全连接神经网络的密文打包

Notion

- $X_m[j]$:第m个样本的第j个特征
- 假设有t维特征，n张图像（即一个样本是一个$t \times 1$的向量）
- $W_{t' \times t}$：权重矩阵，t'表示本层神经元数量，t表示上层神经元（特征数）
- 密文slot：s
- 每张图像取k个特征与其余图像打包，则一个密文中包含s/k个样本（我们可以设batchSize为s/k）

Example

> 以一个三层全连接神经网络为例，t维输入，中间层有t'个神经元，输出层有t''个神经元

槽数s,每张图像取k个特征与其余图像打包，则一个密文中包含s/k个样本

$$
\begin{gathered}
X_0[0], X_1[0] \ldots \ldots X_{s/k-1}[0] | X_0[1], X_1[1] \ldots \ldots X_{s/k-1}[1] | \ldots | X_0[k-1], X_1[k-1] \ldots \ldots X_{s/k-1}[k-1] \\
\odot \\
W_{0,0}, W_{0,0} \ldots \ldots W_{0,0} | W_{0,1}, W_{0,1} \ldots \ldots W_{0,1} | \ldots | W_{0,k-1}, W_{0,k-1} \ldots \ldots W_{0,k-1} \\
= Z_{0,0 \sim k-1}
\end{gathered} \tag{1}
$$

$Z_{0,0-k-1}$表示图像（0-（s/k）-1）与权重矩阵第0行前k列的计算结果，我们需要每个特征与矩阵的一整列相乘，因此，我们还有如下：

$$
\begin{gathered}
X_0[0], X_1[0] \ldots \ldots X_{s/k}[0] | X_0[1], X_1[1] \ldots \ldots X_{s/k}[1] | \ldots | X_0[k-1], X_1[k-1] \ldots \ldots X_{s/k}[k-1] \\
\odot \\
W_{1,0}, W_{1,0} \ldots \ldots W_{1,0} | W_{1,1}, W_{1,1} \ldots \ldots W_{1,1} | \ldots | W_{1,k-1}, W_{1,k-1} \ldots \ldots W_{1,k-1} \\
= Z_{1,0 \sim k-1}
\end{gathered} \tag{2}
$$

......

$$
\begin{gathered}
X_0[0], X_1[0] \ldots \ldots X_{s/k}[0] | X_0[1], X_1[1] \ldots \ldots X_{s/k}[1] | \ldots | X_0[k-1], X_1[k-1] \ldots \ldots X_{s/k}[k-1] \\
\odot \\
W_{t'-1,0}, W_{t'-1,0} \ldots \ldots W_{t'-1,0} | W_{t'-1,1}, W_{t'-1,1} \ldots \ldots W_{t'-1,1} | \ldots | W_{t'-1,k-1}, W_{t'-1,k-1} \ldots \ldots W_{t'-1,k-1} \\
= Z_{t'-1,0 \sim k-1}
\end{gathered} \tag{3}
$$

以上共有t'个,即表示前k个特征与特征矩阵的前k列相乘的结果

同理，我们继续完成特征k~(2k-1）的运算

$$
\begin{gathered}
X_0[k],X_1[k]....X_{s/k-1}[k]|X_0[k+1],X_1[k+1].....X_{s/k-1}[k+1]|...|X_0[2k-1],X_1[2k-1]......X_{s/k-1}[2k-1] \\
\odot \\
W_{0,k},W_{0,k}......W_{0,k}|W_{0,k},W_{0,k}....W_{0,k}|...|W_{0,2k-1},W_{0,2k-1}......W_{0,2k-1} \\
=Z_{0,k\sim(2k-1)}
\end{gathered}
$$

......

$$
\begin{gathered}
X_0[k],X_1[k]....X_{s/k-1}[k]|X_0[k+1],X_1[k+1].....X_{s/k-1}[k+1]|...|X_0[2k-1],X_1[2k-1]......X_{s/k-1}[2k-1] \\
\odot \\
W_{t'-1,k},W_{t'-1,k}......W_{t'-1,k}|W_{,k},W_{0,k}......W_{0,k}|...|W_{0,2k-1},W_{0,2k-1}......W_{0,2k-1} \\
=Z_{t'-1,k\sim(2k-1)}
\end{gathered}
$$

......

......

......

