

Trabajo 3: Programación

Patricia Córdoba Hidalgo

Índice

1. Problema de clasificación	1
2. Problema de regresión	3

1. Problema de clasificación

Se implementó en el archivo `clasificacion.py`.

Este problema consiste en clasificar imágenes de dígitos escritos a mano, asignándole a cada una el dígito que representan. Nuestro espacio de características, χ , está formado por datos de 64 características, cada una de ellas representando la intensidad de trazado de una de las casillas de una matriz 8×8 , donde se ha trazado el dígito. El conjunto de etiquetas, Y , son los dígitos del 0 al 9. La función desconocida f es aquella que a cada imagen (elemento de χ) le asigna el dígito que representa (su etiqueta correspondiente).

Primero leemos los ficheros de datos con la función `readData`, que separa los datos de sus etiquetas. Los datos del fichero test serán los datos que usaremos para calcular el E_{out} y los del fichero training los dividimos en datos de entrenamiento y datos de validación. Un 25 % de los datos del fichero de datos training serán usados para validar. En un problema de aprendizaje corriente lo ideal sería mezclar los datos de ambos ficheros, ya que normalmente nos dan una base de datos y no tenemos un conjunto test, y dividir de ahí los conjuntos de entrenamiento, validación y test. En este caso, esto no es plausible, ya que los datos son números dibujados por personas y si mezclamos los ficheros existe la posibilidad de que haya dígitos trazados por la misma persona tanto en el conjunto training como en el test. Si esto ocurriese, como el algoritmo se entrenó para adaptarse a la caligrafía de ese individuo, la estimación del error fuera de la muestra que nos proporciona el conjunto test no sería realista. Por esto, en este caso, no mezclamos los ficheros, dejamos que el fichero test se use como conjunto test.

Las clases de funciones que usaré para resolver el problema son los polinomios de grado uno y dos. Usaré estas clases de funciones porque son relativamente sencillas y no tienen tanta variabilidad como otras clases de funciones, así no habrá tanta tendencia al sobreajuste y el error E_{out} no será tan alto.

Antes de empezar a trabajar con los datos, se preprocesan. Primero se usa PCA, para deshechar aquellas características que no aporten mucha información al modelo, y nos quedamos con aquellas capaces de explicar el 99 % de la distribución. Tras esto, escalamos los datos, ya que, si una característica tiene una varianza varios órdenes mayor que otra, puede tener repercusiones en el cálculo de la función objetivo y puede hacer que no se aprenda correctamente del resto de características.

Estas transformaciones se ajustan a los datos de entrenamiento (con la función `fit`) y luego se usan las mismas sobre el resto de datos (tanto al conjunto de validación como al de test).

Para clasificar los datos, usaremos regresión logística multietiqueta. Por el teorema de “No-Free-Lunch” todos los algoritmos son iguales en media, no hay un algoritmo mejor que otro, hay problemas donde unos tienen mejor desempeño que otros y elegí usar este algoritmo inicialmente porque ya lo hemos trabajado en otras prácticas, es sencillo y hemos visto como usarlo en caso de clasificación multietiqueta. Los resultados obtenidos fueron buenos, por lo que concluí que era un algoritmo con buen desempeño en éste problema.

La implementación del algoritmo de *Regresión Logística* está en la función `rl_sgd`. La función `rl_sgd` devuelve una lista de 10 vectores, cada uno de ellos calculado en una de las iteraciones del bucle principal (usando gradiente descendente estocástico y el error visto en teoría), que corresponde a los pesos de la función que separa esa clase del resto. Los hiperparámetros usados son: $\eta = 0,005$, se hacen 100 iteraciones y el tamaño de minibatch usado es 32. Probandos con diferentes valores para η , éste fue el que mejor resultado produjo en conjunto en todos los modelos usados, así que es el que se dejó al final. El número de iteraciones y el tamaño de minibatch se ajustaron según un criterio de calidad-tiempo, ya que con muchas más iteraciones, el tiempo que tarda el programa en ejecutarse es demasiado, y con esta proporción se obtenían resultados aceptables. Antes de ejecutar esta función, es necesario ajustar el formato de las etiquetas, pasando de tener dígitos a tener vectores de 10 coordenadas. A la etiqueta que representa el dígito i se le asocia el vector e_i , aquel que tiene ceros en todas sus componentes menos en la posición i , que tiene un 1. La etiqueta 0 pasa a ser $[1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$, la etiqueta 1 pasa a ser $[0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]$, y así sucesivamente, hasta la etiqueta 9 que pasa a ser $[0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1]$.

El error que minimizamos usando el algoritmo de *Regresión Logística* es la pérdida logarítmica, que nos permite penalizar mucho cuando la estimación es errónea y que el error sea muy cercano a cero cuando la estimación es buena. Sin embargo, la métrica que usaremos para elegir el mejor modelo será la precisión (accuracy), que es el porcentaje de etiquetas que acierta nuestro modelo. Usaré esta métrica para ver realmente cuál es el desempeño del modelo y cómo de bien clasifica las etiquetas.

Los resultados obtenidos son:

	CARACTERÍSTICAS LINEALES	CARACTERÍSTICAS CUADRÁTICAS
Error del conjunto training	0.06822748834535933	0.005245633985463137
Error conjunto de validación	0.08416293421735029	0.03036210074385761
Error del conjunto test	0.07509996756431692	0.06367515319684557
Precisión del conjunto training	0.7900976290097629	0.939679218967922
Precisión conjunto de validación	0.7979057591623037	0.8680628272251308

El modelo con características cuadráticas consigue una mayor precisión que el modelo con características lineales, es decir, consigue asignar la etiqueta correcta al mayor número de datos. El error dentro de la muestra es considerablemente menor que con características lineales. Esto se debe a que la clase de funciones es más rica y puede ajustarse mejor a los datos, aunque en el proceso puede producirse sobreajuste. Es por esto que la regularización es importante, para evitar que el modelo se ajuste demasiado bien a los datos de entrenamiento y no tan bien a los datos de la distribución.

