Politechnika Warszawska

**Sprawozdanie projektu grupowego Klasyfikacja cyfr pisanych odręcznie**



*Wydział: Elektryczny  
Kierunek: Informatyka stosowana  
Przedmiot: Podstawy reprezentacji i analizy danych, Laboratoria   
Grupa nr.6, w skład wchodzą:  
Edvin Suchodolskij 308919  
Konrad Žilinski 308920  
Mateusz Pietrzak 307373*

Warszawa 2020.02.06Spis treści:

[1. Wprowadzenie: 3](#_Toc63545136)

[Opis ogólny problemu 3](#_Toc63545137)

[Dane 3](#_Toc63545138)

[Dostępne rozwiązania: 3](#_Toc63545139)

[Metoda testów 4](#_Toc63545140)

[2. Analiza kolejnych modeli 5](#_Toc63545141)

[Nearest Centroid 5](#_Toc63545142)

[K-nearest neighbors 8](#_Toc63545143)

[Gaussian Naive Bayes 10](#_Toc63545144)

[Gaussian process classification 12](#_Toc63545145)

[Decision tree clasifier 14](#_Toc63545146)

[Sieć neuronowa czyli Multi-Layer-Perceptron 17](#_Toc63545147)

[Linear Regression 21](#_Toc63545148)

[3. Analiza uzyskanych wyników 22](#_Toc63545149)

[Najlepszy model 25](#_Toc63545150)

[4. Używanie modeli do przywidywania cyfr 25](#_Toc63545151)

[Udane próby klasyfikacji 25](#_Toc63545152)

[Nieudana próba klasyfikacji 25](#_Toc63545153)

# 1. Wprowadzenie:

## Opis ogólny problemu

Istnieje bardzo dużo różnych wariantów napisania tej samej liczby. W czasach automatyzacji urządzenia powinny nauczyć się rozpoznawać ludzkie pismo, tym samym pozwalając zastąpić pracowników w powtarzalnych pracach, tym samym umożliwić cyfryzację. Program po przetworzeniu tej struktury danych powinien być w stanie odróżnić praktycznie dowolną cyfrę.

## Dane

Struktura danych MNIST zawiera 60000 przykładów i 10.000 testowych zdjęć. Dana struktura jest chętnie używana do uczenia maszynowego oraz jego testowania. Zapisana jest w plikach „.csv” i każdy z nich zawiera 785 liczb. Pierwsza liczba jest cyfrą, którą program ma rozpoznać. Kolejne 784 liczb, od 0 do 255, wskazują na jasność pikseli obrazu tej liczby w skali szarości. Rozmiar obrazu wynosi 28 x 28 pikseli. MNIST jest popularną bazą danych stworzoną dla ludzi, którzy chcą spróbować swoich sił w analizie danych bez spędzania zbytecznych sił na ich formatowanie.

## Dostępne rozwiązania:

Metody które znaleźliśmy w Internecie[[1]](#footnote-1):

* Linear Classifiers
* Boosted Stumps
* Non-Linear Classifiers
* Support vector machines (SVMs)
* Convolutional nets

Sprawdziliśmy poprawność odpowiedzi dla metod:

* Neural Network Multi-Layer-Perceptron (MLP)
* Decision Tree
* Gaussian process classification
* Gaussian Naive Bayes
* K-nearest neighbors
* Nearest centroids

Wybraliśmy te modele ponieważ z ograniczeń czasowych nie moglibyśmy, nie bylibyśmy w stanie sprawdzić dogłębnie i zrozumieć parametrów wszystkich modeli. Wybrane zostały modele omawiane wcześniej na zajęciach z Podstaw Reprezentacji i Analizy Danych. Uwzględnione zostały także: Gaussian process i Neural Network, gdzie dla ostatnich dwóch kryterium była ich skuteczność.

## Metoda testów

Zdecydowaliśmy wypisywać wszystkie parametry w liniach obok siebie sortowanych rosnąco według celności modelu. Pokazywanie tych danych na wykresie wymagało by przygotowania programu, który by mógł interpretować graficznie te dane. Ponieważ mamy jedną wartość liczbową oraz wiele wartości kategorycznych ukazanie tych danych na wykresie byłoby nieproduktywne. Wypisując te dane w linii kosztem estetyki zyskujemy na czytelności.

# 2. Analiza kolejnych modeli

## Nearest Centroid

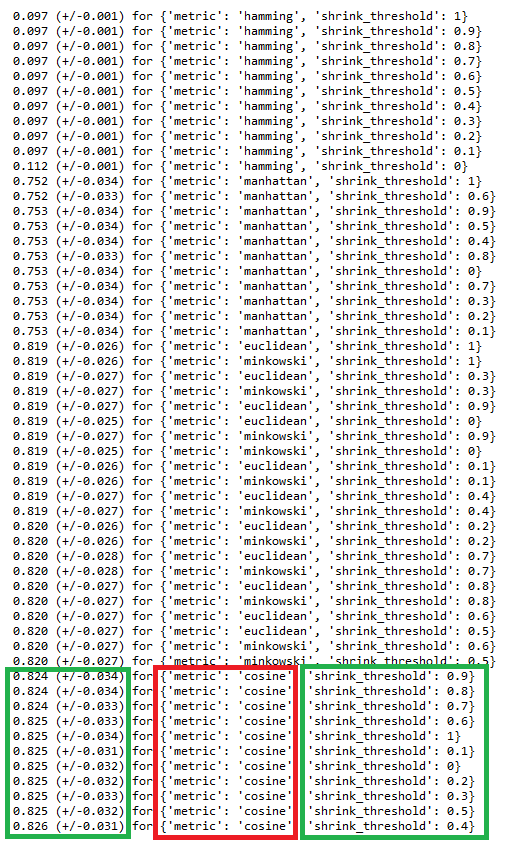
Ta metoda polega na minimalizacji odległości wektorów wartości atrybutów obiektów należących do danego klastra do pewnego punktu charakterystycznego klastra (zwanego jego środkiem lub centroidem), do którego obiekty zostały przyporządkowane. Przyporządkowanie danego obiektu do klastra odbywa się poprzez porównanie jego odległości do wszystkich centroidów. Metoda ta wymaga informacji o liczbie klastrów (grup). Początkowe ich położenia wybierane są losowo albo z użyciem specjalnego algorytmu.

### Test no.1

Testowane wartości parametru „metric”:

* Hamming
* Manhattan
* Euclidean
* Minkowski
* Cosine

Testowane wartości parametru „shrink\_threshold”: od 0 do 1 co 0.1.

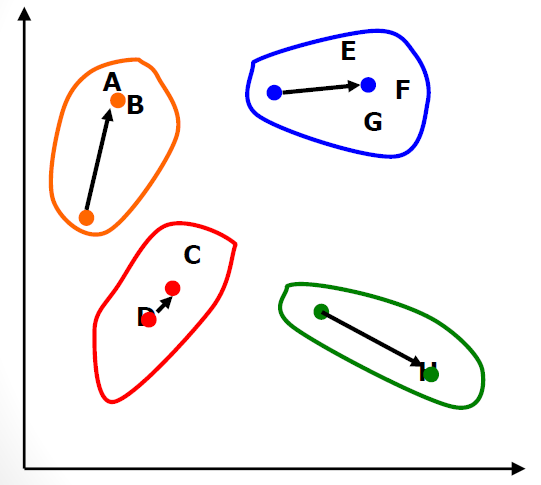


**Widzimy, że najlepszą wartością parametru „metric” jest cosine.**

**Natomiast wartości parametru „shrink\_threschold” maja znikomy wpływ na jakość modelu.**

Parametr „metric” - metryka używana podczas obliczania odległości między wystąpieniami w szyku elementów. Centroidy próbek odpowiadających każdej klasie to punkt, od którego suma odległości (zgodnie z metryką) wszystkich próbek należących do tej konkretnej klasy jest minimalizowana.

Parametr „shrink\_threshold” – próg pomniejszania centroidu w celu zmniejszenia ilości elementów.



## K-nearest neighbors

Zasadą działania metod najbliższego sąsiada jest poszukiwanie najbliższego sąsiada dla nowego obiektu o nieznanej klasie, wśród obiektów znajdujących się w zbiorze uczącym. Klasa, do której najbliższy sąsiad przynależy jest przypisywana klasyfikowanemu obiektowi.

Klasyfikator „k-najbliższych sąsiadów” jest uogólnieniem klasyfikatora najbliższego sąsiada. W jego przypadku, przynależność klasyfikowanego obiektu do klasy określana jest na podstawie znanych klas do których należy ustalona liczba „k” najbliższych sąsiadów. Klasa wynikowa odpowiada klasie dominującej w zbiorze „k-najbliższych sąsiadów".

