DEPARTAMENTO DE COMPUTACION

Facultad de Ciencias Exactas y Naturales - UBA

Trabajo Práctico 2

"Si nos organizamos aprobamos todos..."

Metodos numericos
Primer Cuatrimestre de 2015

Integrante	LU	Correo electrónico
Gastón Zanitti	058/10	gzanitti@gmail.com
Ricardo Colombo	156/08	ricardogcolombo@gmail.com
Dan Zajdband	144/10	Dan.zajdband@gmail.com
Franco Negri	893/13	franconegri200@gmail.com
Alejandro Albertini	924/12	ale.dc@hotmail.com

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Ciudad Universitaria - (Pabellón I/Planta Baja)
Intendente Güiraldes 2160 - C1428EGA
Ciudad Autónoma de Buenos Aires - Rep. Argentina
Tel/Fax: (54 11) 4576-3359
http://www.fcen.uba.ar

Índice

1. Introduccion

El objetivo de este trabajo es la realización y el análisis de algoritmos eficientes para el reconocimiento óptico de caracteres (OCR), particularmente de dígitos, a través de la utilización de técnicas simples de Machine learning.
El trabajo consiste en una serie de experimentaciones. El desarrollo de estas encuentra un hilo conductor en las mejoras aplicadas a un algoritmo basadas en problemas particulares que se pueden encontrar en la resolución del problema:

- Se parte de una base de datos de imágenes ya etiquetadas y otra con imágenes sin etiquetar. Usando la base de datos etiquetada como información de entrenamiento del algoritmo, se intenta etiquetar de modo correcto los dígitos de la base de datos sin etiquetas.
- La primera aproximación a la resolución del problema utiliza el método más intuitivo encontrado: Por cada imagen de la base de datos sin etiquetas, se busca la que más se le parece en la base de datos etiquetada y se marca a la imagen sin etiqueta con la etiqueta de aquella que denominamos como la más parecida. Por supuesto, todavía queda determinar cual es el criterio para decir que dos imágenes se "parecen". Esta definición está dada con profundidad en la sección de desarrollo.
- Surge entonces la pregunta acerca de que pasa si, por una particularidad de la imagen, la etiqueta más parecida no es la correcta para el dígito a averiguar. Para mitigar este problema parcialmente se pueden tomar las k imágenes más parecidas (que a partir de ahora llamaremos vecinos) y elegir como etiqueta aquella que se repita más entre los k vecinos. Detrás de esta idea se encuentra el algoritmo KNN, que se utiliza para mejorar el comportamiento en estos casos donde el vecino más cercano no pertenece necesariamente a la misma clase que la imagen a etiquetar.
- Por último, a esta idea se le puede aplicar una mejora sustancial utilizando un método probabilístico conocido como PCA. Este consiste en aplicar una transformación a las imágenes, de tal manera de solo tener en cuenta aquellas de mayor variabilidad y desechar aquella información que pueda estar introduciendo ruido.

Para entender las diferencias y similitudes entre los métodos y sus variantes, se realizan los experimentos con variaciones en los parámetros. En el caso de KNN se varía la cantidad de vecinos, esto ayuda a entender que valores ayudan a la optimización del algoritmo.
Para el caso de la mejora utilizando el algoritmo de PCA también hay que tener en cuenta el α utilizado. Vamos a ver como modificar este valor conlleva diferentes tiempos de ejecución y pérdida o ganancia de precisión.

2. Desarrollo

2.1. Algortimo de kNN

Como primera aproximación para la resolución del problema de OCR, implementamos el algoritmo de K-vecinos más cercanos (o kNN por sus siglas en inglés). Este método de clasificación consiste básicamente en, dado un dato del que no conocemos a que clase pertenece, buscar entre las imágenes del dataset etiquetado las k más parecidos, llamados también como sus "vecinos"(habiendo que definir que es ser "parecido"), y luego de estos k vecinos, determinar cual es la moda.

2.1.1. Similitud entre imágenes

Para este trabajo en particular, tomamos las imágenes como vectores numéricos y definimos que dos imágenes son "parecidas"si la norma dos entre ellas es pequeña. Luego la idea del knn será tomar todas las imágenes etiquetadas, compararlas contra la nueva imagen a reconocer, ver cuales son las k imágenes cuya norma es la menor posible y, entre esos k vecinos, ver a que clase pertenecen. La etiqueta para esta imagen vendrá dada por la moda.

Para los siguientes pseudocódigos será necesario asumir que todas las estructuras utilizadas almacenan datos enteros a menos que se indique lo contrario, esto se indica agregando entre paréntesis el tipo de dato que almacena.

