MONASH University

FIT 3181/5215 Deep Learning

Quiz for:
Advanced Convolutional Neural Networks

Teaching team

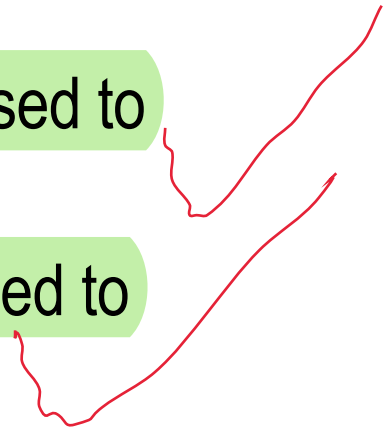
Department of Data Science and AI
Faculty of Information Technology, Monash University
Email: **trunglm@monash.edu**

GROUP OF EIGHT AUSTRALIA

Question 1

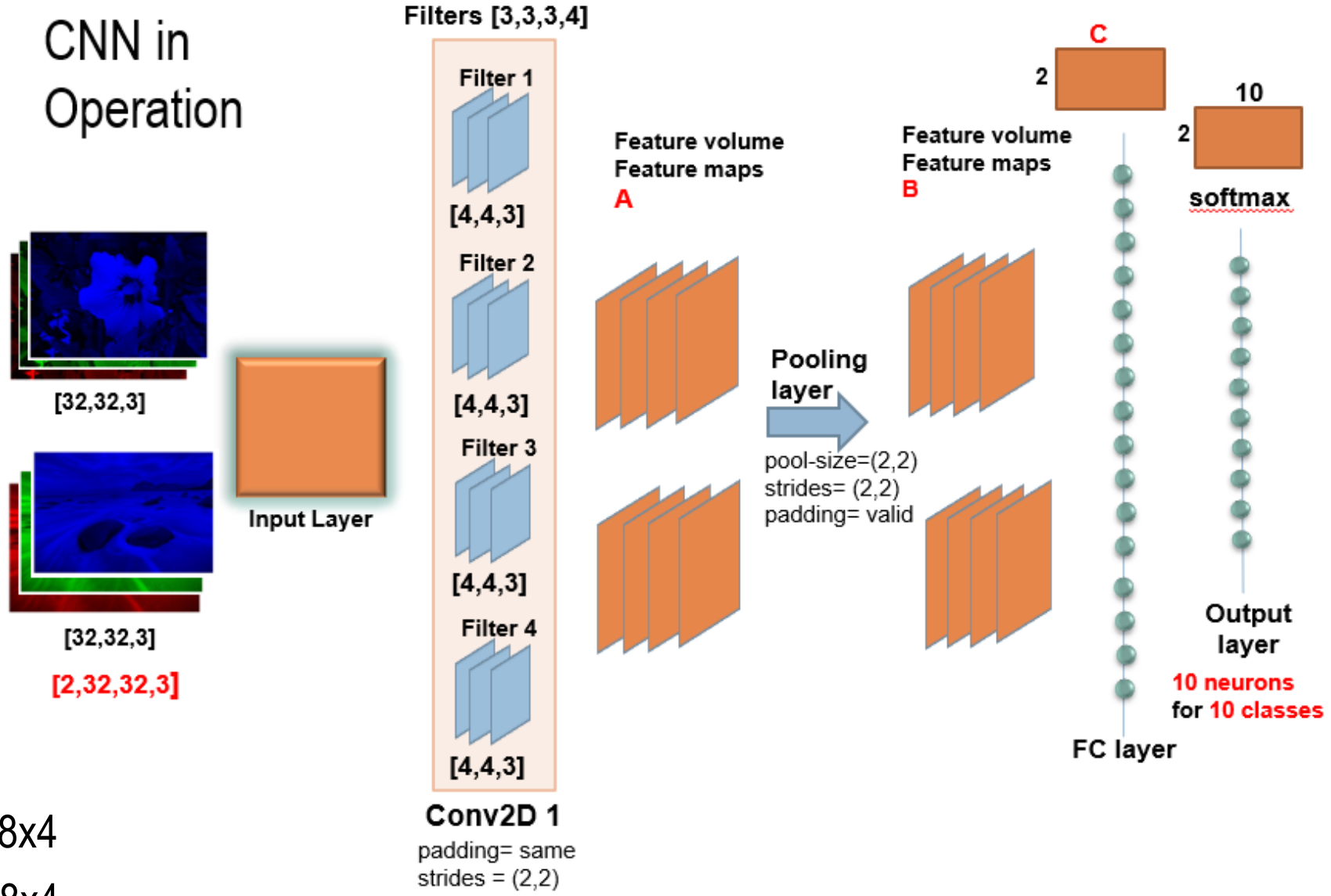
Which statements are correct? (MC)

- A. In traditional approach, the training signal from classifier can be used to improve feature extractor.
- B. In deep learning approach, the training signal from classifier can be used to improve feature extractor.
- C. In traditional approach, the training signal from classifier cannot be used to improve feature extractor.
- D. In deep learning approach, the training signal from classifier cannot be used to improve feature extractor.