### Test no.1

Testowanie wartości parametru „algorithm”:

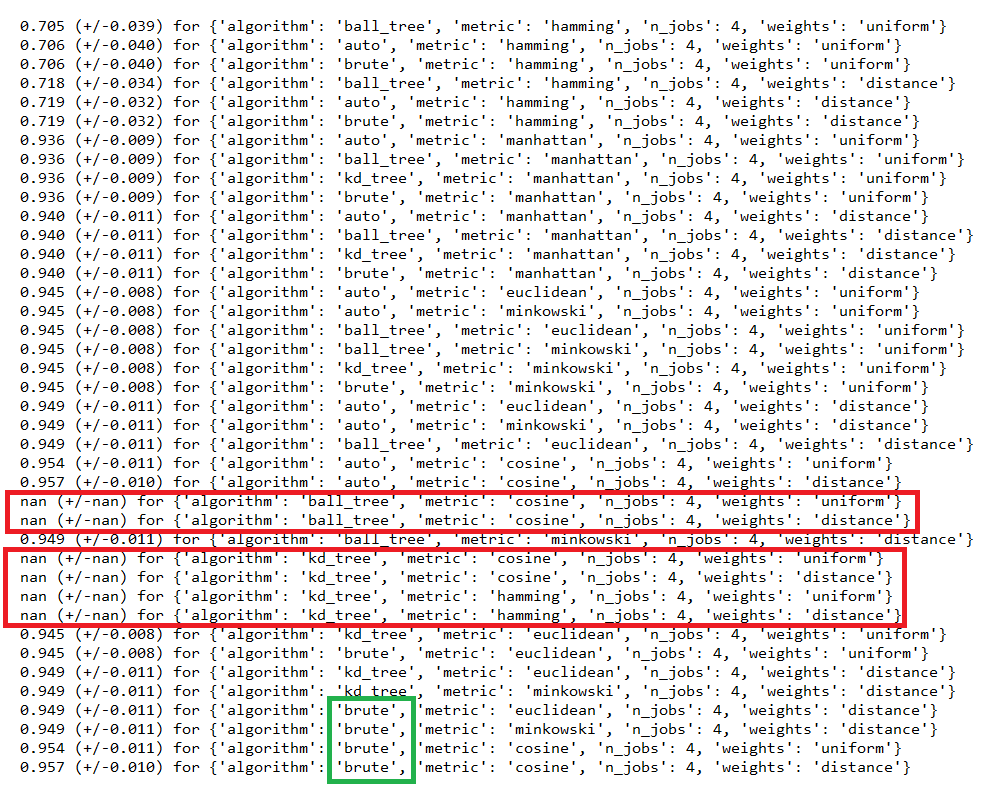
* Ball\_tree
* Auto
* Brute
* Kd\_tree

Testowanie wartosci parametru „metric”:

* Hamming
* Manhattan
* Euclidean
* Minkowski
* Cosine

Testowanie wartosci parametru „weights”:

* Uniform
* Distance



**Dla takich kombinacji parametrów programowi nie udało się stworzyć modelu.**

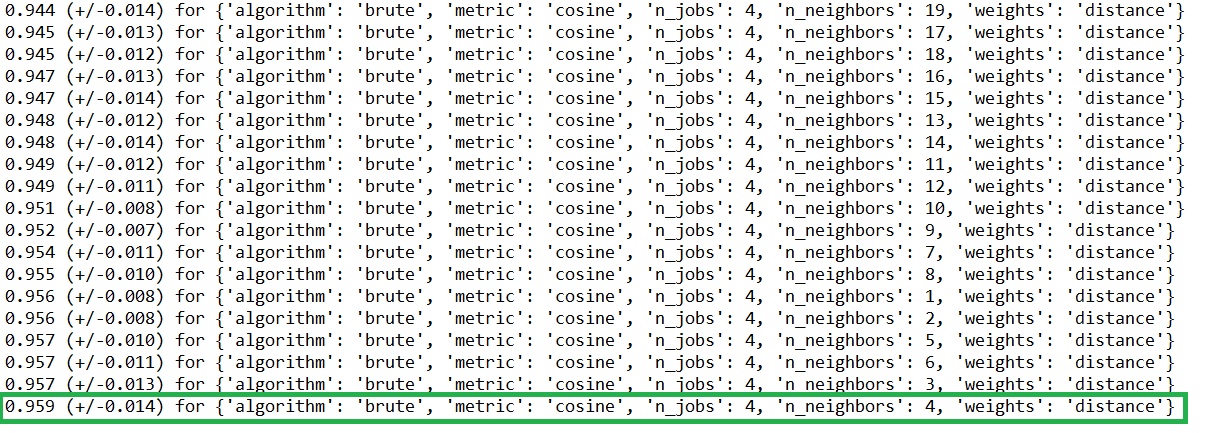
**Wartość parametru „algorithm” „brute” skutkuje najlepszymi rezultatami.**

### Test no.2

**Najlepsze wyniki są dla parametru „metric” o wartości „cosine”**

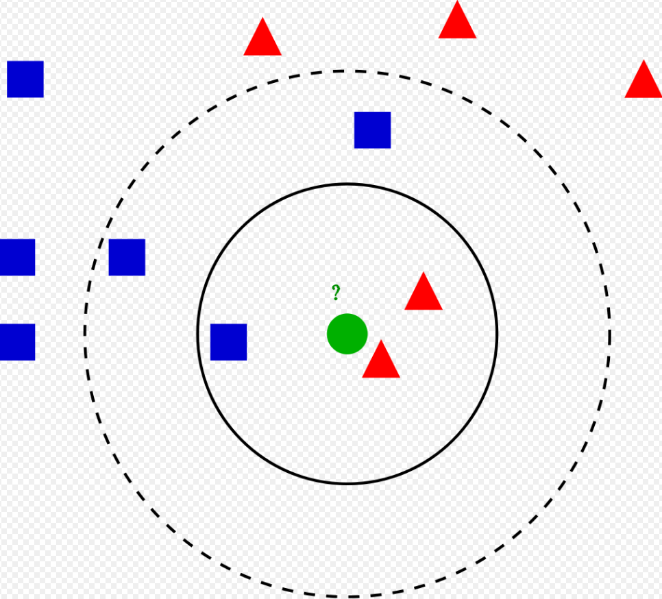
**Wartość „distance” dla parametru „weights” generuje najlepsze modele.**

### Test no.3



**„n\_neighbors” z wartością „4” to najlepszy model**

Parametr „algorithm” – jaki algorytm zostanie użyty do obliczenia najbliższych sąsiadów.

Parametr „metric” – metryka odległości dla drzewa.

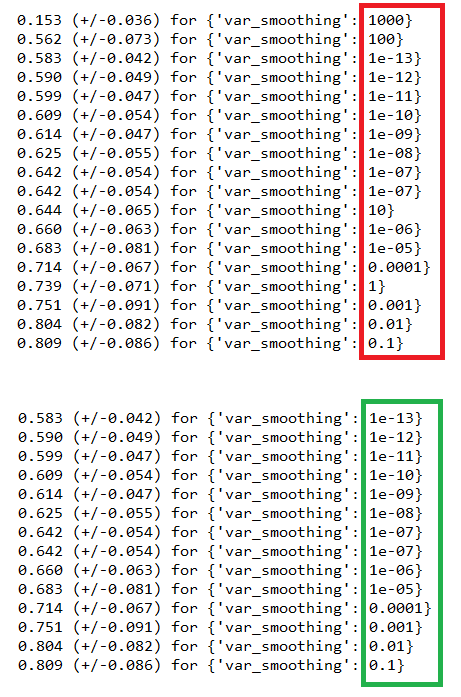
Parametr „weight” – funkcja wagi używana w prognozowaniu.

## Gaussian Naive Bayes

Przynależność obiektu do poszczególnych klas jest określana przy pomocy funkcji dyskryminacyjnych. i-ta funkcja dyskryminacyjna dla obiektu o wektorze atrybutów opisujących jest w tym przypadku tożsama prawdopodobieństwu warunkowemu przynależności obiektu do i-tej klasy pod warunkiem posiadania przez obiekt konkretnych cech. Wygodnym założeniem jest brak zależności między poszczególnymi atrybutami opisującymi. Dzięki niemu można przyjąć, że zdarzenia losowe polegające na posiadaniu przez obiekt konkretnych wartości poszczególnych atrybutów są od siebie niezależne.

### Test no.1

Testowane wartości parametru „var\_smoothing“.



**Wartości powyżej i poniżej 0,1 parametru „var\_smoothing” coraz bardziej pogarszają wynik.**

### Test no.2

**Zmniejszanie wartości przynosi skutki aż do mniej więcej 0.25 gdy rezultaty zaczynają być chaotyczne.**

„var\_smoothing“ - część największej wariancji wszystkich cech, która jest dodawana do wariancji w celu zapewnienia stabilności obliczeń.

