_0(x)\,dx = a_1 a_2 \|\kappa_0\|_1$. Somit muss die Beziehung $a_1 = \frac{1}{a_2\|\kappa_0\|_1}$ gelten. Weiter gilt

$$|p_0^{(b)}(x) - p_0^{(b)}(y)| \le \frac{a_1}{a_2^b}\|\kappa_0^{(b+1)}\|_\infty \left|\frac{x-x_0}{a_2} - \frac{y-x_0}{a_2}\right|^{\beta-b} = \frac{\|\kappa_0^{(b+1)}\|_\infty}{a_2^{\beta+1}\|\kappa_0\|_1}|x-y|^{\beta-b}.$$

Wir wählen also $a_2 = \left(\frac{2\|\kappa_0\|_1}{C\|\kappa_0^{(b+1)}\|_\infty}\right)^{\frac{1}{\beta+1}}$. Die Existenz von geeigneten δ_1 und δ_2 ist offensichtlich.

Als nächstes definieren wir für $x \in \mathbb{R}$ und $h > 0$ die Funktion $p_1(x) := p_0(x) + \frac{C}{2}h^\beta g\left(\frac{x-x_0}{h}\right)$, wobei $g(y) := \kappa(y+1) - \kappa(y)$. Aufgrund des bisher Gezeigten erhalten wir

$$\begin{aligned}
|p_1^{(b)}(x) - p_1^{(b)}(y)| &\le |p_0^{(b)}(x) - p_0^{(b)}(y)| + \frac{C}{2}h^{\beta-b}\left|g^{(b)}\left(\frac{x-x_0}{h}\right) - g^{(b)}\left(\frac{y-x_0}{h}\right)\right| \\
&\le \frac{C}{2}|x-y|^{\beta-b} + \frac{C}{2}h^{\beta-b}\left|\kappa^{(b)}\left(\frac{x-x_0}{h}+1\right) - \kappa^{(b)}\left(\frac{y-x_0}{h}+1\right)\right| \\
&\quad + \frac{C}{2}h^{\beta-b}\left|\kappa^{(b)}\left(\frac{x-x_0}{h}\right) - \kappa^{(b)}\left(\frac{y-x_0}{h}\right)\right| \\
&\le \frac{C}{2}|x-y|^{\beta-b} + \frac{C}{2}h^{\beta-b}\left|\frac{x-y}{h}\right|^{\beta-b} = C|x-y|^{\beta-b}.
\end{aligned}$$

Nach Konstruktion gilt $\int_{\mathbb{R}} p_1(x)\,dx = 1$. Außerdem sieht man leicht, dass $g\left(\frac{x-x_0}{h}\right) < 0$, genau dann wenn $x \in (x_0 - h/2, x_0 + h/2)$. Falls $h \le 2\delta_1$, $h^\beta \le \delta_2(C\|\kappa\|_\infty)^{-1}$ und $x \in (x_0 - h/2, x_0 + h/2)$, folgt also $p_0(x) \ge \delta_2$ und $\frac{C}{2}h^\beta g\left(\frac{x-x_0}{h}\right) \ge -\frac{\delta_2}{2\|\kappa\|_\infty}\left|\kappa\left(\frac{x-x_0}{h}+1\right) - \kappa\left(\frac{x-x_0}{h}\right)\right| \ge -\delta_2$, und somit auch $p_1(x) \ge 0$. Andererseits gilt für $x \in (x_0 - h/2, x_0 + h/2)^c$ immer, dass $p_1(x) \ge 0$. Wir haben also gezeigt, dass für alle

$$h \le \min\left(2\delta_1, \left(\frac{\delta_2}{C\|\kappa\|_\infty}\right)^{\frac{1}{\beta}}\right) =: h_0,$$

$p_0, p_1 \in \mathcal{H}(\beta, C)$ gilt. Wir berechnen nun leicht $|\theta(p_0) - \theta(p_1)| = \frac{C}{2}h^{\beta-m}|g^{(m)}(0)|$ und $d_{\mathrm{TV}}(P_0, P_1) = \frac{1}{2}\int_{\mathbb{R}}|p_0(x) - p_1(x)|\,dx = \frac{C}{4}h^\beta \int_{\mathbb{R}}\left|g\left(\frac{x-x_0}{h}\right)\right|dx = \frac{C}{2}h^{\beta+1}\|\kappa\|_1$. Setzen wir also $\bar{\varepsilon}_0 := h_0^{\beta+1}\frac{C\|\kappa\|_1}{2}$ und wählen $\varepsilon \in (0, \bar{\varepsilon}_0]$ und $h = \left(\frac{2\varepsilon}{C\|\kappa\|_1}\right)^{\frac{1}{\beta+1}}$, so folgt $h \le h_0$ und $d_{\mathrm{TV}}(P_0, P_1) = \varepsilon$. Somit folgt für den Totalvariationsmodul

$$\omega_{d_{\mathrm{TV}}}(\varepsilon) \ge \frac{C}{2}|g^{(m)}(0)|\left(\frac{2\varepsilon}{C\|\kappa\|_1}\right)^{\frac{\beta-m}{\beta+1}}, \quad \forall \varepsilon \in (0, \bar{\varepsilon}_0].$$

□

3.2 Eine obere Schranke für das private Minimax-Risiko

In diesem Kapitel werden wir nun obere Schranken an das α-private Minimax-Risiko

$$\mathcal{M}_{n,\alpha} = \inf_{m\in\mathbb{N}}\inf_{Q\in\mathcal{Q}_\alpha(m)}\inf_{\hat{\theta}_n : \mathcal{Z}^m \to \mathbb{R}}\sup_{P\in\mathcal{P}} \mathbb{E}_{QP^n}\left[l\left(|\hat{\theta}_n - \theta(P)|\right)\right]$$

herleiten, welche von der selben Ordnung in n sind, wie die unteren Schranken im vorherigen Kapitel. Es gibt Fälle in denen die unteren Schranken aus Kapitel 3.1 zu konservativ sind. Zum Beispiel muss man für die Schätzung des quadratischen Funktionals $\theta(p) := \int p^2(x)\,dx$ eine andere Technik anwenden um die Konvergenzrate des privaten Minimax-Risikos zu charakterisieren. Um obere Schranken herzuleiten die unsere unteren Schranken bis auf Konstanten erreichen, müssen

wir also bestimmte Annahmen an das Modell $\mathcal{P}$ und das Funktional $\theta : \mathcal{P} \to \mathbb{R}$ treffen. Im Folgenden werden wir zwei verschiedene Mengen von Annahmen betrachten. Grundsätzlich benötigen wir eine milde Regularitätsbedingung an die Verlustfunktion $l : \mathbb{R}_+ \to \mathbb{R}_+$. In Kapitel 3.2.1 nehmen wir an, dass $\mathcal{P}$ konvex und dominiert ist sowie, dass θ linear und beschränkt ist. Wir werden sehen, dass unter diesen Annahmen eine Hölder-Bedingung an den Hellinger-, oder den Totalvariationsmodul $\omega_{d_{\mathrm{H}}}$ bzw. $\omega_{d_{\mathrm{TV}}}$ von θ über $\mathcal{P}$, wie in Satz 2.2, eigentlich nicht notwendig ist. Unter diesen Annahmen können wir die Existenz von α-NIDP Kanälen $Q^{(n)}$ auf $(\mathbb{R}, \mathcal{B}(\mathbb{R}))$ und von Schätzern $\hat{\theta}_n^* : \mathbb{R} \to \mathbb{R}$ beweisen, so dass

$$\sup_{P \in \mathcal{P}} \mathbb{E}_{Q^{(n)} P^n} \left[l\left(|\hat{\theta}_n^* - \theta(P)| \right) \right] \;\leq\; C_0 \cdot l\left(\omega_{d_{\mathrm{TV}}}\left(\sqrt{\frac{2(e^\alpha+1)^2}{n(e^\alpha-1)^2}} \right) \right).$$

Allerdings sind diese Existenzresultate nicht-konstruktiv. In Kapitel 3.2.3 werden wir daher unter einer alternativen Annahme zeigen, wie man aus einem Schätzer der Form

$$\frac{1}{n} \sum_{i=1}^{n} \ell_h(X_i),$$

im Schätzproblem mit direkten Beobachtungen $X_1, \ldots, X_n$ einen minimax-optimalen α-NIDP Kanal und einen geeigneten Schätzer für das private Problem konstruiert. Beachte, dass $\mathcal{Q}_\alpha(m)$ bisher die Menge aller sequentiell-interaktiven und α-DP Kanäle auf $(\mathbb{R}^m, \mathcal{B}(\mathbb{R}^m))$ bezeichnete und wir untere Schranken für alle solche Kanäle hergeleitet hatten. Wir werden also insbesondere zeigen, dass unter unseren Annahmen die nicht-interaktiven Kanäle in der Menge der sequentiell-interaktiven bereits optimal sind.