TP1 1 Vector KNN(matriz etiquetados, matriz sinEtiquietar,int cantidadVecinos)

```
1: vector etiquetas = vector(cant_filas(sinEtiquetar))
2: for 1 to cant_filas(sinEtiquetar) do
3:    etiquetas_i = encontrarEtiquetas(etiquetados,sinEtiquetar_i,cantidadVecinos)
4: end for
5: return etiquetas
```

TP1 2 int encontrarEtiquetas(matriz etiquetados, vector incognito,int cantidadVecinos)

```
1: colaPrioridad(norma,etiqueta,vectorResultado) resultados
2: for 1 to size(incognito) do
3:    resParcial = restaVectores(etiquetados_i,incognita)
4:    colaPrioridad.push((norma(resParcial),etiqueta(etiquetados_i))
5: end for
6: vector numeros = vector(10)
7: while cantidadVecinos>0 & noesVacia(resultados) do
8:    int elemento =primero(resultados.etiqueta)
9:    numeros_elemento ++
10: end while
11: return maximo(numeros)
```

Una supocición preliminar es que a mayor cantidad de vecinos (o sea, k) menor va a ser la cantidad de aciertos, ya que se empiezan a mirar los elementos de menor prioridad de la cola, eso significa, que se cuentan primero las imágenes que más difieren y eso puede hacer que las chances de acertar el dígito correcto disminuyan. Ahondaremos mas en detalle en la siguiente sección, cuando pongamos a

prueba cual es la mejor cantidad de vecinos para este algoritmo.
Al comienzo del desarrollo de los experimentos pensamos en diferentes maneras de mejorar el procesamiento de las imágenes, ya sea pasandolas a blanco y negro para no tener que lidiar con escala de grises o recortar los bordes de las imágenes, ya que en ellos no hay demasiada información útil (en todas las imágenes vale 0).
Sin embargo, y mas allá de las mejoras que puedan realizarse sobre los datos en crudo, este algoritmo es muy sensible a la variabilidad de los datos. Un conjunto de datos con un cierto grado de dispersión entre las distintas clases de clasificación hace empeorar rápidamente los resultados.
En el siguiente apartado pasaremos a describir una metodología más sofisticada para resolver este problema que mejora tanto los tiempos de ejecución como la tasa de reconocimiento con respecto al método descripto anteriormente.

2.2. Optimización mediante Análisis de componentes principales

El Análisis de Componentes Principales o PCA es un procedimiento probabilístico que utiliza una transformación lineal ortogonal de los datos para convertir un conjunto de variables, posiblemente correlacionadas, a un nuevo sistema de coordenadas conocidas estas como componentes principales tal que la mayor varianza de cualquier proyección de los datos queda ubicada como la primer coordenada (llamado el primer componente principal, aquella que explica la mayor varianza de los datos), la segunda mayor varianza en la segunda posición, etc. En este sentido, entonces, PCA calcula la base mas significativa para expresar nuestros datos. Recordemos que una base es un conjunto de vectores linealmente independientes tal que, en una combinación lineal, puede representar cualquier vector del sistema de coordenadas.
De esta manera entonces, será fácil quedarnos con los λ componentes principales que concentren la mayor varianza y quitar el resto. En la sección de experimentación, uno de los objetivos principales será buscar cual es el λ que concentra la mayor varianza de manera tal de optimizar el número de predicciones. A fines prácticos, lo que haremos es, a partir de nuestra base de datos de elementos etiquetados, sera construir la matriz de covarianza M de tal manera que en la coordenada M_ij se obtenga el valor de la covarianza del pixel i contra el pixel j. Luego, utilizando el método de la potencia, procederemos a calcular los primeros λ autovectores de esta matriz. Una vez obtenidos los autovectores multiplicando cada elemento por los λ autovectores y obtendremos un nuevo set de datos. Sobre este set de datos, ahora aplicaremos el algoritmo KNN nuevamente y lo que esperamos ver es un mayor número de aciertos, ya que hemos quitado ruido del set de datos (mediante esta base que mencionamos al principio), sumado a mejores tiempos de ejecución, ya que hemos reducido la dimensionalidad del problema.
Generalizando entonces, los supuestos de PCA son:

- Linealidad: La nueva base es una combinación lineal de la base original.
- Media y Varianza son estadísticos importantes: PCA asume que estos estadísticos describen la distribución de los datos sobre el eje.
- Varianza alta tiene una dinámica importante: Varianza alta significa señal. Baja varianza significa ruido.
- Las componentes son ortonormales.

Si algunas de estas características no es apropiada, PCA podría producir resultados pobres. Un hecho importante que debemos recordar: PCA devuelve una nueva base que es una combinación lineal de la base original lo cual limita el numero de posibles bases que puedan ser encontradas.

2.3. Cross-validation

Para medir la precisión de nuestros resultados utilizamos la metodología de cross-validation. Esta consiste en tomar nuestra base de datos de entrenamiento y dividirla en k bloques. En una primera iteracion se toma un bloque para testear y los bloques restantes para entrenar a nuestro modelo, observando los resultados obtenidos. En la siguiente, se toma el segundo bloque para testear y los restantes como dataset de entrenamiento. La metodología se repite k veces hasta iterar todo el conjunto de datos. Finalmente, se realiza la media aritmetica de los resultados de cada iteracion para obtener un unico resultado de error y poder evaluar la performance del metodo de entrenamiento.

