به نام خدا



دانشگاه صنعتی خواجه نصیرالدین



دانشکده برق

یادگیری ماشین

گزارش تمرین شماره ۳

شیما سادات ناصری

4.117.114

دکتر مهدی علیاری شوره دلی

فهرست مطالب

شماره صفحه			(عنوان
٣	 	 	 ۲	سوال
λ	 	 	 ۳۳	سوال
λ			 	. ۱
٩				
٩				۳.
١٣				
14	 	 	 	۴.
۱۵				
١٧		 	 ع	مراجا

سوال ۲

روش GenSVM یک رویکرد جدید برای پرداختن به مشکلات طبقه بندی با بیش از دو کلاس را نشان می دهد. در حالی که ماشینهای بردار پشتیبان سنتی (SVM) در تمایز بین دو دسته برتری دارند، زمانی که با دستههای متعدد مواجه میشوند، کارایی کمتری دارند. GenSVM یک راه حل جدید برای رسیدگی موثر به این مشکل چند کلاسه ارائه می دهد.

بخشهای مهم این روش و نوآوریهای آن به صورت زیر است:

• رمزگذاری Simplex:

موقعیتی را در نظر بگیرید که در آن سه نوع گل مختلف برای طبقه بندی دارید. به جای استفاده از یک mais برای نمایش این کلاس ها استفاده می کند.

"سیمپلکس" نسخه پیشرفته تر مثلث یا چهار وجهی است. برای سه طبقه، شبیه قرار دادن هر نوع گل در گوشه های یک مثلث متساوی الاضلاع است. این روش تضمین می کند که کلاس ها به طور مساوی فاصله دارند و به راحتی قابل تشخیص هستند.

• تابع ضرر

GenSVM از یک تابع hinge استفاده می کند که در SVM ها رایج است. طبقهبندیهای اشتباه را جریمه میکند، اما با کمی انعطافپذیری، به آن اجازه میدهد تا بر اساس مجموعه دادههای مختلف تنظیم شود.

در فرایند آموزش، مدل مقادیر بهینه ماتریس وزن W و بردار بایاس t را می آموزد. برای هر نقطه داده، مدل موقعیت خود را در فضای سیمپلکس محاسبه می کند.

در صورتی که مدل پیش بینی نادرستی انجام دهد، تابع ضرر جریمه قابل توجهی را اعمال می کند. این شامل هم از دست دادن لولا و هم یک اصطلاح منظم سازی برای جلوگیری از برازش بیش از حد می شود، که فرآیند برازش مدل بسیار نزدیک به داده های آموزشی است.

• بهینه سازی

بهینه سازی فرآیند شناسایی مقادیر بهینه برای پارامترهای مدل ما برای به حداقل رساندن خطاها است. GenSVM این فرآیند را با پرداختن مستقیم به شکل اولیه مسئله بهینه سازی (یعنی کار با مشکل

اصلی به جای نسخه پیچیده تر) ساده می کند. از یک الگوریتم عمده سازی تکراری استفاده می کند که شامل ایجاد مکرر یک نسخه ساده شده از مسئله، حل آن و استفاده از راه حل برای بهبود نسخه بعدی است. این شبیه به بالا رفتن از یک تپه با برداشتن گام های کوچک و قابل کنترل به جای تلاش برای پرش مستقیم به قله است.

پس از آموزش، مدل می تواند نقاط داده جدید را با نگاشت آنها به فضای سیمپلکس و پیدا کردن نزدیکترین کلاس پیش بینی کند.

پیاده سازی مدل در هر بخش به صورت زیر است.

• بخش رمز گذاری:

```
def _simplex_coordinates(self, K):
    U = np.zeros((K, K - 1))
    for k in range(K):
        | if k > 0:
        | U[k, :k] = -1 / np.sqrt(k * (k + 1))
        if k < K - 1:
        | U[k, k] = k / np.sqrt((k + 1) * (k + 2)) # Avoid division by zero and invalid values
    return U</pre>
```

K- با استفاده از این کد، مختصات سیمپلکس مورد استفاده برای رمزگذاری کلاس ها در فضای بعدی 1 ساخته می شود.