Definition 3.9. *Im Folgenden nennen wir eine Funktion $l : \mathbb{R}_+ \to \mathbb{R}_+$* ***reguläre Verlustfunktion****, falls l nicht-fallend ist, $l(0) = 0$ und es eine Konstante $a \in (1, \infty)$ gibt, so dass*

$$l\left(\frac{3}{2}t\right) \;\leq\; a\, l(t), \quad \forall t \in \mathbb{R}_+.$$

3.2.1 Nicht-konstruktive Schranken

Für einen NI Kanal $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ mit identischen Marginalen Q_1 und $\varepsilon \in [0, \infty)$, schreiben wir

$$\omega_{d_{\mathrm{H}}}^{(Q_1)}(\varepsilon) := \sup\{|\theta(P_0) - \theta(P_1)| : d_{\mathrm{H}}(Q_1 P_0, Q_1 P_1) \leq \varepsilon, P_0, P_1 \in \mathcal{P}\}.$$

Satz 3.10. *Es sei $\mathcal{P}$ konvex, $\theta : \mathcal{P} \to \mathbb{R}$ linear und beschränkt und $l : \mathbb{R}_+ \to \mathbb{R}_+$ eine reguläre Verlustfunktion. Dann gilt für jedes $n \in \mathbb{N}$, jeden messbaren Raum $(\mathcal{Z}, \mathcal{G})$ und jeden NI Kanal $Q : \mathcal{G}^{\otimes n} \times \mathcal{X}^n \to [0,1]$ mit identischen Marginalen Q_1, für den $Q_1\mathcal{P}$ dominiert ist, dass*

$$\mathcal{M}_n(Q, \mathcal{P}, \theta) \;:=\; \inf_{\hat{\theta}_n : \mathcal{Z}^n \to \mathbb{R}} \sup_{P \in \mathcal{P}} \mathbb{E}_{QP^n} \left[l\left(|\hat{\theta}_n - \theta(P)| \right) \right] \;\leq\; C_0 \cdot l\left(\omega_{d_H}^{(Q_1)}(n^{-1/2}) \right),$$

wobei $C_0 = (1+16a)a^{\lceil 2\frac{\log C}{\log 3/2} \rceil}$, $C = \sqrt{2\log(2a)} + 2$ und $a > 1$ die Regularitätskonstante der Verlustfunktion l ist.

Wir verschieben den Beweis auf später und diskutieren zunächst das Resultat sowie seine wichtigsten Konsequenzen.

Bemerkung 3.11.

a) Falls $\mathcal{X}$ eine Teilmenge eines endlich dimensionalen Euklidischen Raumes $\mathbb{R}^m$ ist, und wir $\mathcal{Z} = \mathbb{R}^m$, $\mathcal{G} = \mathcal{B}(\mathbb{R}^m)$ und $Q_1(A|x) = \mathbb{1}_A(x)$, für $A \in \mathcal{G}$ und $x \in \mathcal{X}$ wählen, so folgt aus Satz 3.10 gemeinsam mit unserer unteren Schranke aus Korollar 3.4, eine stärkere Version von Satz 2.2, die keine Hölder-Bedingung mehr benötigt.

b) Das Resultat von Satz 3.10 ist *nicht konstruktiv* in dem Sinne, dass es uns keinen konkreten Schätzer $\hat{\theta}_n^* : \mathcal{Z}^n \to \mathbb{R}$ liefert, so dass

$$\sup_{P\in\mathcal{P}} \mathbb{E}_{QP^n}\left[l\left(|\hat{\theta}_n^* - \theta(P)|\right)\right] \;\le\; C_0 \cdot l\left(\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2})\right).$$

c) Um unsere Charakterisierung von $\mathcal{M}_{n,\alpha}$ abzuschließen, müssen wir noch eine Folge $Q^{(n)}$ von NI Kanälen mit identischen Marginalen $Q_1^{(n)}$ finden, so dass

$$\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2}) \le c_0 \cdot \omega_{d_{\mathrm{TV}}}\left(c_1\sqrt{\frac{1}{n(e^\alpha-1)^2}}\right).$$

Definition 3.12. *Sei $\alpha \in (0,\infty)$ und $\varphi : \mathcal{X} \to \mathbb{R}$ messbar und beschränkt. Der Kanal $Q^{(\alpha,\varphi)} : \mathcal{B}(\mathbb{R})^{\otimes n} \times \mathcal{X}^n \to [0,1]$ mit identischen binären Marginalen*

$$Q_1^{(\alpha,\varphi)}(\{\pm z_0\}|x) := \frac{1}{2}\left(1 \pm \frac{\varphi(x)}{z_0}\right),$$

$x \in \mathcal{X}$, $z_0 := \|\varphi\|_\infty \frac{e^\alpha+1}{e^\alpha-1}$, heißt α-BM. Der α-BM Kanal ist α-DP (vgl. Aufgabe 3.3).

Satz 3.13. *Sei $\mathcal{P}$ konvex und dominiert (durch μ) und $\theta : \mathcal{P} \to \mathbb{R}$ linear. Für $\alpha \in (0,\infty)$ und $\varphi \in L_\infty(\mu)$ sei $Q_1^{(\alpha,\varphi)}$ die Marginale des α-BM Kanals von Definition 3.12. Dann gilt für jedes $\varepsilon \in [0,\infty)$,*

$$\inf_{\varphi:\|\varphi\|_\infty\le 1} \omega_{d_H}^{\left(Q_1^{(\alpha,\varphi)}\right)}(\varepsilon) \;\le\; \omega_{d_{TV}}\left(\left[\varepsilon\frac{e^\alpha+1}{e^\alpha-1}\right]^+\right).$$

Hierbei ist $\omega_{d_{TV}}(\varepsilon^+) := \lim_{\eta\downarrow\varepsilon}\omega_{d_{TV}}(\eta)$.

Beweis. Für $P_0, P_1 \in \mathcal{P}$, $\nu = P_0 + P_1$ und zugehörige ν-Dichten p_0 und p_1 gilt

$$\begin{aligned} d_{\mathrm{TV}}\left(Q_1^{(\alpha,\varphi)}P_0, Q_1^{(\alpha,\varphi)}P_1\right) &= \sup_{A\in\mathcal{B}(\mathbb{R})}\left|\int_{\mathcal{X}} Q_1^{(\alpha,\varphi)}(A|x)[p_0(x)-p_1(x)]\,\nu(dx)\right| \\ &= \max\left\{\left|\int_{\mathcal{X}}\frac{\varphi(x)}{2z_0}[p_0(x)-p_1(x)]\,\nu(dx)\right|, \left|\int_{\mathcal{X}} -\frac{\varphi(x)}{2z_0}[p_0(x)-p_1(x)]\,\nu(dx)\right|\right\} \\ &= \frac{1}{2z_0}\left|\mathbb{E}_{P_0}[\varphi] - \mathbb{E}_{P_1}[\varphi]\right|. \end{aligned} \tag{3.2.1}$$

Für $\varphi \in L_\infty(\mu)$ mit $\|\varphi\|_\infty \le 1$ und $\eta \in [0,\infty)$, definiere

$$\Phi_\varphi(\eta) := \sup\{\theta(P_0) - \theta(P_1) : |\mathbb{E}_{P_0}[\varphi] - \mathbb{E}_{P_1}[\varphi]| \le \eta, P_0, P_1 \in \mathcal{P}\} \ge 0.$$

Somit gilt wegen Satz 2.4.(4) und (3.2.1), dass

$$\begin{aligned} \omega_{d_{\mathrm{H}}}^{\left(Q_1^{(\alpha,\varphi)}\right)}(\varepsilon) &= \sup\{\theta(P_0)-\theta(P_1) : d_{\mathrm{H}}(Q_1^{(\alpha,\varphi)}P_0, Q_1^{(\alpha,\varphi)}P_1) \le \varepsilon, P_0, P_1 \in \mathcal{P}\} \\ &\le \Phi_\varphi(2z_0\varepsilon) \le \Phi_\varphi\left(2\varepsilon\frac{e^\alpha+1}{e^\alpha-1}\right). \end{aligned} \tag{3.2.2}$$

Anstatt diese obere Schranke in φ zu minimieren, können wir auch

$$\Psi_\varphi(\delta) := \inf A_\varphi(\delta) := \inf\{\eta \ge 0 : \Phi_\varphi(\eta) > \delta\},$$

in φ maximieren. Es gilt nämlich für $\delta, \eta \in [0,\infty)$,

Behauptung. *a)* $\Psi_\varphi(\delta) > \eta \;\Rightarrow\; \Phi_\varphi(\eta) \le \delta$.

b) $\sup_{\varphi:\|\varphi\|_\infty\le 1}\Psi_\varphi(\delta)>\eta \;\Rightarrow\; \inf_{\varphi:\|\varphi\|_\infty\le 1}\Phi_\varphi(\eta)\le\delta$.

c) $\Psi_\varphi(\delta)\ge\inf\{|\mathbb{E}_{P_0}[\varphi]-\mathbb{E}_{P_1}[\varphi]| : \theta(P_0)-\theta(P_1)\ge\delta, P_0,P_1\in\mathcal{P}\} =: \inf B_\varphi(\delta)$.

