Project: Stochastic Gradient Descent

Yifei Zhang (.5387), Yue Lin (.3326)

November 2020

1 Introduction

The goal of this project is to implement stochastic gradient descent (SGD) algorithm and conduct a set of experiments considering two scenarios to evaluate the performance of SGD. The logistic loss and binary classification error are used in evaluation.

In this project, we implement an SGD using the following steps.

- Initialize the network weights $\mathbf{w}_1$ to 0 (ensure $\mathbf{w}_1 \in C$ for both scenarios).
- For each input feature vector $\tilde{\mathbf{x}}_t$ and its label y_t, calculate the gradient

$$\nabla f\left(\mathbf{w}_t\right)=\frac{-y_t \tilde{\mathbf{x}}_t \exp \left(-y_t\left\langle\mathbf{w}_t, \tilde{\mathbf{x}}_t\right\rangle\right)}{1+\exp \left(-y_t\left\langle\mathbf{w}_t, \tilde{\mathbf{x}}_t\right\rangle\right)}$$

- Take a projected GD step

$$\mathbf{w}_{t+1}=\Pi_C\left(\mathbf{w}_t-\alpha \nabla f\left(\mathbf{w}_t\right)\right)$$

- Repeat steps 2 and 3 until all n samples are trained, and then output

$$\hat{\mathbf{w}}=\frac{1}{n} \sum_{t=1}^n \mathbf{w}_t$$

2 Experiments

This project is developed in Python. For each of the two scenarios, we test the experimental results using two $\sigma \in \{0.1, 0.35\}$ to generate the Gaussian distribution for both domain and parameter sets. For each σ value, we vary the size of the training set n as $50, 100, 500, 1000$. For each set of the parameters (σ, n), the following experiment is conducted.

- Calculate step size α based on the ρ-Lipschitz properties for each scenario described in the upcoming section.
- Generate data for model training and testing. For each example $(\mathbf{x}, y)$, y is randomly sampled from {-1,1} with equal probability. When $y=-1$, a 4-dimensional vector $\mathbf{u}=(u_1, u_2, u_3, u_4)$ is generated. Each element of $\mathbf{u}$ is randomly picked from Gaussian distribution with mean $-1/4$ and variance σ^2. When $y=1$, each element of $\mathbf{u}$ is randomly picked from Gaussian distribution with mean $1/4$ and variance σ^2(σ is specified above, $\sigma \in \{0.1, 0.35\}$).

- Perform Euclidean projection onto domain set χ,i.e $\mathbf{x} = \Pi_\chi(\mathbf{u})$.
  - Scenario 1: For $\mathbf{u}$ located outside of χ, each element u_i in $\mathbf{u}$ $\big(\forall j \in [4]\big)$ will be scaled into [-1,1] by choosing the closest value to u_i on χ, which is calculated as $sign\,(u_i){*}min\,\big(|u_i|, 1\big)$. For $\mathbf{u}$ within χ, no projection is needed.
  - Scenario 2: For $\mathbf{u}$ located outside of χ, each element u_i in $\mathbf{u}$ will be shrunk so that the norm is 1 ,which is calculated as $\frac{u_i}{\|\mathbf{u}\|}$. For $\mathbf{u}$ within χ, no projection is needed.

- Run the SGD algorithm and evaluate the output $\hat{\mathbf{w}}$ on the test set using two types of metrics: logistic loss and classification error. The logistic loss is computed as

$$.l_{logist}\left(\mathbf{w}, (\mathbf{x}, y)\right) = \ln\Big(1 + \exp\left(-y \left\langle \mathbf{w}, \tilde{\mathbf{x}}\right\rangle\right)\Big)$$

  The classification error is computed as

$$\mathbf{1}\Big(\text{sign}\left(\left\langle \mathbf{w}, \tilde{\mathbf{x}}\right\rangle\right) \neq y\Big)$$

- Repeat steps 2 and 3 for 30 trials (as determined in the project description). Calculate the below statistics for the specific (σ, n) setting.
  - Calculate the mean, minimum, and standard deviation of the 30 loss estimates. Calculate the difference between the mean and the minimum of the loss estimates as the expected excess risk.
  - Calculate the mean and standard deviation of the 30 binary classification error estimates.

