DCMMC

A NOTE IN MACHINE LEARNING

Table of Contents

List of Figures

List of Tables

About this Note

Note that most of symbols in this note are vector, matrix, or tensor. Strictly speaking, we should write them as bold to differ from scalars. But for simplification, most bolds of them are ignored in this note.

Also,$\times$in superscript will leads into overflow in this latex source code. Therefore, all$\times$are replaced by $*$ in superscripts.

When there is no possibility for confusion, we write the propability $Pr(W = w)$ where W is the random variable and w is the specific value to the shorthands $P(w)$.

TODO(DCMMC)...

1 | NLP with DL

Natural Language Processing with Deep Learning – Stanford CS224n Winter 2019

Learning Objectives:

- Word Vector
- Calculus Review
- RNN & Language Model
- Seq2Seq & Attention
- ConvNet for NLP
- Transformer

1.1 Word Vector

Arguably the most simple word vector, i.e., **one-hot vector**: an $\mathbb{R}^{|V|*1}$ vector with one 1 and the rest 0s. Note that these one-hot vectors are **orthogonal** (i.e., no similarity/relastionship) and V is a very big vocabulary ($\sim 500k$ words for english).

Another idea: **distributional representation** in modern statistical NLP. A word's meaning is given by the words that frequently appear close-by. Using some N-dim ($N \ll |V|$) space is sufficient to encode all semantics of our language into a dense vector. Once we get the word embedding matrix where each column is a word vector, we can query the word vector from one-hot representation by treating it as **lookup table** instead of using matrix product.

To evaluate word vectors, there are two fold: *intrinsic* (directly used, e.g. word analogies/similarity) and *extrinsic* (indirectly used in real task, e.g. Q&A). Word vector analygies for $a : b :: c : d$ is calculated by cosine similarity as example shown in Fig. 1.1:

$$d = \arg\max_i \frac{(x_b - x_a + x_c)^\top x_i}{\|x_b - x_a + x_c\|} \tag{1.1}$$

If we have hundreds of millions of words, it's okay to start the vectors *randomly*. If there is a *small* ($\leq 100,000$) training data set, it's best to just treat the pre-trained word vectors as *fixed*. In the other hand, if there is a large dataset, then we can gain by **fine tuning** of the word vectors.

Dependencies: Machine Learning Basic

In traditional NLP (before 2013), words are regarded as discrete symbols (**localist** representation) and cannot capture similarity. One-hot vector is an example.

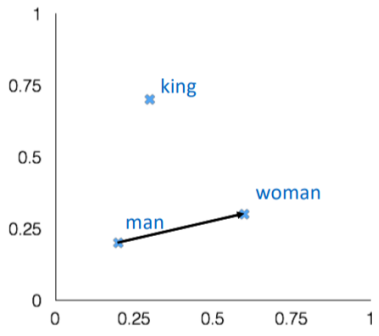

Figure 1.1: An example of word analogy of man:woman :: king:?

1.1.1 Word2vec

Two families of models: **Skip-gram** and **Continuous Bag of Words**.

Idea of **Skip-gram** (predicting context words by a given center word) in Word2vec[1]:

[1] Mikolov et al. 2013

- a large corpus of text T with a vocabulary V
- every word is represented by a vector $w \in \mathbb{R}^d$ and start off as a random vector
- use the (cosine) similarity of the word vectors for c (center word) and o (context/outside word) to calculate the probability of o given c: $p(w_o|w_c)$
- adjusting the word vectors to maximize the probability

Why we use two vectors per word? Make it simpler to calculate the gradient of loss function. Because the center word would be one of the choices for the context word and thus squared terms are imported. Average both vectors at the end is the final word vector.

The conditional probability is calculated by the **softmax** (normalize to probability distribution) of **cosine** similarity (review dot product: $\boldsymbol{a} \cdot \boldsymbol{b} = |\boldsymbol{a}||\boldsymbol{b}| \cos\langle \boldsymbol{a}, \boldsymbol{b} \rangle$). Note that the visualization of word vectos utilizes 2D projection (e.g. PCA) that will loss huge information.

$$p(w_o|w_c) = \frac{\exp(u_o^\top v_c)}{\sum_{w \in V}(u_w^\top v_c)} \tag{1.2}$$

where v_c denotes the center word vector of w when w is used as a center word in the formula, and u_w denotes the context word vector of w as the similar way. A demo of the window size and conditional probability is shown in Fig. 1.2.

The objective function (a.k.a loss or cost function) is given by the (average) negative log likelihood (abbr. **NLL**). The parameters of the model are adjusted by minimizing the loss function $J(\theta)$ or maximizing the likelihood. This is, give a high probability estimate to those words that occur in the context and low probability to those don't typically occur in the context.

$$\begin{aligned}
\arg\max_\theta L(\theta) &= \prod_{c=1}^{T} p(w_{c-m}, \cdots, w_{c-1}, w_{c+1}, \cdots, w_{c+m}|w_c; \theta) \\
&= \prod_{c=1}^{T} \prod_{\substack{-m \le j \le m \\ o=j+c \\ o \ne c}} p(w_o|w_c; \theta) \\
&\Downarrow \\
\arg\min_\theta -\frac{1}{T} \log L(\theta) &= -\frac{1}{T} \sum_{c=1}^{T} \sum_{\substack{-m \le j \le m \\ o=j+c \\ o \ne c}} \log p(w_o|w_c; \theta)
\end{aligned}$$

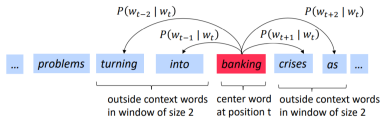

Figure 1.2: A demo of the window size and $p(w_o|w_c)$

$$= -\frac{1}{T}\sum_{c=1}^{T}\sum_{\substack{-m\le j\le m\\ o=j+c\\ o\neq c}}\left(u_o^\top v_c - \log\sum_{w\in V}\exp(u_w^\top v_c)\right) \tag{1.3}$$

where m is the window size, $\theta \in \mathbb{R}^{2d|V|}$ represents all model parameters. And we assume that $p(\cdot|w_c)$ are **i.i.d**.

The properties of log and arg max (arg min) used in Eq. 1.3 are VERY useful. $\exp(\cdot)$ ensures anything positive.

We use **gradient descent** (i.e. averaged gradient of all samples/windows) to optimize the loss function. Note that stochastic (one sample/window with noisy estimates of the gradients) or mini-batch (a subset of samples/windows with size powered of 2 such as 64) gradient descent methods are useful to prevent overfitting and train for large dataset. Calculating the gradient of the loss function is trivial:

$$\begin{aligned}\frac{\partial J}{\partial v_c} &= -\frac{1}{T}\sum_{c=1}^{T}\sum_{\substack{-m\le j\le m\\ o=j+c\\ o\neq c}}\left(u_o - \sum_{x\in V}\frac{\exp(u_x^\top v_c)u_x}{\sum_w \exp(u_w^\top v_c)}\right)\\ &= -\frac{1}{T}\sum_{c=1}^{T}\sum_{\substack{-m\le j\le m\\ o=j+c\\ o\neq c}}\left(u_o - \sum_{x\in V} p(w_x|w_c)\cdot u_x\right)\end{aligned} \tag{1.4}$$

$$\frac{\partial J}{\partial u_o} = -\frac{1}{T}\sum_{c=1}^{T}\sum_{\substack{-m\le j\le m\\ o=j+c\\ o\neq c}}(v_c - p(w_o|w_c)) \tag{1.5}$$

Iteratively update equation (naïve version) is given by:

$$\theta^{new} = \theta^{old} - \alpha\nabla_\theta J(\theta) \tag{1.6}$$

where α is the learning size (step size) such as 10^{-3}.

Note that the summation over $|V|$ ($\sum_{x\in V}$) is very expensive to compute! For every training step, instead of looping over the entire vocabulary, we can just sample several negative examples! **negative sampling**: train binary logistic regression instead. $p(D=1|w_o, w_c)$ denotes the probability when (w_o, w_c) came from the same window pf the corpus data, and $p(D=0|w_o, \tilde{w}_o)$ is the probability given $(w_o, \tilde{w}_o)$ did not come from the same window (i.e. noisy/invalid pair). Randomly sample a bunch of noise words from the **unigram distribution** raised to the power of $3/4$: $p(w) = {}^{U(w)^{3/4}}/_{Z}$, where $U(w)$ is the counts for every unique words (i.e. unigram) and Z is the nomalization term.

To avoid high frequence effect of words such as **of** and **the**, one simple way is just lop off the first biggest component in the word vector. The unigram with power of $3/4$ in word2vec is also a trick to handle the effect, where it decrease how often you sample very common words and increase how often you sample rare words.

The objective function is also come from NLL:

$$J(\theta) = -\frac{1}{T}\sum_{c=1}^{T}\sum_{\substack{-m\le j\le m\\ o=j+c\\ o\neq c}}\left(\log\sigma\left(u_o^\top v_c\right) + \sum_{j\sim p(w)}\left[\log\sigma\left(-u_j^\top v_c\right)\right]\right) \tag{1.7}$$

where **sigmoid** function is $\sigma(x) = \frac{1}{1+e^{-x}}$ which can be seen as the 1D (binary) version of softmax and used to output the probability, and k is the number of negative samples such as 5 and 15. Note that according to the symmetric property of sigmoid function we get: $P(D=0|\tilde{w}_j, w_c) = 1 - P(D=1|\tilde{w}_j, w_c) = \sigma\left(-u_j^\top v_c\right)$.

Although word2vec model is fairly simple and clean, there are actually many tricks which aren't particularly theoretical.

Continuous Bag of Words (CBOW): predict center word from (bag of) context words. Similar to Skip-gram, the objective function is formulated as:

$$J = -\frac{1}{T}\sum_{c=1}^{T}\log P(w_c|w_{c-m},\cdots,w_{c-1},w_{c+1},\cdots,w_{c+m}) \tag{1.8}$$

$$= -\frac{1}{T}\sum_{c=1}^{T}\log p(v_c|\hat{u}) \tag{1.9}$$

$$= -\frac{1}{T}\sum_{c=1}^{T}\log \underset{c}{\text{softmax}}(v_c^\top \hat{u}) \tag{1.10}$$

$$= -\frac{1}{T}\sum_{c=1}^{T}(v_c^\top \hat{u} - \log\sum_{j=1}^{|V|}\exp(v_j^\top \hat{u})) \tag{1.11}$$

where $\hat{u} = \frac{1}{2m}\sum_{\substack{-m\le j\le m\\ o=j+c\\ o\neq c}} u_o$

Although word2vec can capture complex patterns beyond word similarity, it has inefficient usage of statistics (i.e. rely on sampling rather than directly use counts of words).

1.1.2 HW1

A simple intro to co-occurrence matrix, SVD, cosine similarity, and some applications (e.g. word analogy) of word2vec.

1.1.3 GloVe

1. I enjoy flying.
2. I like NLP.
3. I like deep learning.

The resulting counts matrix will then be:

$$X = \begin{array}{c} \\ I \\ like \\ enjoy \\ deep \\ learning \\ NLP \\ flying \\ . \end{array} \begin{array}{c} \begin{array}{cccccccc} I & like & enjoy & deep & learning & NLP & flying & . \end{array} \\ \begin{bmatrix} 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Figure 1.3: An example of co-occurrence matrix with window size of 1

Co-occurrence matrix $X \in \mathbb{R}^{|V|*|V|}$ with window size k. Fig. 1.3 shows an example. Note that such matrix is extremely sparse and very high dimensional, and the dimensions of the matrix change very often as new words are added very frequently and corpus changes in size. We can perform SVD on X to reduce the dimensionality to $25 \sim 1000$-dim. In addition, there are some hacks to X that transform the raw count introduced by [2]: (1) set upper bound (e.g. 100) or just ignore them all for the counts of too frequent words, (2) ramped windows that count closer words more. (3) use Pearson correlations instead of counts. Note that they made some interesting observation in their word vector that the verb (e.g. swim) and the corresponding doer (e.g. swimmer) pairs are roughly *linear components* (e.g. $\boldsymbol{v}_{swimmer} - \boldsymbol{v}_{swim} = k(\boldsymbol{v}_{driver} - \boldsymbol{v}_{drive})$).

[2] Rohde et al. 2005

TODO(DCMMC)...SVD

Although the aforementioned conventional method has disproportionate importance given to large counts and mainly only capture word similarity, it enjoys the fast training and efficient usage of statistics. GloVe (**Glo**bal **Ve**ctor) [3] combines the advantages from both of this conventional method (global count matrix factorization) and the DL-based methods (local context window methods) such as word2vec. It captures global corpus statistics directly.

[3] Pennington et al. 2014

Probability and Ratio	k = *solid*	k = *gas*	k = *water*	k = *fashion*
$P(k\|ice)$	1.9×10^{-4}	6.6×10^{-5}	3.0×10^{-3}	1.7×10^{-5}
$P(k\|steam)$	2.2×10^{-5}	7.8×10^{-4}	2.2×10^{-3}	1.8×10^{-5}
$P(k\|ice)/P(k\|steam)$	8.9	8.5×10^{-2}	1.36	0.96

Figure 1.4: An example of the conditional probabilities and their ratio in GloVe paper.