Esta técnica, que es una mejora de la técnica de holdout donde simplemente se divide el set de datos en dos conjuntos (uno para entrenamiento y otro para testing), trata de garantizar que los resultados obtenidos sean independientes de la partición de datos contra la que se esta evaluando porque ofrece el beneficio de que los parámetros del método de predicción no pueden ser ajustados exhaustivamente a casos particulares. Es por esto que se utiliza principalmente en situaciones de predicción, dado que intenta evitar que el aprendizaje se realice sobre un cuerpo de datos especifico y busca obtener respuestas mas generales.

La única desventaja que presenta es la necesidad esperable de correr los algoritmos en varias iteraciones, situacion que puede tener un peso significativo si el método de predicción tiene un costo computacional muy alto durante el entrenamiento.

2.4. Algoritmo PCA

TP1 3 void PCA(matriz etiquetados, matriz sinetiquetar,int cantidadAutovectores)

```
1: matriz covarianza = obtenerCovarianza(etiquetados)
2: vector(vector) autovectores
3: for 1 to cantidadAutovectores do
4:    vector autovector=metodoDeLasPotencias(covarianza)
5:    agregar(autovectores,autovector)
6:    double lamda = encontrarAutovalor(auovector,covarianza)
7:    multiplicarXEscalar(auovector,lamda)
8:    restaMatrizVector(covarianza,auovector,lamda)
9: end for
```

TP1 4 matriz obtenerCovarianza(matriz entrada,vector medias)

```
1: matriz covarianza, vector nuevo
2: for i=1 to size(medias) do
3:    for j=1 to cant_filas(entrada) do
4:          nuevoVector_j = entrada_(j,i) − medias_i
5:    end for
6:    agregar(covarianza,nuevoVector)
7: end for
8: for i=1 to cant_filas(entrada) do
9:    for k=1 to cant_filas(entrada) do
10:      covarianza_i = multiplicarVectorEscalar(covarianza_k, cantidad_filas(entrada)
11:   end for
12: end for
13: return covarianza
```

TP1 5 Vector metodoDeLasPotencias(matriz covarianza,cantIteraciones)

```
1: vector vectorInicial= vector(cant_filas(covarianza))
2: for 1 to cantIteraciones do
3:    vector nuevo = multiplicar(covarianza,vectorInicial)
4:    multiplicarEscalar(nuevo,1/norma(nuevo))
5:    vectorInicial = nuevo
6: end for
7: return vectorInicial
```

TP1 6 Vector medias(matriz entrada)

```
1: vector medias=vector(cant_columnas(entrada))
2: for i=1 to cant_columnas(entrada) do
3:     suma = 0
4:     for j=1 to cant_columnas(entrada) do
5:         suma + = entrada_{i,j}
6:     end for
7:     medias_i = suma/cant_filas(entrada)
8: end for
9: return vectorInicial
```