## Gaussian process classification

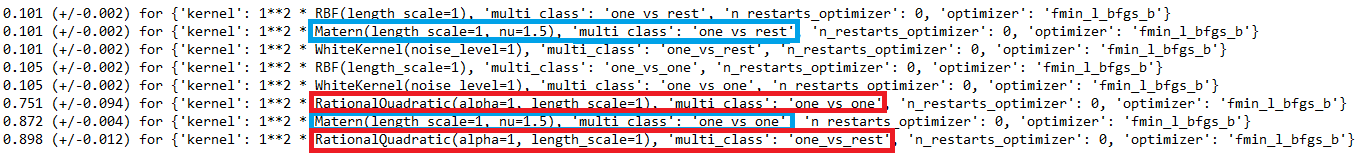
Proces Gaussa jest procesem stochastycznym (zbiorem zmiennych losowych indeksowanych w czasie lub przestrzeni), tak że każdy skończony zbiór tych zmiennych losowych ma wielowymiarowy rozkład normalny, tj. Każda skończona ich kombinacja liniowa ma rozkład normalny.

### Test no.1

Testowane wartości parametru „kernel”:

* 1\*\*2 \* RBF(length\_scale=1)
* 1\*\*2 \* Matern(length\_scale=1, nu=1.5)
* 1\*\*2 \* WhiteKernel(noise\_level=1)
* 1\*\*2 \* RationalQuadratic(alpha=1, lenght\_scale=1)

Testowanie wartości parametru „multi\_class”:

* One\_vs\_rest
* One\_vs\_one

**Obserwujemy mniejszy wpływ parametru „multi\_class” dla jądra „RationalQuadratic”. Ten parametr jest kluczowy dla dobrych wyników modelu.**

**Dla jądra „Matern” ważne żeby „multi\_class” był „one\_vs\_one”.**

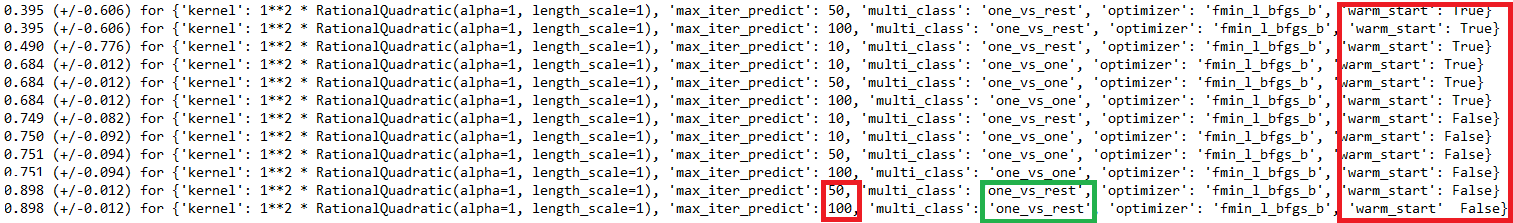
### Test no.2

Testowanie wartości parametru „max\_iter\_predict”:

* 10
* 50
* 100

Testowanie wartości parametru „warm\_start”:

* True
* False



**Parametr „warm\_start” u najlepszych modeli jest ustawiony na „false”**

**Najlepsze wyniki uzyskuje model z parametrem „multi\_class” z wartościa „one\_vs\_rest”**

„kernel” - Jądro określające funkcję kowariancji GP.

„multi\_class” - Określa, w jaki sposób są obsługiwane problemy klasyfikacji wieloklasowej.

„max\_iter\_predict” - Maksymalna liczba iteracji w metodzie Newtona aproksymacji późniejszej podczas przewidywania.

„warm\_start” - Jeśli włączone są ciepłe starty, rozwiązanie ostatniej iteracji Newtona w przybliżeniu Laplace'a trybu późniejszego jest używane jako inicjalizacja dla następnego wywołania \_posterior\_mode ().

Skuteczność tej metody jest nawet dość wysoka, jednak ogromnie duży czas jaki potrzebuje do trenowania jest nie do przyjęcia, co poskutkowało zaprzestaniem dalszych testów z nią.

## Decision tree clasifier

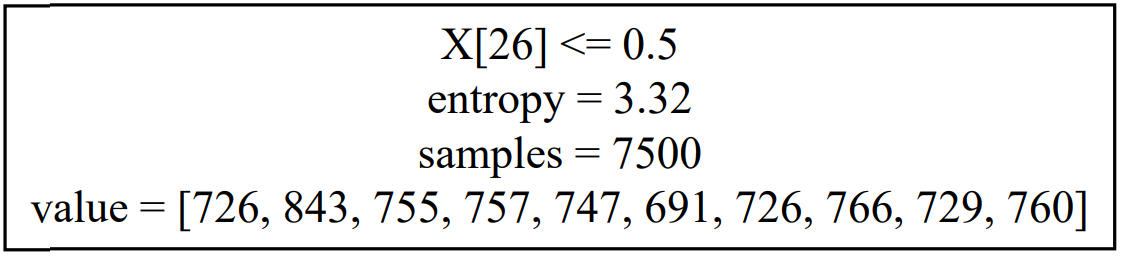
Omówmy znaczenie atrybutów opisujących na podstawie zbioru Tytanic Data Set który zawiera informacje o pasażerach, takie jak klasa podróżna czy też wiek. Celem klasyfikacji jest odgadnięcie czy pasażer przeżył.

W tym zbiorze w korzeniu drzewa atrybutem opisującym jest płeć. Ponieważ najpierw ratowane kobiety to przeżyło ich znacznie więcej. Jest to także bardzo dobry podział pasażerów na dwie grupy.

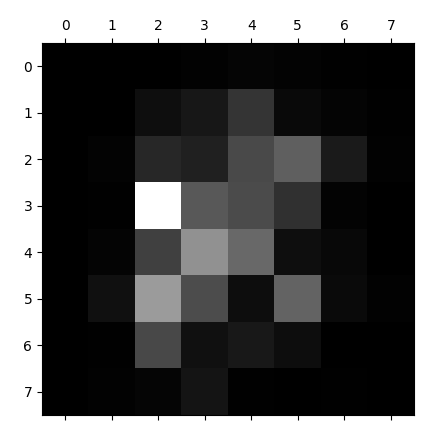
Dzięki temu podziałowi zyskujemy jak najwięcej informacji.

Drzewa decyzyjne są strukturą grafowa przedstawiającą zależności między atrybutami obiektów. Dzięki hierarchicznej reprezentacji tych zależności drzewo nie tylko jest klasyfikatorem, ale także umożliwia analizę istotności poszczególnych atrybutów w klasyfikacji konkretnego zbioru danych.

Jak to wygląda w drzewie decyzyjnym którego atrybutami są pojedyncze piksele? Szukamy piksela, który często występuje w jednej z grup liczb.

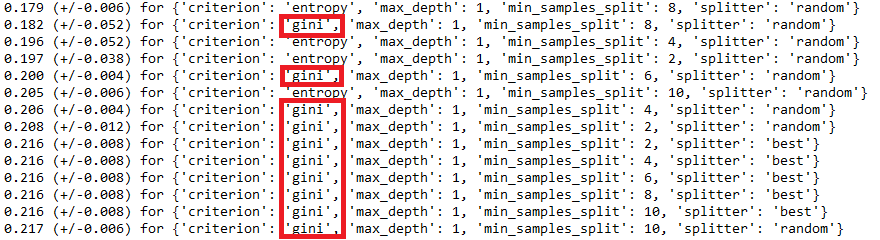


Poniżej zamieszczona jest grafika obrazująca wagę atrybutów. Widzimy na niej biały piksel w 2 kolumnie 3 rzędu. Nasze dane przechowujemy w liście o długości 64(8x8) indeksowanej od 0, dlatego element o indeksie 26 to nasz biały kwadrat. Ma największą wagę, ponieważ dokonuje największego podziału danych. Możemy więc powiedzieć, że ten piksel jest różnicą pomiędzy dwoma połowami naszych danych. Co za tym idzie, ten wykres przedstawia nam najważniejsze piksele obrazu.

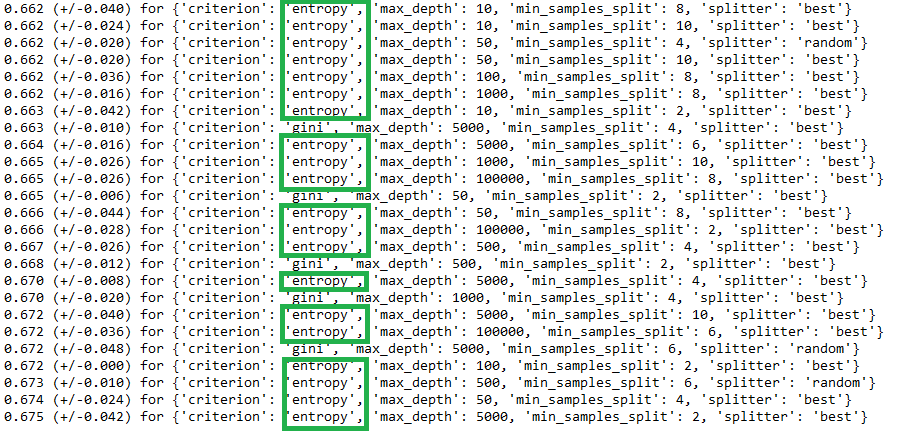


### Test no.1

Testowanie wartości parametru „criterion”:

* Entropy
* Gini

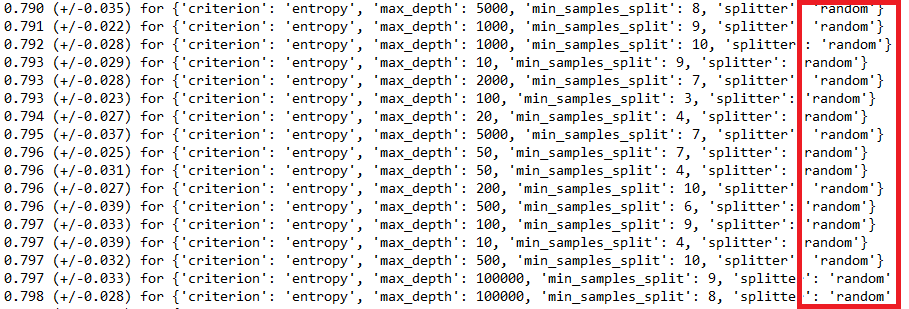
**Najgorsze modele powstają przy parametrze „criterion” dla wartości „gini”**



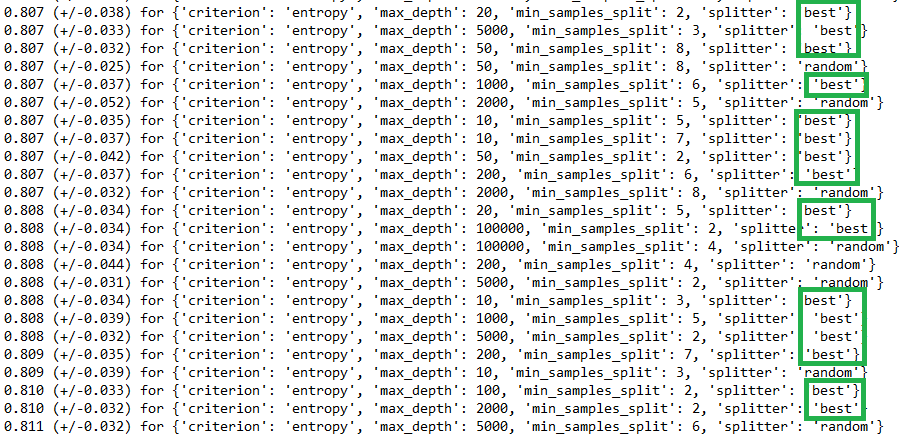
**Natomiast najlepsze dla „entropy”**

### Test no.2

Testowane wartości „splitter”:

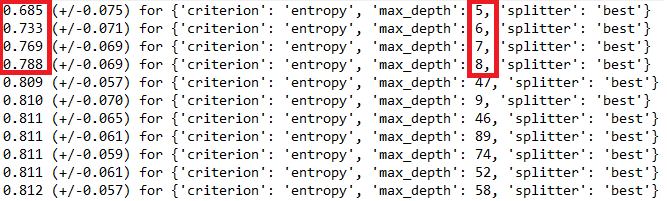
* Random
* Best

**Parametr „splitter” z wartością „random” nie jest najlepszym generuje najlepszego modelu**

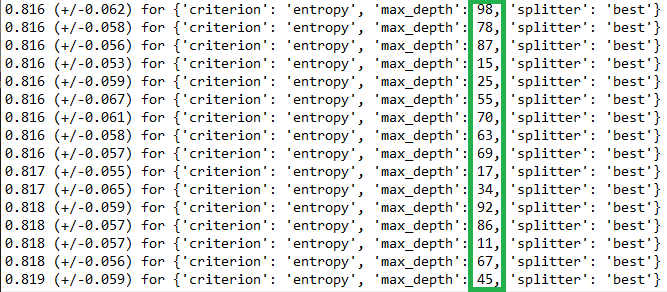


**Najlepsze wyniki uzyskuje model z parametrem „splitter” z wartością „best”**

### Test no.3

Testowanie wartości parametru „max\_depth”: od 5 do 100

**Wartości parametru „max\_depth” poniżej 10 coraz bardziej obniżają jakość modelu.**



**W przedziale wartości od 10 do 100 dla parametru „max\_depth” nie obserwujemy większej zależności.**

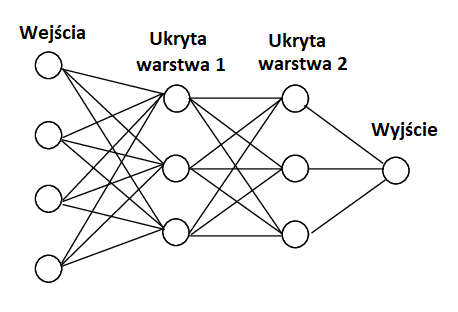
„criterion” – Funkcja do pomiaru jakości podziału.

„max\_depth” – maksymalna głębokość drzewa.

„splitter” – Strategia użyta do wyboru podziału w każdym węźle.

## Sieć neuronowa czyli Multi-Layer-Perceptron

MLP składa się z co najmniej trzech warstw węzłów: warstwy wejściowej, warstwy ukrytej i warstwy wyjściowej. Z wyjątkiem węzłow wejściowych, każdy węzeł jest neuronem wykorzystujący nieliniową funkcję aktywacji. MLP wykorzystuje technikę nadzorowanego uczenia się zwaną wsteczną propagacją do treningu.



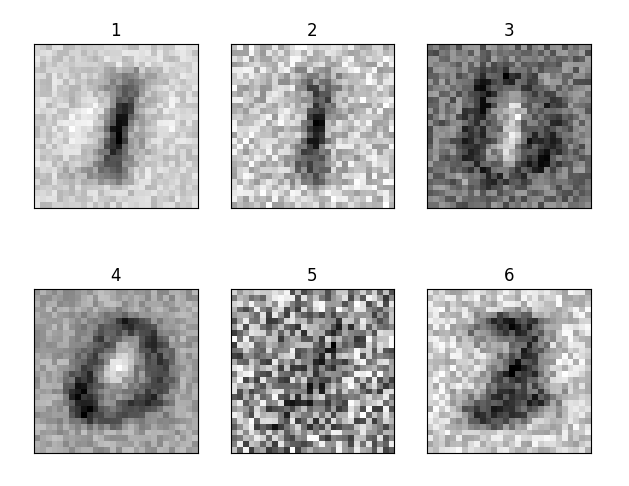
Wartości na węzłach na poprzedniej warstwie są mnożone przez współczynniki na połączeniach a następnie sumowanie jako wartość węzła. Ten proces jest powtarzany aż w końcu otrzymamy wynik. Gdy zadaniem naszego modelu jest klasyfikacja, wyjść może być wiele i zazwyczaj wartości na węzłach odpowiadają „pewności” że taki jest wynik. W naszym wypadku model może podejrzewać z dużą pewnością że jakaś liczba to 8 oraz 0. Wybierany jest najpewniejszy wynik. Niestety jednak komputer „nie widzi” liczb tak jak my i dla dużej ilości węzłów oraz warstw trudno zrozumieć działanie poszczególnych węzłów.

Zagadnienie sieci neuronowych oraz algorytmów używanych do ich działania oraz trenowania mogły by na osobności stanowić temat obszernego projektu. Z racji na ograniczony procent treści merytorycznej dokładniejsze objaśnienie mija się z celem.

Sprawdźmy to za pomocą wartości współczynników dla atrybutów dla każdego węzła. W ten sposób możemy zobaczyć co najbardziej wpływa na wartość naszego węzła.

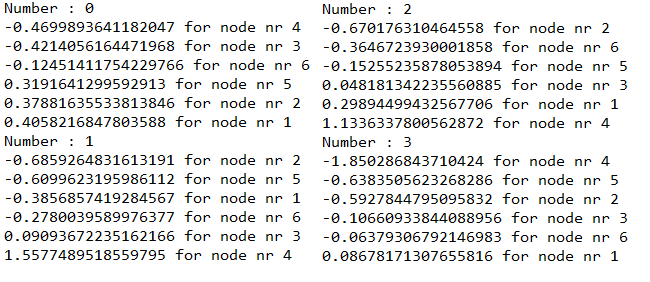
Poniżej przedstawione są wyniki dla modelu o 6 warstwach, uwzględniającego 4 klasy czyli cyfry od 0 do 3.

Oto 6 wykresów przedstawiających 6 węzłów. Obraz który widzimy to współczynniki dla każdego atrybutu(‘piksela’). To nie są liczby ze zbioru MINST, człowiek tych cyfr nie napisał. To co widzimy to percepcja modelu.



No dobrze więc gdzie tutaj jest 3? No nie ma. Według naszego spojrzenia nie ma jej tutaj. Ale to nie my decydujemy, tylko komputer.

Obejrzyjmy wartości współczynników dla wyjść. Mamy 4 cyfry czyli 4 wyjścia. Wypisujemy współczynniki powiązania węzłów ukrytej warstwy z wyjściami.