Some notations: X_{ij} tabulate the number of times word j occurs in the context of word i, $X_i = \sum_k X_{ik}$ is the number of times any word appears in the context of word i i.e., the nomalization denominator. $P_{ij} = P(j|i) = {}^{X_{ij}}/_{X_i}$ is the probability that word j appear in the context of word i. The crucial insight is that the *ratios* of co-occurrence probabilities as shown in Fig. 1.4 to encode meaning components. We'd like to leverage the word vectors $w_i, w_j, \tilde{w}_k$ to represent such ratio: $F(w_i, w_j, \tilde{w}_k) = {}^{P_{ik}}/_{Pjk}$, where $\tilde{w}$ is a seperate *context* word vector for various *probe words* k, instead of the word vector w (similar to center word vector in skip-gram).

We can select a unique choice of F by enforcing a few desiderata (i.e. restrictions). To fit the demand of the *linear components* and the output *scalar* value, in addition to the *homomorphism* between the groups $(\mathbb{R}, -)$ and $(\mathbb{R}^+, \div)$ (i.e., $F(i,j) = {}^{P_{ik}}/_{Pjk} = {}^{1}/_{F(j,i)} = {}^{P_{jk}}/_{Pik}$), we can derivate that $F(w_i, w_j, \tilde{w}_k) = F\left((w_i - w_j)^\top \tilde{w}_k\right) = {}^{F(w_i^\top \tilde{w}_k)}/_{F(w_j^\top \tilde{w}_k)} = {}^{P_{ik}}/_{P_{jk}}$. Therefore, $F = \exp, w_i^\top \tilde{w}_k = \log(P_{ik}) = \log(X_{ik}) - \log(X_i)$. Note that the symmetry property of co-occurrence: $X_{ik} = X_{ki}$. We add two biases to restore the symmetry: $w_i^\top \tilde{w}_k + b_i + \tilde{b}_k = \log(X_{ik})$, where we can analogy that $b_i + \tilde{b}_j = \log X_i$.

More details, the relationship to the "global skip-gram" and the complexity refer to the original GloVe paper [4].

[4] Pennington et al. 2014

To handle the ill-defined log function when its argument be 0 (its common that $X_{ij} = 0$), the authors use the factorized log: $\log(X_{ik}) \to \log(1 + X_{ik})$.

$$w_i \cdot w_j = \log P(i|j) \tag{1.12}$$

$$w_x \cdot (w_a - w_b) = \log \frac{P(x|a)}{P(x|b)} \tag{1.13}$$

Therefore, the ratios of co-occurrence probabilities is the **log-bilinear model with vector differences**. The final objective function is *weighted* **least squares** (MSE) for this regression problem.

$$J = \sum_{i,j=1}^{V} f(X_{ij}) \left(\boldsymbol{w}_i^\top \tilde{\boldsymbol{w}}_j + b_i + \tilde{b}_j - logX_{ij} \right)^2 \tag{1.14}$$

where weighted function (is also a hyperparamter) is:

$$f(x) = \begin{cases} \left(\frac{x}{x_{max}}\right)^\alpha & \text{if } x < x_{max} \\ 1 & \text{otherwise} \end{cases} \tag{1.15}$$

where $x_{max} = 100, \alpha = 3/4$ (*empirical* value).

1.1.4 Word sense ambiguity

Because most words have lots of meanings. One crude way [5] is to cluster word windows around words, retrain with each word assigned to multiple different clusters bank_1, bank_2, etc. Another method [6] is weighted sum of different senses of a word reside in a linear superposition, e.g.:

[5] Huang et al. 2012

[6] Arora et al. 2018

$$v_{\text{pike}} = \alpha_1 v_{\text{pike}_1} + \alpha_2 v_{\text{pike}_2} + \alpha_3 v_{\text{pike}_3} \tag{1.16}$$

where $\alpha_i = \frac{f_i}{\sum_{j=1}^{3} f_j}$ for frequency f.

The result is counterintuitive very well, because of the idea from *sparse* coding you can actually separate out the senses.

1.2 Math Backgrounds

For **multi-class classification** problem, **NLL** (negative likelihood loss) is the objective function of **Maximum Likelihood Estimate** (abbr, MLE):

$$J(\boldsymbol{\theta}) = -\sum_i \log p(y = y_i^{true}|\boldsymbol{x}_i; \boldsymbol{\theta}) \tag{1.17}$$

cross entropy (distance measure) between (discrete) distribution p and q is more convenient way:

$$H(p, q) = -\sum_{c=1}^{C} p(c) \log q(c) \tag{1.18}$$

However, in the multi-class (with single label) setting, the p(c) is the **ground truth distribution** which has the *one-hot* style (**empirical distribution**), i.e. $p = [0, \cdots, 0, 1, 0, \cdots, 0]$ where 1 at the right class and 0 everywhere else. Therefore, the **cross entropy** in the multi-class classification is *equal* to the NLL.

A simple k-class model example is **dense layer** with *softmax*:

$$p(y|\boldsymbol{x}; \boldsymbol{\theta}) = softmax(\boldsymbol{W}_2 f(\boldsymbol{W}_1 \boldsymbol{x} + \boldsymbol{b})) \tag{1.19}$$

where $\boldsymbol{\theta} = [\boldsymbol{W}_1, \boldsymbol{b}, \boldsymbol{W}_2]^\top$ are the parameters, $\boldsymbol{x} \in \mathbb{R}^m, \boldsymbol{W}_1 \in \mathbb{R}^{n*m}, \boldsymbol{b} \in \mathbb{R}^n, \boldsymbol{W}_2 \in \mathbb{R}^{k*n}$, $f(\cdot)$ is a kind of simple activate (non-linear) function to provide non-linearity, such as $ReLU(x) = max(0, x)$. The visualization of neural network refer to [7].

[7] ConvNetJS: https://cs.stanford.edu/people/karpathy/convnetjs/demo/classify2d.html

The **Jacobian Matrix** (generalization of the gradient) of function $\boldsymbol{f}(\boldsymbol{x}) : \mathbb{R}^n \to \mathbb{R}^m$ is a $m \times n$ matrix: $\left(\frac{\partial \boldsymbol{f}}{\partial \boldsymbol{x}}\right)_{ij} = \frac{\partial f_i}{x_j}$.

Supposed that we have a function $\boldsymbol{g}(\boldsymbol{f}(x)), \boldsymbol{f} : \mathbb{R} \to \mathbb{R}^2, \boldsymbol{g} : \mathbb{R}^2 \to \mathbb{R}^2$, we can compute the partial derivative of $\boldsymbol{g}$ w.r.t x by **chain rule**:

$$\frac{\partial \boldsymbol{g}}{\partial x} = \begin{bmatrix} \frac{\partial g_1}{\partial f_1}\frac{\partial f_1}{x} + \frac{\partial g_1}{\partial f_2}\frac{\partial f_2}{x} \\ \frac{\partial g_2}{\partial f_1}\frac{\partial f_1}{x} + \frac{\partial g_2}{\partial f_2}\frac{\partial f_2}{x} \end{bmatrix} \tag{1.20}$$

$\frac{dg_1}{d\boldsymbol{y}} = \frac{\partial g_1}{y_1} + \frac{\partial g_2}{y_2}$ is the relationship of the full differential and the partial differential.

It is the same as multiplying the two Jacobians:

$$\frac{\partial \boldsymbol{g}}{\partial x} = \frac{\partial \boldsymbol{g}}{\partial \boldsymbol{f}}\frac{\partial \boldsymbol{f}}{\partial x} = \begin{bmatrix} \frac{\partial g_1}{\partial f_1} & \frac{\partial g_1}{\partial f_2} \\ \frac{\partial g_2}{\partial f_1} & \frac{\partial g_2}{\partial f_2} \end{bmatrix} \begin{bmatrix} \frac{\partial f_1}{\partial x} \\ \frac{\partial f_2}{\partial x} \end{bmatrix} \tag{1.21}$$

There are some useful identities:

- $\frac{\partial \boldsymbol{x}}{\partial \boldsymbol{x}} = \boldsymbol{I}$
- $\frac{\partial \boldsymbol{W}\boldsymbol{x}}{\partial \boldsymbol{x}} = \boldsymbol{W}$, $\frac{\partial \boldsymbol{u}^\top \boldsymbol{x}}{\partial \boldsymbol{x}} = \boldsymbol{u}^\top$
- $\frac{\partial \boldsymbol{x}^\top \boldsymbol{W}}{\partial \boldsymbol{x}} = \boldsymbol{W}^\top$

- For elemenwise function $\boldsymbol{f}(\boldsymbol{x})$: $\frac{\partial \boldsymbol{f}}{\partial \boldsymbol{x}} = \texttt{diag}(\boldsymbol{f}'(\boldsymbol{x}))$
- $\frac{\partial \boldsymbol{\theta}^\top (\boldsymbol{W} \cdot \boldsymbol{h})}{\partial \boldsymbol{W}} = \boldsymbol{\theta}\boldsymbol{h}^\top$ where $\boldsymbol{\theta} \in \mathbb{R}^{D_\theta * 1}, \boldsymbol{W} \in \mathbb{R}^{D_\theta * D_h}, \boldsymbol{h} \in \mathbb{R}^{D_h * 1}$
- For cross entropy loss: $J(\boldsymbol{h}) = -\boldsymbol{y}^\top \log(\hat{\boldsymbol{y}}) = -\boldsymbol{y}^\top \log \texttt{softmax}(\boldsymbol{h})$ ($\boldsymbol{y}$ is one-hot vector) is: $\frac{\partial J}{\partial \boldsymbol{h}} = (\hat{\boldsymbol{y}} - \boldsymbol{y})^\top$

We can use **backward propagation** (reversed of the *topological sort*) and *re-use* intermediate nodes to reduce complexity in the *computation graph*.

Other machine learning basic concepts are: **regularization** (e.g. L2) to prevent **overfitting**, vectorization to parallelization, (non-linear) **activation function** (e.g. sigmoid, tanh, (leaky) ReLU), parameter initialization (e.g. Xavier), **Optimizer** (e.g. RMSprop, Adam), learning rate.

Compared with activations such as sigmoid and tanh, ReLU does not *saturate* even for larger values. Note that ReLU is not *differentiable* at 0, where we can use *sub-derivatives* in implementation with a certain value such as 0 or 1.

1.2.1 Data Preprocessing

- **Mean Subtraction (Shifting)**: Shifting all data so that they have zero mean as shown in Fig. 1.5. Formally, $\boldsymbol{x}^{(i)} \leftarrow \boldsymbol{x}^{(i)} - \mathbb{E}[\boldsymbol{x}^{(i)}]$ for sample i, where $\mathbb{E}$ indicates mean.
- **Normalization (Scaling)**: Scale every input feature dimension to have similar ranges of magnitudes, as shown in Fig. 1.6. This is useful since input features are often measured in different "units", but we often want to initially consider all features as equally important. Formally, $x_j^{(i)} \leftarrow \frac{x_j^{(i)}}{\sigma_i(x_j^{(i)})}$ for feature j in sample i where $\sigma(\cdot)$ is the standard variance over $x_j^{(0)}, \cdots, x_j^{(N)}$.
- **Whitening**: Whitening converts the data to a have an identity covariance matrix - that is, features become uncorrelated and have a variance of 1. In the specific, we can divide the principal components achieved from PCA by the square roots of their eigenvalues (singular value).

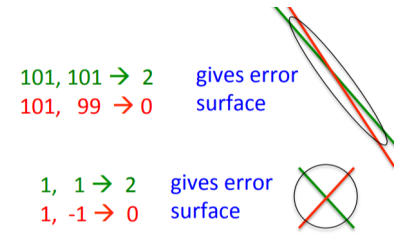

Figure 1.5: An exmaple of mean subtration.

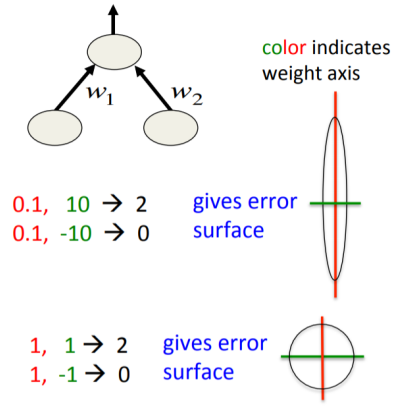

Figure 1.6: An example of normalization.

1.2.2 Parameter Initialization

If two hidden units have exactly the same bias and exactly the same incoming and outgoing weights (e.g. different channels for learning different features in the same convolutional layer), they will always get exactly the same gradient. So we should initialize the weights to small random values.

A good starting strategy is to initialize the weights to small random numbers of **normal distribution** with the mean around 0. Xavier et al. [8] suggest that for sigmoid and tanh activation units,

[8] Glorot and Bengio 2010

it's better for the weight matrix $W \in \mathbb{R}^{n^{(l+1)} * n^{(l)}}$ to be initialized randomly with a **uniform distribution**:

$$W \sim U\left[-\sqrt{\frac{6}{n^{(l)}+n^{(l+1)}}}, \sqrt{\frac{6}{n^{(l)}+n^{(l+1)}}}\right] \tag{1.22}$$

where $n^{(l)}, n^{(l+1)}$ are also called **fan-in** and **fan-out**. Besides, bias units are initialized to 0.

1.2.3 Optimizer

To avoid a diverging loss (too large learning step) or unconverging (too small learning step), there are some learning strategies.

