**Privacidad diferencial**

**(preservación de la privacidad en la SVM)**

**GUION.**

**David Santiago Garzón Monje**

**Matemáticas, Universidad Nacional de Colombia, Sede Bogotá.**

**Diapositiva 1:** Breve introducción al proyecto.

* En este vídeo veremos qué es la privacidad diferencial y su importancia en el aprendizaje de máquina, en particular nos enfocaremos en la preservación de la privacidad en la SVM. ( 7s)

Explicación clara del problema abordado.

**Diapositiva 2:** ¿Cuál es el problema general que ha abordado?

* Pues bien, a lo largo de la historia han surgido problemas en los que por ejemplo una entidad quiere revelar cierta información acerca de sus estadísticas sin comprometer información de las personas participantes en el estudio, lo cual se hace generando ruido. Sin embargo, se ha demostrado que se requiere más trabajo para lograr evitar estas fugas de datos como lo hace notar Latanya Sweeney en un trabajo donde muestra cómo re-identifica un grupo de personas con datos que parecían seguros. Por cosas como estas, en el año 2006 gracias a trabajos hechos por [Cynthia Dwork](https://en.wikipedia.org/wiki/Cynthia_Dwork) entre otras personas, se da la definición formal de privacidad diferencial, donde se quiere ver como incluir la privacidad en un algoritmo al trabajar con datos que se desean con confidencialidad. La idea principal es aprender de un grupo mientras se aprende poco sobre un individuo en particular con una prueba matemática. ( 47s)

**Diapositiva 3:**

* De manera formal, para un epsilon positivo, se dice que un algoritmo A con entradas en un conjunto de datos proporciona un epsilon-diferencial de privacidad si para todos los conjuntos de datos D1 y D2 que difieren en un solo dato (o bien una persona) y todo evento S se tiene que la probabilidad de que ocurra S cuando el conjunto de datos es D1 es a lo más exponencial de epsilon veces la probabilidad de que ocurra S cuando el conjunto de datos es D2. Como observación, note que en esta definición si epsilon está cerca de cero entonces la parte de la derecha es exactamente esta probabilidad y cambiando los papeles de D1 y D2 en la definición, observamos que la desigualdad anterior se hace una igualdad, de modo que se garantiza bajo un epsilon pequeño que el dato de una persona en particular no interviene mucho en el resultado final. Concluímos que el epsilon nos indica la pérdida de privacidad, así para un epsilon pequeño se pierde poca privacidad. ( 58s)

**Diapositiva 4:**

* Para relajar la definición, se dirá que para un delta positivo el algoritmo genera un delta-epsilon diferencial de privacidad, si las probabilidades ya mencionadas están cerca por un delta, claramente entre más pequeño sea el delta, más nos acercamos a la definición original. Denotemos por delta de f a esta cantidad que llamamos sensibilidad; es claro que esta sensibilidad expresa la condición de diferencia de datos entre los conjuntos D1 y D2. Por lo anterior, se remarca que la forma de usar la definición de privacidad diferencial es agregando un ruido aditivo a la función objetivo, para luego determinar un epsilon adecuado, considerando la sensibilidad de la función. ( 43s)

**Diapositiva 5:**

* En pantalla aparecen garantías de privacidad diferencial para algunas de las distribuciones más usadas, es de destacar que la más poderosa de ellas por su fácil comprensión y frecuencia en uso de algoritmos es la distribución Laplaciana. Para quien esté interesado en consultar las pruebas de estos hechos puede ver la descripción de este video. En particular, del mecanismo Laplaciano, se observa que entre mayor privacidad se quiera; es decir, un epsilon más pequeño, mayor debe hacerse el parámetro de Laplace y por tanto mayor ruido tenemos que agregar. ( 30s)

**Diapositiva 6:**

* Surgen pues complicaciones visibles en el aprendizaje de máquina, una de ellas es que al disminuir el epsilon tendremos que aumentar el ruido y por tanto la información para el aprendizaje se va haciendo inutil a medida que se quiere más privacidad. Otro problema es que debemos fijarnos en la cantidad de ejemplos necesarios para aprender y mantener la privacidad. Un ejemplo claro se da en un problema donde se quiere aprender sobre la frecuencia de visitas a un establecimiento por horas, como muestra la figura hay una hora en donde posiblemente hay una contribución en particular, lo cual no es bueno en cuanto a privacidad, así que ahora no solo debemos preocuparnos por el número de ejemplos necesarios para garantizar generalización, si es que se puede lograr, si no que también debemos fijarnos en el número de contribuciones necesarias para garantizar privacidad. ( 29s)

**Diapositiva 7:** ¿Cuál es el problema específico de aprendizaje de máquina abordado? y ¿Por qué este problema es importante en el aprendizaje de máquina?

