Fundamentos Estadísticos de Privacidad

Descripción

Este curso está dedicado al estudio de la noción de privacidad diferencial y sus adaptaciones a diversos contextos estadísticos. A través de ejemplos concretos se muestra la importancia de la privacidad, la cual es analizada subsecuentemente utilizando herramientas estadísticas diversas. El curso es predominantemente teórico, aunque se da especial énfasis a las motivaciones prácticas.

Prerrequisitos

Se recomienda haber cursado con anterioridad al menos un curso de probabilidad o estadística a nivel posgrado. Si bien el curso se enfoca principalmente en aspectos teóricos, es útil que el alumno tenga experiencia previa con algún programa de cómputo estadístico (e.g., Python).

Objetivos

Al finalizar el curso los participantes deberán:

- reconocer la importancia de la privacidad en problemas estadísticos;
- identificar los retos técnicos en el diseño y análisis de mecanismos de privacidad;
- aprender herramientas básicas para el estudio de la privacidad (diferencial);
- conocer problemas de privacidad contemporáneos y sus soluciones.

Contenido

Módulo 1: Privacidad Diferencial

1. Motivación y Primeros Ejemplos
2. Definición de Privacidad Diferencial
3. Privacidad Diferencial Aproximada
4. Privacidad Diferencial Local
5. Otras Variantes de Privacidad Diferencial

Módulo 2: Análisis basado en Teoría de la Información

1. Entropía, Divergencia e Información Mutua
2. Desigualdad de Procesamiento de la Información (DPI)
3. f-Divergencia y Coeficientes de Contracción
4. Privacidad Diferencial Local como Contracción
5. Teoremas de Conversión y Composición

Módulo 3: Privacidad en Contextos Estadísticos Específicos

1. Pruebas de Hipótesis Binarias
2. Minimización del Riesgo Empírico
3. Estabilidad y Generalización
4. Algoritmos de Optimización Iterativos

Bibliografía Básica

- T. M. Cover. *Elements of Information Theory*. John Wiley & Sons, 1999.
- J. C. Duchi. *Information Theory and Statistics*. Lecture Notes for Stanford University STATS311, 2019.
- C. Dwork & A. Roth. *The Algorithmic Foundations of Differential Privacy*. Foundations and Trends in Theor. Computer Science, 2014.
- Y. Polyanskiy & Y. Wu. *Lecture Notes on Information Theory*. Lecture Notes for MIT 6.441, 2017.
- S. Vadhan. *The Complexity of Differential Privacy*. Tutorials on the Foundations of Cryptography, 2017.

Acerca del Curso

– Evaluación: tareas (70%) y proyecto final (30%)

– Horario: Viernes de 12:00 a 3:00

– Instructor: Mario Diaz, IIMAS - Oficina 115, mario.diaz@sigma.iimas.unam.mx