Annealing: start off with a high learning rate to approach a minimum quickly, after several iterations, the learning rate is reduced in some way under a more fine-grained scope.

- Exponential decay: $\alpha(t) = \alpha_0 e^{-kt}$ where α_0 is initial learning rate.
- Decrease over time: $\alpha(t) = {(\alpha_0 \tau)}/{\max(t,\tau)}$ where τ denotes the time at which the learning rate should start reducing.

Momentum (a picture of it can be seen in Fig.1.7) based methods:

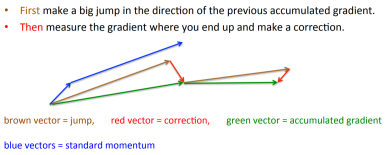

Figure 1.7: A picture of momentum.

- AdaGrad: $\boldsymbol{m} \leftarrow \boldsymbol{m} + \left(\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta})\right)^2, \boldsymbol{\theta} \leftarrow \boldsymbol{\theta} - \alpha \nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}) \odot \left(\sqrt{\boldsymbol{m}} + \epsilon\right)^{-1}$ where $\odot, (\cdot)^{-1}, (\cdot)^2, \sqrt{\cdot}$ are all element-wise operators, and ϵ is a very small value such as 10^{-8} to prevent **arithmetic underflow**. It leads to that parameters that have not been updated much in the past are likelier to have higher learning rates now.
- RMSprop: $\boldsymbol{m} \leftarrow \beta \boldsymbol{m} + (1-\beta)\left(\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta})\right)^2, \boldsymbol{\theta} \leftarrow \boldsymbol{\theta} - \alpha \nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}) \odot \left(\sqrt{\boldsymbol{m}} + \epsilon\right)^{-1}$ where β is the decay rate with default value 0.9. Unlike AdaGrad, its updates do not become monotonically smaller.
- Adam[9]: $\boldsymbol{m} \leftarrow \beta_1 \boldsymbol{m} + (1-\beta_1)\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}), \boldsymbol{v} \leftarrow \beta_2 \boldsymbol{v} + (1-\beta_2)\left(\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta})\right)^2, \hat{\boldsymbol{m}} = \boldsymbol{m}/(1-\beta_1^t), \hat{\boldsymbol{v}} = \boldsymbol{v}/(1-\beta_2^t), \boldsymbol{\theta} \leftarrow \boldsymbol{\theta} - \alpha \hat{\boldsymbol{m}}/\left(\sqrt{\hat{\boldsymbol{v}}} + \epsilon\right)$, where / is also a element-wise operator, hyperparameters $\beta_1 = 0.9, \beta_2 = 0.999 \in [0,1)$. $\hat{\boldsymbol{m}}, \hat{\boldsymbol{v}}$ are the bias-corrected $\boldsymbol{m}, \boldsymbol{v}$, and they indicate a rolling average of the gradients and a rolling average of the magnitudes of the gradients, respectively. In adition, $\boldsymbol{m}, \boldsymbol{v}$ are all initialized to $\mathbf{0}$ Adam is like a combination of RMSProp and momentum.

[9] Kingma and Ba 2014

For the implementation of momentum such as RMSprop, there is a interesting small trick: use $\boldsymbol{m} = \boldsymbol{m} - (1-\beta)(\boldsymbol{m} - (\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta}))^2)$ instead of $\boldsymbol{m} = \beta \boldsymbol{m} + (1-\beta)\left(\nabla_{\boldsymbol{\theta}} J(\boldsymbol{\theta})\right)^2$. In such way, we need calculate only one multiplication, compared with original two multiplications.

1.2.4 Regularization

1. Dropout

During training, **dropout** [10] randomly disables units in the hidden layer by a mask vector drawn from Bernoulli distribution where each entry is 0 with probability p_{drop} and 1 with probability $(1 - p_{\text{drop}})$:

[10] Srivastava et al. 2014

$$\text{Dropout Layer: } d_i \sim \text{Bernoulli}(1 - p_{\text{drop}}), \hat{\boldsymbol{h}}^{(t)} = \frac{1}{1 - p_{\text{drop}}} \boldsymbol{d} \odot \boldsymbol{h}^{(t)} \tag{1.23}$$

where $\odot$ is element-wise product, $\boldsymbol{d} \in \{0, 1\}^{D_h}, \boldsymbol{h}^{(t)} \in \mathbb{R}^{D_h}$.

If the expected output of a neuron during testing if far different as it was during training, the magnitude of the outputs could be radically different, and the behavior of the network is no longer well-defined. Therefore, all the parameters should divided by retain rate $1 - p$ (blue part in above formula), so that $\mathbb{E}_{p_{\text{drop}}}[\boldsymbol{h}_{\text{drop}}]_i = h_i$. If we do not such correction in training, we should multiply $1 - p$ to all related parameters.

If we use dropout in testing, the result is *unstable* (vary from every testing) because of the dropout is drawn from Bernoulli distribution. Therefore, we should apply dropout only during training but not during evaluation or testing.

A motivation of dropout is to reduce complex *co-adaptations* among the hidden units which comes from the superiority of sexual reproduction compared with asexual. The criterion for natural selection may be the mix-ability of genes. A gene which rely only on a *small* number of other genes is able to work well with another random set of genes that could come from another paraent's genes in sexual reproduction. Hence, it will more robust aginst noises and increases the chance of a new gene improving the fitness of an individual.

2. Batch Normalization

Although **batch nomalization** [11] is like nomalization used in data preprocessing with N be the mini-batch size instead of the dataset size, it is inserted between hidden layers to normalize the output of last layer. It leads to achieve the fixed distributions of inputs that would remove the ill effects of the internal covariate shift. *Internal Covariate Shift* is defined as the change in the distribution of network activations due to the change in network parameters during training.

[11] Ioffe and Szegedy 2015

The batch normalization in training is defined as follows:

$$\text{BN}(h_i) = \gamma \frac{h_i - \mu_{\mathcal{B}}}{\sqrt{\sigma_{\mathcal{B}}^2 + \epsilon}} + \beta \tag{1.24}$$

where γ, β are **trainable parameters**, $\mu_{\mathcal{B}}, \sigma^2_{\mathcal{B}}$ are the mean and variance over the mini-batch as the way of normalization for data preprocessing. Since the mean subtraction will *ignore* the learned bias which may useful to the model. The trainable γ and β are used to corrected them and make the BN layer trainable. Them ensure that the batch normalization inserted in the network can represent the identity transform.

However, when testing, we cannot use mini-batch in most time. We instead feed one sample into the model. Therefore, we leverage m training mini-batches to perform **unbiased estimates** of them:

$$\mathbb{E}[h_i] \leftarrow \mathbb{E}_{\mathcal{B}}[\mu_{\mathcal{B}}]$$
$$\texttt{Var}[h_i] \leftarrow \frac{m}{m-1}\mathbb{E}_{\mathcal{B}}[\sigma^2_{\mathcal{B}}]$$

Note that in many implementations, the above estimation is replaced with the way like the momentum used in RMSprop. More details refer to the source code, e.g. Keras. For the motivation, the use of BatchNorm makes models much less sensitive to parameter initialization.

1.2.5 Practice: Named Entity Recognition

To find and classify words as entities (e.g. location, or organization) in text. One simple idea is that train softmax classifier to classify a center word by taking *concatenation* of word vectors surrounding it in a window (*word window*) [12]. To perform NER of localtion, we need (unnormalized) score for each window, and make *true window*s (i.e. location in the center) score larger and other *corrupt window*s score lower. The model is formulated as:

[12] Collobert and Weston 2008

$$s = \boldsymbol{W}_2 f(\boldsymbol{W}_1 \boldsymbol{x} + \boldsymbol{b}) \tag{1.25}$$

The objective function (*max-margin loss*) is:

$$J = max(0, s_c - (s - 1)) \tag{1.26}$$

where s and s_c is the score of true window and corrupt window. It ensure each window with an NER location at its center should have a score $+1$ higher than any window without a location at its center.

1.2.6 HW2

Gradient calculation and implementation of word2vec.

1. Written: Understanding word2vec

(a) $\hat{y}_o = P(O = o|C = c)$

(b) $\dfrac{\partial J}{\partial \boldsymbol{v}_c} = (\hat{\boldsymbol{y}} - \boldsymbol{y})^\top \boldsymbol{U}^\top$

(c) $\dfrac{\partial J}{\partial \boldsymbol{U}} = \boldsymbol{v}_c(\hat{\boldsymbol{y}} - \boldsymbol{y})^\top$

(d) $\sigma(\boldsymbol{x}) = \dfrac{1}{1+\exp(-\boldsymbol{x})}, \dfrac{d\sigma(\boldsymbol{x})}{\boldsymbol{x}} = \texttt{diag}(\sigma(x_i)(1-\sigma(x_i)))$

(e) $\dfrac{\partial J}{\partial \boldsymbol{v}_c} = \sum_k \sigma(\boldsymbol{u}_k^\top \boldsymbol{v}_c)\boldsymbol{u}_k^\top - (1-\sigma(\boldsymbol{u}_o^\top \boldsymbol{v}_c))\boldsymbol{u}_o^\top$

$\dfrac{\partial J}{\partial \boldsymbol{u}_o} = (\sigma(\boldsymbol{u}_o^\top \boldsymbol{v}_c) - 1)\boldsymbol{v}_c^\top$

$\dfrac{\partial J}{\partial \boldsymbol{u}_k} = \sigma(\boldsymbol{u}_k^\top \boldsymbol{v}_c)\boldsymbol{v}_c^\top$

(f) $(i)\dfrac{\partial J}{\partial \boldsymbol{U}} = \sum_o \boldsymbol{v}_c(\hat{\boldsymbol{y}}_o - \boldsymbol{y}_o)^\top$

$(ii)\dfrac{\partial J}{\partial \boldsymbol{v}_c} = \sum_o (\hat{\boldsymbol{y}}_o - \boldsymbol{y}_o)^\top \boldsymbol{U}^\top$

$(iii)\dfrac{\partial J}{\partial \boldsymbol{v}_w} = \boldsymbol{0}$

2 Coding: Implementing word2vec

Use shape convention to check the result.

Note that $\boldsymbol{U}, \boldsymbol{V}$ in the handout are the matrices whose i-th column is the n-dimensional embedded vector for word w_i. However, in the codes of HW2, all the centerWordVectors and outsideVectors are as rows.

1.3 Dependency Parser

Two views of linguistic structure: (1) constituency (i.e., phrase structure grammar, or context-free grammar) (2) Dependency structure. Dependence parse trees (single root with optional fake root, acyclic) use binary asymmetric relations which depicted as typed arrows going from *head* to *dependent*. Note that the natural language is ambiguity.

Basic transition-based dependency parser [13] with stack σ = [ROOT], buffer $\beta = w_1, \cdots, w_n$, set of dependency arcs $A = \emptyset$, and a set of actions (*transitions*) based on the above 3-tuple:

[13] Nivre 2003

1. Shift: $\sigma, w_i|\beta, A \Rightarrow \sigma|w_i, \beta, A$
2. Left-Arc reduction: $\sigma|w_i|w_j, \beta, A \Rightarrow \sigma|w_j, \beta, A \cup \{r(w_j, w_i)\}$
3. Right-Arc reduction: $\sigma|w_i|w_j, \beta, A \Rightarrow \sigma|w_i, \beta, A \cup \{r(w_i, w_j)\}$

where $r(w_j, w_i)$ denotes w_i is the dependency of w_j (e.g. nsubj(ate $\rightarrow$ I)), | and $\cup$ stand for concatenate. The finish state is: $\sigma = [w], \beta = \emptyset$.

How to select (search) the best choice among the exponential size of different possible parse trees is the problem. In 1960s, they use *dynamic programming algorithms* ($\mathcal{O}(n^3)$). In paper [14], the authors predict each action by a discriminative classifier (e.g. SVM classifier) which is more efficient but the accuracy is fractionally below the state-of-the-art.

[14] Nivre 2003

1.3.1 Neural Dependency Parsing

Compared with traditional sparse feature-based discriminative dependency parsers, the work by [15] utilizes **feedforward neural network model** with simple **dense layers** and the softmax layer to predict each transition. The input features with embedding dimension d are:

[15] Chen and Manning 2014

1. $x^w \in \mathbb{R}^{d*N_w}$: The top 3 words on the stack and buffer $s_1, s_2, s_3, b_1, b_2, b_3$; the first and second leftmost / rightmost children of the top two words on the stack $lc_1(s_i), rc_1(s_i), lc_2(s_i), rc_2(s_i), i = 1, 2$; the leftmost of leftmost / rightmost of rightmost children of the top two words on the stack $lc_1(lc_1(s_i)), rc_1(rc_1(s_i)), i = 1, 2$; In total, $N_w = 18$.
2. $x^t \in \mathbb{R}^{d*N_t}$: The corresponding POS (Part-of-speech, e.g. noun, verb, adjective) tags for S_{word}, $N_t = 18$.
3. $x^l \in \mathbb{R}^{d*N_l}$: The corresponding arc labels of words, excluding those 6 words on the stack/buffer, $N_l = 12$.

Note that we use a special **NULL** token for non-existent elements: when the stack and buffer are empty or dependents have not been assigned yet.