Die Aussage in *a)* folgt sofort aus den entsprechenden Definitionen, und die Aussage in *b)*, da man das Supremum beliebig genau durch ein geeignetes φ mit $\|\varphi\|_\infty\le 1$ approximieren kann. Falls $A_\varphi(\delta)=\varnothing$, so ist die Aussage *c)* trivial, da $\inf\varnothing=\infty$. Andernfalls sei $\eta\in A_\varphi(\delta)$. Dann gilt also $\Phi_\varphi(\eta)>\delta$. Nach Definition von Φ_φ gibt es also $P_0,P_1\in\mathcal{P}$, so dass $\theta(P_0)-\theta(P_1)>\delta$ und $\gamma:=|\mathbb{E}_{P_0}[\varphi]-\mathbb{E}_{P_1}[\varphi]|\le\eta$. Nach Definition von $B_\varphi(\delta)$ ist dann aber $\gamma\in B_\varphi(\delta)$. Wir haben also gezeigt, dass es für jedes $\eta\in A_\varphi(\delta)$ ein $\gamma\in B_\varphi(\delta)$ gibt, mit $\gamma\le\eta$. Somit folgt also $\inf A_\varphi(\delta)\ge\inf B_\varphi(\delta)$.

Wir verwenden nun die Aussage *c)* und die Darstellung $\mathbb{E}_{P_0}[\varphi]-\mathbb{E}_{P_1}[\varphi]=\int_{\mathcal{X}}\varphi\,d(P_0-P_1)$, um zu schließen, dass

$$\sup_{\varphi:\|\varphi\|_\infty\le1}\Psi_\varphi(\delta)\ge\sup_{\varphi:\|\varphi\|_\infty\le1}\inf B_\varphi(\delta)\ge\sup_{\varphi\in\mathbb{T}}\inf_{\sigma\in\mathbb{S}_\delta}\int_{\mathcal{X}}\varphi\,d\sigma,$$

wobei $\mathbb{T}=\{\varphi\in L_\infty(\mu):\|\varphi\|_\infty\le1\}$ und $\mathbb{S}_\delta=\{P_0-P_1:\theta(P_0)-\theta(P_1)\ge\delta,P_0,P_1\in\mathcal{P}\}$. Wegen Linearität von $\theta:\mathcal{P}\to\mathbb{R}$ und Konvexität und Dominiertheit von $\mathcal{P}$ sieht man sofort, dass $\mathbb{S}_\delta$, für jedes $\delta\in[0,\infty)$, eine konvexe, dominierte Menge von endlichen signierten Maßen ist. Wir können also Satz 2.6 anwenden. Wähle nun $\xi_1,\xi_2\in(0,\infty)$ beliebige, $\eta:=\varepsilon\frac{e^\alpha+1}{e^\alpha-1}\in[0,\infty)$ und $\delta:=\omega_{d_{\mathrm{TV}}}(\eta+\xi_1)+\xi_2\in[0,\infty]$. Falls $\delta=\infty$ für alle $\xi_1>0$, so ist die Aussage des zu beweisenden Satzes 3.13 trivial. Andernfalls gilt $\delta\in[0,\infty)$, für alle $\xi_1,\xi_2>0$ welche hinreichend klein sind. Für alle solchen hinreichend kleinen $\xi_1,\xi_2>0$ erhalten wir also wegen Aufgabe 3.4, dass

$$\begin{aligned}\sup_{\varphi:\|\varphi\|_\infty\le1}\Psi_\varphi(\delta)&\ge\inf_{\sigma\in\mathbb{S}_\delta}\sup_{\varphi\in\mathbb{T}}\int_{\mathcal{X}}\varphi\,d\sigma=2\inf_{\sigma\in\mathbb{S}_\delta}\|\sigma\|_{TV}\\&=2\inf\{d_{\mathrm{TV}}(P_0,P_1):\theta(P_0)-\theta(P_1)\ge\delta,P_0,P_1\in\mathcal{P}\}\\&\ge2\inf\{d_{\mathrm{TV}}(P_0,P_1):\theta(P_0)-\theta(P_1)>\omega_{d_{\mathrm{TV}}}(\eta+\xi_1),P_0,P_1\in\mathcal{P}\}\\&\ge2(\eta+\xi_1)>2\eta.\end{aligned}$$

Mit (3.2.2) und der Behauptung *b)* folgt also

$$\inf_{\varphi:\|\varphi\|_\infty\le1}\omega_{d_{\mathrm{H}}}^{\left(Q_1^{(\alpha,\varphi)}\right)}(\varepsilon)\;\le\;\inf_{\varphi:\|\varphi\|_\infty\le1}\Phi_\varphi(2\eta)\;\le\;\delta=\omega_{d_{\mathrm{TV}}}\left(\varepsilon\frac{e^\alpha+1}{e^\alpha-1}+\xi_1\right)+\xi_2,$$

für alle kleinen $\xi_1,\xi_2>0$. □

Korollar 3.14. *Es sei $\mathcal{P}$ konvex und dominiert, $\theta:\mathcal{P}\to\mathbb{R}$ linear und beschränkt und $l:\mathbb{R}_+\to\mathbb{R}_+$ eine reguläre Verlustfunktion. Dann gilt für jedes $n\in\mathbb{N}$ und $\alpha\in(0,\infty)$, dass*

$$\begin{aligned}\mathcal{M}_{n,\alpha}(\mathcal{P},\theta):=\inf_{m\in\mathbb{N}}\inf_{Q\in\mathcal{Q}_\alpha(m)}\inf_{\hat\theta_n:\mathcal{Z}_m^n\to\mathbb{R}}\sup_{P\in\mathcal{P}}\mathbb{E}_{QP^n}\left[l\left(|\hat\theta_n-\theta(P)|\right)\right]\\\le C_0\cdot l\left(\omega_{d_{TV}}\left(\sqrt{\frac{2(e^\alpha+1)^2}{n(e^\alpha-1)^2}}\right)\right),\end{aligned}$$

wobei $C_0=C_0(a)$ die Konstante aus Satz 3.10 ist.

Beweis. Sei $n\in\mathbb{N}$ und $\alpha\in(0,\infty)$. Wegen Satz 3.13 und der strikten Monotonie von $\varepsilon\mapsto\omega_{d_{\mathrm{TV}}}(\varepsilon)$ (vgl. Aufgabe 3.5) gibt es einen α-DPNI Kanal $Q^{\alpha,n}$ mit identischen Marginalen $Q_1^{\alpha,n}:\mathcal{B}(\mathbb{R})\times\mathcal{X}\to[0,1]$, so dass

$$\omega_{d_{\mathrm{H}}}^{(Q_1^{\alpha,n})}(n^{-1/2})\le\omega_{d_{\mathrm{TV}}}\left(\sqrt{\frac{2(e^\alpha+1)^2}{n(e^\alpha-1)^2}}\right).$$

Da $Q_1^{\alpha,n}$ α-DP ist, so ist auch $Q_1^{\alpha,n}\mathcal{P}$ dominiert (vgl. Aufgabe 2.4). Das Resultat folgt jetzt aus Satz 3.10. □

Bemerkung 3.15. *Gemeinsam mit Korollar 3.4 haben wir also gezeigt, dass unter den Annahmen von Korollar 3.14 gilt*

$$\frac{1}{4}l\left(\frac{1}{2}\omega_{d_{TV}}\left(\sqrt{\frac{1}{9n(e^\alpha-1)^2}}\right)\right) \;\le\; \mathcal{M}_{n,\alpha}(\mathcal{P},\theta) \;\le\; C_0\cdot l\left(\omega_{d_{TV}}\left(\sqrt{\frac{2(e^\alpha+1)^2}{n(e^\alpha-1)^2}}\right)\right).$$

Leider haben uns die Beweise der oberen Schranken aber keinen Kanal $Q:\mathcal{G}_m^{\otimes n}\times\mathcal{X}^n\to[0,1]$ und keinen Schätzer $\hat\theta_n:\mathcal{Z}_m^n\to\mathbb{R}$ geliefert, so dass die obere Schranke auch für

$$\sup_{P\in\mathcal{P}}\mathbb{E}_{QP^n}\left[l\left(|\hat\theta_n-\theta(P)|\right)\right]$$

anstatt von $\mathcal{M}_{n,\alpha}(\mathcal{P},\theta)$ gilt.