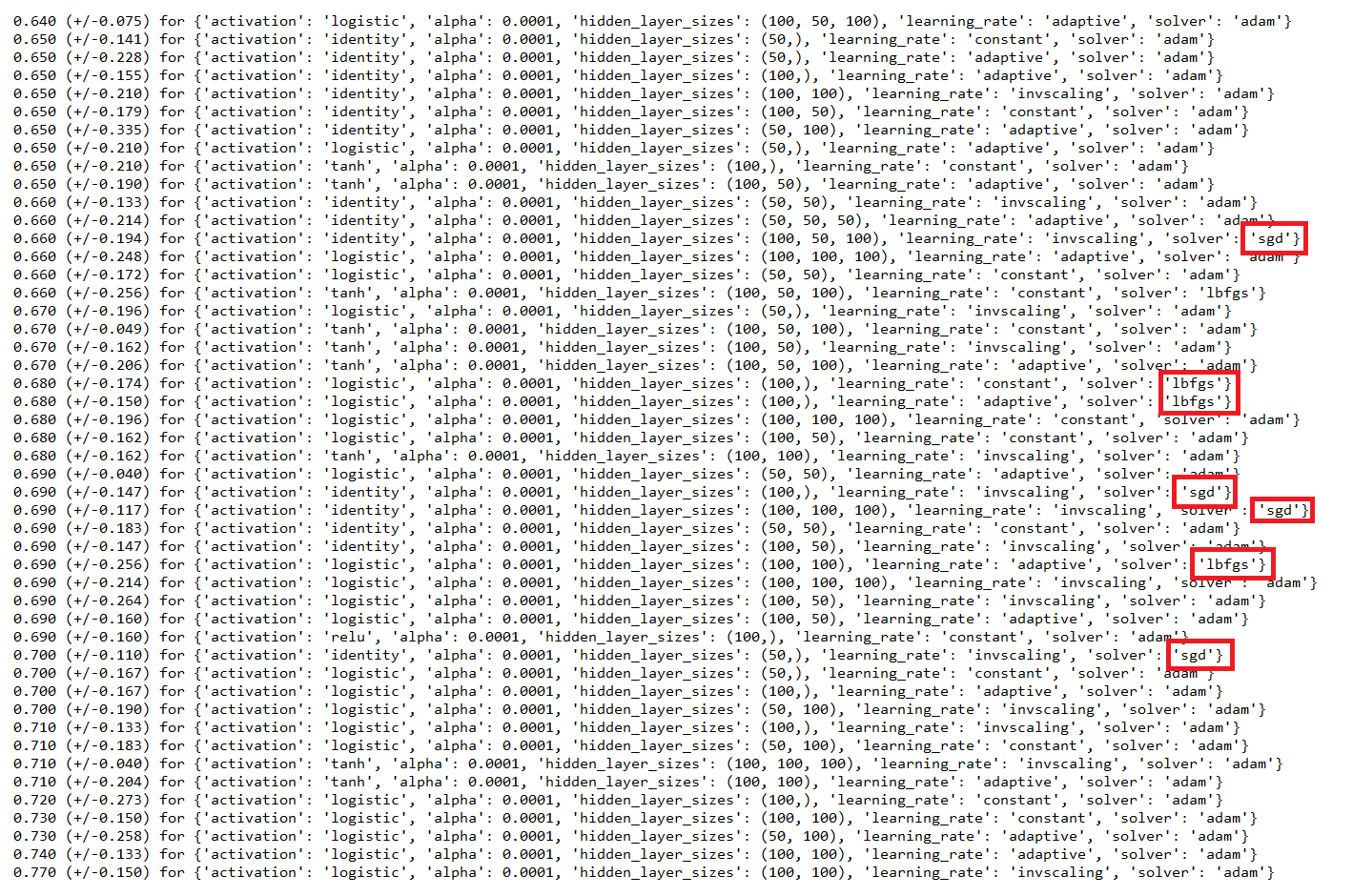
Z tych danych wyczytujemy że za uzyskanie odpowiedzi: 1 najbardziej odpowiadają węzły 2,5,1 , co ma sens, na obrazie węzła 5 trudno spostrzec cokolwiek, ale na 1 i 2 widzimy jedynkę.

Za zero odpowiada natomiast 4,3 i widzimy tam okrągły kształt.

### Test no.1

Testowane wartości parametru „solver”:

* Adam
* Sgd
* Lbfgs



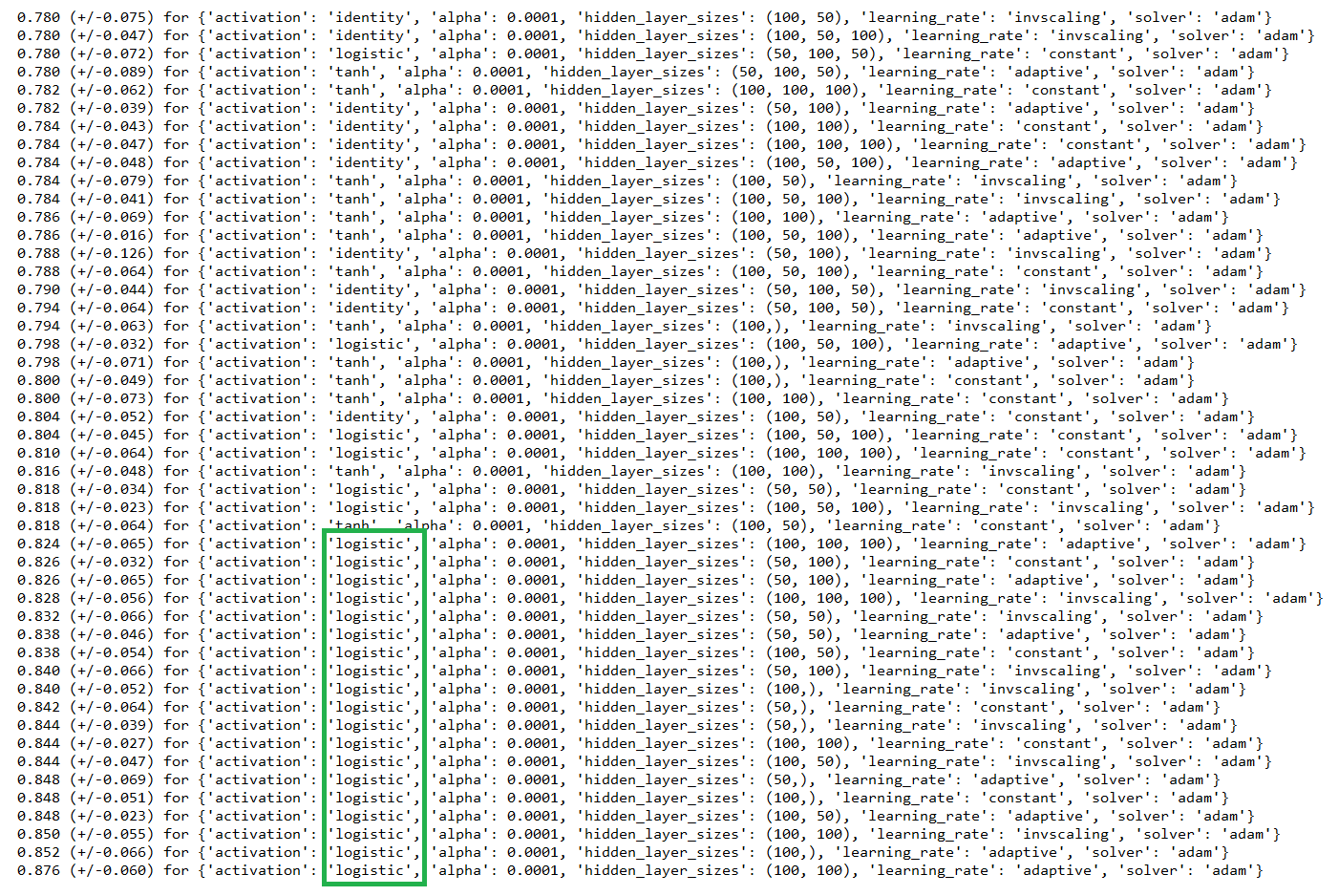
**Inne wartości dla parametru „solver” niż „adam” nie generują najlepszych modeli.**

(„solver” z wartością „adam” nie wymaga doprecyzowania parametru „learning\_rate”)