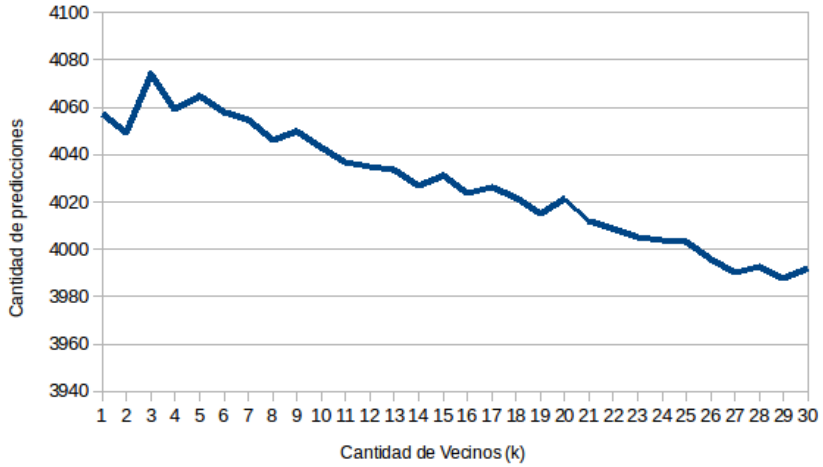
3. Análisis

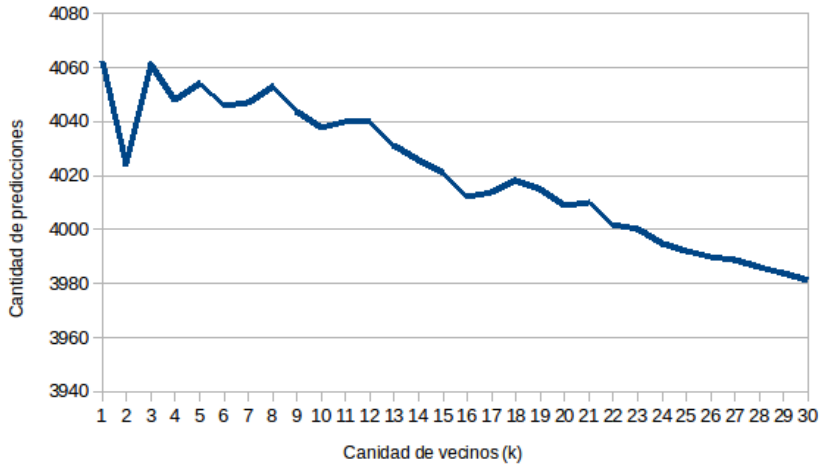
3.1. KNN

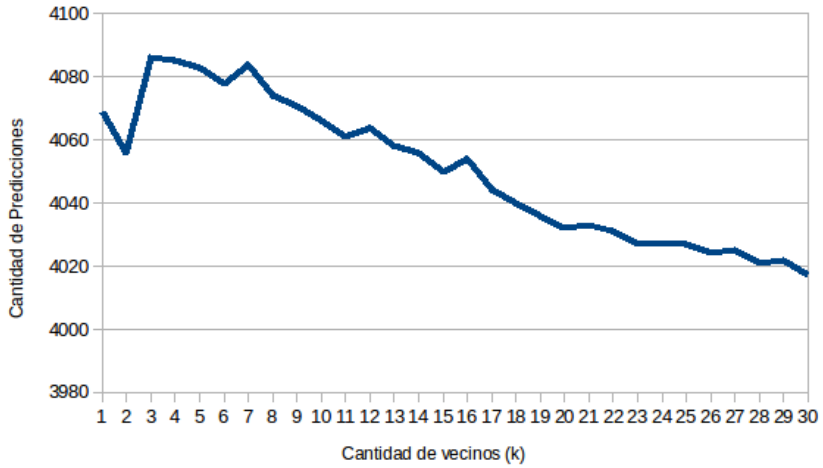
En esta sección definimos:

- k: cantidad de vecinos a considerar en el algoritmo kNN.

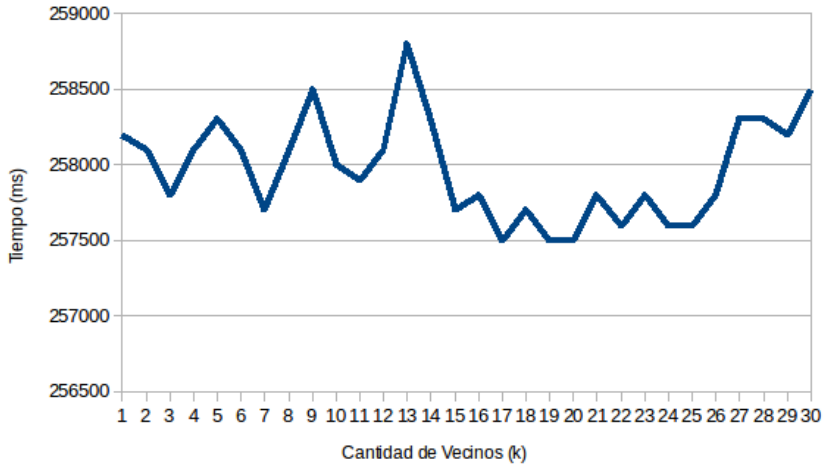
El análisis sobre el algoritmo KNN (k vecinos más cercanos) se realiza para distintos valores de k, la idea detrás de esta elección, busca entender la variación en la efectividad (cantidad de aciertos) del algoritmo.
Para ello variamos k desde 1 hasta 30 para ver cual era el comportamiento que se obtenía. Para cada uno de los ks realizamos una corrida cross-validation con 10 conjuntos.
Cada uno de los conjuntos contaba con 4200 imagenes a testear, en los siguientes graficos presentamos algunos de los sets obtenidos:







Como puede verse hay un patrón bastante claro en los tres test corridos, para valores muy pequeños de k (k=1,K=2) podemos observar que los resultados son peores que para $k = 3$,luego para valores más grandes se observa lo que nos decía la intuición, tal que para un gran número de vecinos se empiezan a perder aquellos que son realmente relevantes y las predicciones empiezan a ser peores, lo que no se esperaba era el salto en la cantidad de aciertos que vemos en los primeros valores de k pero podemos entonces saber que dentro de los primeros k se encuentran los mejores resultados.
Ademas para estos tests realizamos una medición de tiempos para ver cómo se comportaba el algoritmo frente a un cambio en la cantidad de vecinos. Los valores promediados para cada k pueden verse en el siguiente gráfico:



Como puede observarse, los tiempos de los algoritmos no se ven muy afectados por la variación en la cantidad de vecinos. Es muy probable que esto se deba a que el algoritmo debe comparar a la imagen que se desea comparar contra un número muy extenso de imagenes que estan en el mismo orden de magnitud.