3.2.2 Beweis von Satz 3.10

Wir erinnern uns an

$$\eta_A^{(n)}(Q,\Delta):=\sup_{t\in\mathbb{R}}\rho_T\left(\operatorname{conv}\left(Q\mathcal{P}^n_{\le t}\right),\operatorname{conv}\left(Q\mathcal{P}^n_{\ge t+\Delta}\right)\right).$$

Lemma 3.16. *Sei $(\mathcal{Z},\mathcal{G})$ ein messbarer Raum, $\Delta\in(0,\infty)$ und $M:=\sup_{P\in\mathcal{P}}|\theta(P)|<\infty$. Weiter sei $Q:\mathcal{G}^{\otimes n}\times\mathcal{X}^n\to[0,1]$ ein NI Kanal mit identischen Marginalen Q_1 und $N:=N(\Delta,M):=\min\{n\in\mathbb{Z}:n\Delta>2M\}$. Für $l\in\mathbb{N}_0$, setze $\eta_l:=(l+1)\Delta$. Falls $Q_1\mathcal{P}$ dominiert ist, so gibt es einen Schätzer $\hat\theta_n^\Delta:\mathcal{Z}^n\to\mathbb{R}$, so dass für alle $l\in\mathbb{N}_0$ gilt*

$$\sup_{P\in\mathcal{P}}QP^n\left(z\in\mathcal{Z}^n:|\hat\theta_n^\Delta(z)-\theta(P)|>\eta_l\right)\;\le\;4\sum_{k=l+1}^{N-2}\left[\eta_A^{(n)}(Q,k\Delta)\vee 0\right].$$

Beweis. Durch Schätzung von $\theta(P)+M$ statt $\theta(P)$ können wir o.B.d.A. annehmen, dass $0\le\theta(P)\le 2M$ gilt. Falls $N(\Delta,M)\le 2$, so folgt wegen Definition von $N=N(\Delta,M)$, dass $\Delta>M$. Wählen wir also $\hat\theta_n^\Delta\equiv M$, so sehen wir, dass $|\hat\theta_n^\Delta-\theta(P)|=|M_\theta(P)|\le M<\Delta=\eta_0\le\eta_l$, für alle $z\in\mathcal{Z}^n$ und all $l\in\mathbb{N}_0$. Die gewünschte Ungleichung ist also trivialer weise erfüllt. Es sei also ab jetzt $N\ge 3$. Für $k\in\{1,\dots,N-1\}$ und $j\in\{1,\dots,k\}$, sei $l_{kj}=(j-1)\Delta$, $u_{k,j}=l_{kj}+(N-k+1)\Delta$, $a_{kj}=l_{kj}+\Delta$ und $b_{kj}=u_{kj}-\Delta$, so dass $d_k:=b_{kj}-a_{kj}=(N-k-1)\Delta$. Dies definiert eine Familie von Subintervallen von $[0,N\Delta)\supset[0,2M]$ wie in Abbildung 3.1. Weiter sei $\xi_{kj}:\mathcal{Z}^n\to[0,1]$ ein Minimax-Test für $H_0:[Q_1\mathcal{P}_{\le a_{kj}}]^n$ gegen $H_1:[Q_1\mathcal{P}_{\ge b_{kj}}]^n$ (zur Existenz vgl. Aufgabe 2.1). Falls $H_0=\varnothing$ und $H_1\ne\varnothing$, wähle $\xi^*_{kj}\equiv 1$, falls $H_0\ne\varnothing$ und $H_1=\varnothing$, so wähle $\xi^*_{kj}\equiv 0$, falls $H_0=\varnothing=H_1$, wähle $\xi^*_{kj}\equiv 1$ und falls $H_0\ne\varnothing$ und $H_1\ne\varnothing$, so wähle $\xi_{kj}=\mathbb{1}_{(1/2,1]}(\xi_{kj})$. Im letzten Fall $H_0\ne\varnothing\ne H_1$ und wegen der Markov-Ungleichung, gilt also für $R\in Q_1\mathcal{P}$,

$$\begin{aligned}&\mathbb{E}_R[\xi^*_{kj}]=R(\xi_{kj}>1/2)\le 2\mathbb{E}_R[\xi_{kj}],\quad\text{und}\\&\mathbb{E}_R[1-\xi^*_{kj}]=R(\xi_{kj}\le 1/2)=R(1-\xi_{kj}\ge 1/2)\le 2\mathbb{E}_R[1-\xi_{kj}].\end{aligned}$$

In jedem Fall gilt also wegen Korollar 2.7

$$\begin{aligned}\sup_{\substack{R_0\in[Q_1\mathcal{P}_{\le a_{kj}}]^n\\R_1\in[Q_1\mathcal{P}_{\ge b_{kj}}]^n}}\mathbb{E}_{R_0}[\xi^*_{kj}]+\mathbb{E}_{R_1}[1-\xi^*_{kj}]\;&\le\;2\sup_{\substack{R_0\in[Q_1\mathcal{P}_{\le a_{kj}}]^n\\R_1\in[Q_1\mathcal{P}_{\ge b_{kj}}]^n}}\mathbb{E}_{R_0}[\xi_{kj}]+\mathbb{E}_{R_1}[1-\xi_{kj}]\\&=\;2\inf_{\text{Tests }\phi}\sup_{\substack{R_0\in Q\mathcal{P}^n_{\le a_{kj}}\\R_1\in Q\mathcal{P}^n_{\ge b_{kj}}}}\mathbb{E}_{R_0}[\phi]+\mathbb{E}_{R_1}[1-\phi]\\&=\;2\rho_T\left(\operatorname{conv}\left(Q\mathcal{P}^n_{\le a_{kj}}\right),\operatorname{conv}\left(Q\mathcal{P}^n_{\ge b_{kj}}\right)\right)\\&\le\;2\eta_A^{(n)}(Q,b_{kj}-a_{kj})=2\eta_A^{(n)}(Q,d_k).\end{aligned}\tag{3.2.3}$$

Um den Wert von $\theta(P)$ möglichst genau einzugrenzen, verfahren wir jetzt mit Hilfe der nichtrandomisierten Tests ξ^*_{kj} in einer binären Suche, in dem wir zunächst $\xi^*_{11}(z)$ berechnen. Falls $\xi^*_{11}(z) = 0$, so verwerfen wir das Intervall $[b_{11}, u_{11})$ und setzen unsere Suche im Interval $[l_{21}, u_{21}) = [l_{11}, b_{11})$ fort. Falls aber $\xi^*_{11}(z) = 1$, so verwerfen wir das Intervall $[l_{11}, a_{11})$ und setzen unsere Suche im Interval $[l_{22}, u_{22}) = [a_{11}, u_{11})$ fort. Nun berechnen wir, je nachdem ob wir uns für $[l_{21}, u_{21})$ oder $[l_{22}, u_{22})$ entschieden haben, den Test $\xi^*_{21}(z)$ oder $\xi^*_{22}(z)$ und verfahren analog um wieder ein um Δ verkürztes Teilintervall zu erhalten. Nachdem $N-2$ solche Testverfahren durchgeführt wurden, endet die Prozedur und wir wählen für $\hat{\theta}^{\Delta}_n(z)$ den Mittelpunkt des zuletzt erhaltenen Teilintervalls der Länge 2Δ (vgl. Abbildung 3.1 und Abbildung 3.2).