3 Analysis of ρ-Lipschitz properties

For logistic loss function

$$l_{logist}\left(\mathbf{w}, (\mathbf{x}, y)\right) = \ln\Big(1 + \exp\left(-y \left\langle \mathbf{w}, \tilde{\mathbf{x}}\right\rangle\right)\Big)$$

where $\mathbf{x} \in \chi \subset \mathbb{R}^{d-1}$, $\tilde{\mathbf{x}} \triangleq (\mathbf{x}, 1)$, $y \in \{-1, +1\}$, $\mathbf{w} \in \mathbb{R}^d$, and $z = (\mathbf{x}, y)$.

Let's define $g_1\left(\mathbf{w}\right) \triangleq y\langle \mathbf{w}, \tilde{\mathbf{x}}\rangle$, $g_2\left(a\right) = \log\big(1 + \exp(-a)\big)$.

Note $l_{logist}\left(\cdot, (\mathbf{x}, y)\right) = g_2 \circ g_1$, g_1 is linear and $\|\tilde{\mathbf{x}}\|$-Lipschitz, g_2 is convex and 1-Lipschitz. Hence, $l_{logist}\left(\cdot, (\mathbf{x}, y)\right)$ is convex and $\|\tilde{\mathbf{x}}\|$-Lipschitz.

- For Scenario 1, $\|\tilde{\mathbf{x}}\|$ is bounded by $\rho = \sqrt{5}$.
  To prove C is a convex set, C is 5-dimensional hypercube in $\mathbb{R}^5$ i.e.

$$C = \Big\{\mathbf{w} = (w_1, w_2, w_3, w_4, w_5) \in \mathbb{R}^5 : |w_j| \leq 1, \forall j \in [5]\Big\}$$

  We can re-write the above as $C = \big\{\mathbf{w} = (w_1, w_2, w_3, w_4, w_5) \in \mathbb{R}^5 : \|\mathbf{w}\|_\infty \leq 1\big\}$,
  where $\|\mathbf{w}\|_\infty = \underset{j\in[d}{max}|x_j|$.
  Let $\mathbf{a}, \mathbf{b} \in C$. For any $\lambda \in [0, 1]$, consider a vector $\mathbf{e}$ where

$$\mathbf{e} \triangleq \lambda\mathbf{a} + (1 - \lambda)\,\mathbf{b}$$

We have

$$\begin{aligned}
\|\mathbf{e}\|_\infty &= \left\|\lambda \mathbf{a} + (1-\lambda)\,\mathbf{b}\right\|_\infty \\
&= \underset{j\in[5]}{max}|\lambda a_j + (1-\lambda)\, b_j| \\
&\leq \lambda \underset{j\in[5]}{max}|a_j| + (1-\lambda)\underset{j\in[5]}{max}|b_j| \\
&\leq \lambda \|\mathbf{a}\|_\infty + (1-\lambda)\|\mathbf{b}\|_\infty \\
&\leq \lambda + (1-\lambda)\,(\mathbf{a},\mathbf{b}\in C) \\
&= 1
\end{aligned}$$

Hence, $\mathbf{e} \in C$. By the definition of convex set, C is convex set and bounded by $M = \sqrt{5 * 2^2} = 2\sqrt{5}$.

- For Scenario 2, $\|\tilde{\mathbf{x}}\|$ is bounded by $\rho = \sqrt{5}$.
  To prove C is a convex set, C is 5-dimensional unit ball in $\mathbb{R}^5$ i.e.

  $$C = \left\{\mathbf{w}\in\mathbb{R}^5 : \|\mathbf{w}\| \leq 1\right\}$$

  Let $\mathbf{a},\mathbf{b}\in C$. For any $\lambda\in[0,1]$, consider a vector $\mathbf{e}$ where

  $$\mathbf{e} \triangleq \lambda\mathbf{a} + (1-\lambda)\,\mathbf{b}$$

  We have

  $$\begin{aligned}
  \|\mathbf{e}\| &= \left\|\lambda\mathbf{a} + (1-\lambda)\,\mathbf{b}\right\| \\
  &= \|\lambda\mathbf{a}\| + \left\|(1-\lambda)\,\mathbf{b}\right\| \\
  &\leq \lambda\|\mathbf{a}\| + (1-\lambda)\|\mathbf{b}\| \\
  &\leq \lambda + (1-\lambda)\left(\mathbf{a},\mathbf{b}\in C, \|\mathbf{a}\|, \|\mathbf{b}\| \leq 1\right) \\
  &= 1
  \end{aligned}$$

  Hence, $\mathbf{e}\in C$. By the definition of convex set, C is convex set and bounded by $M = 2$.