Luego de los test decidimos que vamos a usar $k = 3$ porque nos dio los mejores resultados, cantidad de aciertos.

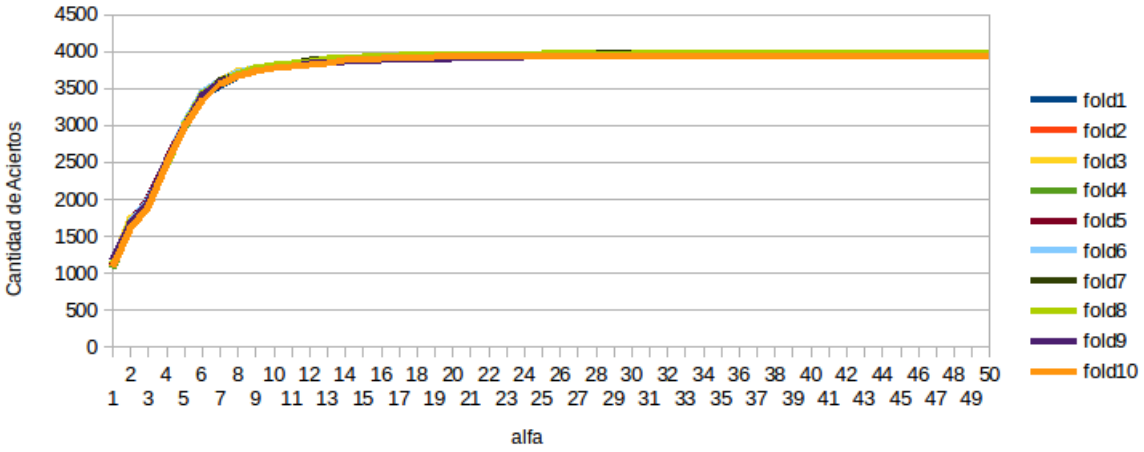
3.2. PCA

3.2.1. Busqueda del mejor valor de α

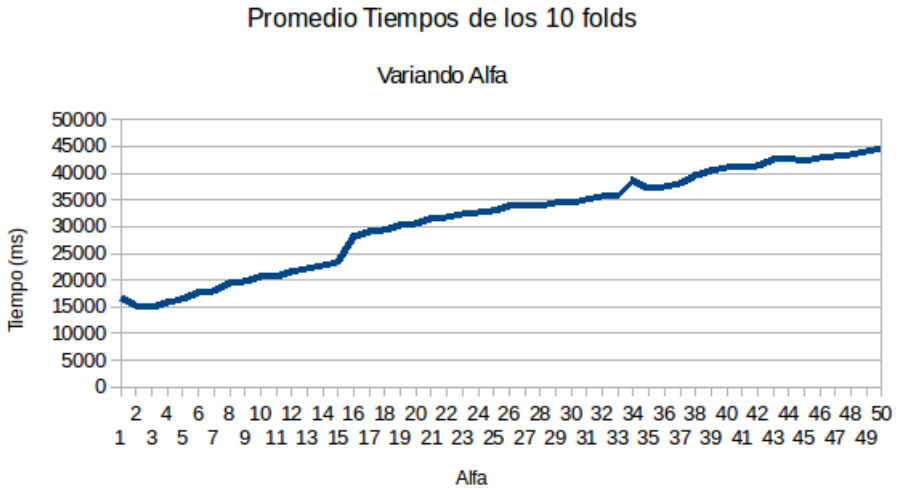
En esta sección definimos:

- α: a la cantidad de componentes principales a tomar para el PCA.
- k: cantidad de vecinos a considerar en el algoritmo kNN.

En primera instancia vamos a utilizar cross-validation para intentar determinar el mejor α posible. Supondremos en este momento que el mejor k para este caso es el encontrado en la sección anterior (aunque esto podría no ser así) y luego testeamos si esto es así o si para el α encontrado existe algun otro k que mejora la cantidad de predicciones del sistema.
Por lo tanto enfocamos nuestro análisis en obtener un valor óptimo de α. Para este fin, partimos el conjunto de datos de entrenamiento en 10 subconjuntos y aplicamos cross-validation. Dado que este parámetro representa la cantidad de componentes principales a tener en cuenta y teniendo en mente el funcionamiento del algoritmo de PCA, es esperable que valores pequeños no sean beneficiosos (teniendo en cuenta que el máximo a considerar es bastante elevado), pero dado que PCA las ordena en base a su relevancia, se alcance un valor óptimo sin necesidad de considerarlas todas. Para esta partición de los datos de entrenamiento con 4200 imagenes para testear, tomamos α desde 1 hasta 50 y graficamos lo obtenido:



Puede verse que para valores pequeños, aumentar en uno el α produce un gran aumento de aciertos. Por ejemplo, considerando el primer set para α igual a 1 se obtienen 1112 aciertos, mientras que para α igual a 2 se obtienen 1680 aciertos, esto es un 52 % mas de aciertos.
Para valores mas grandes de α (alrededor de $\alpha = 12$) esta tendencia empieza estabilizarse. Por ejemplo para $\alpha = 12$ se obtienen 3845 imagenes correctamente predecidas, pero para $\alpha = 13$ se obtienen 3869 imagenes correctas, esto es el crecimiento de aciertos es de menos de un 1 %.
Ademas, para este k-fold medimos los tiempos de ejecución y los promediamos para poder ver de que manera varía la ejecución de los algoritmos en función de α:

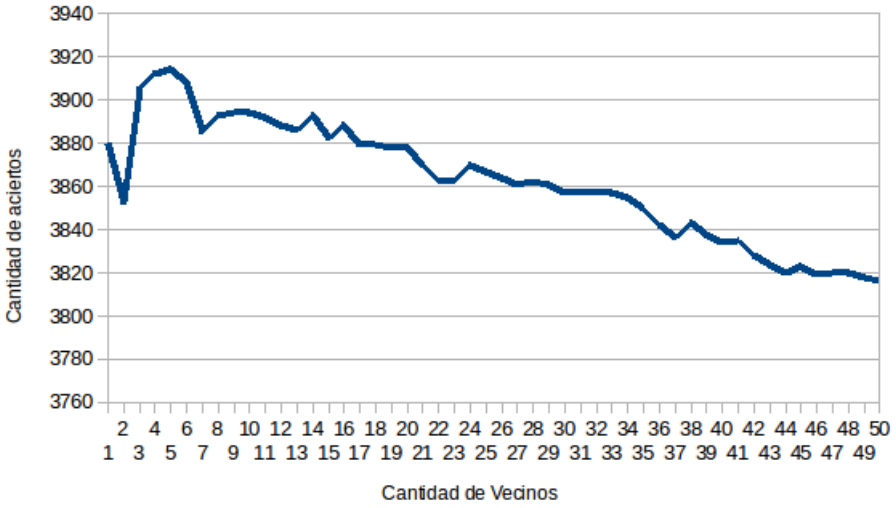


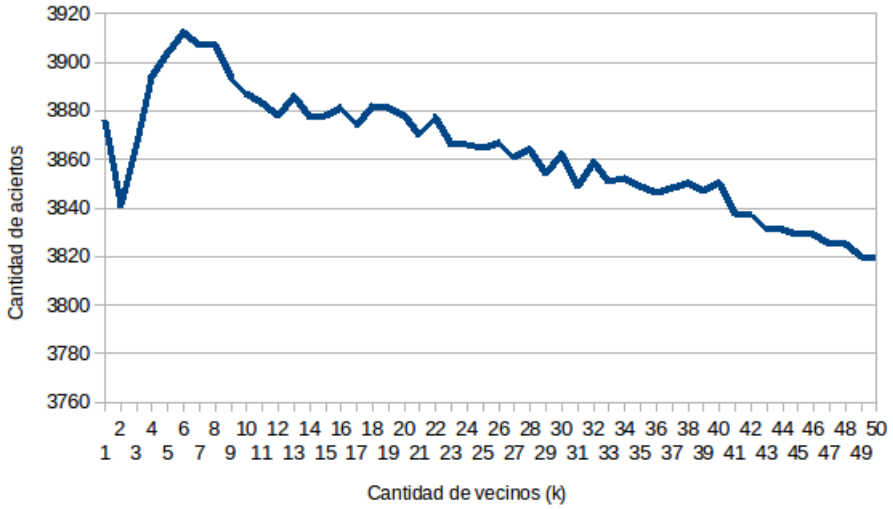
Cabe aclarar que estos tiempos no contemplan todo lo que se considera el 'entrenamiento' del sistema, osea, todo el preprocesamiento que resultará en encontrar los valores principales. La justificación de esto es que esto se realizará una vez, para entrenar el sistema, luego, al momento de clasificar las nuevas imagenes este tiempo podrá ser despreciado.
En este grafico se puede ver que aumentar el α produce un aumento lineal de los tiempos de ejecución, de lo que se desprende que aumentar la cantidad valores principales no resulta gratuito y tiene cierto costo asociado.
Ademas aumentar de manera desmedida el α puede provocar lo que en machine learning se denomina 'Overfitting' o sobreajuste, que consiste en que el modelo, en vez de buscar patrones sobre los cuales predecir, empieza a 'memorizar' de alguna manera los datos de entrenamiento. Esto puede conducir a que, si bien en la etapa de desrrollo se obtienen buenos niveles de predicción, cuando el modelo es

puesto a prueba en algun caso real su desempeño no es el esperado[1].
Debido a todas las razones expuestas consideramos que con α igual a 14 será el mejor valor que podemos tomar.