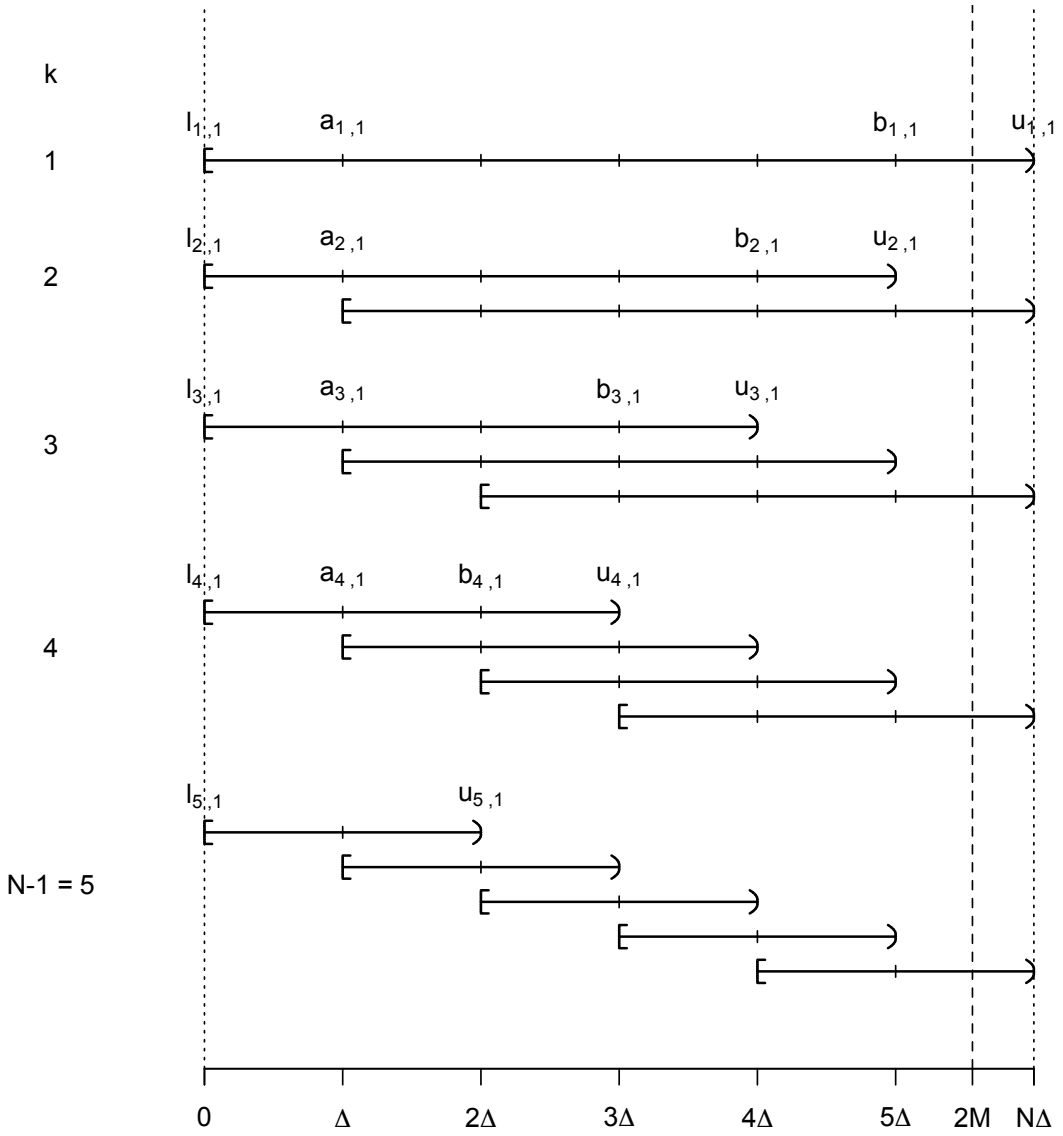


Abbildung 3.1: Ein Beispiel für die Konstruktion der Intervalle im binären Suchalgorithmus.

Formal können wir dieses Verfahren wie folgt beschreiben. Für $z \in \mathcal{Z}^n$, sei $j_1(z) = 1$ und für $k \in \{2, \ldots, N-1\}$, sei $j_k(z) = j_{k-1}(z) + \xi^*_{k-1,j_{k-1}(z)}(z)$. Schließlich setzen wir $\hat{\theta}^{\Delta}_n(z) := \frac{1}{2}(l_{N-1,j_{N-1}(z)} + u_{N-1,j_{N-1}(z)}) = j_{N-1}(z) \cdot \Delta$.

Um den Wert von $\hat{\theta}^{\Delta}_n(z)$ zu bestimmen, müssen also zunächst die Tests $\xi^*_{11}(z)$, $\xi^*_{2,j_2(z)}(z)$,

$\dots, \xi^*_{N-2,j_{N-2}(z)}(z)$ berechnet werden. Dabei sagen wir, dass der Test $\xi^*_{k,j_k(z)}(z)$ einen Fehler erster Art begeht, falls $\xi^*_{k,j_k(z)}(z) = 1$, und $\theta(P) \in [l_{k,j_k(z)}, a_{k,j_k(z)})$, wohingegen ein Fehler zweiter Art begangen wird, falls $\xi^*_{k,j_k(z)}(z) = 0$, und $\theta(P) \in [b_{k,j_k(z)}, u_{k,j_k(z)})$. Wir sprechen also nur von einem Fehler eines Tests, wenn dessen Entscheidung dazu geführt hat, dass wir ein Teilintervall von $[0, N\Delta)$ entfernt haben, welches den wahren Parameter $\theta(P)$ enthielt. Beachte, dass somit per Definition und nach Konstruktion des Tests $\xi_{k,j_k(z)}(z)$, im Fall $\mathcal{P}_{\leq a_{k,j_k(z)}} \cap \mathcal{P}_{\geq b_{k,j_k(z)}} = \varnothing$ sicher kein Fehler begangen wird. Für $P \in \mathcal{P}$ definieren wir die zugehörigen Ereignisse

$$F_1(k,P) := \{z \in \mathcal{Z}^n : \xi^*_{k,j_k(z)}(z) = 1, \theta(P) \in [l_{k,j_k(z)}, a_{k,j_k(z)})\}$$
$$F_2(k,P) := \{z \in \mathcal{Z}^n : \xi^*_{k,j_k(z)}(z) = 0, \theta(P) \in [b_{k,j_k(z)}, u_{k,j_k(z)})\}.$$

Ist also für ein $z \in \mathcal{Z}^n$, der absolute Schätzfehler $|\hat{\theta}^\Delta_n(z) - \theta(P)|$ größer als $\eta_0 = \Delta$, so muss irgendeiner der durchgeführten Tests einen Fehler begangen haben. Es gibt also ein $k \in \{1, \dots, N-2\}$, so dass $z \in F_1(k,P) \cup F_2(k,P)$. Ist $|\hat{\theta}^\Delta_n(z) - \theta(P)| > \eta_1 = 2\Delta$, so muss irgendeiner der durchgeführten Tests einen Fehler begangen haben, aber der Fehler kann nicht von $\xi^*_{N-2,j_{N-2}(z)}(z)$ begangen worden sein. Es gibt also ein $k \in \{1, \dots, N-3\}$, so dass $z \in F_1(k,P) \cup F_2(k,P)$. Im Allgemeinen gilt also, ist $|\hat{\theta}^\Delta_n(z) - \theta(P)| > \eta_l$ für ein $l \in \{0, N-3\}$, so gibt es ein $k \in \{1, \dots, N-2-l\}$, so dass $z \in F_1(k,P) \cup F_2(k,P)$. Somit erhalten wir, dass

$$QP^n\left(\left|\hat{\theta}^\Delta_n - \theta(P)\right| > \eta_l\right) \leq \sum_{k=1}^{N-2-l} \left[QP^n\Big(F_1(k,P)\Big) + QP^n\Big(F_2(k,P)\Big)\right].$$

Da die Intervalle $[(j-1)\Delta, j\Delta)$, $j = 1, \dots, N$, eine disjunkte Überdeckung von $[0, 2M]$ bilden, gibt es ein $m_0 \in \{1, \dots, N\}$, so dass $\theta(P) \in [(m_0-1)\Delta, m_0\Delta)$. Da $a_{k,j_k(z)} = j_k(z)\Delta \leq k\Delta$, ist also für $k < m_0$ die Menge $F_1(k,P)$ leer, wohingegen für $k \geq m_0$, $F_1(k,P) = \{z \in \mathcal{Z}^n : \xi^*_{k,j_0}(z) = 1, j_k(z) = m_0\} \subseteq \{z \in \mathcal{Z}^n : \xi^*_{k,m_0}(z) = 1\}$. Somit erhalten wir $QP^n(F_1(k,P)) = 0$, falls $k > m_0$, und andernfalls $QP^n(F_1(k,P)) \leq \mathbb{E}_{QP^n}[\xi^*_{k,m_0}]$. Falls jetzt auch noch $\mathcal{P}_{\geq b_{k,m_0}} = \varnothing$, so ist nach unserer Konvention $\xi^*_{k,m_0} \equiv 0$, da $\mathcal{P}_{\leq a_{k,m_0}} = \mathcal{P}_{\leq m_0\Delta} \neq \varnothing$. Die interessierende Wahrscheinlichkeit lässt sich also mittels (3.2.3) in jedem Fall abschätzen durch

$$\begin{aligned} QP^n(F_1(k,P)) \leq \mathbb{E}_{QP^n}[\xi^*_{k,m_0}] &\leq 0 \vee \left(\sup_{\substack{R_0 \in \left[Q_1\mathcal{P}_{\leq a_{k,m_0}}\right]^n \\ R_1 \in \left[Q_1\mathcal{P}_{\geq b_{k,m_0}}\right]^n}} \mathbb{E}_{R_0}[\xi^*_{k,m_0}] + \mathbb{E}_{R_1}[1 - \xi^*_{k,m_0}] \right) \\ &\leq 2\eta^{(n)}_A(Q, d_k) \vee 0. \end{aligned}$$