4 Results

The experimental results are shown in Table 1. The expected excess risk and the standard deviation of risks can be found in Figure 1. The classification error and its standard deviation can be found in Figure 2.

In general, for two scenarios in different parameter settings, both excess risk and average classification error drop when n increases. When n takes larger values, such decrease seems less significant. The variances of risk and classification error follow the similar trend.

					Logistic loss				Classification error	
Scenario	σ	n	N	#trials	Mean	Std Dev	Min	Excess Risk	Mean	Std Dev
1	0.10	50	30	0.422277	0.010352	0.411645	0.010632	0.129000	0.144156	0.234416
1	0.10	100	30	0.384937	0.003894	0.378639	0.006298	0.050833	0.073381	0.148509
1	0.10	500	30	0.349927	0.000998	0.348222	0.001705	0.021167	0.012260	0.004687
1	0.10	1000	30	0.334924	0.000884	0.333487	0.001437	0.007917	0.002745	0.000000
1	0.35	50	30	0.469225	0.014753	0.440774	0.028450	0.231083	0.078882	0.102299
1	0.35	100	30	0.424214	0.006871	0.404873	0.019341	0.161250	0.046752	0.131237
1	0.35	500	30	0.394387	0.002106	0.388598	0.005790	0.151833	0.013600	0.019663
1	0.35	1000	30	0.395125	0.001107	0.393135	0.001990	0.155917	0.007971	0.012599
2	0.10	50	30	0.547088	0.007108	0.538538	0.008550	0.459667	0.113414	0.253846
2	0.10	100	30	0.524749	0.003036	0.520318	0.004431	0.433167	0.130877	0.234262
2	0.10	500	30	0.495873	0.000809	0.494196	0.001677	0.360000	0.071987	0.022411
2	0.10	1000	30	0.488987	0.000740	0.487631	0.001356	0.332583	0.049939	0.000000
2	0.35	50	30	0.566451	0.008860	0.549793	0.016658	0.389833	0.094205	0.198564
2	0.35	100	30	0.541597	0.006745	0.531674	0.009923	0.319000	0.066928	0.172125
2	0.35	500	30	0.520846	0.001430	0.518031	0.002815	0.277250	0.037629	0.085103
2	0.35	1000	30	0.507197	0.000753	0.505576	0.001621	0.257667	0.017090	0.044888

Table 1: Experimental results.

Figure 1: Expected excess risk and standard deviation of risks.