• بخش آموزش (تابع ضرر و بهینه سازی):

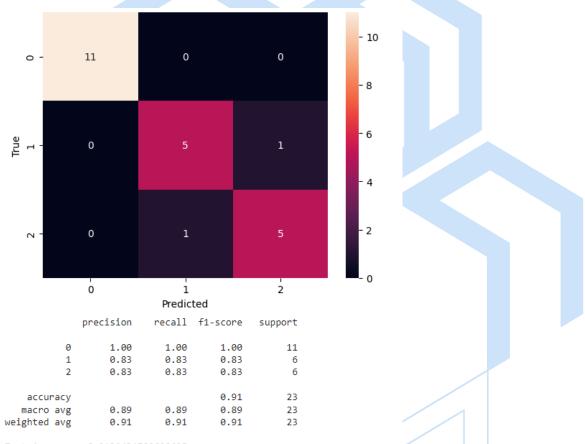
```
def fit(self, X, y, rho):
    n_samples, n_features = X.shape
     classes = np.unique(y)
n_classes = len(classes)
     self.classes_ = classes
     # Initialize weights and bias
     U = self. simplex coordinates(n classes)
     def loss(params):
          W = params[:n_features * (n_classes - 1)].reshape(n_features, n_classes - 1)
t = params[n_features * (n_classes - 1):]
           loss = 0.0
           yi = y[i]
si = np.dot(xi, W) + t
                q = np.array([si@(U[yi] - U[j]) for j in range(n_classes) if j != yi]) hinge_loss = np.sum(np.maximum(0, 1 - q)**self.p) loss += rho[i] * hinge_loss
          loss /= n_samples
loss += self.lambd * np.sum(W**2)
          return loss
     initial_params = np.hstack([self.W.ravel(), self.t])
     result = minimize(loss, initial_params, method='L-BFGS-B', tol=self.epsilon, options={'maxiter': self.max_iter})
self.W = result.x[:n_features * (n_classes - 1)].reshape(n_features, n_classes - 1)
self.t = result.x[n_features * (n_classes - 1):]
```

¹ Iterative Majorization Algorithm

روش برازش پارامترهای مدل را آغاز می کند و بهینه سازی را انجام می دهد. سپس برنامه با استفاده از تابع _simplex_coordinates مختصات سیمپلکس را محاسبه می کند.

همانطور که در مقاله توضیح داده شده است، تابع ضرر به عنوان یک افت لولا با یک اصطلاح منظم تعریف می شود. تابع Minimize از scipy.optimize برای به حداقل رساندن تلفات و شناسایی مقادیر بهینه \mathbf{W} و \mathbf{t} استفاده می شود.

نتایج این پیاده سازی پس از جدا کردن داده آموزش و تست از هم به صورت زیر است:



Test Accuracy: 0.9130434782608695 Test Recall: 0.9130434782608695

Test F1-score: 0.9130434782608695 Test Precision: 0.9130434782608695

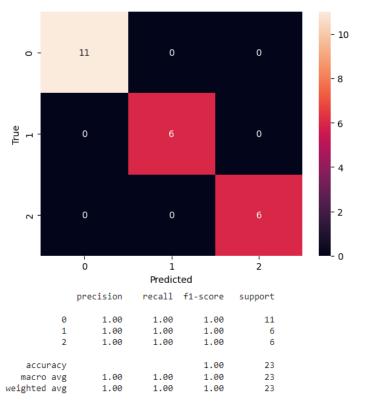
با مقایسه نتایج بدست آمده با نتیجه مقاله، مشاهده می شود نیاز است تا براساس مقاله از gridsearch با مقایسه نتایج بدست آمده با نتیجه مقاله، مشاهده می شود نیاز است تا بهترین پارامتر استفاده کنیم. این متد را با کمک gridsearch اما با بازههایی آزادانه تر بررسی می کنیم تا بهترین پارامتر را پیدا کنیم. کد به صورت زیر است:

```
1 from sklearn.metrics import accuracy_score
 3 # Define parameters
 4 rho = np.ones(X_train.shape[0])
 5 from sklearn.model selection import GridSearchCV
 6 from sklearn.metrics import make_scorer, accuracy_score
 8
     # Define a custom scorer
 9
     accuracy_scorer = make_scorer(accuracy_score)
10
11
    # Define the parameter grid
12
     param_grid = {
        'C': [0.1, 1.0, 10.0],
13
         'p': [1.0, 2.0],
14
15
        'kappa': [0.1, 0.5, 1.0],
        'lambd': [0.01, 0.1, 1.0],
16
        'epsilon': [1e-6, 1e-4, 1e-2]
17
18
19
20
    # Initialize the grid search with cross-validation
21
     grid_search = GridSearchCV(GenSVM(), param_grid, scoring=accuracy_scorer, cv=5 , verbose=2)
22
23
    # Fit the grid search on the training data
24
     grid_search.fit(X_train, y_train, rho=rho)
25
    # Get the best parameters and the best score
26
27
     best_params = grid_search.best_params_
28
    best_score = grid_search.best_score_
29
30 print("Best parameters found: ", best_params)
31
    print("Best cross-validation accuracy: {:.2f}".format(best_score))
32
33
    # Predict and evaluate on the test set using the best parameters
    best_model = grid_search.best_estimator_
35
    y_pred = best_model.predict(X_test)
```