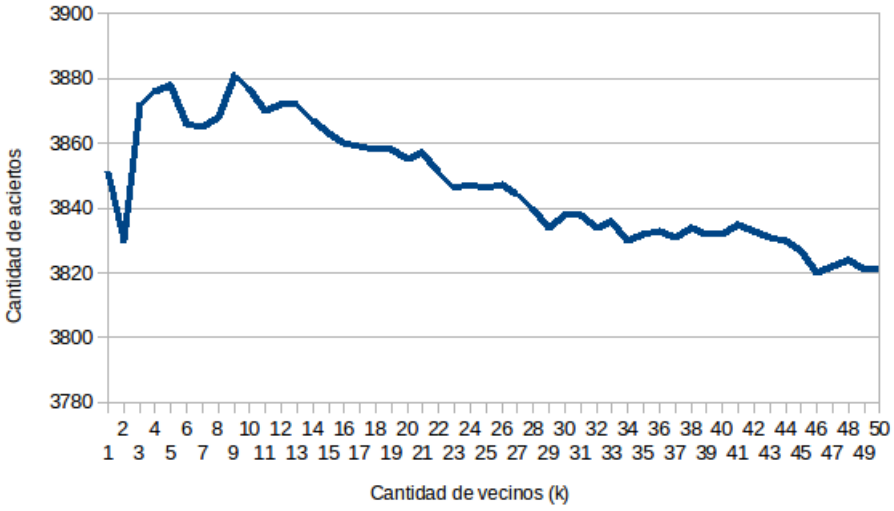
3.2.2. Busqueda del mejor valor de k

La segunda prueba a realizar es, fijando un valor de α, analizar para que cantidad de vecinos se obtiene la mayor cantidad de aciertos.
Para esto tomamos $\alpha = 14$ volvemos a dividir el conjunto de datos en 10 sets y realizamos cross validation sobre estos, variando el k desde 1 hasta 30.
En el siguientes graficos mostramos que paso con tres de los sets cuando se variaba el numero de vecinos:

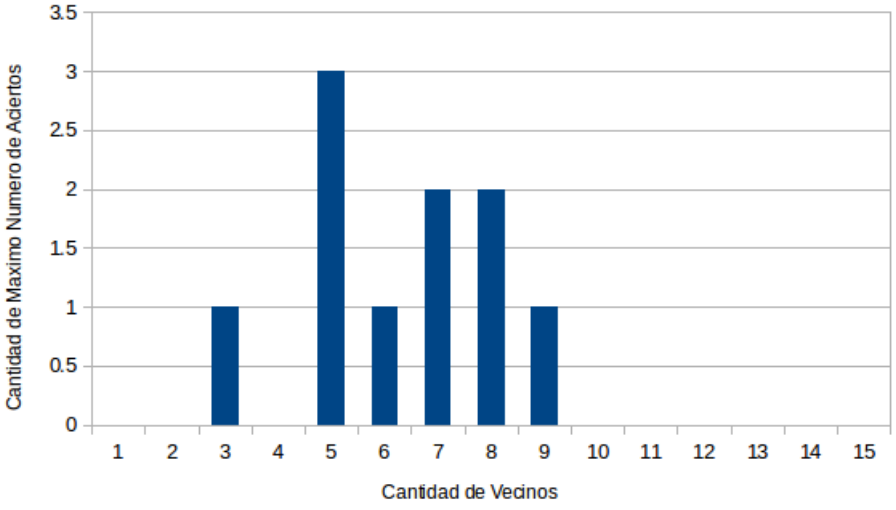




[1] A Few Useful Things to Know about Machine Learning, Pedro Domingos, Department of Computer Science and Engineering, University of Washington