Völlig analog zeigt man, dass auch $QP^n(F_2(k,P)) \leq 2\eta^{(n)}_A(Q,d_k) \vee 0$. Da $d_k = (N-k-1)\Delta$, ergibt sich die gesuchte obere Schranke durch Umkehrung der Summationsreihenfolge. □

Lemma 3.17. *Sei $\mathcal{P}$ konvex und $\theta : \mathcal{P} \to \mathbb{R}$ linear. Weiter sei $n \in \mathbb{N}$, $(\mathcal{Z}, \mathcal{G})$ ein messbarer Raum, $Q : \mathcal{G}^{\otimes n} \times \mathcal{X} \to [0,1]$ ein NI Kanal mit identischen Marginalen Q_1 und $\Delta \in [0, \infty)$. Dann gilt*

$$\eta^{(n)}_A(Q, \Delta) \leq \sup_{t \in \mathbb{R}} \sup_{\substack{P_0 \in \mathcal{P}_{\leq t} \\ P_1 \in \mathcal{P}_{\geq t+\Delta}}} \left(1 - \frac{1}{2} d^2_H(Q_1P_0, Q_1P_1)\right)^n.$$

Beweis. Wegen der Konvexität von $\mathcal{P}$ und der Linearität von θ sind die Mengen $\mathcal{P}_{\leq t} = \{P \in \mathcal{P} : \theta(P) \leq t\}$ und $\mathcal{P}_{\geq t+\Delta} = \{P \in \mathcal{P} : \theta(P) \geq t + \Delta\}$ beide Konvex. Da die Abbildung $P \mapsto Q_1P$ linear ist, sind also auch die Mengen $Q_1\mathcal{P}_{\leq t}$ und $Q_1\mathcal{P}_{\geq t+\Delta}$ konvex. Es bleibt jetzt nur mehr den Satz 2.4.(6), die Produktstruktur von Q, den Satz 2.5, sowie den Satz 2.4.(2) anzuwenden, um die

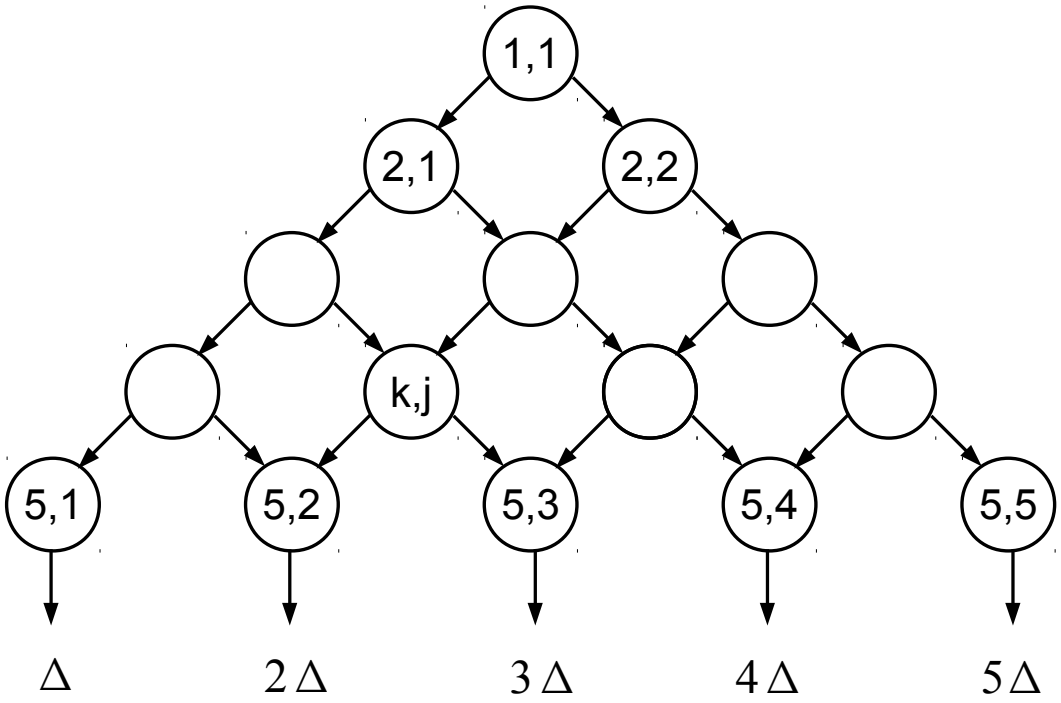


Abbildung 3.2: Graphische Darstellung des binären Suchalgorithmus.

folgenden Abschätzungen zu erhalten.

$$\begin{aligned}
\eta_A^{(n)}(Q,\Delta) &= \sup_{t\in\mathbb{R}} \rho_T\left(\operatorname{conv}\left(Q\mathcal{P}_{\le t}^n\right), \operatorname{conv}\left(Q\mathcal{P}_{\ge t+\Delta}^n\right)\right) \\
&\le \sup_{t\in\mathbb{R}} \rho_H\left(\operatorname{conv}\Big([Q_1\mathcal{P}_{\le t}]^n\Big), \operatorname{conv}\Big([Q_1\mathcal{P}_{\ge t+\Delta}]^n\Big)\right) \\
&\le \sup_{t\in\mathbb{R}} \rho_H\left(\operatorname{conv}\Big(Q_1\mathcal{P}_{\le t}\Big), \operatorname{conv}\Big(Q_1\mathcal{P}_{\ge t+\Delta}\Big)\right)^n \\
&= \sup_{t\in\mathbb{R}} \rho_H\Big(Q_1\mathcal{P}_{\le t}, Q_1\mathcal{P}_{\ge t+\Delta}\Big)^n \\
&= \sup_{t\in\mathbb{R}} \sup_{\substack{P_0\in Q_1\mathcal{P}_{\le t} \\ P_1\in Q_1\mathcal{P}_{\ge t+\Delta}}} \left(1-\frac{1}{2}d_{\mathrm{H}}^2(P_0,P_1)\right)^n.
\end{aligned}$$

□

Lemma 3.18. *Sei $k\in\mathbb{N}$, $\varepsilon\in[0,\infty)$, $\mathcal{P}$ konvex, $(\mathcal{Z},\mathcal{G})$ ein messbarer Raum, $Q:\mathcal{Z}\times\mathcal{X}\to[0,1]$ ein Kanal und $\omega_{d_H}^{(Q)}(k\varepsilon)<\infty$. Dann gilt*

$$\omega_{d_H}^{(Q)}(k\varepsilon) \le k^2\omega_{d_H}^{(Q)}(\varepsilon).$$

Beweis. Im Fall $k=1$ ist die Aussage trivial. Sei also $k\ge 2$ und $\delta\in(0,\infty)$ beliebig. Da $\omega_{d_{\mathrm{H}}}^{(Q)}(k\varepsilon) = \sup\{|\theta(P_0)-\theta(P_1)| : d_{\mathrm{H}}(QP_0,QP_1)\le k\varepsilon, P_0,P_1\in\mathcal{P}\}$ endlich ist, gibt es $P_0,P_1\in\mathcal{P}$, so dass $D := d_{\mathrm{H}}(QP_0,QP_1)\le k\varepsilon$ und $|\theta(P_0)-\theta(P_1)|+\delta\ge\omega_{d_{\mathrm{H}}}^{(Q)}(k\varepsilon)$. Für $\lambda\in[0,1]$ setze $P_\lambda = (1-\lambda)P_0+\lambda P_1\in\mathcal{P}$ und beachte, dass mit Satz 2.4.(2), mit $\mu = QP_0+QP_1$, $q_0 = \frac{dQP_0}{d\mu}$, $q_1 = \frac{dQP_1}{d\mu}$,