بهترین پارامتر بدست آمده به صورت زیر است:

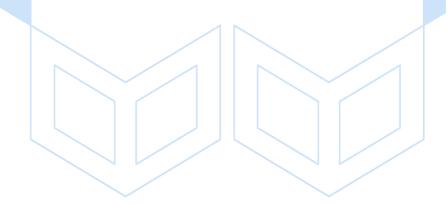
Best parameters found: {'C': 0.1, 'epsilon': 1e-06, 'kappa': 0.1, 'lambd': 0.01, 'p': 2.0}





Test Accuracy: 1.0 Test Recall: 1.0 Test F1-score: 1.0 Test Precision: 1.0

نتیجه بدست آمده نشان میدهد که برای دیتاست ایریس، مقادیر بدست آمده کاملا مناسب است. از طرف دیگر زمان آموزش برای این دیتاست کوتاه بود و توانسته به صورت کامل دیتای تست را که در فرایند آموزش نبوده را طبقه بندی کند.



سوال ۳

١

• دادههای نامتوازن

یکی از بزرگترین چالشها در تشخیص تقلب، نامتوازن بودن شدید دادهها است، بهطوری که تراکنشهای تقلبی درصد بسیار کمی از کل تراکنشها را تشکیل میدهند. این نامتوازن بودن باعث میشود که مدلهای طبقهبندی سنتی نتوانند به طور مؤثر تقلب را تشخیص دهند، زیرا تمایل به تشخیص کلاس اکثریت دارند. برای رفع این موضوع ۲ راهکار عمده وجود دارد، یا باید از کلاس بزرگتر دادهها برای آموزش حذف شود یا باید دادههای کلاس اقلیت مشابه سازی و زیاد شوند تا توازن برقرار شود. در این مقاله، برای مقابله با نامتوازن بودن کلاسها، از تکنیک بازنمونه گیری با استفاده از SMOTE برای تولید نمونههای مصنوعی از کلاس اقلیت استفاده میشود و به این ترتیب دادهها را متوازن می کند.

• نویز در دادهها

دادههای واقعی اغلب حاوی نویز هستند که میتواند منجر به خطا در طبقهبندی شود. در این مقاله از خودرمزگذار رفع نویز برای مقابله با نویز در دادهها استفاده شدهاست. DAE میتواند یاد بگیرد که نویز را حذف کند و دادههای ورودی تمیز را بازسازی کند، بنابراین ویژگیهای مورد استفاده برای طبقهبندی را بهبود میبخشد.

• رفتار تقلبی دینامیک

رفتارهای تقلبی با گذشت زمان تغییر می کنند، که این موضوع مدلهای استاتیک را برای هماهنگی با تغییرات دشوار می کند.

انتخاب ویژگیها

شناسایی ویژگیهای مرتبط برای تشخیص تقلب نیز چالشبرانگیز و بسیار مهم است.

• معیارهای عملکرد

دقت تنها معیار مناسبی برای ارزیابی مدلهای تشخیص تقلب نیست به دلیل نامتوازن بودن دادهها. برای این موضوع، به جای استفاده (detection rate) recall عملکرد مدل با استفاده از نرخ

¹ Denoising Autoencoder (DAE)

ارزیابی می شود تا اطمینان حاصل شود که کلاس اقلیت (تراکنشهای تقلبی) به طور مؤثر تشخیص داده می شود.