* Ya sabemos que la privacidad diferencial repercute en gran manera en algoritmos de aprendizaje de máquina, en particular y en lo que sigue, nos enfocaremos en la preservación de la privacidad para la SVM. Recuerde que la SVM usa varios algoritmos que buscan clasificar puntos en dos categorías, hoy por hoy son los algoritmos más utilizados, de modo que estudiar más este tema nos dará mayor recorrido en la teoría; incluso considere un caso hipotético donde usted desee hacer un proyecto implementando la SVM, luego podrá garantizar cierta confianza matemática para el conjunto de datos que esté utilizando en el entrenamiento. Yendo al lado útil y actual, Google hace este tipo de consideraciones en sus servicios, disponiendo de un repositorio de fácil acceso con el que puede evidenciar como se maneja la seguridad de sus datos al compartir información como la ubicación. ( 67s)

**Diapositiva 8:** ¿Cómo se relaciona con las temáticas cubiertas en el curso?

* Ahora, es clara la relación de la problemática con el curso, puesto que estamos tratando de unificar dos temas que se trataron. ( 7s)

Estado del arte.

**Diapositiva 9:** Revisión corta de lo que se sabe respecto al problema y/o como se ha abordado previamente.

* Hagamos una revisión rápida de algunas de las maneras para abordar este problema La primera de ellas trabaja con el modelo lineal de la SVM, que ya conocemos del curso, requiere la definición de utilidad (alfa-beta) para probar que al garantizar un epsilon-diferencial de privacidad y aprender, se requiere cierto número de ejemplos. Otra perspectiva trata el problema de manera más general pero considerando técnicas de kernel y SVM’s con un espacio de características finito, para poder aprender con una garantía de privacidad diferencial. El problema también se ha llevado a otros escenarios como la computación multi-parte segura, es decir los datos están distribuidos en múltiples partes pero sin revelar los datos de cada parte a los demás, y se puede realizar un análisis de la preservación de la privacidad en la SVM, de una manera más sencilla que al considerar un epsilon-diferencial de privacidad, este tipo de análisis es más moderno. Incluso otros autores hacen uso de la idea de particionar los datos con ciertas especificaciones, pero sin el uso de la computación multi parte, en vista de que este tipo de técnicas suelen ser ineficientes en aplicaciones reales como en Google. ( 62s)

Estrategias propuestas y/o resultados principales.

**Diapositiva 10:** Se deberá explicar de forma clara y sencilla las estrategias propuestas para el abordaje del problema y/o los resultados principales relacionados con el problema.

* De estas estrategias, la que usa una utilidad (alfa,beta) que básicamente establece una garantía de que con respecto al mecanismo usado, el desempeño del modelo estará a una distancia alfa de la función objetivo, con probabilidad mayor que 1-beta. Es posible demostrar que para lograr una utilidad (alfa,beta) y un epsilon-diferencial de privacidad, se requieren al menos el número de ejemplos que aparece en pantalla. ( 28s)

**Diapositiva 11:**

* Para el estudio que considera el kernel, recordemos que un kernel proyecta la información del problema original a un espacio de características de mayor dimensión para aumentar la capacidad computacional de las máquinas de aprendizaje lineal. Este análisis nos dice que en un espacio con características finitas, podemos asegurar bajo suposiciones bastantes restrictivas, como lo ve, que la SVM nos da garantía de privacidad diferencial. Así mismo, se puede hacer mayor profundización en los parámetros expuestos por este teorema para establecer el mejor epsilon. ( 35s)

Perspectivas de trabajo en esta dirección.

**Diapositiva 12:**

* Ya se mencionó que otra perspectiva de trabajo más moderna y efectiva es particionar los datos, cuyas particiones se pueden clasificar en 3. La idea principal es que los datos en cada parte se mantengan privados y el modelo final se construya en un sitio independientemente. Luego, el sitio independiente realiza la clasificación de nuevas instancias. Note que para mantener el secreto en cada parte, se puede usar privacidad diferencial. ( 24s)

**Diapositiva 13:**

* Para finalizar, se anota que el estudio de la privacidad en la SVM es actualmente muy importante en diversas aplicaciones, tanto así, que en cualquiera de estas ramas puede encontrar artículos independientes que trabajan lo visto en este video de forma más particular. Otra anotación que va más en general, correspondiente a la privacidad diferencial, y es que hoy somos conscientes de los defectos en empresas como Google o Apple, en cuanto estos hacen un uso fuerte de la privacidad diferencial. ( 28s)

**Diapositiva 11:** Referencias y Despedida.

* Eso es todo por hoy, gracias por ver este video. ( 2s)

Tiempo total: 7m con 58s