Question 2

What are the shapes of tensors in A, B and the value of the width in C?



floor((32-1)/2) + 1 = 16

- A. [15,15,4], [8,8,4], 8x8x4
- B. [2,15,15,4], [2,8,8,4], 2x8x8x4
- C. [2,16,16,4], [2,8,8,4], 2x8x8x4
- D. [2,16,16,4], [2,8,8,4], 8x8x4

Question 3

What are correct statements about the receptive field? (MC)

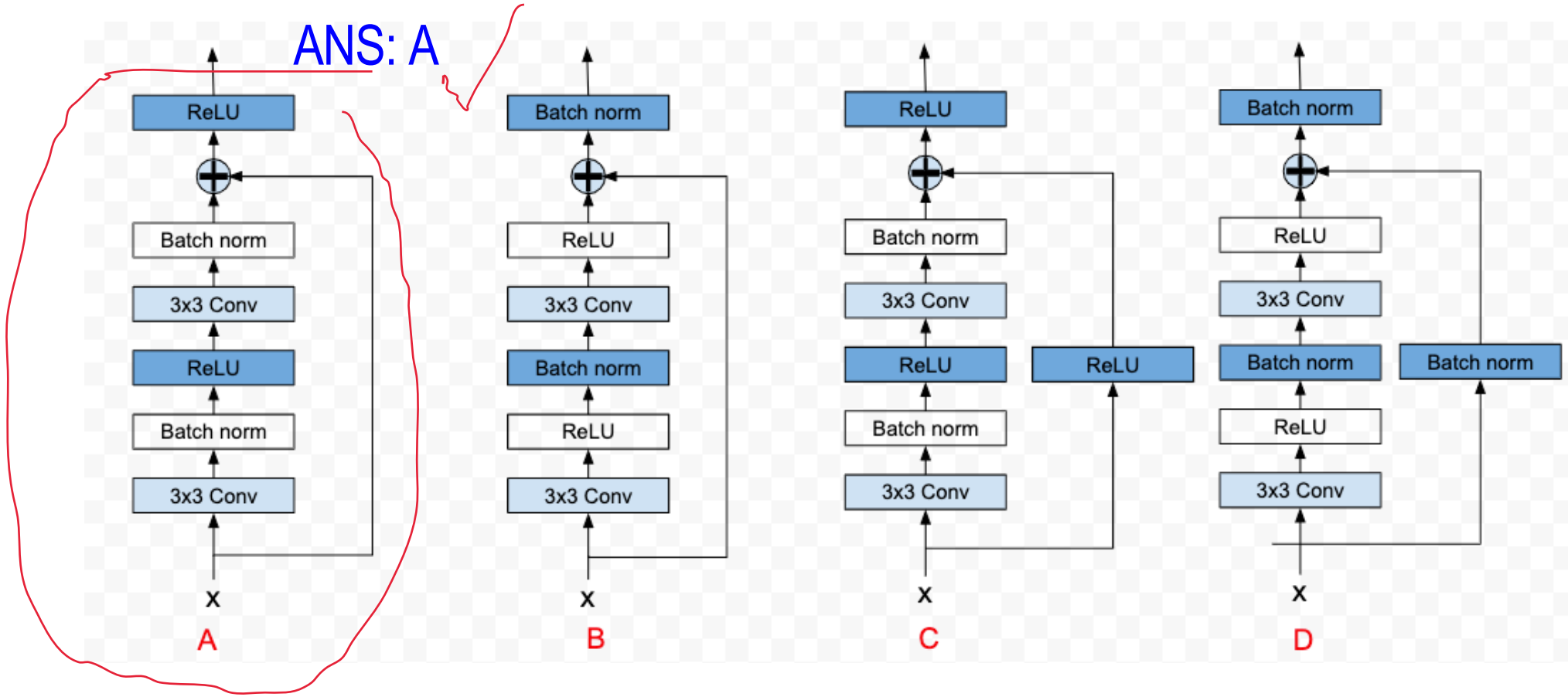
- A. Receptive field of neurons on higher layers become smaller.
- B. The value of a neuron is not computationally relevant to its receptive field.
- C. Receptive field of neurons on higher layers become larger.
- D. The value of a neuron is computationally relevant to its receptive field.

the higher the layers, the larger the weights, (recap: backpropagation)

Question 4

Which illustration is correct for the residual block? (SC).

ANS: A



Question 5

Given an implementation of the residual block as below? What is the shape of Y (SC).