٢

معماری شبکه توضیح داده شده در مقاله شامل دو بخش اصلی است:

- خودرمزگذار رفع نویز (DAE):
- لایه ورودی: دادههای ورودی با نویز را دریافت می کند.
- لایههای رمزگذار: چندین لایه کاملاً متصل که ابعاد دادههای ورودی را کاهش میدهند.
- لایه گلوگاه: کوچکترین لایه در معماری که ویژگیهای رمزگذاری شده را نمایش میدهد.
- لایههای رمزگشا: چندین لایه کاملاً متصل که دادهها را از ویژگیهای رمزگذاری شده بازسازی میکنند.
 - لایه خروجی: خروجی تمیز شده را تولید می کند.
 - معماری شامل یک سری لایههای کاملاً متصل با ساختار:

Input (29) \rightarrow FC (22) \rightarrow FC (15) \rightarrow FC (10) \rightarrow FC (15) \rightarrow FC (22) \rightarrow Output (29)

۲. مدل طبقهبندی:

- لایه ورودی: دادههای تمیز شده از خودرمزگذار را میگیرد.
 - لایههای پنهان: چندین لایه کاملاً متصل.
- لایه خروجی: از تابع SoftMax برای خروجی احتمالات برای دو کلاس (تقلبی و غیرتقلبی) استفاده می کند.
 - معماری شامل لایههایی با ساختار:

Input (29) \rightarrow FC (22) \rightarrow FC (15) \rightarrow FC (10) \rightarrow FC (5) \rightarrow Output (2)

٣

مدل به صورت زیر پیاده سازی شد:

۱. اضافه کردن نویز و اعمال SMOTE:

```
from imblearn.over_sampling import SMOTE

# Oversampling using SMOTE

mote = SMOTE(sampling_strategy=1.0, random_state=14)

X train_res, y train_res = smote.fit_resample(X_train, y_train)

import numpy as np

# Adding Gaussian noise
noise_factor = 0.2
X_train_noisy = X_train_res + noise_factor * np.random.normal(loc=0.0, scale=1.0, size=X_train_res.shape)
```

لازم به ذکر است که پیش از این داده های تست با نسبت ۰.۲ به کل دادهها جدا شدند و در ادامه در فرایند آموزش نیز ۰.۲ داده های آموزش برای validation استفاده خواهند شد.

DAE .Y

مدل بر اساس مقاله به صورت زیر پیاده سازی شد:

```
1 from tensorflow.keras.models import Sequential
    from tensorflow.keras.layers import Dense, Input, Dropout
    from tensorflow.keras.callbacks import EarlyStopping, ModelCheckpoint
    import tensorflow as tf
 6
    # Building the Denoising Autoencoder
7
    def build_autoencoder(input_dim):
8
        model = Sequential()
9
        model.add(Input(shape=(input_dim,)))
10
        model.add(Dense(22, activation='relu'))
        model.add(Dense(15, activation='relu'))
11
12
        model.add(Dense(10, activation='relu'))
13
        model.add(Dense(15, activation='relu'))
        model.add(Dense(22, activation='relu'))
14
        model.add(Dense(input_dim, activation='sigmoid'))
15
16
        model.compile(optimizer='adam', loss='mse')
17
       return model
19 # Training the Autoencoder
20
    input_dim = X_train_res.shape[1]
21
    autoencoder = build_autoencoder(input_dim)
22
    # Callbacks for early stopping and saving the best model
24
    autoencoder_callbacks = [
25
         EarlyStopping(monitor='val_loss', patience=3, verbose=1),
26
        ModelCheckpoint('best_autoencoder.h5', monitor='val_loss', save_best_only=True, verbose=1)
27
28
29
    history = autoencoder.fit(X_train_noisy, X_train_res,
30
                    epochs=100,
31
                    batch_size=256,
32
                    shuffle=True,
33
                    validation_split=0.2,
34
                    callbacks=autoencoder_callbacks)
35
    # Load the best autoencoder model
37
    autoencoder.load_weights('best_autoencoder.h5')
38
39
    # Denoising the training and test datasets
40
    X_train_denoised = autoencoder.predict(X_train_res)
41  X_test_denoised = autoencoder.predict(X_test)
```

رمزگذار حذف نویز را آموزش دیده و با حذف آن، مجموعه داده را بهبود میبخشد.