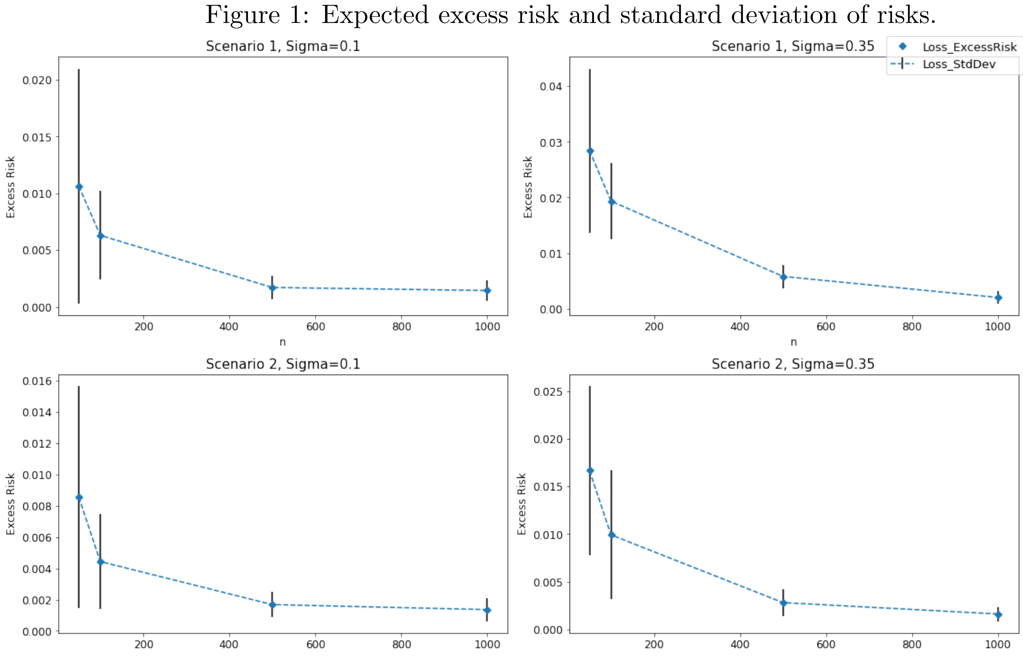
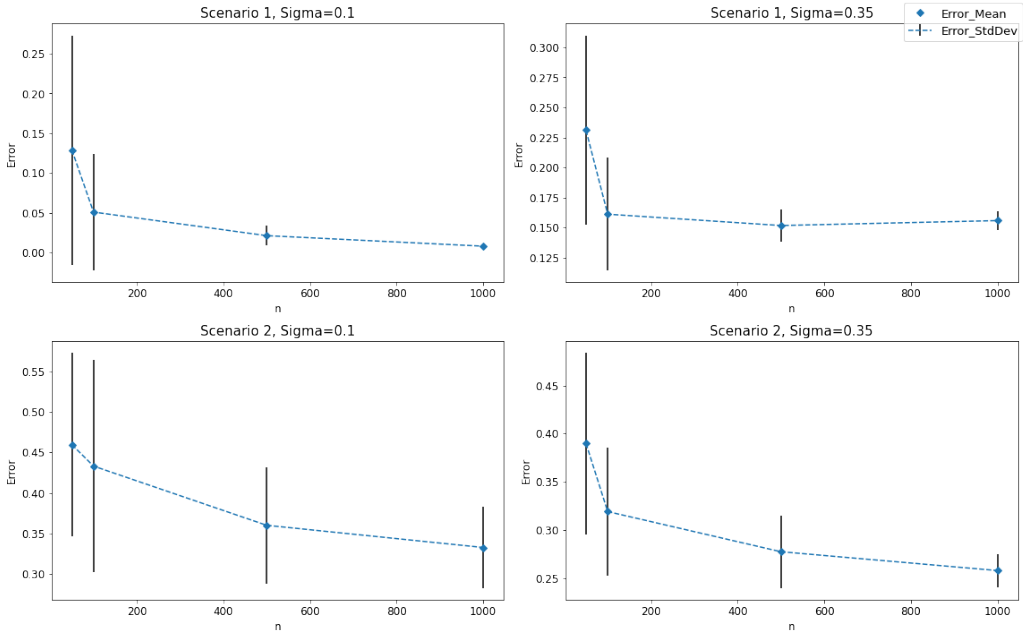


Figure 2: Classification error and its standard deviation.



5 Conclusion

- The experiment results agree with theoretical results.
  Based on convergence theorem, the excess risk is bound by $\frac{M\rho}{\sqrt{T}}$ (T= sample size n here). For $n = [50, 100, 500, 1000]$, the theoretical bound of scenario 1 is [1.4142, 1.0, 0.4472, 0.3162], the theoretical bound of scenario 2 is [0.6325, 0.4472, 0.2, 0.1414]. For both scenarios, the theoretical bound of excess risk decrease as n increase. From the above table and figures, we can see that the experiment result shows the same trend as theoretical result when n increase for both scenarios with $\sigma \in \{0.1, 0.35\}$. All the excess risk values are under the theoretical bound.

- The excess risk of scenario 1 is larger than scenario 2. By convergence theorem, the bound is calculated by $\frac{M\rho}{\sqrt{T}}$. The ρ values are equivalent in two scenarios, but the $M = 5\sqrt{2}$ for scenario 1,which is larger than $M = 2$ of scenario 2. Hence, theoretically the excess risk of scenario 1 should have tighter bound than scenario 2. [ERROR NOT COMPARED YET]

- From figure 1, the variance of the excess risk derived from the data with $\sigma = 0.35$ is larger than $\sigma = 0.1$ for both scenarios. The randomness of excess risk comes from the fresh example from Gaussian distribution that feed to SGD. If the distribution has larger variance, the variance of excess risk will be enlarged. [ERROR NOT COMPARED YET]

A Appendix: Symbol Listing

Symbol	Description	Variable name in code
$\mathbf{w}_t$	weight vector at t	w_t
$\tilde{\mathbf{x}}_t$	extended feature vector at t	X
y_t	label at t	y
$\nabla f(\mathbf{w}_t)$	gradient at t	g
Π_χ	Euclidean projection onto χ	prj_data
Π_C	Euclidean projection onto C	prj_grad
α	step size	l_rate
n	training set size	bs
N	test set size	test_n
$\mathbf{w}$	weight vector	w
$\mathbf{x}$	feature vector	X
$\tilde{\mathbf{x}}$	extended feature vector (with '1' appended at the end of x)	X