### Test no.2

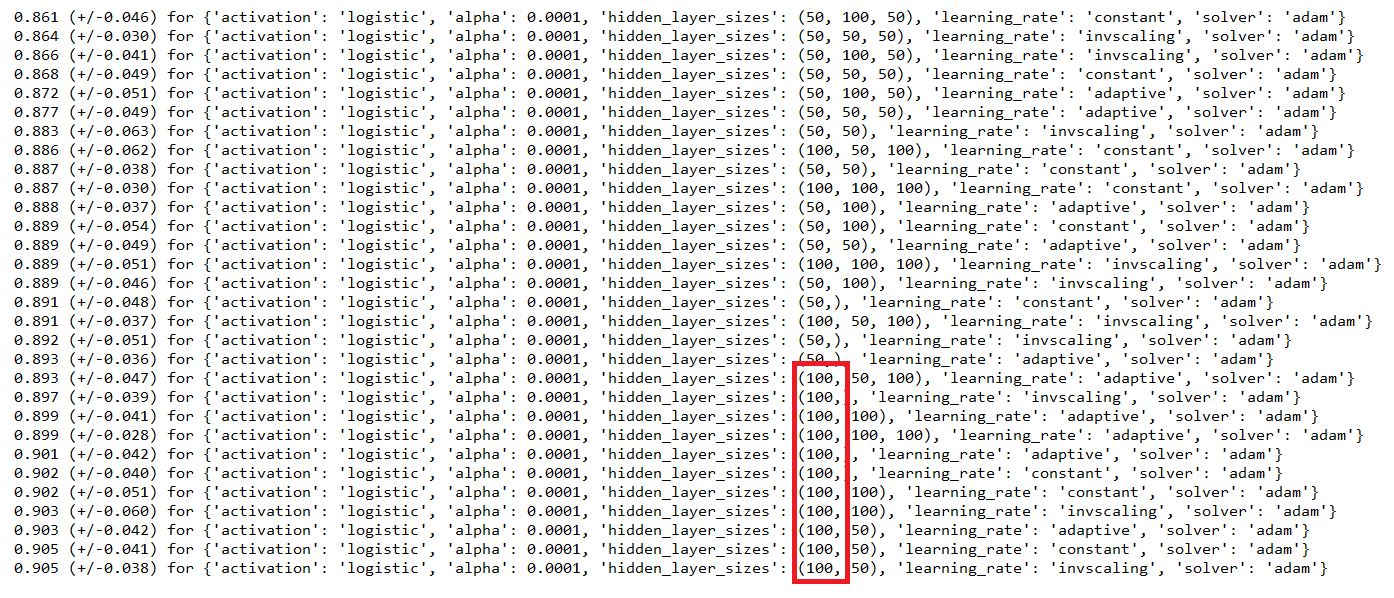
Testowanie wartości parametru „activation”:

* Tanh
* Identity
* Logistic
* Relu



**W przedziale wartości od 10 do 100 dla parametru „max\_depth” nie obserwujemy większej zależności.**

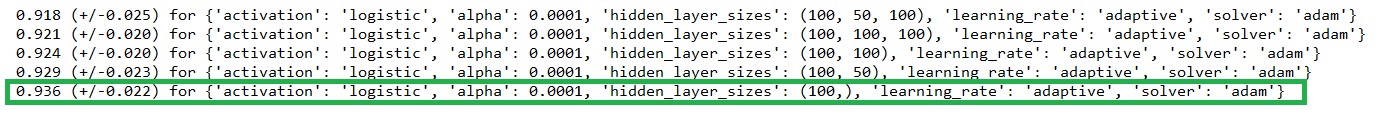
### Test no.3



**Pierwsza ukryta warstwa powinna zawierać 100 neuronów.**

### Test no.4

**Najlepszy model jest dla jednej ukrytej warstwy o wartości 100**

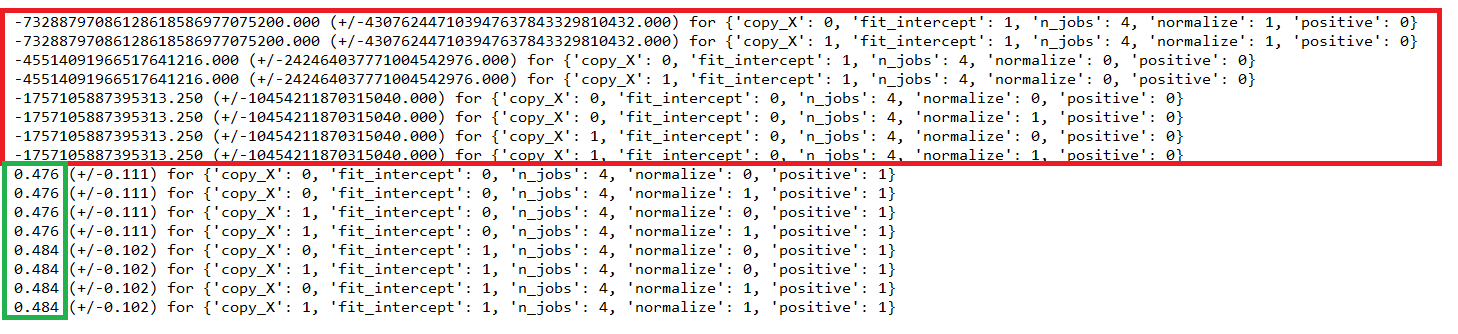


## Linear Regression

Miara korelacji (Pearsona) pozwala na stwierdzenie stopnia zależności liniowej atrybutów (cech).

Test no.1

Testujemy wartości parametru „positive”: 0 lub 1



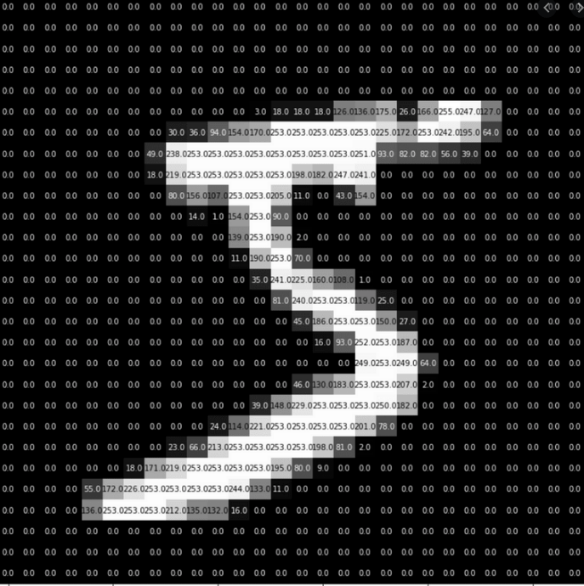
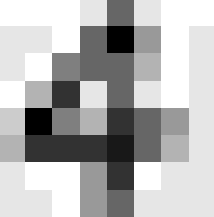
**Widzimy, że wartość parametru „positive” musi być ustawiona na 1, żeby model w ogóle działał.**

**Rozwiązanie problemu metodą regresji liniowej jest wyjątkowo nieefektowne**

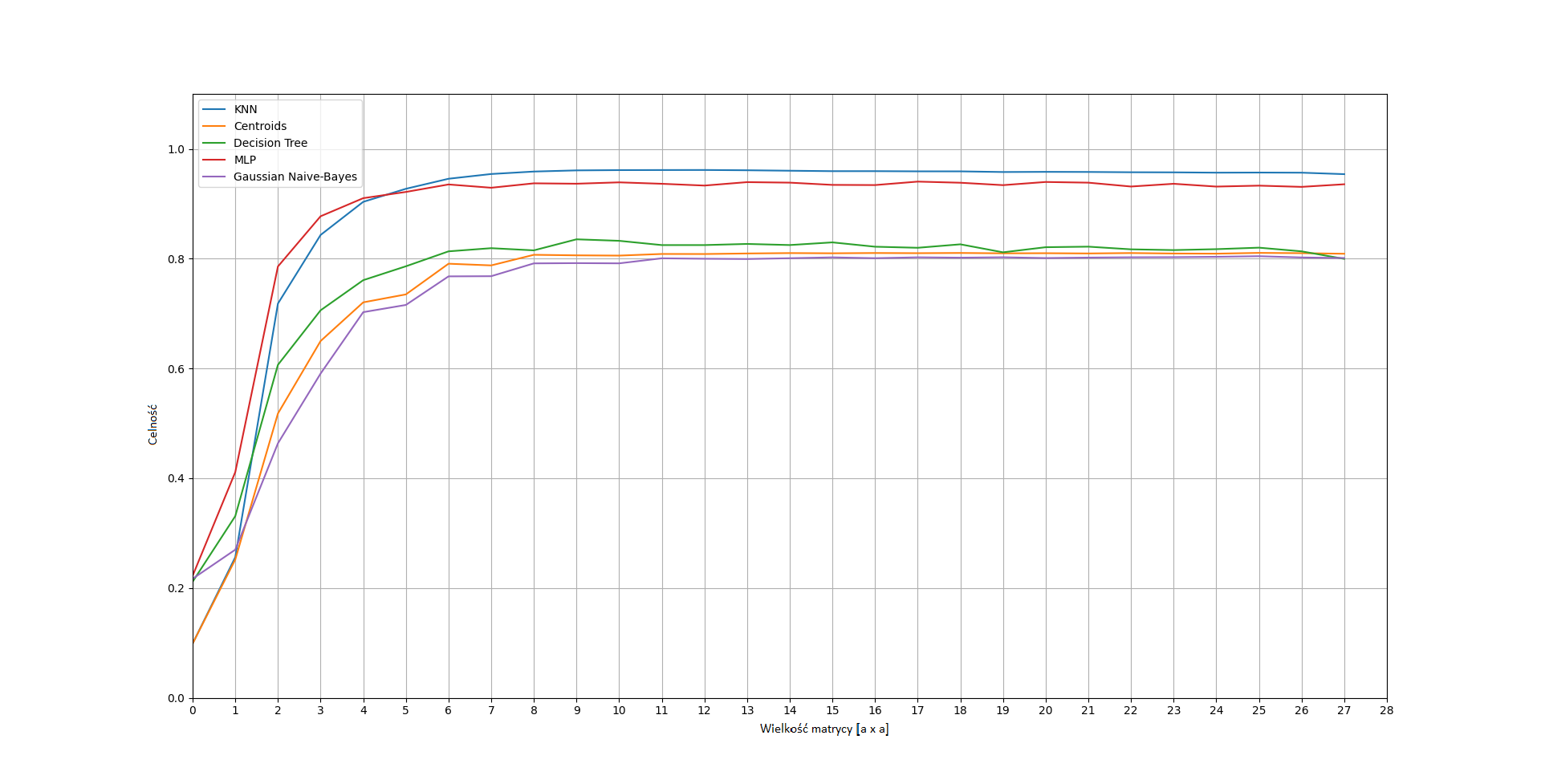
Żeby rozwiązywanie problemu metodą liniową miało sens powinniśmy mocno zmienić dane wejściowe.