The predicted class is the one of transitions (i.e. shift, left/right arc reduction): $p = \texttt{softmax}(\boldsymbol{W}_2 f(\boldsymbol{W}_1^w \boldsymbol{x}^w + \boldsymbol{W}_1^t \boldsymbol{x}^t + \boldsymbol{W}_1^l \boldsymbol{x}^l + \boldsymbol{b}_1) + \boldsymbol{b}_2)$, where $f(\cdot)$ is the activation function (e.g. ReLU, or x^3). The number of class is 3 when untyped reductions or $T * 2 + 1$ when typed reductions (e.g. left-arc reduction with type *nsubj*).

Here are mainly four types of parsing error:

- **Prepositional Phrase Attachment Error**
- **Verb Phrase Attachment Error**
- **Modifier Attachment Error**
- **Coordination Attachment Error**

1.3.2 HW3

1. Machine Learning & Neural Networks

(a) Adam

(i) Because $\beta = 0.9$, most of the final gradients ($\boldsymbol{m}$) come from the past (90%). Even if current gradients are varying much from previous, it only occupy $1 - \beta_1 = 0.1$ of the final gradients.

(ii) Parameters that have not been updated much in the past are likelier to have higher learning rates.

(b) Dropout

(i) If the expected output of a neuron during testing if far different as it was during training, the magnitude of the outputs could be radically different, and the behavior of the network is no longer well-defined. Thus, all the parameters should divided by retain rate $1 - p$, so that $\mathbb{E}_{p_{\text{drop}}}[\boldsymbol{h}_{\text{drop}}]_i = h_i$.

(ii) If we use dropout in testing, the result is unstable because of the dropout is drawn from Bernoulli distribution.

2. Neural Transition-Based Dependency Parsing

(a) The remaindered configuration is:

Stack	Buffer	New dependency	Transition
[ROOT, parsed, this]	[sentence, correctly]		SHIFT
[ROOT, parsed, this, sentence]	[correctly]		SHIFT
[ROOT, parsed, sentence]	[correctly]	sentence → this	LEFT-ARC
[ROOT, parsed]	[correctly]	parsed → sentence	RIGHT-ARC
[ROOT, parsed, correctly]	[]		SHIFT
[ROOT, parsed]	[]	parsed → correctly	RIGHT-ARC
[ROOT]	[]	ROOT → parsed	RIGHT-ARC

(b) $2n$

(e) dev UAS: 88.56, test UAS: 89.07

(f) Refer to Stanford CoreNLP to visualize the results of dependencies parses (also may contain errors).

(i) Verb Phrase Attachment Error, wedding -> fearing should be heading -> fearing.

(ii) Coordination Attachment Error, makes -> rescue should be rush -> rescue.

(iii) Prepositional Phrase Attachment Error, named -> Midland should be guy -> Midland.

(iv) Modifier Attachment Error, elements -> most should be crucial -> most.

Note that in the source code, the restriction that the version of PyTorch must be 1.0.0 is meaningless and thus I remove it.

1.4 Language Modeling and Recurrent Neural Networks

Language Modeling: given a sequence of words $\boldsymbol{x}^{(1)}, \cdots, \boldsymbol{x}^{(t)}$, compute the probability distribution of the next word at $\boldsymbol{x}^{(t+1)}$:

$$P(\boldsymbol{x}^{(t+1)}|\boldsymbol{x}^{(1)}, \cdots, \boldsymbol{x}^{(t)}) \tag{1.27}$$

The joint probability of a text is:

$$P(\boldsymbol{x}^{(1)}, \cdots, \boldsymbol{x}^{(T)}) = \prod_{t=1}^{T} P(\boldsymbol{x}^{(t)}|\boldsymbol{x}^{(t-1)}, \cdots, \boldsymbol{x}^{(1)}) \tag{1.28}$$

n-gram is a chunk of n consecutive words: unigram, bigram, trigram, 4-gram, ... n-gram language model is based on a simplifying assumption: $\boldsymbol{x}^{(t+1)}$ depends only on the preceding $n-1$ words with i.i.d.:

$$\begin{aligned} P(\boldsymbol{x}^{(t+1)}|\boldsymbol{x}^{(t)}, \cdots, \boldsymbol{x}^{(1)}) &= P(\boldsymbol{x}^{(t+1)}|\boldsymbol{x}^{(t)}, \cdots, \boldsymbol{x}^{(t-n+2)}) \\ &= \frac{P(\boldsymbol{x}^{(t+1)}, \boldsymbol{x}^{(t)}, \cdots, \boldsymbol{x}^{(t-n+2)})}{P(\boldsymbol{x}^{(t)}, \cdots, \boldsymbol{x}^{(t-n+2)})} \end{aligned}$$

where the n-gram and (n-1)-gram probabilities are calculated by *counting*. There are some *sparsity problems* with the above n-gram models such as the numerator or denominator is zero. Some tricks such as *smoothing* (add small δ to the count) and *backoff* (e.g. 4-gram backoff to 3-gram) are proposed to solve them.

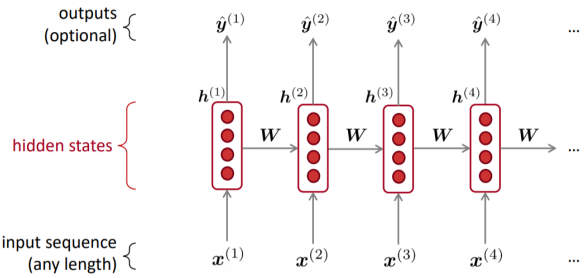

Figure 1.8: Principle of RNN

Note that for n-gram, increasing n makes sparsity problems worse. Typically $n \leq 5$.

To process *variable* length **sequential input** such as text, **Recurrent Neural Network** (RNN) is introduced. As the principle of RNN shown in Fig. 1.8: *repeat* (i.e. **unfold** or unroll) the same RNN cell for each time-step but with different input and previous **hidden state**. A vanilla RNN for language modeling is:

$$\begin{aligned} \boldsymbol{h}^{(t)} &= \sigma\left(\boldsymbol{W}_h \boldsymbol{h}^{(t-1)} + \boldsymbol{W}_x \boldsymbol{x}^{(t)} + \boldsymbol{b}_1\right) \\ \hat{\boldsymbol{y}} &= P(\boldsymbol{x}^{(t)}|\boldsymbol{x}^{(t-1)}, \cdots, \boldsymbol{x}^{(1)}) \\ &= \texttt{softmax}(\boldsymbol{U}\boldsymbol{h}^{(t)} + \boldsymbol{b}_2) \end{aligned}$$

where $\sigma(\cdot)$ is the activation function, and $\boldsymbol{h}^{(0)}$ is the initial (random or zero) hidden state. The gradient w.r.t. the weight matrix is the *sum* of the gradients w.r.t each time it appears using **back-propagation through time** (BPTT, just as same as normal back-prop). And the **evaluation metric** for language modeling is *perlexity* which is equal to the exponential of the cross-entropy losses:

$$\begin{aligned}\text{perplexity} &= \prod_{t=1}^{T}\left(\frac{1}{P_{LM}(\boldsymbol{x}^{(t+1)}|\boldsymbol{x}^{(t)},\cdots,\boldsymbol{x}^{(1)})}\right)^{1/T} \\ &= \exp\left(\frac{1}{T}\sum_{t=1}^{T}-\log\hat{\boldsymbol{y}}^{(t)}\right)\end{aligned} \tag{1.29}$$

There are some other applications of RNN: part-of-speech tagging, named entity recognition, sentence classification, text generator, encoder module, etc. The final feature can be the final hidden state or elemen-wise max/mean of all hidden states. Using chain rule, we get $\frac{\partial J^{(n)}}{\partial \boldsymbol{h}^{(1)}} = \frac{\partial J^{(n)}}{\partial \boldsymbol{h}^{(n)}} \times \prod_{i=2}^{n} \frac{\partial \boldsymbol{h}^{(n)}}{\partial \boldsymbol{h}^{(n-1)}} = \frac{\partial J^{(n)}}{\partial \boldsymbol{h}^{(n)}} \times \prod_{i=2}^{n} \sigma' \circ \boldsymbol{W}_h$. For a large n and small $\boldsymbol{W}_h$, it's easy to encounter the vanishing gradient problem. In overall, the *vanilla* RNN has these disadvantages: (1) recurrent computation is slow (2) hard to access long-term information (**long-term dependencies**) due to *gradient vanish* and *gradient explosion*.

We can formalize the above vanishing intuitions according to [16]. Let $\boldsymbol{W}_h$ have the **eigenvalues** $\lambda_1,\cdots,\lambda_n$ such that $|\lambda_1| > |\lambda_2| > \cdots > |\lambda_n|$ and the corresponding (left) eigenvectors $\boldsymbol{q}_1^\top,\cdots,\boldsymbol{q}_n^\top$ which have unit norms: $\boldsymbol{q}_i^\top \boldsymbol{W}_h = \lambda_i \boldsymbol{q}_i$. We can rewrite the gradients $\frac{\partial J^{(n)}}{\partial \boldsymbol{h}^{(n)}} = \sum_{i=1}^{N} c_i \boldsymbol{q}_i^\top$ where $c_i = 0$ for $i < j$ and $c_j \neq 0$. Thus, the overall gradient is:

[16] Pascanu et al. 2013

$$\begin{aligned}\frac{\partial J^{(n)}}{\partial \boldsymbol{h}^{(1)}} &= \frac{\partial J^{(n)}}{\partial \boldsymbol{h}^{(n)}} \times \prod_{i=2}^{n} \sigma' \circ \boldsymbol{W}_h \\ &= \sum_{i=1}^{N} c_i \boldsymbol{q}_i^\top (\texttt{diag}(\sigma'))^{n-1} (\boldsymbol{W}_h)^{n-1} \\ &= \sum_{i=1}^{N} c_i \boldsymbol{q}_i^\top (\boldsymbol{W}_h)^{n-1} (\texttt{diag}(\sigma'))^{n-1} \\ &= c_j \lambda_j^{n-1} \boldsymbol{q}_j^\top (\texttt{diag}(\sigma'))^{n-1} + \lambda_j^{n-1} \sum_{i=j+1}^{N} c_i \left(\frac{\lambda_i}{\lambda_j}\right)^{n-1} \boldsymbol{q}_i^\top (\texttt{diag}(\sigma'))^{n-1} \\ &\approx c_j \lambda_j^{n-1} (\sigma')^{n-1} \boldsymbol{q}_j^\top\end{aligned}$$

where $\frac{\lambda_i}{\lambda_j} < 1$, and for large n we have $\lim_{n\to\infty}\left(\frac{\lambda_i}{\lambda_j}\right)^{n-1} = 0$. Therefore, if $\forall j, \sigma' < \frac{1}{\lambda_j}$ then we get vanishing gradient. Note that,

$\sup(\text{sigmoid}') = \frac{1}{4}, \sup(ReLU') = 1$. Thus, the largest eigenvalue $\lambda_1 < \frac{1}{\sigma'}$ will lead to vanishing.

For avoid gradient explosion, one simple method is *gradient clipping*: $\hat{\boldsymbol{g}} \leftarrow \frac{threshold}{\|\boldsymbol{g}\|}\boldsymbol{g}$ if $\|\boldsymbol{g}\| \geq threshold$. As for fixing vanishing gradient, many RNN variants are introduced such as **Long Short-Term Memory** (LSTM) [17] and **Gated Recurrent Unit** (GRU) [18]. LSTM uses two *separated* memories: *hidden state* $\boldsymbol{h}^{(t)}$ for *short-term* information and *cell state* $\boldsymbol{c}^{(t)}$ for *long-term* information. There are three *gates* performed in each LSTM *cell*:

[17] Hochreiter and Schmidhuber 1997

[18] Cho et al. 2014

Forget gate: $\boldsymbol{f}^{(t)} = \sigma(\boldsymbol{W}_f\boldsymbol{h}^{(t-1)} + \boldsymbol{U}_f\boldsymbol{x}^{(t)} + \boldsymbol{b}_f)$

Input gate: $\boldsymbol{i}^{(t)} = \sigma(\boldsymbol{W}_i\boldsymbol{h}^{(t-1)} + \boldsymbol{U}_i\boldsymbol{x}^{(t)} + \boldsymbol{b}_i)$

Output gate: $\boldsymbol{o}^{(t)} = \sigma(\boldsymbol{W}_o\boldsymbol{h}^{(t-1)} + \boldsymbol{U}_o\boldsymbol{x}^{(t)} + \boldsymbol{b}_o)$

New cell content: $\tilde{\boldsymbol{c}}^{(t)} = \tanh\left(\boldsymbol{W}_c\boldsymbol{h}^{(t-1)} + \boldsymbol{U}_c\boldsymbol{x}^{(t)} + \boldsymbol{b}_c\right)$

Cell state: $\boldsymbol{c}^{(t)} = \boldsymbol{f}^{(t)} \circ \boldsymbol{c}^{(t-1)} + \boldsymbol{i}^{(t)} \circ \tilde{\boldsymbol{c}}^{(t)}$

Hidden state: $\boldsymbol{h}^{(t)} = \boldsymbol{o}^{(t)} \circ \tanh \boldsymbol{c}^{(t)}$

where σ is sigmoid function, $\circ$ is element-wise product, and $\tanh$ used in hidden state (the last formula) is to provide non-linearity and normalize $\boldsymbol{c}^{(t)}$ to $(0, 1)$. The structure of LSTM is shown in Fig.1.9 made by colah's blog.