$q_\lambda = \frac{dQP_\lambda}{d\mu} = (1-\lambda)q_0 + \lambda q_1$ und wegen Konkavität der Quadratwurzel gilt,

$$\begin{aligned} d_{\mathrm{H}}^2(QP_0, QP_\lambda) &= 2(1-\rho_H(QP_0, QP_\lambda)) = 2\left(1 - \int_{\mathcal{Z}} \sqrt{q_0[(1-\lambda)q_0 + \lambda q_1]}\, d\mu\right) \\ &\leq 2\left(1 - \int_{\mathcal{Z}} \sqrt{q_0}[(1-\lambda)\sqrt{q_0} + \lambda\sqrt{q_1}]\, d\mu\right) \\ &= 2\left(1 - (1-\lambda) - \lambda\int_{\mathcal{Z}} \sqrt{q_0 q_1}\, d\mu\right) \\ &= \lambda 2\,(1-\rho_H(QP_0, QP_1)) = \lambda d_{\mathrm{H}}^2(QP_0, QP_1). \end{aligned} \tag{3.2.4}$$

Für $j \in \{0, \dots, k^2\}$, wähle $\lambda_j := \frac{j}{k^2}$ und beachte, dass damit $P_{\lambda_0} = P_0$ und $P_{\lambda_{k^2}} = P_1$. Wegen (3.2.4) folgt $d_H(QP_0, QP_{\lambda_1}) \leq \sqrt{\lambda_1} d_{\mathrm{H}}(QP_0, QP_1) \leq \varepsilon$. Die selbe Ungleichung (3.2.4), mit vertauschten Rollen von P_0 und P_1, liefert $d_{\mathrm{H}}(QP_{\lambda_j}, QP_1) \leq \sqrt{1-\lambda_j} D$, für jedes $j \in \{0, \dots, k^2\}$. Für $j \in \{1, \dots, k^2 - 1\}$, setze $\eta_j := \frac{\lambda_{j+1} - \lambda_j}{1-\lambda_j}$, und beachte, dass damit $1 - \eta_j = \frac{1-\lambda_{j+1}}{1-\lambda_j}$ und

$$\begin{aligned} (1-\eta_j)P_{\lambda_j} + \eta_j P_1 &= (1-\eta_j)(1-\lambda_j)P_0 + (1-\eta_j)\lambda_j P_1 + \eta_j P_1 \\ &= (1-\lambda_{j+1})P_0 + (1-\lambda_j)\eta_j P_1 + \lambda_j P_1 \\ &= (1-\lambda_{j+1})P_0 + \lambda_{j+1} P_1 = P_{\lambda_{j+1}}. \end{aligned}$$

Neuerliches Anwenden von (3.2.4), mit P_{λ_j} anstelle von P_0 und $P_{\lambda_{j+1}}$ anstelle von P_λ, liefert

$$d_{\mathrm{H}}(QP_{\lambda_j}, QP_{\lambda_{j+1}}) \leq \sqrt{\eta_j} d_{\mathrm{H}}(QP_{\lambda_j}, QP_1) \leq \sqrt{\eta_j}\sqrt{1-\lambda_j} D = \sqrt{\frac{1}{k^2}} D \leq \varepsilon.$$

Somit haben also für jedes $j \in \{0, \dots, k^2 - 1\}$ die Maße QP_{λ_j} und $QP_{\lambda_{j+1}}$ eine Hellinger-Distanz von höchstens ε. Daher ergibt sich

$$|\theta(P_0) - \theta(P_1)| = \left|\sum_{j=0}^{k^2-1} \theta(P_{\lambda_j}) - \theta(P_{\lambda_{j+1}})\right| \leq \sum_{j=0}^{k^2-1} |\theta(P_{\lambda_j}) - \theta(P_{\lambda_{j+1}})| \leq k^2 \omega_{d_{\mathrm{H}}}^{(Q)}(\varepsilon).$$

Folglich gilt $\omega_{d_{\mathrm{H}}}^{(Q)}(k\varepsilon) \leq k^2 \omega_{d_{\mathrm{H}}}^{(Q)}(\varepsilon) + \delta$. Da $\delta > 0$ beliebig war, ist der Beweis erbracht. □

Wir widmen uns nun dem eigentlichen Beweis von Satz 3.10. Das Resultat ist trivial falls $\theta : \mathcal{P} \to \mathbb{R}$ konstant ist. Andernfalls wähle $\delta \in (0,1)$, so dass $\bar{C} := \frac{\sqrt{2\log(2a)}+1}{\sqrt{\delta}} \leq C$, wobei C die Konstante aus dem Satz ist und $a > 1$ die Regularitätskonstante der Verlustfunktion l. Betrachte weiter $\Delta := \bar{C}^2 \omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2}) \geq \bar{C}^2 \omega_{d_{\mathrm{H}}}(n^{-1/2}) > 0$, wegen Satz 2.8 und Aufgabe 2.10. Es sei nun $\hat{\theta}_n^\Delta : \mathcal{Z}^n \to \mathbb{R}$ der Schätzer aus Lemma 3.16, $\eta_m = (m+1)\Delta$ wie in diesem Lemma definiert und $\eta_{-1} = 0$. Der Verlust $l\left(|\hat{\theta}_n^\Delta - \theta(P)|\right)$ dieses Schätzers lässt sich durch die Treppenfunktion

$$\sum_{m=0}^{\infty} l(\eta_m) \mathbb{1}_{\{\eta_{m-1} < |\hat{\theta}_n^\Delta - \theta(P)| \leq \eta_m\}}$$

beschränken. Das maximale Risiko über dem Modell $\mathcal{P}$ können wir also wegen monotoner Konvergenz, Lemma 3.16 und Lemma 3.17 wie folgt abschätzen,

$$\begin{aligned} \sup_{P\in\mathcal{P}} \mathbb{E}_{QP^n}\left[l\left(|\hat{\theta}_n^\Delta - \theta(P)|\right)\right] &\leq \sum_{m=0}^{\infty} l(\eta_m) \sup_{P\in\mathcal{P}} QP^n\left(|\hat{\theta}_n^\Delta - \theta(P)| > \eta_{m-1}\right) \\ &\leq l(\Delta) + 4\sum_{m=1}^{\infty} l(\eta_m) \sum_{k=m}^{N-2} \left[\eta_A^{(n)}(Q, k\Delta) \vee 0\right] \\ &\leq l(\Delta) + 4\sum_{m=1}^{\infty} l(\eta_m) \sum_{k=m}^{N-2} \left[0 \vee \sup_{t\in\mathbb{R}} \sup_{\substack{P_0\in\mathcal{P}_{\leq t} \\ P_1\in\mathcal{P}_{\geq t+k\Delta}}} \left(1 - \frac{1}{2} d_{\mathrm{H}}^2(Q_1P_0, Q_1P_1)\right)^n\right]. \end{aligned} \tag{3.2.5}$$

Für $k \in \{1, \dots, N-2\}$, definiere nun $r := \lfloor \sqrt{k\bar{C}^2\delta} \rfloor \geq 1$ und beachte, dass wegen Lemma 3.18 gilt

$$\begin{aligned} k\Delta &= k\bar{C}^2\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2}) > k\bar{C}^2\delta\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2}) \geq r^2\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2}) \geq \omega_{d_{\mathrm{H}}}^{(Q_1)}(rn^{-1/2}) \\ &= \sup\{|\theta(P_0) - \theta(P_1)| : d_{\mathrm{H}}(Q_1P_0, Q_1P_1) \leq rn^{-1/2}, P_0, P_1 \in \mathcal{P}\}. \end{aligned}$$