# 3. Analiza uzyskanych wyników

W celu minimalizacji czasu jaki metoda będzie potrzebowała do wyprodukowania wyniku na oryginalnych danych można przeprowadzić kompresję.

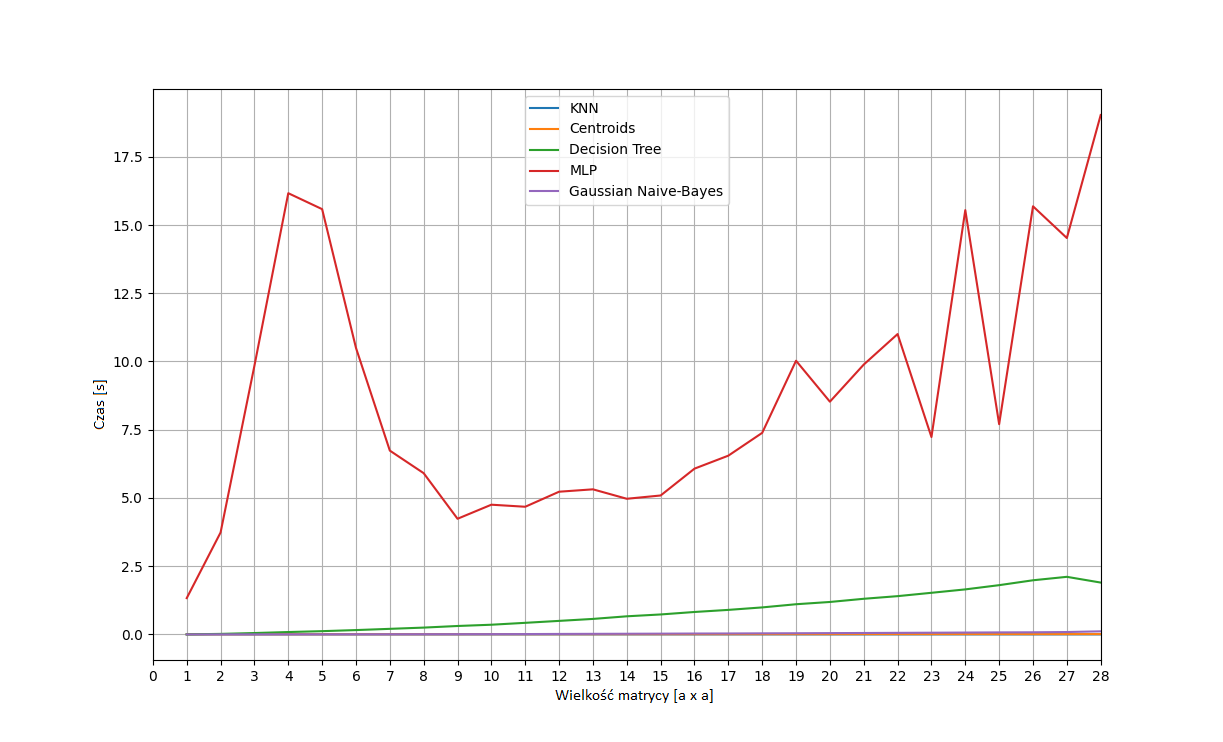


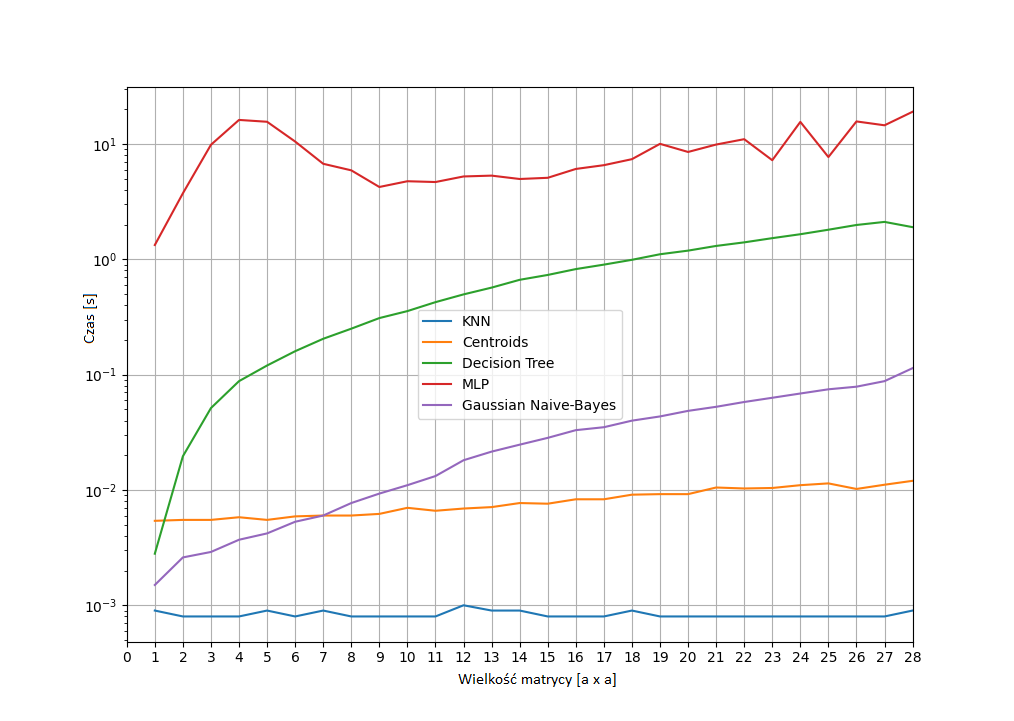
Początkowo zdjęcie jest matrycą 28\*28 pikseli w skali szarości. Więc łatwo się skaluje, bo mamy tylko jedną wartość w pikselu z których później liczymy średnią arytmetyczną i znajdujemy nowe mniejsze piksele.



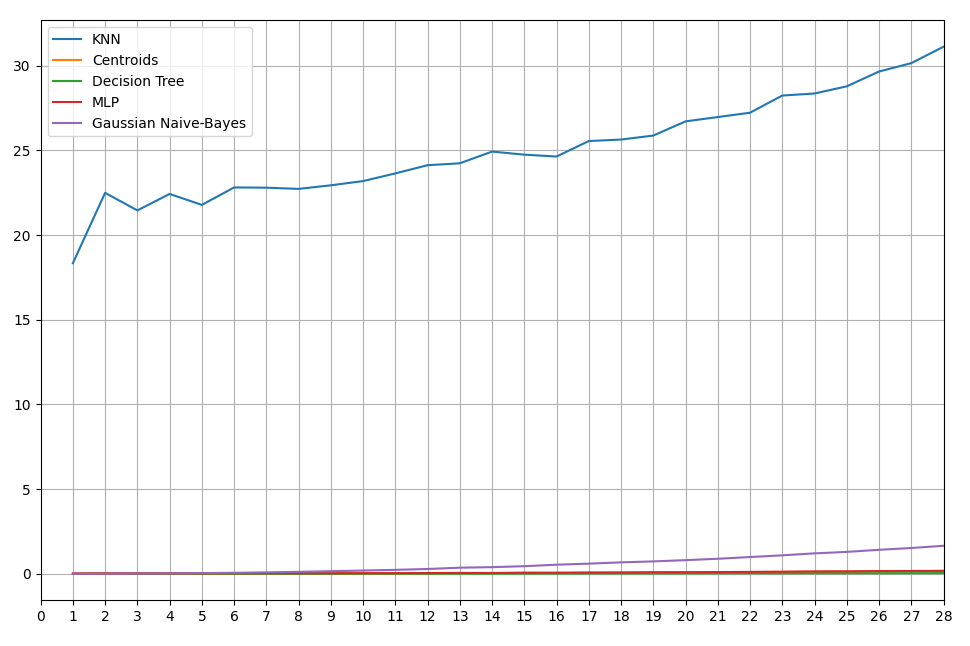
Z tego wykresu widzimy, że większość metod poprawnie działa gdy mają co najmniej 8\*8 pikseli.