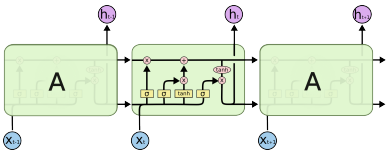

Figure 1.9: The repeating module in an LSTM contains four interacting layers.

Those three gates (forget, input, output) enable the abilities of erase, read and write for LSTM. Each element of the gates are between 1 (open) and 0 (close). While The LSTM architecture makes it *easier* for the RNN to preserve long-distance dependencies, it does not *guarantee* that there is no vanishing/exploding gradient.

In the other hand, GRU combines input and forget gate into *update* gate, and add new *reset* gate to select useful part of previous hidden state to compute new state content. While there is no conclusive evidence that GRU consistently performs better than LSTM or vice versa, GRU is computed more efficient due to fewer parameters.

Update gate: $\boldsymbol{u}^{(t)} = \sigma(\boldsymbol{W}_u\boldsymbol{h}^{(t-1)} + \boldsymbol{U}_u\boldsymbol{x}^{(t)} + \boldsymbol{b}_u)$

Reset gate: $\boldsymbol{r}^{(t)} = \sigma(\boldsymbol{W}_r\boldsymbol{h}^{(t-1)} + \boldsymbol{U}_r\boldsymbol{x}^{(t)} + \boldsymbol{b}_r)$

New hidden state content: $\tilde{\boldsymbol{h}}^{(t)} = \tanh(\boldsymbol{W}_h(\boldsymbol{r}^{(t)} \circ \boldsymbol{h}^{(t-1)}) + \boldsymbol{U}_h\boldsymbol{x}^{(t)} + \boldsymbol{b}_h)$

Hidden state: $\boldsymbol{h}^{(t)} = (1 - \boldsymbol{u}^{(t)}) \circ \boldsymbol{h}^{(t-1)} + \boldsymbol{u}^{(t)} \circ \tilde{\boldsymbol{h}}^{(t)}$

The vanishing gradient problem appears not only in RNNs, but also for most all other neural networks inlcuding MLP (dense layers) and CNNs, especially for deep ones. One solution is add more *direct connections* between future apart layers to allow gradients flow more easier. For example, **Residual connections** (aka.

ResNet [19] or skip-connections) is shown in Fig.1.10 where an identity skips two layers. Another example is **Dense connections** (aka. DenseNet [20]) which directly connect every layers to every layers where the output of each layer will **concatenate** the input as presented in Fig.1.11. **Highway connections** is inspired from the gates of LSTM and similar to residual connections, where the identity connect and the transformation layer is controlled by a dynamic gate.

Apart from the above RNNs, there are other important RNN architectures: **Bidirectional RNNs** and **Multi-layer RNNs** (aka. stacked RNNs). The definition of bidirectional RNNs is given by:

$$\text{Forward RNN: } \overrightarrow{\boldsymbol{h}}^{(t)} = \overrightarrow{\text{RNN}}_{FW}(\overrightarrow{\boldsymbol{h}}^{(t-1)}, \boldsymbol{x}^{(t)})$$
$$\text{Backward RNN: } \overleftarrow{\boldsymbol{h}}^{(t)} = \overleftarrow{\text{RNN}}_{BW}(\overleftarrow{\boldsymbol{h}}^{(t-1)}, \boldsymbol{x}^{(t)})$$
$$\boldsymbol{h}^{(t)} = [\overrightarrow{\boldsymbol{h}}^{(t)}; \overleftarrow{\boldsymbol{h}}^{(t)}]$$

While LSTM bacame the dominant approach between 2013 to 2016, *Transormer* is the state-of-the-art now in 2019. More descriptions refer to Section 1.6. And another notable fact is that RNNs parallelize badly and are slow compared with CNNs.

[19] He et al. 2016

[20] Huang et al. 2017

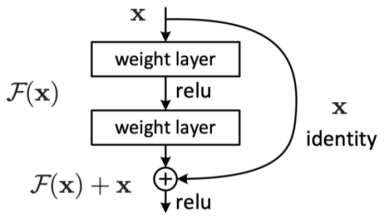

Figure 1.10: Residual connections.

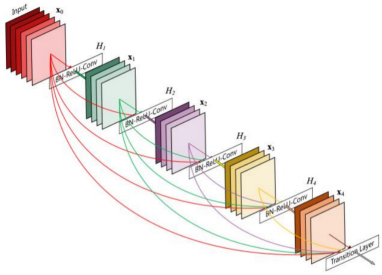

Figure 1.11: Dense Net.

1.5 Seq2Seq and Attention

Pre-neural machine translation: (1) Rule-based bilingual dictionary in 1950s (2) Statistical machine translation from 1990s to 2010s. More formally, statistical machine translation from *source language* x to *target language* y is given by:

$$\begin{aligned}\arg\max_y P(y|x) &= \arg\max_y \frac{P(x,y)}{P(x)} \\ &= \arg\max_y \frac{P(x|y)P(y)}{P(x)} \\ &= \arg\max_y P(x|y)P(y)\end{aligned}$$

where $P(y|x)$ is broke down to two components according to **Baye's rule**: $P(x|y)$ is the translation model which learn from parallel (bilingual) data to model the fidelity of words and phrases whether x is well- or ill-formed, $P(y)$ is the language model which learn from monolingual data of target language to model the fluency of the whole sentence regardless of their connection to the French.

In practice, we further consider **alignment** (word-level correspondence) because there are one-to-many, many-to-one, many-to-many, and even no couterpart apart from one-to-one

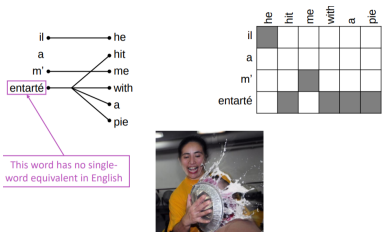

Figure 1.12: Alignment from french to english translation.

reflection relations. One example of one-to-many (entarté) and no counterpart (a) is shown in Fig.1.12. More examples refer to the original paper [21]. Therefore, we add alignment to the model: $P(x, a|y)$.

[21] Brown et al. 1993

The core idea of Seq2Seq model is using two RNN to construct an *encode-decode* architecture. At test time, first we feed source sentence (with embedding) into the encoder RNN, then we use the last hidden state of the encode RNN as the initial state of the decoder RNN as a conditional language model. The output word at position t is given by:

$$w_t = \texttt{softmax}(RNN(h^{(t-1)}, W_e \arg\max \texttt{softmax}(h^{(t-1)})))$$

where W_e is the embedding table of the target language and the first input x_1 = <START> is a special token and repeatedly output until output <END>. Note that there are two different embedding lookup table for source and target language. When traning, we need provide parallel dataset whose samples consist of bilingual sentences. As for traning, the diagram is represented in Fig.1.13.

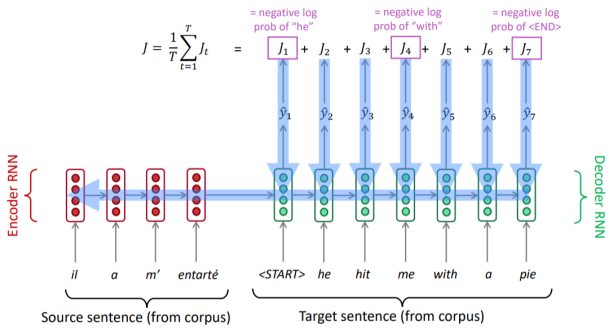

Figure 1.13: Training phase for NMT.

However, the aforementioned (greedy) decoding has no way to undo decisions. This is, if one of the output words are wrong, all the follow-up outputs are also wrong. **Beam search** decoding is utilized to fix this problem: on each step of decoder, keep track of the k (in practice around 5 to 10) most probable partial translation (*hypotheses*, path, or branch). The target is the path with the largest cumulative log probabilities with shortest one (i.e. average). Apart from all paths reach <END> as the stop sign, we can set some pre-defined cutoff for maximum number of timesteps or finished paths.

Although NMT is much simple and less human engineering effort while achieves better performance, NMT is diffcult to control (i.e. specify rules or guidelines) and less interpretable which leads to hard to debug.

The popular evaluation metric for MT is **BLEU** (Bilingual Evaluation Understudy). Its calculation is based on n-gram precision

For NMT, increasing beam size too much much decreases BLEU scores. Because large-k beam search produces too-short translations. In open-ended task such as chit-chat dialogue, large beam size make output more generic.

plus a penality for too-short translations. Note that BLEU is useful but imperfect because there are many valid translations which has low n-gram overlap with the ground truth translation. NMT outperforms SMT quickly, but there are still many difficulties remain:

- Out-of-vocabulary words.
- Domain mismatch between train and test data.
- Maintaining context over longer text (long-term dependencies).
- Low-resource language pairs (few-shot learning).
- Using common sense is still hard.

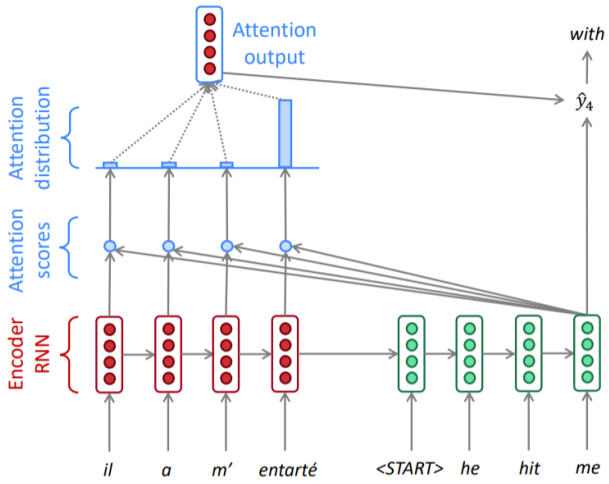

Figure 1.14: Seq2Seq with attention.

We notice that only the last hidden state from encoder RNN to represent the whole source sentence may be the information bottleneck. Thus we introduce Seq2Seq with **attention**: on each step of the decoder, we use the attention distribution (like soft version of alignment) for each hidden states of encoder RNN to take a weighted sum of the encoder hidden states as the current decoder hidden state. Note that sometimes the input of decoder RNN will concatenate the previous translated word vector and the previous attention output. The diagram can be seen in Fig.1.14. In addition, attention in here helps with vanishing gradient problem by providing shortcut to faraway states, and also provides

some interpretability. More formally, the attention for Seq2Seq is:

$$
\begin{aligned}
&\boldsymbol{e}^{(t)} = [\boldsymbol{s}_t^\top \boldsymbol{h}_1, \cdots, \boldsymbol{s}_t^\top \boldsymbol{h}_n] \in \mathbb{R}^n \\
&\text{Attention distribution: } \boldsymbol{\alpha}^{(t)} = \texttt{softmax}(\boldsymbol{e}^{(t)}) \\
&\text{Attention output: } \boldsymbol{a}^{(t)} = \sum_{i=1}^{n} \alpha_i^{(t)} \boldsymbol{h}_i \in \mathbb{R}^h \\
&\text{Attention decoder hidden state: } [\boldsymbol{a}^{(t)}; \boldsymbol{s}_t] \in \mathbb{R}^{2h}
\end{aligned} \tag{1.30}
$$

where encoder hidden states $\boldsymbol{h}_1, \cdots, \boldsymbol{h}_n \in \mathbb{R}^h$, and decoder hidden state at timestep t is $\boldsymbol{s}_t \in \mathbb{R}^h$.

More general definition of attention: given a set of vector *values*, and a vector *query*, attention is to compute a weighted sum of the values, dependent on the query. We can found that attention is a way to obtain a *fixed-size* representation of an arbitrary set of representations (e.g. sequential features). There are many ways to obtain query vector: dot product $e_i = \boldsymbol{s}^\top \boldsymbol{h}_i$, multiplicative $e_i = \boldsymbol{s}^\top \boldsymbol{W} \boldsymbol{h}_i$, additive $e_i = \boldsymbol{v}^\top \tanh(\boldsymbol{W}_1 \boldsymbol{h}_i + \boldsymbol{W}_2 \boldsymbol{s})$, where $\boldsymbol{v}, \boldsymbol{W}, \boldsymbol{W}_1, \boldsymbol{W}_2$ are trainable parameters.

As for *out-of-vocabulary* (OOV) problem in NMT, we can increase the size of vocabulary. However, large vocabulary leads to huge computations in the softmax layer. To solve it, we can use *hierarchical softmax* (tree-structured vocabulary). We can also use character-based [22] (or sub-word) model instead of word-based to handle OOV problem. But pure character-level seq2seq is very slow (as longer sequence got through LSTM, see HW5).

[22] Kim et al. 2016

1.5.1 HW4

1. Neural Machine Translation with RNNs

Refer to the source codes for detail. Note that pack_padded_sequence is often used to reduce unnecessary computations of paded elements for variable length sequence. In implementation, I found that for reshaping the last_hidden with shape (2, b, h) to shape (b, 2h), I had to use `torch.cat((last_hidden[0, :], last_hidden[1, :]), axis=1)` instead of `.permute(1, 0, 2).view(b, -1)`. Common used torch function include: `torch.squeeze`, `torch.unsqueeze`, `torch.split`, `torch.cat`, `torch.stack`, `torch.Tensor.view`, `torch.Tensor.permute`, `torch.Tensor.size`.

(i) Corpus BLEU score when testing: 22.68.