Nosotros, que poseemos un conjunto de test, podemos ver que realmente el modelo con características cuadráticas se ajusta mejor a los datos de fuera de la muestra, pero esta información no debería impulsarnos a tomar ninguna decisión ya que, en teoría, esta información no la poseemos.

Para comprobar que no hemos sobreajustado el modelo a los datos y para limitar la varianza de la clase, que influye en el error E_{out} , es muy importante hacer siempre regularización. En mi caso, para regularizar usé la función `rl_reg` que usa el algoritmo de *Regresión Logística* minimizando ahora el error $E_{aug} = E_{in} + \lambda ||w||^2$, que es equivalente a imponer la restricción de que $||w||^2$ no supere cierta constante, y así acotamos la variabilidad de la clase. En el algoritmo, como calculamos cada uno de los 10 vectores de peso por separado, w sí es un vector, pero en el cálculo del error de regularización, con `Err_reg`, w es una matriz (contiene a los 10 vectores), luego lo que usamos es la norma de Frobenius, que es equivalente a la norma 2 por filas. Se tomó $\lambda = 0,0001$, ya que fue el valor de lambda que mejores resultados obtuvo entre los probados (mayor precisión). Este valor de λ es el que se usará siempre que se haga regularización (para comparar modelos, con el modelo final y para la validación cruzada).

Los resultados obtenidos con la regularización son:

	CARACTERÍSTICAS LINEALES	CARACTERÍSTICAS CUADRÁTICAS
Error del conjunto training	0.11641129755974719	0.17732784788169068
Error conjunto de validación	0.2385966274134429	0.5587784527220588
Error del conjunto test	0.16734674140002598	0.3341999985046917
Precisión del conjunto training	0.8009065550906556	0.944560669456067
Precisión conjunto de validación	0.7853403141361257	0.8869109947643979

Como podemos observar, el error tanto dentro como fuera de la muestra aumenta, ya que ahora el error que usamos penaliza también el tamaño del w resultante. Por esto nos basamos en la precisión para ver la bondad del modelo, ya que el porcentaje de datos que clasifica correctamente no depende del tamaño de los pesos elegidos, solo depende del buen desempeño del modelo. En este caso, el modelo con características lineales empeora con los datos de validación. Esto se debe a que el modelo en sí ya era bastante sencillo y no se estaba produciendo sobreajuste, así que al restringir la clase, no pudimos conseguir el mejor clasificador de ésta. En el modelo con características cuadráticas, la precisión sí que aumenta en el conjunto de validación, por lo que ahora el modelo se ajusta mejor a los datos que no son de entrenamiento.

Como el modelo con mejor precisión es aquel con características cuadráticas regularizadas, esta es la clase que usaremos, nuestro “mejor modelo”. Ahora, calculamos el w que se ajuste a todos los datos del fichero training. Este será el modelo definitivo, aquel que propondríamos como solución del problema de aprendizaje. Una vez calculado, calculamos la precisión del modelo con el conjunto test.

En la función de validación cruzada no sólo se devuelve el error medio de validación, sino que también se devuelve la precisión media del modelo. En teoría sabemos que, en media, el error de validación cruzada es una cota pesimista del error E_{out} , luego podemos usar ese error para acotarlo. De hecho, como podemos ver, el error $E_{out} = 0,1530888485750021 < 0,6634750029595697 = E_{cv}$. Sin embargo, la precisión del modelo por validación cruzada no es una cota pesimista de la precisión fuera de la muestra. Esto se debe a que los datos del conjunto training están escritos por las mismas personas y los del conjunto test por otras diferentes. Por eso, el modelo se ajusta mejor a los datos de validación que a los datos de test, ya que se ha entrenado con esa caligrafía, y proporciona mejores resultados con los datos de validación que con los de test. Lo que quiero decir con esto es que, aunque el error de regularización sí sea realmente mayor que el otro, este error depende de los pesos de los w que va calculando en gran medida, y si estos son más grandes puede dispararse, pero la bondad del modelo no depende tanto de estos pesos, y la bondad del modelo usando validación cruzada NO es una cota pesimista de la bondad del modelo fuera del conjunto por el razonamiento anterior.

Si una empresa me encargara el problema, el modelo que le daría sería el de características cuadráticas regularizado, porque según la métrica de error que he utilizado, la precisión, es aquel que mejor comportamiento tiene. La cota que les daría sería que el modelo, en el peor de los casos, tiene una precisión del 86,806 %. Esto sabemos que es falso por el problema de sobreajuste provocado por la caligrafía de la misma persona en los datos de entrenamiento y validación, y sabemos que en nuestro conjunto test tenemos una precisión del 83,361 %, que es menor a la cota dada, pero como en un problema real no contamos con esta información, lo mejor que le podemos decir a nuestro jefe es eso.

Al final del ejecutable, se muestra, a modo de ejemplo, el funcionamiento del modelo usando SOFTMAX. SOFTMAX crea un vector donde en cada casilla escribe la probabilidad de que el dato x pertenezca a esa clase. En nuestro caso, en la casilla i está la probabilidad de que el dato x sea el dígito i (si empezamos a contar las casillas por 0). Al dato se le asigna la etiqueta con mayor probabilidad de ocurrencia. Saqué por pantalla la etiqueta real, la etiqueta que se predice y la probabilidad de ésta. En este ejemplo, siempre acierta la etiqueta (Pero podría no acertar alguna, ya que la precisión no es del 100 %).

2. Problema de regresión