B Appendix: Library Routines

Functions from `NumPy`:

- `numpy.linalg.norm`: calculate the vector norm; `ord` specifies the order of the vector
- `np.apply_along_axis`: apply a function to 1-D slices of an array along the given axis
- `np.random.normal`: draw random samples from a Gaussian distribution; `loc` specifies the mean of the distribution, and `scale` specifies the standard deviation of the distribution

C Appendix: Code

```python
import numpy as np
import random
import matplotlib.pyplot as plt
import pandas as pd


def cube_prj(sample):
    '''
    This function projects both domain and parameter sets to a hypercube.

    sample: features or gradients, 1*d array (d: #dimension)

    return:
        the projected vector onto a hypercube with edge length 2 and centered around the origin
    '''
    return [np.sign(i) * min(np.abs(i), 1) for i in sample]
```

```
def ball_prj(sample):
    '''
    This function projects both domain and parameter sets to a unit ball.

    sample: features or gradients, 1*d array (d: #dimension)

    return:
        the projected vector onto a unit ball centered around the origin
    '''
    if np.linalg.norm(sample, ord=2) > 1:
        return sample / np.linalg.norm(sample, ord=2)
    else:
        return sample


def prj_data(X, y, prj_code):
    '''
    This function projects the domain set in terms for two scenarios.

    X: feature vectors, n*d array (n: #sample, d: #dimension)
    y: labels, 1*n array with values of -1 or +1
    prj_code: type of projection, 0 for cube, 1 for ball

    return:
        prj_x: projected feature vectors
        y: labels, same as the input
    '''
    if prj_code == 0:
        prj_x = np.apply_along_axis(cube_prj, 1, X)
    elif prj_code == 1:
        prj_x = np.apply_along_axis(ball_prj, 1, X)
    else:
        print("Please input correct code for projection type: 0 for cube, 1 for ball.")

    b = np.ones((prj_x.shape[0], 1))
    prj_x = np.append(prj_x, b, axis=1)
    return prj_x, y


def prj_grad(g, prj_code):
    '''
    This function projects the parameter set for two scenarios.

    g: gradients, 1*d array (d: #dimension)
    prj_code: type of projection, 0 for cube, 1 for ball
```

```
    return:
        prj_g: projected gradients
    '''
    if prj_code == 0:
        prj_g = cube_prj(g)
    elif prj_code == 1:
        prj_g = ball_prj(g)
    else:
        print("Please input correct code for projection type: 0 for cube, 1 for ball.")
    return prj_g


def gen_data(sig, n, d_dimension):
    '''
    This function generates the data for training and test.

    sig: standard deviation of the Gaussian function
    n: number of samples
    d_dimension: dimensionality of the feature vectors

    Return:
        X: feature vectors, n*d array (n: #sample, d: #dimension)
        y: labels, 1*n array with values of -1 and +1
    '''
    y = np.random.choice([-1, 1], p = [0.5, 0.5], size = n)
    X = np.array([])
    for i in range(n):
        if y[i] == -1:
            mu = -(1 / 4)
            negvec = np.random.normal(mu, sig, d_dimension)
            X = np.concatenate([X, negvec], axis=0)
        else:
            mu = (1 / 4)
            posvec = np.random.normal(mu, sig, d_dimension)
            X = np.concatenate([X, posvec], axis=0)
    X = np.reshape(X, (n, d_dimension))
    return X, y


def log_loss(X, y, w):
    '''
    This function outputs the logistic loss.

    X: feature vector, 1*d array (d: #dimension)
    y: label
```

```
    w: weight vector, 1*d array

    Return: logistic loss
    '''
    return np.log(1 + np.exp(-y * np.dot(w.T, X)))


def err(X, y, w):
    '''
    This function outputs the classification error.

    X: feature vector, 1*d array (d: #dimension)
    y: label
    w: weight vector, 1*d array

    Return: classification error
    '''
    yhat = -1 if np.dot(w.T, X) < 0.5 else 1
    return 0 if yhat == y else 1


def sdg(train_x, train_y):
    '''
    train_x: feature vectors one batch
    train_y: lables in one batch
    return:
            w: weight vector trained on one batch