最后k个特征

$$
\begin{gathered}
X_0[t-k]......X_{s/k-1}[t-k]|X_0[t-k+1]......X_{s/k-1}[t-k+1]|...|X_0[t-1],X_1[t-1]......X_{s/k-1}[t-1] \\
\odot \\
W_{0,t-k},W_{0,t-k}......W_{0,t-k}|W_{0,t-k+1}......W_{0,t-k+1}|...|W_{0,t-1},W_{0,t-1}......W_{0,t-1} \\
=Z_{0,k\sim(2k-1)}
\end{gathered} \tag{6}
$$

......

$$
\begin{gathered}
X_0[t-k]......X_{s/k-1}[t-k]|X_0[t-k+1]......X_{s/k-1}[t-k+1]|...|X_0[t-1],X_1[t-1]......X_{s/k-1}[t-1] \\
\odot \\
W_{t'-1,t-k},W_{t'-1,t-k}......W_{t'-1,t-k}|W_{t'-1,t-k+1}......W_{t'-1,t-k+1}|...|W_{t'-1,t-1},W_{t'-1,t-1}......W_{t'-1,t-1} \\
=Z_{t'-1,k\sim(2k-1)}
\end{gathered} \tag{7}
$$

接下来将上述中间结果合并

For i=0-t'-1
Z^i=$\sum_{j=0}^{t/k-1} Z_{i,j*k-(j+1)*k-1}$

将Z^i进行$logk$次旋转和$\oplus$，得到的结果如下

$$
Z_0^i,Z_1^i,Z_2^i,Z_3^i....Z_{s/k}^i|Z_0^i,Z_1^i,Z_2^i,Z_3^i....Z_{s/k}^i|....|Z_0^i,Z_1^i,Z_2^i,Z_3^i....Z_{s/k}^i \tag{8}
$$

上述Z_m^i表示第m个样本与权重矩阵的第i行的计算结果，形如上述的结果共有t'个,即第m个样本在第i个神经元的输出结果

之后我们对上述t'个密文做激活函数$\phi(Z^i)$，得到如下的密文

$$U_0^i,U_1^i,U_2^i,U_3^i....U_{s/k}^i|U_0^i,U_1^i,U_2^i,U_3^i....U_{s/k}^i|....|U_0^i,U_1^i,U_2^i,U_3^i....U_{s/k}^i \tag{9}$$

我们此时生成一些掩码

$$\begin{aligned} m_1 &= [1,1,1,1,1,1......|0,0,0,0,0,0,0....|0,0,0,0,0,0........|0,0,0,0,0,0,0.......] \\ m_2 &= [0,0,0,0,0,0......|1,1,1,1,1,1,1....|0,0,0,0,0,0........|0,0,0,0,0,0,0.......] \\ m_3 &= [0,0,0,0,0,0......|0,0,0,0,0,0,0....|1,1,1,1,1,1........|0,0,0,0,0,0,0.......] \\ & .... \\ m_{t'-1} &= [0,0,0,0,0,0......|0,0,0,0,0,0,0......|0,0,0,0,0,0,0.....|1,1,1,1,1,1,1.....] \end{aligned} \tag{10}$$

将上述掩码与对应的Z^i相乘，再相加，得到如下的t'/k个密文

$$U_0^0,U_1^0,U_2^0....U_{s/k-1}^0|........|U_0^{k-1},U_1^{k-1},......U_{s/k-1}^{k-1} \tag{11}$$

$$U_0^k,U_1^k,U_2^k....U_{s/k-1}^k|........|U_0^{2k-1},U_1^{2k-1},......U_{s/k-1}^{2k-1} \tag{12}$$

....

$$U_0^{t'-k},U_1^{t'-k},U_2^{t'-k}....U_{s/k-1}^{t'-k}|........|U_0^{t'-1},U_1^{t'-1},......U_{s/k-1}^{t'-1} \tag{13}$$

得到上述的t'-k 个密文后，与输出层的权重矩阵$W_{t''\times t'}$进行运算

$$\begin{gathered} U_0^0,U_1^0,U_2^0....U_{s/k-1}^0|........|U_0^{k-1},U_1^{k-1},......U_{s/k-1}^{k-1} \\ \odot \\ W_{0,0},W_{0,0},W_{0,0}....W_{0,0}|........|W_{0,k-1},W_{0,k-1}.......W_{0,k-1} \\ =O_{0,0\sim k-1} \end{gathered} \tag{14}$$

$$\begin{gathered} U_0^0,U_1^0,U_2^0....U_{s/k-1}^0|........|U_0^{k-1},U_1^{k-1},......U_{s/k-1}^{k-1} \\ \odot \\ W_{1,0},W_{1,0},W_{1,0}....W_{1,0}|........|W_{1,k-1},W_{1,k-1}.......W_{1,k-1} \\ =O_{1,0\sim k-1} \end{gathered} \tag{15}$$