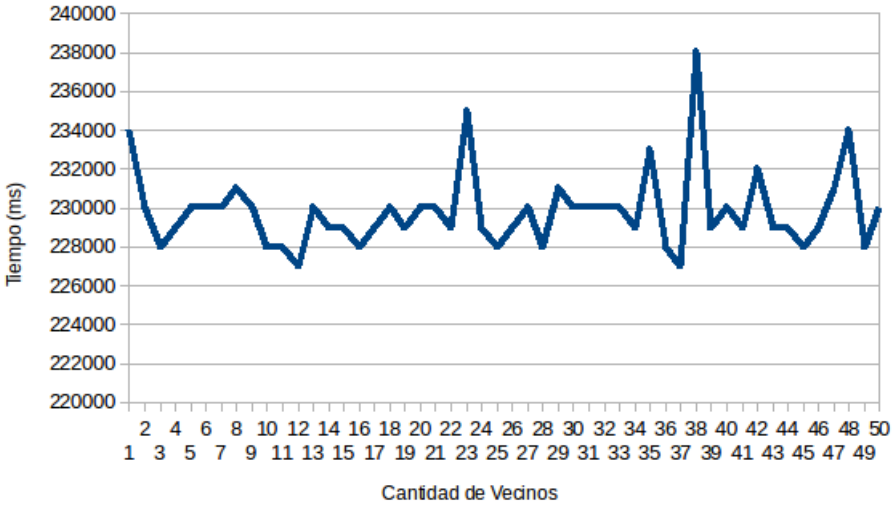


En total, de los diez sets en dos de ellos se encontró que el numero de vecinos que maximizaba la cantidad de aciertos era 8, en dos se encontró que el maximo fue $k = 7$, en otros dos el mejor fue 5 vecinos, y los demas se encontraban cerca de estos mismos valores.
En el siguiente grafico expresamos como se distribuyeron los maximos en cada canjunto del cross-validation:



De esto podemos determinar que el k optimo se encuentra en un rango entre 3 y 9.

Ademas medimos los tiempos y los promediamos para obtener una idea de cómo afectan las variaciones de k a este método:



Como podemos ver, el numero de vecinos contiúa sin afectar mayormente los tiempos de ejecución incluso luego de haber reducido la dimencion de la entrada.

4. Resultados

4.1. Resultados del testeo

Del apartado de experimentación podemos deducir que el mejor metodo de prediccion es el metodo de knn, que, con un $k = 3$, obtiene al rededor de un 96 % de aciertos. Sin embargo esto viene asociado con tiempos de ejecución increiblemente altos y que podrían no resultar apropiados. Recordemos que en el apartado anterior determinamso que para clasificar 4200 imagenes obtuvimos tiempos cercanos a los 4,35 minutos.
Tambien vimos que el PCA, si bien no llega a tasas tan altas de prediccion como el KNN, obtiene resultados aceptables para el mejor k y α encontrados, que rondan entre un 92 % y 90 %. La ventaja de este metodo es que sus tiempos de ejecución son mucho menores que los del KNN, clasificar 4200 imagenes tardaba 0,36 minutos, osea un 8,4 % de lo que tardaba la metodologia de KNN!.
Luego a la hora de elejir alguna de estas dos metodologías de resolución uno debe sopesar que es lo que mas le interesa, resultados rapidos pero con una menor tasa de aciertos o resultados mas precisos pero que requieren de tiempos elevados de procesamiento.

5. Conclusiones

El análisis realizado nos lleva a sacar una serie de conclusiones en base a lo experimentado.
El algoritmo KNN presenta una gran efectividad, entendiendo que es una técnica que cuenta con varios años de antiguedad. Sin embargo, los tiempos necesarios para todas las comparaciones resultan considerablemente elevados. Como dato importante de destacar, entendemos que la efectividad de este algoritmo depende en gran medidad de la variación de los datos a analizar. En aquellos conjuntos donde la varianza es elevada y los datos se encuentran muy dispersos, promediar el resultado en base a sus vecinos más cercanos puede no resultar la mejor técnica a implementar. Lo mismo podria ocurrir en situaciones donde los datos se äsemejen̈demasiado por la eleccion de las características a medir (situacion que podria, o bien eligiendo nuevas formas de representar los datos o realizando un preprocesamiento previo a estos).
Teniendo en cuenta esto, la relación costo-beneficio de la implementación y ejecución previa de una optimización como la del algoritmo de PCA, resulta mínima. Si bien es cierto que, como pudimos observar en el analisis, se pierde una efectividad de alrededor de un digito, atribuimos este comportamiento a algunas de los supuestos que mencionamos que asumia el algoritmo de PCA. Sin embargo, dada la característica principal del algoritmo de PCA (ordenar las componentes principales en base a su relevancia), se permite ajustar la cantidad de datos a considerar, dando lugar a una mejora mas que considerable en la performance de aplicar sobre estos el algoritmo KNN y el uso de memoria. Como vimos durante nuestro análisis, la cantidad óptima está bastante por debajo del máximo y no tienen ningún beneficio considerar una mayor cantidad de estas.
Como resultado de esta característica, los tiempos de analisis se reducen drasticamente, todavia lejos de poder implementar este tipo de soluciones en ẗiempo realp̈ero mucho mas cercanos que utilizando solo el algoritmo de KNN.
Como se menciona al comienzo del trabajo y de este apartado, el preprocesamiento de las imágenes es otro factor que puede mejorar la eficiencia algorítmica. Así como PCA quita ruido del dataset, es posible homogeneizar las imágenes por separado aplicando otros filtros.
Si bien el propósito del trabajo busca encontrar dígitos en imágenes este mecanismo se puede utilizar de un modo muy parecido para encontrar otras características tanto en imágenes como en audios y así etiquetar según clases que no tienen que ver necesariamente con la extracción de dígitos.