    '''
    w_all = []
    w_t = np.zeros(train_x.shape[1])
    for idx in range(train_x.shape[0]):
        # Read data
        X = train_x[idx]
        y = train_y[idx]
        w_t = np.array(w_t)
        # Calculate gradient
        g = (-y * X * np.exp(-y * np.dot(w_t.T, X)) / (1 + np.exp(-y * np.dot(w_t.T, X))))
        # Project gradient
        w_t = prj_grad(np.add(w_t, np.multiply(-l_rate, g)), prj_code)
        # Backward propagation
        w_all.append(w_t)
    return np.average(np.array(w_all), axis=0)


def train(train_x, train_y, test_x, test_y, l_rate, n_epoch, bs, prj_code):
    '''
```

```
    This function implements and tests the SGD algorithm for logistic regression.

    train_x: feature vectors for training, n*d array (n: #sample, d: #dimension)
    train_y: labels for training, 1*n array
    test_x: feature vectors for test, n*d array (n: #sample, d: #dimension)
    test_y: labels for test, 1*n array
    l_rate: learning rate
    n_epoch: number of trials
    bs: training set size
    prj_code: type of projection, 0 for cube, 1 for ball

    Return:
        w: final weights
        risk_ave: average risk
        risk_min: minimum of all risks
        risk_var: standard deviation of all risks
        exp_excess_risk: expected excess risk
        cls_err_ave: average classification error
        cls_err_var: standard deviation of all classification errors
    '''
    risk_all = []
    cls_err_all = []

    for epoch in range(n_epoch):
        risk = cls_err = 0.
        train_x0 = train_x[epoch * bs: (epoch + 1) * bs] ## use current batch to for trainning
        train_y0 = train_y[epoch * bs: (epoch + 1) * bs] ## use current batch to for trainning
        w = sdg(train_x0, train_y0)

        # Evaluate
        for idx in range(test_x.shape[0]):
            # Read data
            X = test_x[idx]
            y = test_y[idx]
            # Evaluate
            risk += log_loss(X, y, w) / test_x.shape[0]
            cls_err += err(X, y, w) / test_x.shape[0]

        risk_all = np.append(risk_all, risk)
        cls_err_all = np.append(cls_err_all, cls_err)

    # Report risk
    risk_ave = np.average(risk_all)
    risk_min = np.amin(risk_all)
    risk_var = np.sqrt(np.var(risk_all))
    exp_excess_risk = risk_ave - risk_min
```

```python
    # Report classification error
    cls_err_ave = np.average(cls_err_all)
    cls_err_var = np.sqrt(np.var(cls_err_all))
    return [w, risk_ave, risk_min, risk_var, exp_excess_risk, cls_err_ave, cls_err_var]


# Set up hyperparameters
n_epoch = 30    # training epochs
test_n = 400    # size of test set
d_dimension = 4
train_bs = np.array([50, 100, 500, 1000])  # batch size for each training epoch

np.random.seed(1)

result_list = []
for prj_code in [0, 1]:
    for sigma in [0.1, 0.35]:
        for bs in train_bs:

            if prj_code == 0:
                m = 2 * np.sqrt(d_dimension + 1)
            else:
                m = 2

            rho = np.sqrt(d_dimension + 1)
            l_rate = m / (rho * np.sqrt(bs))

            # Generate training data
            train_x, train_y = gen_data(sigma, bs * n_epoch, d_dimension)
            train_px, train_py = prj_data(train_x, train_y, prj_code)

            # Generate test data
            test_x, test_y = gen_data(sigma, test_n, d_dimension)
            test_px, test_py = prj_data(test_x, test_y, prj_code)

            # Train
            output = train(train_px, train_py, test_px, test_py, l_rate, n_epoch, bs, prj_code)

            print('>scenario=%d, sigma=%.2f, n=%d, lr=%.2f, log_loss_mean=%.3f, \
                log_loss_std_dev=%.3f, log_loss_min=%.3f, \
                excess_risk=%.3f, cls_error_mean=%.3f, cls_error_std_dev=%.3f'
                % (prj_code + 1, sigma, bs, l_rate, output[1], output[3], \
                    output[2], output[4], output[5], output[6]))
            result = [prj_code + 1, sigma, bs, n_epoch,output[1], output[3], \
                output[2], output[4], output[5], output[6]]
            result_list.append(result)
```