۳. طبقه بندی دادههای بدون نویز

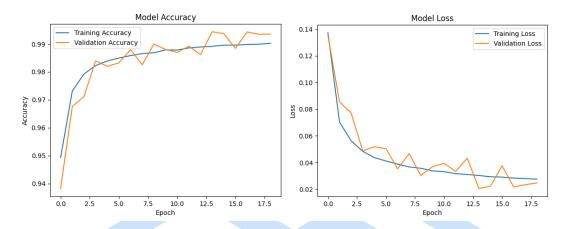
این بخش بر اساس مقاله به صورت زیر پیادهسازی شد:

```
def build_classifier(input_dim):
   model = Sequential()
   model.add(Input(shape=(input_dim,)))
   model.add(Dense(22, activation='relu'))
   model.add(Dense(15, activation='relu'))
   model.add(Dense(10, activation='relu'))
   model.add(Dense(5, activation='relu'))
   model.add(Dense(2, activation='softmax'))
   model.compile(optimizer='adam', loss='sparse_categorical_crossentropy', metrics=['accuracy', recall_m,precision_m,f1_m])
classifier = build_classifier(input_dim)
classifier_callbacks = [
   EarlyStopping(monitor='val_loss', patience=5, verbose=1),
   ModelCheckpoint('best_classifier.h5', monitor='val_loss', save_best_only=True, verbose=1)
history = classifier.fit(X_train_denoised, y_train_res,
              epochs=100,
              batch_size=256,
              shuffle=True,
              validation_split=0.2,
              callbacks=classifier_callbacks)
classifier.load_weights('best_classifier.h5')
```

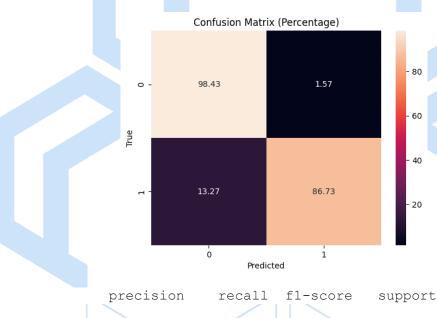
برای آموزش متعادل تر از معیارهای زیر در کامپایل استفاده شدهاست:

- recall_m(y_true, y_pred: نسبت مثبتهای واقعی به مجموع مثبتهای درست و منفیهای غلط.
- precision_m(y_true, y_pred): نسبت مثبت های واقعی به مجموع مثبت های درست و مثبت های غلط.
- y_pred) ،f1_m(y_true: امتیاز ۴۱، میانگین هارمونیک دقت و یادآوری را محاسبه می کند.

استفاده از این موارد، درک بهتر توانایی مدل در طبقه بندی صحیح نمونه های مثبت و منفی را امکان پذیر میکند. درنهایت مدل به صورت زیر آموزش دید:



مشاهده می شود که مدل اورفیت ندارد و تابع early stopping، آموزش مدل را در زمان مناسبی متوقف کرده است:



0 1.00 0.98 0.99 56864 0.09 0.87 0.16 98 1 0.98 56962 accuracy 0.54 0.93 0.57 56962 macro avg 1.00 0.98 0.99 56962 weighted avg

Test AUC: 0.9258126083860668

Test Recall: 0.9840771040342685

Test F1-score: 0.9840771040342685

Test Precision: 0.9840771040342685

همان طور که مشاهده می شود، طبقه بندی کننده دقت بالا و عملکرد قوی را از خود نشان می دهد.