Da $d_{\mathrm{H}}^2 = 2(1-\rho_H) \leq 2$, sehen wir, dass die Menge $\bar{\mathcal{P}} := \{(P_0, P_1) \in \mathcal{P}^2 : \theta(P_1) - \theta(P_0) \geq k\Delta\}$ über die das Supremum in (3.2.5) läuft, leer ist, falls $rn^{-1/2} \geq \sqrt{2}$. Falls jedoch $rn^{-1/2} < \sqrt{2}$, so gilt für jedes Paar $(P_0, P_1) \in \bar{\mathcal{P}}$, dass $|\theta(P_0) - \theta(P_1)| > \omega_{d_{\mathrm{H}}}^{(Q_1)}(rn^{-1/2})$, was zur Folge hat, dass $d_{\mathrm{H}}(Q_1P_0, Q_1P_1) > rn^{-1/2}$ sein muss. Somit folgt wegen $\log(1+x) \leq x$, für alle $x > -1$, aber auch, dass

$$\begin{aligned} \left(1 - \frac{1}{2}d_{\mathrm{H}}^2(Q_1P_0, Q_1P_1)\right)^n &\leq \left(1 - \frac{1}{2}\frac{r^2}{n}\right)^n \leq \exp\left(-n\frac{1}{2}\frac{r^2}{n}\right) = e^{-r^2/2} \\ &\leq \exp\left(-\frac{1}{2}\left[\sqrt{k\bar{C}^2\delta} - 1\right]^2\right) = \exp\left(-k\frac{1}{2}\left[\sqrt{\bar{C}^2\delta} - 1/\sqrt{k}\right]^2\right) \\ &\leq \exp\left(-k\frac{1}{2}\left[\bar{C}\sqrt{\delta} - 1\right]^2\right) = \exp\left(-k\log(2a)\right) = \left(\frac{1}{2a}\right)^k. \end{aligned}$$

Der Ausdruck in (3.2.5) lässt sich unter Verwendung von $x \leq (3/2)^x$ also weiter abschätzen durch

$$\begin{aligned} l(\Delta) + 4\sum_{m=1}^{\infty} l(\eta_m) \sum_{k=m}^{N-2} \left(\frac{1}{2a}\right)^k &\leq l(\Delta) + 4\sum_{m=1}^{\infty} l((m+1)\Delta) \sum_{k=m}^{\infty} \left(\frac{1}{2a}\right)^k \\ &\leq l(\Delta) + 4\sum_{m=1}^{\infty} l((3/2)^{m+1}\Delta) \left(\frac{1}{2a}\right)^m \frac{2a}{2a-1} \\ &\leq l(\Delta)\left[1 + 8a\sum_{m=1}^{\infty} a^m \left(\frac{1}{2a}\right)^m\right] \\ &\leq l\left(\bar{C}^2\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2})\right)[1+16a] \\ &\leq l\left((3/2)^{\lceil 2\frac{\log C}{\log 3/2}\rceil}\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2})\right)[1+16a] \\ &\leq l\left(\omega_{d_{\mathrm{H}}}^{(Q_1)}(n^{-1/2})\right)[1+16a]a^{\lceil 2\frac{\log C}{\log 3/2}\rceil}. \end{aligned}$$

Wir erhalten also die gewünschte obere Schranke. □

3.2.3 Konstruktive Schranken

3.3 Übungsaufgaben

Aufgabe 3.1. Angenommen wir wollen für ein vorgegebenes Privatisierungsniveau $\alpha \in (0, \infty)$ die Werte von k Funktionalen $\theta_1, \dots, \theta_k : \mathcal{P} \to \mathbb{R}$, α-differentiell privat schätzen. Für jedes $j = 1, \dots, k$ und für die Schätzung von θ_j, sei bereits ein α_j-differentiell privater Kanal $Q^{(j)} : \mathcal{G}_j \times \mathcal{X}^n \to [0,1]$ sowie ein Schätzer $\hat{\theta}_j : \mathcal{Z}_j \to \mathbb{R}$ gegeben, wobei die privatisierten Daten jeweils auf dem abstrakten messbaren Raum $(\mathcal{Z}_j, \mathcal{G}_j)$ generiert werden. Konstruieren Sie daraus eine α-DP Schätzprozedur, also einen α-DP Kanal Q und einen Schätzer für $\theta(P) = (\theta_j(P))_{j=1}^k$, und finden Sie eine Bedingung an die α_j um α-DP zu garantieren? Vergleichen Sie das Konzept der Bonferroni-Korrektur beim multiplen Testen. **(2P)**

Aufgabe 3.2. Zeigen Sie, dass die Huber-Verlustfunktion

$$l_\gamma(t) := \begin{cases} \frac{t^2}{2}, & 0 \leq t \leq \gamma, \\ \gamma(t - \frac{\gamma}{2}), & t \geq \gamma, \end{cases}$$

regulär ist. **(2P)**

Aufgabe 3.3. Zeigen Sie, dass der α-BM Kanal $Q^{(\alpha,\varphi)} : \mathcal{G}_m^{\otimes n} \times \mathcal{X}^n \to [0,1]$ für jedes beschränkte und messbare $\varphi : \mathcal{X} \to \mathbb{R}$, α-differentiell privat ist. **(2P)**

Aufgabe 3.4. Zeigen Sie, dass für ein signiertes Maß σ auf $(\Omega, \mathcal{A})$ gilt,

$$\|\sigma\|_{TV} := \sup_{A\in\mathcal{A}} |\sigma(A)| = \sup_{\varphi:\|\varphi\|_\infty\le 1} \frac{1}{2}\int_\Omega \varphi \, d\sigma.$$

(2P)

Hinweis: Verwenden Sie die Hahn-Jordan Zerlegung.

Aufgabe 3.5. Zeigen Sie die folgenden Eigenschaften von $\omega_{d_{\mathrm{H}}}$ und $\omega_{d_{\mathrm{TV}}}$ im Fall $\mathcal{P}$ konvex und $\theta : \mathcal{P} \to \mathbb{R}$ linear und beschränkt.

1. Falls θ nicht konstant ist, dann gibt es $c_0 = c_0(\mathcal{P}, \theta) > 0$ und $c_1 = c_1(\mathcal{P}, \theta) > 0$, so dass $\frac{\omega_{d_{\mathrm{TV}}}(\varepsilon)}{\varepsilon} \ge c_0$ und $\frac{\omega_{d_{\mathrm{H}}}(\varepsilon)}{\varepsilon^2} \ge \frac{c_0}{2}$ für alle $\varepsilon \in (0, c_1]$. **(4P)**
2. Für $\varepsilon_1, \varepsilon_2 \in [0,\infty)$ gilt, $\omega_{d_{\mathrm{TV}}}(\varepsilon_1 + \varepsilon_2) \le \omega_{d_{\mathrm{TV}}}(\varepsilon_1) + \omega_{d_{\mathrm{TV}}}(\varepsilon_2)$. **(1P)**
3. Finden Sie ein Beispiel für ein konvexes Modell $\mathcal{P}$ und ein lineares und beschränktes Funktional θ, so dass $\omega_{d_{\mathrm{TV}}}$ nicht stetig bei 0 ist. **(2P)**

Literaturverzeichnis

Del Moral, P., M. Ledoux, and L. Miclo (2003). On contraction properties of Markov kernels. *Probab. Theory Relat. Fields 126*(3), 395–420.

Donoho, D. L. and R. C. Liu (1991). Geometrizing rates of convergence, II. *Ann. Statist. 19*(2), 633–667.

Duchi, J. C., M. I. Jordan, and M. J. Wainwright (2014). Local privacy, data processing inequalities, and statistical minimax rates. *arXiv preprint arXiv:1302.3203*.

Dwork, C. (2008). Differential privacy: A survey of results. In *International Conference on Theory and Applications of Models of Computation*, pp. 1–19. Springer.

Dwork, C., F. McSherry, K. Nissim, and A. Smith (2006). Calibrating noise to sensitivity in private data analysis. In S. Halevi and T. Rabin (Eds.), *Theory of Cryptography*, Lecture Notes in Computer Science, pp. 265–284. Springer.

Evfimievski, A., J. Gehrke, and R. Srikant (2003). Limiting privacy breaches in privacy preserving data mining. In *Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pp. 211–222. ACM.

Klenke, A. (2008). *Probability Theory: A Comprehensive Course*. London: Springer.

LeCam, L. (1986). *Asymptotic Methods in Statistical Decision Theory*. Springer Series in Statistics. New York: Springer.

Mattila, P. (1995). *Geometry of Sets and Measures in Euclidean Spaces*. Cambridge: Cambridge University Press.

Narayanan, A. and V. Shmatikov (2006). How to break anonymity of the netflix prize dataset. *arXiv preprint cs/0610105*.

Nöle, G. and D. Plachky (1967). Zur schwachen Folgenkompaktheit von Testfunktionen. *Z. Wahrscheinlichkeitstheorie verw. Geb. 8*(3), 182–184.

Rohde, A. and L. Steinberger (2018). Geometrizing rates of convergence under differential privacy constraints. *arXiv preprint arXiv:1805.01422*.

Rudin, W. (1973). *Functional Analysis*. New York: McGraw-Hill.

Sion, M. (1958). On general minimax theorems. *Pacific J. Math. 8*(1), 171–176.

Tsybakov, A. B. (2009). *Introduction to Nonparametric Estimation*. Springer Series in Statistics. New York: Springer.