(j) Dot product attention is simple but requires $\boldsymbol{s}_t, \boldsymbol{h}_i$ have the same shape. Additive attention could learn more complicated features but need more computations.

2. Analyzing NMT Systems

(a)

(i) Error: duplication of translations ("favorite"), Reason: model limitations in preventing duplications, Solution: add penalty on duplicated translations.

(ii) Error: the superlative comparison is mistranslated (most instead of more), Reason: could be because specific linguistic construct of comparison in Spanish, Solution: train with more comparision examples or add penalty for comparision examples.

(iii) Reason: out-of-vocabulary words of names, Reason: the model do not consider out-of-vocabulary words, Solution: keep the out-of-vocabulary the same according to named entity regconization or attention output, or just increase the size of vocabulary.

(iv) Error: "go around" is mistranslated to "go back," "block" is mistranslated to "apple", Reason: "apple" and "block" are same in Spanish "manzana", "go around" and "go back" are also similar in Spanish, Solution: train with more examples about such polysemic words.

(v) Error: "teacher" is mistranslated to "women" for Spanish "profesores", Reason: training dataset may contain the above mistakes, Solution: correct the dataset and add rules to correct this error.

(vi) Error: "hectareas" (1/4 acres) is mistranslated to "acres", Reason: there is no such measure unit in English, Solution: identify measure unit in the source sentence and perform some rules.

(b)
(c) BLEU

Note that despite the HW taking sentence-level BLEU, BLEU is used as a **corpus-level measure**.

(i) $p_1 = 0.5477, p_2 = 0.6325$, c_2, agree.

(ii) $p_1 = 0.4484, p_2 = 0.2589$, c_1, disagree.

(iii) There are often many valiad translations for one sentence.

(iv) Pros and cons of BELU:

- Pros: 1. BLEU has frequently been reported as correlating well with human judgement. 2. few human effort with inexpensive computations.
- Cons: 1. A good translation can get a poor BLEU score because it has low n-gram overlap with the human (reference) translation. 2. It does not consider meaning and sentence structure, etc.

1.5.2 Tips for Research

Two basic start points:

- Start with a (domain) problem of interest and try to find good/better ways to address it than currently known/used.
- Start with a technical approach of interest, and work out good ways to extend or improve it or new ways to apply it.
- Experimental strategy: start from simple model and work incrementally on models, initially run on a tiny dataset (e.g. 8 exmaples), make sure get 100% accuracy on testing, then run your model on a large dataset that still get score to 100% on training (it's okay to overfitting), and try to regularize the model.

Recommendation sources: ACL, NeurIPS, ICML, ICLR, arXiv (arXiv-sanity), PapersWithCode (leaderboards for various tasks).

1.6 Contextual Word Representations and Pretraining

The context-independent word representations (such as Word2Vec and GloVe) have limitations: the same word will have a ton of meanings in different contexts, but has a fixed word representation in these models. Instead of a fixed embedding table, we can (unsupervisely) pre-train a neural network model and freeze it as a word representation model (e.g., $f(w, c(w))$).

TagLM [23] ("Pre-ELMo"): pre-train a Neural Language Modeling on large unlabeled corpus and get the output as the contextual word representation. Use both (context-independent) word embeddings (e.g., Word2Vec) and (frozen) LM embeddings in the downstream sequence tagging model (NER task) w/ small task-labeled data.

[23] Peters et al. 2017

CoVe [24]: Use NMT as the pre-training task. But, the results aren't as strong as the simpler NLM.

[24] McCann et al. 2017

ELMo [25]: the word representation is the (learnable) weighted sum of hidden features of each layer in stacked BiLSTM.

[25] Peters et al. 2018

Transformer [26]: scaled dot-product self-attention (QKV formula, the softmax scores are derived from the same source as the target sequence), multihead (like channels in CNN), position embedding (because self-attention has not position-aware), good parallelization than RNN (sequential because of the unroll operation), feed-forward layer (like 1×1 convolution), residual connection (propagate the position information to higher layers), layer normalization, masked attention. Key resource:

[26] Vaswani et al. 2017

http://nlp.seas.harvard.edu/2018/04/03/attention.html. Other applications [27] of the transformer are shown in the sidenote.

[27] Parmar et al. 2018; Huang et al. 2019

BERT [28] (Bidirectional Encoder Representations from Transformers): two tasks: masked (bidirectional) LM and next sentence prediction (NSP, but is useless according to follow up papers because this task is misconstrcuted and too easy).

[28] Devlin et al. 2019

Transformer for Image: due to the self-similarity (or translational equivariance) in images, we can limite the receptive field of the self-attention by masking with diagonal matrix (e.g., tridiagonal matrix). Transformer for Music Generation: decrease memory usage for storing the relative position embeddings of $L \times L$ to L by padding, reshape, and slice.

1.7 Attention Model and Question Answering

Compared with previous versions, Stanford Question Answering Dataset (SQuAD) 2.0 has many unanswerable questions. Each question has 3 gold answers, and there are two evaluation metrics:

- Exact match (EM): 1/0 accuracy on whether match one of 3 answers.
- F1: take system (predict) and gold answers as bag of words to calculate F1 scores.

where both metrics ignore punctuation and articles. Disadvantages: the answer is only sub-span of the paragraph (the answers are directly appeared in the question), without indirect answers, e.g., yes/no, counting, and implicit why.

A simple and successful aechitecture is the Stanford Attentive Reader [29] which likes the attentive Seq2Seq model. For paragraph $[\boldsymbol{p}_1, \cdots, \boldsymbol{p}_m]$ and question $[\boldsymbol{q}_1, \cdots, \boldsymbol{q}_n]$ with GloVe embedding, the index of start token and end token for the sub-span answer is:

[29] Chen et al. 2016

$$\boldsymbol{q} = [\overrightarrow{\text{LSTM}}(\overrightarrow{\boldsymbol{h}}^{(m-1)}, \boldsymbol{q}_{m-1}); \overleftarrow{\text{LSTM}}(\overleftarrow{\boldsymbol{h}}^{(2)}, \boldsymbol{q}_2)]$$

$$\tilde{\boldsymbol{p}}_i = \text{Bi-LSTM}(\boldsymbol{p}_i)$$

$$\text{Start token: } \text{softmax}_i(\boldsymbol{q}^\top \boldsymbol{W}_s \tilde{\boldsymbol{p}}_i)$$

$$\text{End token: } \text{softmax}_i(\boldsymbol{q}^\top \boldsymbol{W}_e \tilde{\boldsymbol{p}}_i)$$

Compared with SAR, Stanford Attentive Reader++ [30] mainly leverages these updates: (1) use weighted sum (attention) of all hidden states in the encoder of question, (2) multi-layers Bi-LSTM (3) add more features in the encoder of the paragraph, including linguistic features such as POS&NER tags&term frequency, exact match (wether the word appears in the question), aligned question embedding ($\sum_j \texttt{softmax}_{j'}(\alpha(p_i) \cdot \alpha(q_{j'})) \times q_j$ where α is dense layer with ReLU activation and p_i, q_j are embedding of the paragraph and the question word.

[30] Chen et al. 2017

Bi-Directional Attention Flow (DiDAF) [31] is a state-of-the-art (SoTA) method in 2018 and 2017. It comes up with word and char embedding, and the main innovation is attention flow layer

[31] Seo et al. 2016

which consists of Query2Context (i.e. Question2Paragraph) and Context2Query. C2Q attention is defined as:

$$\text{Similarity matrix: } s_{ij} = w_s^\top [p_i; q_j; p_i \circ q_j] \in \mathbb{R} \tag{1.31}$$

$$\alpha_i = \text{softmax}(s_{i,:}) \tag{1.32}$$

$$a_i = \sum_j \alpha_{ij} q_j \in \mathbb{R}^{2h} \tag{1.33}$$

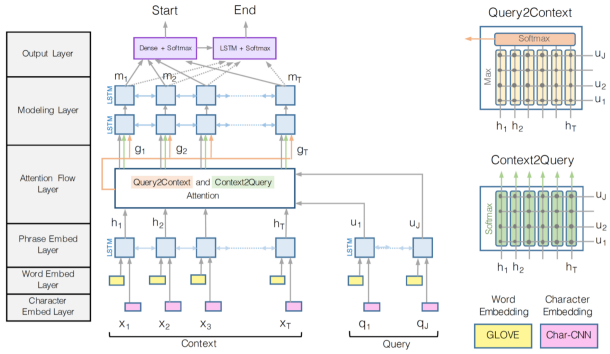

Figure 1.15: Architecture of BiDAF

Q2C attention (the weighted sum of the most important words in the context w.r.t the query) is given by:

$$m_i = \max_j s_{ij} \tag{1.34}$$

$$\beta = \text{softmax}(m) \tag{1.35}$$

$$p' = \sum_i \beta_i p_i \tag{1.36}$$

The BiDAF layer output of each paragraph position is: $b_i = [p_i; a_i; p_i \circ a_i; p_i \circ p'] \in \mathbb{R}^{8h}$. The overall architecture is presented in Fig.1.15. The start token comes from the output of dense layer with softmax built upon the concatenation of the BiDAF output and the output M_1 of modelling layer (2-layer Bi-LSTM) whose input is BiDAF output. And the end token is the dense layer with softmax upon the concatenation of the BiDAF output and the output M_2 of another modelling layer whose input is M_1.

1.8 ConvNets for NLP

Convolutions are classically used to extract (position-invariant) features from images by leveraging fixed-size *filter* (*kernel*) weights which are used to perform element-wise product with certain window (patch) of the whole image. *Zero padding* ("same" padding) is often used to keep the length. The kernel window slides with a stride (e.g. 1) over the whole sentence. One more variant about

convolutions is *dilation convolution* (skip conv) which can access more wide *receptive field* with smaller filter. Same as the *channels* (aka. feature maps) in CNNs, we can also define the dimensions of word embedding as channels like 3 channels (RBG) of images. Each channel may indicates one feature (e.g. words about food or sport). *Pooling* (e.g. max, average) over time (aka. global pooling) is utilized to aggregate the information of the whole sentence. k-max (global) pooling is also a common technique used in ConvNet for NLP. Besides, local pooling is more common used in CNN circumstances. 1x1 convolution (aka. Network-in-Network connection) is a famous technique that can be seen as a fully connection linear layer across chennels. It can be also (often) used to map from many channels to fewer channels to reduce computation while keeping performance.

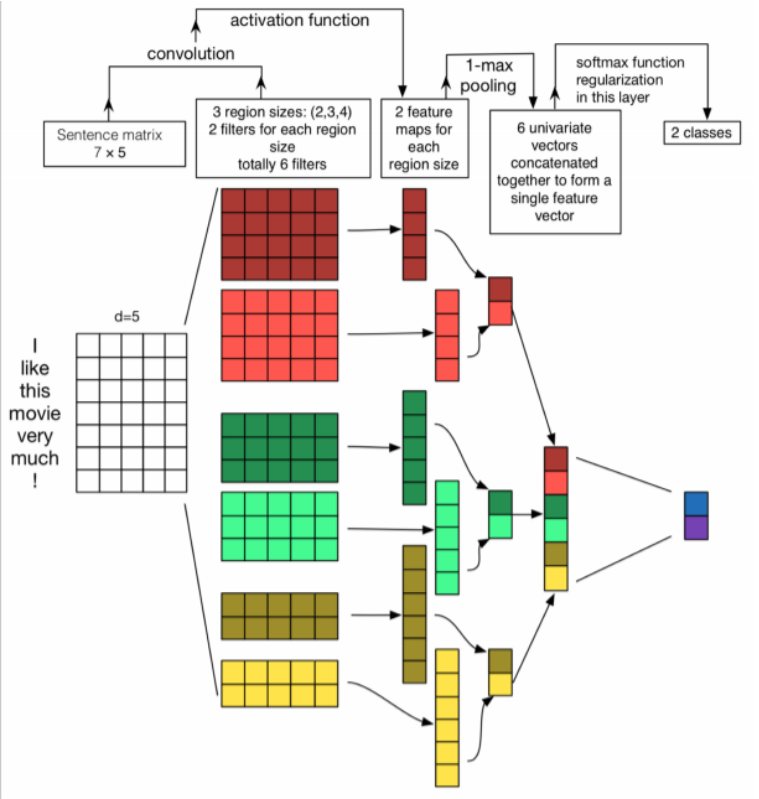

Figure 1.16: Simple ConvNet for NLP classification.

Above is an example [32] of single layer CNN for sentence classification. Fig.1.16 illustrates the architecture. Multiple single convolution layer with different kernel size and global max pooling are used. Specifically, there are 100 feature maps for each of kernel size 3, 4, and 5. The input is two copies of pre-trained word vector (word2vec-300). Keep one as 'static' (no gradient), and the

[32] Kim 2014

other 'dynamic' will be updated during training. The 'static' word vector gives unseen words appeared in the test set a better chance of being interreted correctly. There are several ways of handling these two channels, most common is to simply average them before using in a CNN. The other method is to double the length of the CNN filters. The output of max poolings are concatenated into a vector, which is then fed into a dense layer with softmax to perform classification. Dropout and L2 regularization are used.

VD-CNN [33] for text classification is to build a ResNet like very deep CNN which has 29 depth and many shortcut (residual) connections. Note that 29 depth is not as deep as ResNet whose depths are typically 34, 50, and 101. The researchers found that, for more deep one like 47 layers, the results are fraction worse than the one with 29 layers. The input text sequence will pad into fixed length (1024).