....

$$\begin{gathered} U_0^0,U_1^0,U_2^0....U_{s/k-1}^0|........|U_0^{k-1},U_1^{k-1},......U_{s/k-1}^{k-1} \\ \odot \\ W_{t'',0},W_{t'',0},W_{t'',0}....W_{t'',0}|........|W_{t'',k-1},W_{t'',k-1}.......W_{t'',k-1} \\ =O_{t'',0\sim k-1} \end{gathered} \tag{16}$$

以上为第0～s/k个样本在前k个隐藏层的神经元的输出与输出层的权重矩阵相乘的中间结果

....

$$
\begin{gathered}
U_0^{t'-k}, U_1^{t'-k}, U_2^{t'-k} \ldots . U_{s/k-1}^{t'-k} | \ldots \ldots . . | U_0^{t'-1}, U_1^{t'-1}, \ldots \ldots U_{s/k-1}^{t'-1} \\
\odot \\
W_{0,t'-k}, W_{0,t'-k}, W_{0,t'-k} \ldots . W_{0,t'-k} | \ldots \ldots . . | W_{0,t'-1}, W_{0,t'-1} \ldots \ldots W_{0,t'-1} \\
= O_{0,t'-k \sim t'-1}
\end{gathered} \tag{17}
$$

$$
\begin{gathered}
U_0^{t'-k}, U_1^{t'-k}, U_2^{t'-k} \ldots . U_{s/k-1}^{t'-k} | \ldots \ldots . . | U_0^{t'-1}, U_1^{t'-1}, \ldots \ldots U_{s/k-1}^{t'-1} \\
\odot \\
W_{1,t'-k}, W_{1,t'-k}, W_{1,t'-k} \ldots . W_{1,t'-k} | \ldots \ldots . . | W_{1,t'-1}, W_{1,t'-1} \ldots \ldots W_{1,t'-1}
\end{gathered} \tag{18}
$$

....

$$
\begin{gathered}
U_0^{t'-k}, U_1^{t'-k}, U_2^{t'-k} \ldots . U_{s/k-1}^{t'-k} | \ldots \ldots . . | U_0^{t'-1}, U_1^{t'-1}, \ldots \ldots U_{s/k-1}^{t'-1} \\
\odot \\
W_{t'',t'-k}, W_{t'',t'-k}, W_{t'',t'-k} \ldots . W_{t'',t'-k} | \ldots \ldots . . | W_{t'',t'-1}, W_{t'',t'-1} \ldots \ldots W_{t'',t'-1}
\end{gathered} \tag{19}
$$

同理上述为第0～s/k个样本在t'-k～t'-1个隐藏层神经元的输出与输出层的权重矩阵第t'-k～t'-1列相乘的结果

同隐藏层，我们将上述结果合并

For i=0～t''-1

$O_i = \sum_{j=0}^{t/k-1} O_{i,j*k-(j+1)*k-1}$

O_i 进行$logk$ 次旋转和⊕操作后，形式如下

$$
O_0^i, O_1^i, O_2^i, O_3^i \ldots . O_{s/k-1}^i | O_0^i, O_1^i, O_2^i, O_3^i \ldots . O_{s/k-1}^i | \ldots . | O_0^i, O_1^i, O_2^i, O_3^i \ldots . O_{s/k-1}^i \tag{20}
$$

其中O_i^j表示第i个样本与权重矩阵第j行的计算结果（即输出层第j个神经元的输出），这样的密文我们有t''个，

若我们可以指数函数近似计算该结果

则有

$$
e^{O_0^i}, e^{O_1^i}, e^{O_2^i} \ldots . . | e^{O_0^i}, e^{O_1^i}, e^{O_2^i} \ldots . . | \ldots \ldots . \tag{21}
$$

将上述t''个密文采用⊕操作后，可以得到如下$\sum_{j=0}^{t''} e^{O_0^j}, \sum_{j=0}^{t''} e^{O_1^j}, \sum_{j=0}^{t''} e^{O_2^j} \ldots \ldots$.即softmax函数的分母部分

此时我们就可以计算得到Softmax函数的结果