بررسی معیارهای ارزیابی مدل در مسائل با دادههای نامتوازن

استفاده از معیار دقت (Accuracy) به تنهایی در مسائل با توزیع نامتوازن برچسبها، معمولاً نمایانگر صحیحی از عملکرد مدل نمیباشد و میتواند گمراه کننده باشد. دلیل این موضوع این است که دقت تنها نسبت پیشبینیهای صحیح به کل پیشبینیها را اندازه گیری می کند، بدون توجه به توزیع کلاسها. در مواردی که دادهها نامتوازن هستند، یک مدل میتواند با پیشبینی غالب کلاس اکثریت، دقت بالایی کسب کند در حالی که نتوانسته است به درستی کلاس اقلیت را پیشبینی کند که اغلب از اهمیت بیشتری برخوردار است. برای مثال اگر فرض کنیم یک مسئله دسته بندی دودویی داریم که ۹۵٪ نمونهها به کلاس و فقط ۵٪ به کلاس ۱ تعلق دارند؛ مدلی که همیشه کلاس و را پیشبینی می کند، دقتی برابر با ۹۵٪ خواهد داشت که به نظر بالا می آید، اما این مدل به طور کامل قادر به شناسایی نمونههای کلاس ۱ نیست.

برای ارزیابی بهتر مدلها روی دادههای نامتوازن، معیارهای زیر باید مورد توجه قرار گیرند:

• دقت (Precision):

تعریف: دقت نسبت پیشبینیهای مثبت صحیح به کل پیشبینیهای مثبت (مثبت صحیح + مثبت کاذب) است.

اهمیت: دقت بالا نشان دهنده نرخ پایین مثبتهای کاذب است.

$$Precision = \frac{TP}{TP + FP}$$

• بازخوانی (Recall یا Sensitivity):

تعریف: بازخوانی نسبت پیش بینیهای مثبت صحیح به کل نمونههای واقعی مثبت (مثبت صحیح + منفی کاذب) است.

اهمیت: بازخوانی بالا نشان دهنده نرخ پایین منفیهای کاذب است.

$$Recall = \frac{TP}{TP + FN}$$

• امتياز (F1-Score)

تعریف: امتیاز F1 میانگین هارمونیک دقت و بازخوانی است که یک معیار توازن بخش بین این دو محسوب می شود.

اهمیت: برای موقعیتهایی که توازن بین دقت و بازخوانی مهم است مفید میباشد.

$$F1\text{-Score} = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}$$

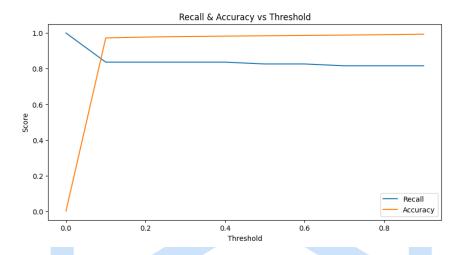
این معیارها می توانند در حین آموزش کمک کننده باشند و معیارهایی مانند ماتریس درهمریختگی و مساحت زیر منحنی (ROC (ROC-AUC) برای بررسی مدل آموزش دیده می توانند بسیار کمک کننده باشند. از سه معیار نام برده شده همانطور که دیده شد در فرایند آموزش استفاده شدند و از معیارهای ماتریس درهمریختگی و AUC نیز در بخش تست مدل روی دادههای تست استفاده شد.

۴

به صورت زیر این مورد بررسی شد:

```
# Lists to store recall and accuracy values
accuracies = []
for threshold in thresholds:
    # Oversampling using SMOTE with the current threshold
    smote = SMOTE(sampling_strategy=threshold, random_state=14)
X train res_v train res = smote.fit_resample(X_train, y_train)
    # Adding Gaussian noise
    X_train_noisy = X_train_res + noise_factor * np.random.normal(loc=0.0, scale=1.0, size=X_train_res.shape)
    autoencoder = build autoencoder(input dim)
    autoencoder.fit(X_train_noisy, X_train_res, epochs=100, batch_size=256, shuffle=True, validation_split=0.2, callbacks=autoencoder_callbacks) autoencoder.load_weights('best_autoencoder.h5')
    # Denoising the training dataset
    X_train_denoised = autoencoder.predict(X_train_res)
    # Training the Classifier
    classifier = build_classifier(input_dim)
    classifier.fit(X_train_denoised, y_train_res, epochs=100, batch_size=256, shuffle=True, validation_split=0.2, callbacks=classifier_callbacks)
    classifier.load_weights('best_classifier.h5')
    # Denoising the test dataset
    X_test_denoised = autoencoder.predict(X_test)
    # Evaluating the Classifier
    y_pred = classifier.predict(X_test_denoised)
    y_pred = np.argmax(y_pred, axis=1)
    # Calculating recall and accuracy
    recall = recall_score(y_test, y_pred)
    accuracy = accuracy_score(y_test, y_pred)
    # Appending to the lists
    recalls.append(recall)
    accuracies.append(accuracy)
```