[33] Conneau et al. 2017

Quasi-recurrent neural network takes the best and parallelizable parts of RNNs and CNNs. It achives $3 \sim 16$ times faster than LSTM. One Quasi-RNN layer consists of a normal convolution layer with left same padding to learn new hidden content z, forget gate f, optional output gate i, and optional input gate i, and three dynamic average pooling (non-parametric) variants to perform RNN-like unfolding.

New hidden contents: $\boldsymbol{Z} = \tanh(\boldsymbol{W}_z * \boldsymbol{X})$

Forget gates: $\boldsymbol{F} = \sigma(\boldsymbol{W}_f * \boldsymbol{X})$

Optional output gates: $\boldsymbol{O} = \sigma(\boldsymbol{W}_o * \boldsymbol{X})$

Optional input gates: $\boldsymbol{I} = \sigma(\boldsymbol{W}_i * \boldsymbol{X})$

f-pooling: $\boldsymbol{h}_t = \boldsymbol{f}_t \odot \boldsymbol{h_{t-1}} + (1 - \boldsymbol{f}_t) \odot \boldsymbol{z}_t$

fo-pooling:

$\boldsymbol{c}_t = \boldsymbol{f}_t \odot \boldsymbol{c}_{t-1} + (1 - \boldsymbol{f}_t) \odot \boldsymbol{z}_t)$

$\boldsymbol{h}_t = \boldsymbol{o}_t \odot \boldsymbol{c}_t$

ifo-pooling:

$\boldsymbol{c}_t = \boldsymbol{f}_t \odot \boldsymbol{c}_{t-1} + \boldsymbol{i}_t \odot \boldsymbol{z}_t)$

$\boldsymbol{h}_t = \boldsymbol{o}_t \odot \boldsymbol{c}_t$

where the hidden state $\boldsymbol{h}$ and the cell state $\boldsymbol{c}$ are initialized to zeros, $*$ indicates convolution operator, and $\odot$ denotes element-wise product. A variant dropout called zoneout is adopt in the forget gate channels of stacked QRNN. Dense connection layers from DenseNet are also extended in stacked QRNN. Note that QRNN often need deeper network to get as good performance as LSTM.

1.9 Subword models

Although what our mouths produce is continuous space, phonology posits phonetics the sound stream that consists of smaller distinctive categorical units: phonemes. In linguistics, morphemes (subwords) is the smallest semantic unit that has meanings, e.g. unfortunately can be divided into tree structure of morephemes using *recursive neural networks* [34]:

[34] Luong et al. 2013

$$[[\text{un}\ [[\text{fortun(e)}]_{\text{ROOT}}\ \text{ate}]_{\text{STEM}}]_{\text{STEM}}\ \text{ly}]_{\text{WORD}}$$

There are many languages that do not segment words or has many separated and joined words, e.g. Chinese, French. Moreover, subword models solve the OOV problem.

1.9.1 Byte Pair Encoding

Like gzip compression. Replace bytes with character ngrams. Merge together several bytes that are common sequences into a new byte. Rather than splitting the word into pieces, the sentence piece [35] tokenizes from the raw text. For example, `[Hello] [_Wor] [ld] [.]`.

[35] https://github.com/google/sentencepiece

BERT uses a variant of the wordpiece model:

1. (Relatively) common words directly in the vocabulary.
2. Other words are built from wordpieces. e.g., `hypatia = h, ##yp, ##ati, ##a` (non-initial word pieces are start with `##`)

1.9.2 FastText embeddings

Proposed by the authors of Word2Vec. Represent word as char n-grams augmented with boundary symbols and as whole word. For example, `where = <wh, whe, her, ere, re>, where`.

1.9.3 HW5

Enhance the NMT model with character-based CNN encoder and LSTM decoder.

1. Character-based convolutional encoder for NMT [36]

[36] Kim et al. 2016

(a) Characters are significantly less diverse than words. So, characters have less semantic information. Besides, we will use CharCNN to map $e_{\text{char}} \times m_{\text{word}}$ to e_{word}.

(b)

$$\begin{aligned}\#\text{parameters(char-based)} &= V_{\text{char}}\times e_{\text{char}} + k\times e_{\text{char}}\times e_{\text{word}} + e_{\text{word}} + (2e_{\text{word}}+2)\times e_{\text{word}}\\ &= 200,640\\ \#\text{parameters(word-based)} &= V_{\text{word}}\times e_{\text{word}}\\ &\approx 12,800,000\end{aligned}$$

The parameters of char-based embedding are much less than word-based. However, the char-based embedding need more computation resources.

(c) The computational efficiency of CNN is better than RNN. Although CNN works worse than RNN on sequential information due to the sliding window, CNN has good ability to capture sequential information inside the kernel window (e.g. $k = 5$). Also, the parameters of CNN is less than LSTM in this scenario.

(d) If the position of objects is not important, Max Pooling seems to be the better choice. If it is, it seems that better results can be achieved with Average Pooling. For me, I dont think one of the poolings has any significant advantage over the other.

(l) The test q1 result is 99.29792465574434 BLEU.

2. Character-based LSTM decoder for NMT

The key idea of this [37] is that when word-level decoder produces an `<UNK>` token, we can run character-level decoder to generate the rare and out-of-vocabulary target words. CharDecoderLSTM is trained like LSTM-based LM but on character-level of every word. If the target word is `music`, the input seq is `[<START>, m, u, s, i, c]`, and the target seq is `[m, u, s, i, c, <END>]`.

[37] Luong and Manning 2016

The test q2 result is 99.29792465574434 BLEU.

The final score of the full test is 24.660168424600386 (which is a lot more than the score required for full points).

1.10 Natural Language Generation

Natural Language Generation (NLP) is a subcomponent of: Machine Translation, (Abstractive) Summarization, Dialogue, Creative writting, Freeform Question Answering (the answer is not the raw part of the question but a newly generated text), and Image captioning.

Conditional Language Modeling: $P(y_t|y_1,\cdots,y_{t-1},x)$. Examples: Machine Translation (x=source sentence, y=target sentence), Summarization (x=input text, y=summarized text).

Sampling-based decoding: like greedy decoding in NMT, on each step t, randomly sample from the probability distribution

(output of softmax) P_t to obtain the next word instead of argmax.

Softmax temperature:

$$P_t(w) = \frac{\exp(s_w/\tau)}{\sum_{w' \in V} \exp(s_{w'}/\tau)} \tag{1.37}$$

Raising the temperature τ leads to P_t more uniform.

Summarization evaluation metric: ROUGE (Recall-Oriented Understudy for Gisting Evaluation) is based on recall, while BLEU is based on precision. Copy mechanisms [38] (seq2seq + attention) in Neural summarization: mixture of an attention distribution over the source text that indicates copy, and a generating distribution that generates new word. But copy mechanisms copy too much and are bad at overall content selection on long documents. Bottom-up summarization [39] splits to two stages (like pre-neural methods): content selection stage to tag words as *include* or *don't include*, bottom-up attention stage to use seq2seq+attention model to generate summarization w/ word tagged *don't include* are masked. Reinforcement learning summarization [40] uses RL to directly optimize ROUGE-L because ROUGE-L is a non-differentiable function and standard maximum likelihood (ML) training doesn't work. However, like BLEU, ROUGE-L was not really a perfect analogy to actual summarization quality. With only RL, we can get high ROUGE-L socres but lower human judgement scores. So the authors also combine RL and ML.

[38] See et al. 2017

[39] Gehrmann et al. 2018

[40] Paulus et al. 2018

Naïve seq2seq-based dialogue has serious pervasive deficiencies (with their solutions):

1. **Genericness/ boring responses**: upweight rare words during beam search; use sampling-based decoding algorithm; condition the decoder on some additional content; train a retrieve-and-refine model.
2. **Repetition problem**: block repetition during beam search; prevent the repeated attention attending to the same word multiply times; a training objective to discourage repetition (maybe a non-differentiable and require RL).

NLG evaluation: word overlap based metrices (e.g., BLEU, ROUGE, METEOR, F1) are not ideal for many NLP tasks (e.g., NMT, summarization, dialogue). Word embedding based metrices still do not correlate well with human judgements. But we can define more focused automatic metrices to capture particular aspects of generated text (e.g., fluency, diversity). Human evaluation also has some problems (e.g., inconsistent, illogical).

1.11 Coreference Resolution

Def: Identify all mentions that refer to the same entity (e.g., a person can be refered as him, they, and his name). Its applications include text understanding (e.g., QA, summarization), machine translation (e.g., gender).

Def of *anaphora*: the interpretation of the *anaphor* is in some way determined by the interpretation of the *antecedent*. For example, "We went to see a concert last night. The tickets were really expensive." The term "tickets" (*anaphor*) is interpreted by the term "a concert" (*antecedent*). *Cataphora*: when the *antecedent* comes after the *anaphor*. For example, "From the corner of the divan of Persian saddle-bags on which he was lying, smoking, as was his custom, innumerable cigarettes, Lord Henry Wotton could just catch the gleam of the honey-sweet and honey-coloured blossoms of a laburnum...". Knowledge-based pronominal coreference: for example, Winograd Schema: "She poured water from the pitcher into the cup until it was full", and "She poured water from the pitcher into the cup until it was empty". Based on the knowledge (through logical reasoning), which antecedents the term "it" refers in both sentences are different.

Coreference resolution in two steps (pipelined system): (1) detect the mentions (easy, POS, NER, dependency parser for noun phrases, but over-generating mentions is a problem), (2) cluster the mentions (hard).

Coreference Models:

1. **Rule-based**(pronominal anaphora resolution): Hobbs naive algorithm (based on the dependency parse tree).
2. **Mention Pair**: Train a binary classifier that assigns every pair of mentions a probability of being coreferent. Cons: C_n^2 is large for long document.
3. **Mention Ranking**: Assign each mention its highest scoring candidate antecedent according to the model (there is only one antecedent for each anaphor).
4. **Clustering-based**: Coreference is a clustering task. Use agglomerative clustering. Iteratively merge the clusters (initial clusters are the mention and antecedent candidates).

End-to-End Coref model [41]: Word embedding => LSTM => 3-gram span representation $\boldsymbol{g_i} = [\boldsymbol{x}^*_{\text{START}(i)}, \boldsymbol{x}^*_{\text{END}(i)}, \hat{\boldsymbol{x}}^*_i, \phi(i)]$ ($\hat{\boldsymbol{x}}^*_i$ denotes the soft attention-based representation over words in the span, $\phi(i)$ denotes a extra feature vector such as Grammatical

[41] Lee et al. 2017

Role and Semantic Compatibility) => Score every pair of spans to decide if they are coreferent mentions (is span i a mention? do a pair of spans looks coreferent?) Problems: $O(L^2)$ pairs of spans, computational impracticable. Thus they do lots of pruning.

Coreference Evaluation: B-cubed: the average of the precisions and recalls of each cluster. Coreference is still far to a solved problem. 2016's state-of-the-art [42] got 67 B-cubed result.

[42] Lee et al. 2017

1.12 Multitask Learning

Unified models can decide how to transfer knowledge (domain adaption, weight sharing, transfer and zero-shot learning)

2 | Recommentation System

Sequence-based Recommentation System – Intern @ Tencent

Learning Objectives:
- Recommentation System
- Contrastive Learning
- Sequence Modeling
- Graph Neural Network

2.1 Recommender Systems

Stages:

- **Matching**: Generates hundreds of candidate items from the extremely large item pool (million-level or even billion-level). Usually contains multiple matching channels with multiple (lightweight) models, such as embedding matching, geographical matching, popularity matching, social matching, etc.
- **Ranking**: Candidate items merged from different channels are scored by a single ranking model.
- **Re-ranking**: To meet the requirements of freshness, diversity, fairness, etc, a re-ranking stage removes certain items or changes the order of the list of items.

Dependencies: NLP Basic

Scenarios:

- **Social Recommendation**: *social influence*: users behavior (e.g., like) may be influenced by what their friends might do or think. *social homophily*: people tend to build social relations with others who have similar preferences with them.
- **Sequential Recommendation**: Users will produce a large number of interaction behaviors over time (i.e., historical behaviors). The goal is to predict the next item the user will interact, w.r.t. historical behaviors.
- **Session-based Recommendation**: It is impossible or not necessary to track the users behaviors over a long period of time due to limited storage resources. Session-based recommendation aims to predicting the next item with a given behavioral session data.

- **Bundle Recommendation**: Bundle recommendation aims to recommend a combination of items (e.g., music playlists) for users instead of independent items.
- **Cross-Domain Recommendation**: Utilize information from multiple domains can improve performance.
- **Multi-behavior Recommendation**: Users may interact with multiple types of behaviors (e.g., user clicks on the video may also collect or comment).

Objectives:

- **Diversity**: individual-level (the dissimilarity of the recommended items for certain user) and system-level diversity (dissimilarity of recommendation results of different users).
- **Explainability**: Current representing explainable information requires graph-structural item attributes with the power of GNN.
- **Fairness**: user fairness and item faireness.

2.1.1 Sequential Recommendation

Challenges [1]:

[1] Chang et al. 2021

1. User behaviors in long sequences contain implicit (e.g., clicks and watches compared with explicit such as likes and favorities) and noisy (user may click on items that are not of their interest most of the time and will not choose similar items for interaction afterward) preference signals.
2. User behaviors are always drifting over the time due to their diversity.