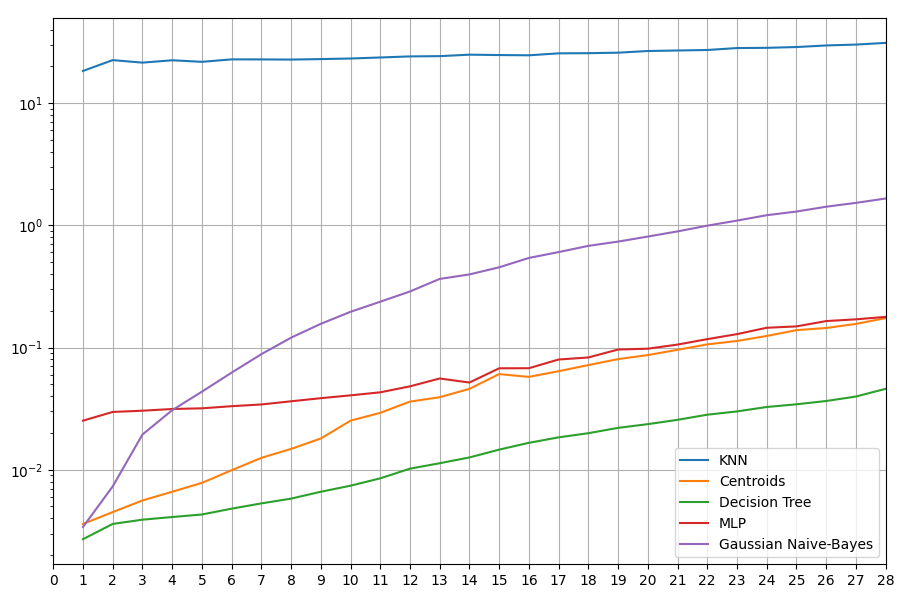
Widzimy także, że najlepiej spisuje się metoda k – średnich sąsiadów. Jednak w przedziale, gdy mamy małą matryce MLP radzi sobie znacznie lepiej. Skuteczność tych metod jest powyżej 93%. Istnieje także druga grupa metod złożona z Decision Tree, Gaussa i Cetrodów, których skuteczność oscyluje wokół 80%.

Na pierwszym wykresie dobrze widać, że MLP potrzebuje dużo czasu i nie koniecznie wprost proporcjonalnego do ilości danych.   
Także widzimy, że drzewo decyzyjne lekko wzrasta sugerując zlożoność super liniową.



Dzieję się tak, ponieważ zarówno MLP, jak i drzewo decyzyjne, wymagają trenowania na danych. Pozostałe modele tego treningu nie potrzebują.

Z kolei na tym wykresie obserwujemy, że modele które nie polegają na treningu mają znacznie dłuższe czasy klasyfikacji. Ta zależność jest jednym z powodów, dlaczego istnieje tak wiele modeli, a także tak wiele z nich nadal jest używanych.



Drugi wykres znacznie lepiej obrazuje różnice najlepszych modeli. Widzimy że drzewo decyzyjne działa jak zakładano, po czasie około liniowym. Metoda Gausowska natomiast bardzo szybko powoduje duże opóźnienia.

Moglibyśmy wyobrazić sobie sytuację, w której potrzebny byłby model potrafiący zgadywać niemal natychmiastowo po otrzymaniu danych wstępnych. Z kolei na drugiej stronie spektrum widzimy modele, które utworzone raz błyskawicznie przewidywałyby nowe wpływające dane.

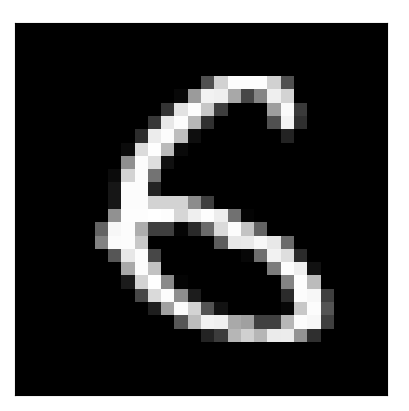
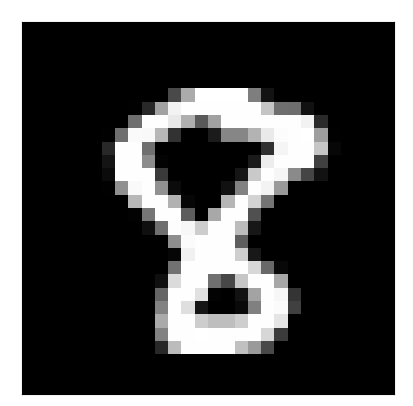
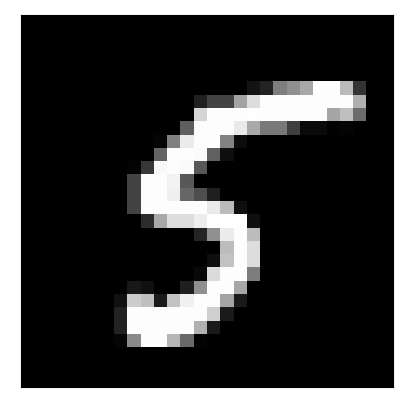
## Najlepszy model

Na podstawie naszych wyników widzimy, że najlepszą celność posiada model KNN (K-nearest neighbors) z parametrami n\_neighbors = 4, weights = 'distance', algorithm = 'brute', metric = 'cosine'. Ponieważ model ten nie wymaga prawie żadnego trenowania, to możemy go niemal natychmiastowo utworzyć. Oczywiście możemy spodziewać się, że modele takie jak drzewo decyzyjne będą o wiele szybciej dokonywać klasyfikacji.

# 4. Używanie modeli do przywidywania cyfr

## Udane próby klasyfikacji

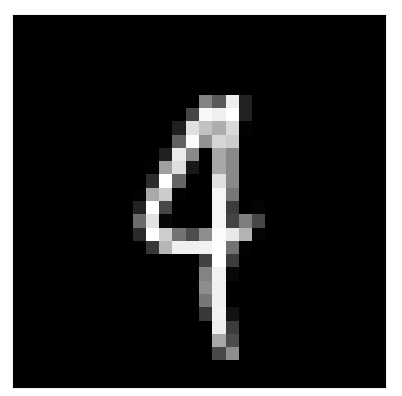
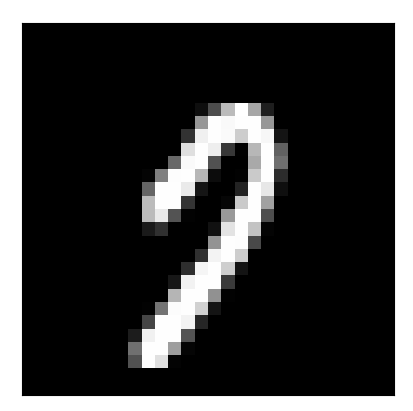
Poniżej są przedstawione udane klasyfikacje przy użyciu wybranego modelu.



Myślę, że wyniki są naprawdę niezwykłe. Głupia maszyna zdaję się przejawiać zrozumienie, inteligencję. Tym bardziej, że większość z tych testów osądzana jest szybciej, niż mógłby to wykonać człowiek.

## Nieudana próba klasyfikacji

Zobaczmy teraz kiedy program popełnia błędy. Poniżej znajdują się 3 przykłady niepoprawnie oszacowanych cyfr.



Pierwsza cyfra została przewidziana jako 8, jednak według autora jest to 3. Widzimy, że górny ogonek trójki złączył się ze środkowym. Gdyby jeszcze połączyć środkowy z dolnym, to wyszłaby dość wyraźna ósemka. Mimo że widzimy tam przerwę trzeba pamiętać, że żaden z modeli nie polega na kształcie jako element decyzyjny. W większości wypadków jest to pokrycie otrzymanego obrazu z idealnym wzorcem danej liczby.

Drugi obrazek ma zestaw przewidziany jako 9, natomiast oryginalne jest to 7. Przeciętny człowiek również z pewnością miałby problemy z określeniem tego przypadku. Jednak nie byłby to spor pomiędzy 7 i 9 a miedzy 7 i 1. Ta różnica jest spowodowana innym sposobem określania cyfry, człowiek patrzy na kształt, a nasz program na jasność konkretnych pikseli.

Tutaj wyjaśnia się absurdalny przypadek cyfry 4 podobnej. Program na tym obrazku „zobaczył” 9, co jest logiczne biorąc pod uwagę, że zmiana jasności pikseli jest wręcz identyczna do zmian jasności występujących u typowych przypadków cyfry 9. Jedyna różnica to mały koniuszek lekko występujący poza linie poziomą. Dla ludzkiego oka to jest oczywisty sygnał, a dla programu mały szczegół.

1. http://yann.lecun.com/exdb/mnist/ [↑](#footnote-ref-1)