خروجی این به صورت زیر است:



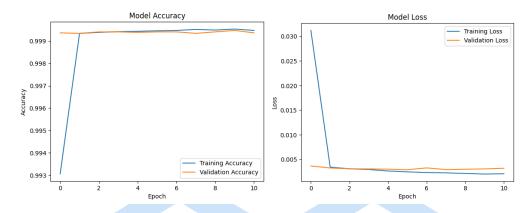
نمودار یادآوری و دقت را برای آستانه هایی از ۰.۱ تا ۰.۹ نشان می دهد. آستانه ۰.۲ ایده آل است. این به طور قابل توجهی هم یادآوری و هم دقت را افزایش داده و نشان می دهد مدل در این مرحله به خوبی متعادل و موثر عمل می کند.

۵

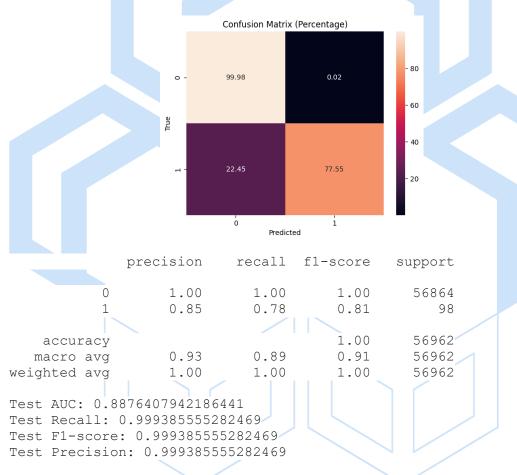
دادههای نامتوازن را آغشته به نویز کرده و وارد مدل میکنیم. از استفاده از معیارهای precision دادههای التفاده از معیارهای recall و F1 نیز در فرایند آموزش صرف نظر میکنیم:

```
X_train_noisy_norez = X_train + noise_factor * np.random.normal(loc=0.0, scale=1.0, size=X_train.shape)
def build_classifier(input_dim):
   model = Sequential()
   model.add(Input(shape=(input_dim,)))
   model.add(Dense(22, activation='relu'))
   model.add(Dense(15, activation='relu'))
   model.add(Dense(10, activation='relu'))
   model.add(Dense(5, activation='relu'))
   model.add(Dense(2, activation='softmax'))
   model.compile(optimizer='adam', loss='sparse_categorical_crossentropy', metrics=['accuracy'])
   return model
input_dim = X_train_noisy_norez.shape[1]
classifier_noisy = build_classifier(input_dim)
classifier_callbacks = [
   EarlyStopping(monitor='val_loss', patience=5, verbose=1),
   ModelCheckpoint('best_classifier_noisy.h5', monitor='val_loss', save_best_only=True, verbose=1)
history = classifier_noisy.fit(X_train_noisy_norez, y_train_res,
               epochs=100,
               batch_size=128,
               shuffle=True,
               validation_split=0.2,
               callbacks=classifier_callbacks)
```

مدل به صورت زیر آموزش دید:



مشاهده می شود که مدل کمی اورفیت دارد ولی تابع early stopping، آموزش مدل را در زمان مناسبی متوقف کرده است. نتیجه تست مدل روی داده های تست به صورت زیر است:



اثر وجود نویز و عدم توازن به خوبی دیده می شود. مدل اکنون در تشخیص موارد اکثریت بسیار خوب عمل می کند و False Negatives بهبود یافته نشان دهنده تعادل بهتر کلی است اما افزایش F1-score عمل می کند و نشان می دهد مدل موارد بیشتری از اقلیت را از دست می دهد. این موضوع در مقدار کننده است و نشان می دهد مدل موارد بیشتری از اقلیت را از دست می دهد. این موضوع در مقدار AUC نیز به خوبی دیده می شود.

مراجع