A. [10,32,32,3]
B. [10,16,16,3]
C. [3,32,32,3]
D. Raise an error.

```
class Residual(tf.keras.Model):
    def __init__(self, num_channels, use_1x1conv=False, strides=1):
        super().__init__()
        self.conv1 = tf.keras.layers.Conv2D(
            num_channels, padding='same', kernel_size=3, strides=strides)
        self.conv2 = tf.keras.layers.Conv2D(num_channels, kernel_size=3, padding='same')
        self.conv3 = None
        if use_1x1conv:
            self.conv3 = tf.keras.layers.Conv2D(
                num_channels, kernel_size=1, strides=strides)
        self.bn1 = tf.keras.layers.BatchNormalization()
        self.bn2 = tf.keras.layers.BatchNormalization()

    def call(self, X):
        Y = tf.keras.activations.relu(self.bn1(self.conv1(X)))
        Y = self.bn2(self.conv2(Y))
        if self.conv3 is not None:
            X = self.conv3(X)
        Y += X
        return tf.keras.activations.relu(Y)

blk = Residual(num_channels=3)
X = tf.random.uniform((10, 32, 32, 3))
Y = blk(X)
print(Y.shape)
```

Question 6

Given an implementation of the residual block as below? What is the shape of Y (SC).

A. [10,32,32,3]

B. [10,16,16,3]

C. [3,32,32,3]

D. Raise an error.

```
class Residual(tf.keras.Model):
    def __init__(self, num_channels, use_1x1conv=False, strides=1):
        super().__init__()
        self.conv1 = tf.keras.layers.Conv2D(
            num_channels, padding='same', kernel_size=3, strides=strides)
        self.conv2 = tf.keras.layers.Conv2D(num_channels, kernel_size=3, padding='same')
        self.conv3 = None
        if use_1x1conv:
            self.conv3 = tf.keras.layers.Conv2D(
                num_channels, kernel_size=1, strides=strides)
        self.bn1 = tf.keras.layers.BatchNormalization()
        self.bn2 = tf.keras.layers.BatchNormalization()

    def call(self, X):
        Y = tf.keras.activations.relu(self.bn1(self.conv1(X)))
        Y = self.bn2(self.conv2(Y))
        if self.conv3 is not None:
            X = self.conv3(X)
        Y += X
        return tf.keras.activations.relu(Y)

blk = Residual(num_channels=6)
X = tf.random.uniform((10, 32, 32, 3))
Y = blk(X)
print(Y.shape)
```

Question 7

Which statements are correct for ResNet architecture? (MC).

- A. In ResNet architecture, ReLU activation function is followed by Batch Normalization layer.
- B. It is possible to replace ReLU by Sigmoid activation function because of the skip-connection can help to reduce gradient vanishing.
- C. 1x1 Conv in skip-connection is used to change number of output channels.
- D. A ResNet model consists of many ResNet blocks, each ResNet block consists of many residual blocks, each residual block includes several convolutional and activation layers.

Question 8

Given an adversarial example x_{adv} of a clean example x w.r.t. model f, $y \in \{1,2,\ldots,M\}$ is the true label. Which statements are correct? (MC).

- A. x_{adv} and x look very similar under human perspective
- B. x_{adv} and x look very different under human perspective
- C. $argmax_{1\leq m\leq M} f_m(x_{adv}) = y$
- D. $argmax_{1\leq m\leq M} f_m(x_{adv}) \neq y$

Question 9

Given a constraint of an adversarial example as follow: $x_{adv} \in B_\epsilon(x) = \{x' : \|x' - x\|_\infty \leq \epsilon\}$. *Which statements are correct? (MC)*

- A. This constraint to make sure that x_{adv} and x look very similar under human perspective
- B. This constraint to make sure that x_{adv} and x look very different under human perspective
- C. This constraint to make sure that $argmax_{1 \leq m \leq M} f_m(x_{adv}) = argmax_{1 \leq m \leq M} f_m(x)$
- D. The highest absolute difference between pixels of x_{adv} and x is less than or equal ϵ

Question 10

Given a DL model $f(x;\theta)$ parameterized by θ where $f(x;\theta)$ represents the prediction probabilities of x associated with a ground-truth label $y \in \{1, \ldots, M\}$, we find an adversarial example by $\boldsymbol{x_{adv} = argmax_{x' \in B_\epsilon(x)} l(f(x';\theta), y)}$. Which statements are correct? (MC)

- A. We maximally increase the chance to predict x_{adv} with label y.
- B. We maximally decrease the chance to predict x_{adv} with label y.
- C. We maximally increase the chance to predict x_{adv} with any else label $y' \neq y$.
- D. It is a targeted attack.
- E. It is an untargeted attack.

Question 11

Given a DL model $f(x;\theta)$ parameterized by θ where $f(x;\theta)$ represents the prediction probabilities of x associated with a ground-truth label $y \in \{1, \dots, M\}$, we find an adversarial example by $\boldsymbol{x_{adv} = argmin_{x' \in B_\epsilon(x)} l(f(x';\theta), y_{\neq})}$ *with* $y_{\neq} \neq y$.

Which statements are correct? (MC)

- A. We maximally increase the chance to predict x_{adv} with label y.
- B. We maximally increase the chance to predict x_{adv} with label $y_{\neq}$.
- C. It is a targeted attack.
- D. It is an untargeted attack.