2.2 Contrastive Self-supervised Learning

Self-supervised Learning: a learning paradigm which aims to capture the intrinsic patterns and properties of input data without using human-provided labels. For example, the two objectives of BERT.

Contrastive Self-supervised Learning: generate (large number of) augmented examples of original data examples, create a task to predict whether two augmented examples come from the same original data example or not. In CV, the augmentation includes cropping, flipping, distortion and rotation. In NLP, it includes word deletion, reordering, and substitution.

SimCLR [2]: $\boldsymbol{z}$ is a latent representation of the input image $\boldsymbol{x}$. Given a similar pair $(\boldsymbol{x}_i, \boldsymbol{x}_j)$, and a set of negative images $\boldsymbol{x}_k$ that dissimilar from the original image of $\boldsymbol{x}_i$, the contrastive loss is:

[2] Chen et al. 2020

$$-\log \frac{\exp(\text{sim}(\boldsymbol{z}_i, \boldsymbol{z}_j)/\tau)}{\exp(\text{sim}(\boldsymbol{z}_i, \boldsymbol{z}_j)/\tau) + \sum_k \exp(\text{sim}(\boldsymbol{z}_i, \boldsymbol{z}_k)/\tau)} \tag{2.1}$$

where τ is a temperature parameter.

But SimCLR requires a large minibatch size to yield high performance. MoCo (Momentum Contrast) [3] addresses this problem w/ the hypothesis that good features can be learned by a *large* dictionary (by a queue) that covers a rich set of negative samples, while the encoder for the dictionary keys is kept as *consistent* as possible (by momentum update) despite its evolution. The queue contains many mini-batches. In each step, the current mini-batch is enqueued to the dictionary queue, and the oldest mini-batch in the queue is removed. To avoid rapidly changing encoder that reduces the key (i.e., the second parameter of $\text{sim}(\cdot, \cdot)$ in Eq. 2.1, and the first parameter is query) representations consistency. The authors propose a momentum update ($\theta_k \leftarrow m\theta_k + (1-m)\theta_q$ where m is a large momentum coefficient, e.g., 0.99, θ_q is parameters of the representation model of the query) to address this issue. MoCo uses *dual-encoder* architecture, i.e., a encoder f_q for the query, and another encoder f_k for keys.

[3] He et al. 2020a

CERT (Contrastive Self-supervised Learning for Language Understanding) [4] utilizes MoCo to fine-tune (aka., secondary pre-train) pre-trained BERT (or any other pre-training models). The augmentation approach is *back-translation*: given sentence x of source language S, translate x to y in language T, and then translate y back to augmented sample x' in language S. With different T and different translation model, we can collect many augmented samples. However, the results of CERT are not significant and worse than ALBERT.

[4] Fang et al. 2020

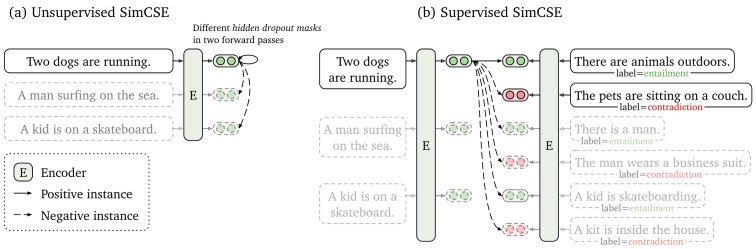

Figure 2.1: General idea of SimCSE.

SimCSE [5] (Simple Contrastive Learning of Sentence Embeddings) leverages the dropout mask (like in BERT) to achieve the positve sample pairs, and proposes a supervised SimCSE w/ a

[5] Gao et al. 2021

natural language inference (NLI) datasets. In the dataset, each sentence (aka., query) contains one entailment and one contradication. The entailment is the positive sample (aka., key), the contradiction is the negative sample (key). According to Want et al. [6], the quality of contrastive learning can be measured by alignment (the distance of the latent representations of the positive pair should close) and uniformity (the distance of the query and all the negative keys should scatter uniformly on the hypersphere). It's shown [7] that the anisotropy problem appears in language representations. The number of (dominating and significant) singular values of the word embedding matrix in a language model decay drastically. This is unfavorable to the uniformity.

[6] Wang and Isola 2020

[7] Wang and Isola 2020

ELECTRA [8] utilizes a GAN-style training process to learn a more powerful LM. It uses MLM (masked language modeling, e.g., BERT) as the generator. The output of the generator replaces the masked tokens with the predicted ones. The discriminator is also a transformer encoder, whose *replaced token detection* task is to predict whether each token in the output of generator is replaced by the generator or not. The discriminator is the final pre-trained LM and the generator is a auxiliary network. Compared with MLM-based methods, ELECTRA substantially outperforms them with less computations. COCO-LM [9] enhances the replaced token detection of ELECTRA with CLM (Correcting Language Modeling). The CLM is with a multi-task setting that combines the copy mechanism (aka., replaced token detection) and (a harder task) correction of the replaced tokens. Pretraining at token level does not explicitly learn language semantics at the sequence level. In addition to the token level pretraining, COCO-LM also introduces a sequence contrastive learning task (SCL). The SCL is just a vanilla contractive learning where the query is the original sequence and the positive key is the randomly cropping of the query. The output of `[CLS]` token is used as the representation of the whole sequence.

[8] Clark et al. 2020

[9] Meng et al. 2021

DeCLUTR [10] proposes a token-level contrastive learning task based on span sampling. The anchor is a randomly sampled span in a document. For each anchor, there are multiple positive spans sampled near by the anchor. The length of the anchor is longer than it's positives. In most cases, the positive span is overlapped or subsumed with the anchor. The negative spans inlcude easy (sampled from other documents) and hard negatives (sampled from the same document of the anchor). A pooler (aka., mean pooling) maps the encodings of the tokens in the sample into a fixed-length encoding. The performance of the mean pooling outperforms the embedding of `[CLS]` token.

[10] Giorgi et al. 2021

2.2.1 Relation to Metric Learning

Metric learning is a type of representation learning that aims to learn an embedding space where the vector representations of similar data are mapped close together, and vice versa. As a most successful approach of deep metric learning, contrastive learning attempts to close the distance between the anchor (aka., query) data point and some corresponding positive data points. Under the setting of metric learning, MLM can be seen as an instance of contrastive learning.

2.3 Graph Neural Networks

Types:

- **Homogeneous graph**: only one type of nodes and edges.
- **Heterogeneous graph**: there are multiple types of nodes or edges.
- **Hypergraph**: degree of the edge may large than two.

GNN:

- GCN
- GraphSAGE
- GAT
- HetGNN
- HGNN

Model Optimization:

- (TBD)

SURGE [11] proposes a novel GNN architecture to approach sequential recommendation by taking into consideration the implicit and noisy signal behaviors and fast-changing preferences. According to the prior assumption that neighbor nodes are similar, and dense subgraphs are the core interests of users. The authors construct graph with metric learning. Given two item (node) embeddings h_i, h_j, the multi-head similarity metric function is:

[11] Chang et al. 2021

$$M_{ij}^{\delta} = \cos(w_{\delta} \odot h_i, w_{\delta} \odot h_j), \tag{2.2}$$

$$M_{ij} = \frac{1}{\phi} \sum_{\delta=1}^{\phi} M_{ij}^{\delta} \tag{2.3}$$

where each head can be seen as one perspective and each element in weight vector w_{δ} is used to adaptively highlight different dimensions of the item embeddings.

Constructing graph from the similarity matrix M w/ ϵ-sparseness:

$$A_{ij} = \begin{cases} 1, & M_{ij} \geq \text{Rank}_{\epsilon n^2}(M); \\ 0, & \text{otherwise}; \end{cases} \tag{2.4}$$

where A is the adjacency matrix of the generated graph and $\text{Rank}_{\epsilon n^2}(\cdot)$ returns the value of ϵn^2-th largest value.

To gather weak (implicit) signals to strong (explicit) ones that accurately reflect user perferences, the information in the graph is aggregated (interest fusion) via cluster- and query (current target prediction item)-aware graph attentive convolution:

$$h_i' = \|_{\delta=1}^{\phi} \sigma(W_a^{\delta} \cdot \text{Agg}(E_{ij}^{\delta} \cdot h_j | j \in \mathcal{N}(i)) + h_i) \tag{2.5}$$

where $\text{Agg}(\cdot)$ is the aggregation function such as mean, sum, etc, E_{ij}^{δ} are normalized attention coefficients obtained by the δ-th attention head, W_a^{δ} is a linear transformation, and $\|$ denotes the concatenation operation.

The cluster- and query-aware attention E_{ij} (for one head) is given by:

$$\alpha_i = \text{Att}_c(W_c h_i \parallel h_{i_c} \parallel W_c h_i \odot h_{i_c}), \tag{2.6}$$

$$\beta_j = \text{Att}_q(W_q h_j \parallel h_t \parallel W_q h_j \odot h_t), \tag{2.7}$$

$$E_{ij} = \text{softmax}_j(\alpha_i + \beta_j) = \frac{\exp(\alpha_i + \beta_j)}{\sum_{k \in \mathcal{N}_i}(\exp(\alpha_i + \beta_k))} \tag{2.8}$$

where h_{i_c} is the average value of all nodes' embedding in the cluster (k-hop neighborhood) of the node h_i, Att is a two-layer MLP w/ LeakyReLU, h_t is the target (query) item embedding (*viz.* learn the user interest's independent evolution for different target intertests), and E_{ij} is the additive attention to consider the factors of cluster and query simultaneously.

Graph pooling is applied to fuse (aka. evolution) implicit interest signals to explicit ones.

$$S_{i,:} = \text{softmax}(W_p \cdot \text{Agg}(A_{ij}) \cdot h'_j | j \in \mathcal{N}_i), \tag{2.9}$$

$$[h_1^*, \cdots, h_m^*] = S^\top [h'_1, \cdots, h'_n]^\top, \tag{2.10}$$

$$[\gamma_1^*, \cdots, \gamma_m^*] = S^\top [\gamma'_1, \cdots, \gamma'_n]^\top, \tag{2.11}$$

$$\gamma_i = \text{softmax}_i(\beta_i), \tag{2.12}$$

$$A^* = S^\top A S \tag{2.13}$$

where $S \in \mathbb{R}^{n \times m}$ is a soft cluster assignment matrix.

However, it is difficult to train S and the temporal order of the nodes h_i and the pooled nodes h_i^* reflect the historical user interest. The authors use some trivial regularization terms to alleviate the issue.

$$L_M = \|A - SS^\top\|_F, \quad \text{make two nodes with greater connection strength map to the same cluster}, \tag{2.14}$$

$$L_A = \frac{1}{n} \sum_{i=1}^{n} H(S_{i,:}), \quad \text{approach rach row a one-hot vector}, \tag{2.15}$$

$$L_P = \|p_n S - p_m\|_2, \quad \text{make the position of the non-zero elements in S closer to the main diagonal elements}, \tag{2.16}$$

where position encoding vectors $p_n = [1, 2, \cdots, n], p_m = [1, 2, \cdots, m]$.

Graph readout to aggregates all node embeddings of the raw graph (before pooling):

$$h_g = \text{Readout}([\gamma_i \cdot h'_i | i \in \mathcal{G}]) \tag{2.17}$$

where Readout$(\cdot)$ is just the sum in the paper to ensure permutation invariant.

Any sequential recommendation method can be used to model the pooled sequence h^*, where this paper uses $h_s = \text{AUGRU}(h_1^*, \cdots, h_m^*)$. The final prediction is:

$$\hat{y} = \text{Pred}(h_s \parallel h_g \parallel h_t \parallel h_g \odot h_t) \tag{2.18}$$

where Pred is a two-layer MLP.

The task is CTR (CTR). The loss is vanilla NLL (negative log-likelihood) w/ L2 regularization term.

LightGCN [12] conducts extensive ablation studies on NGCF and finds that feature transformation and nonlinear activation of GCN contribute little and even negatively to collaborative filtering. For NGCF [13] (Neural Graph Collaborative Filtering), given the ID embedding $e_u^{(0)}$ of user u and $e_i^{(0)}$ of item i, the outputs of the layer $(k+1)$ are:

[12] He et al. 2020b

[13] Wang et al. 2019

$$
\begin{aligned}
e_u^{(k+1)} &= \sigma\left(W_1 e_u^{(k)} + \sum_{i \in \mathcal{N}_u} \frac{1}{\sqrt{|\mathcal{N}_u||\mathcal{N}_i|}}(W_1 e_i^{(k)} + W_2(e_i^{(k)} \odot e_u^{(k)}))\right), \\
e_i^{(k+1)} &= \sigma\left(W_1 e_i^{(k)} + \sum_{u \in \mathcal{N}_i} \frac{1}{\sqrt{|\mathcal{N}_u||\mathcal{N}_i|}}(W_1 e_u^{(k)} + W_2(e_u^{(k)} \odot e_i^{(k)}))\right)
\end{aligned}
\tag{2.19}
$$

where $\mathcal{N}_i$ denotes the set of users that interact with item i, $\mathcal{N}_u$ denotes the set of items that are interacted by user u.

The above formula 2.19's matrix form is implemented with graph Laplacian (exact the one used in GCN [14]):

[14] Kipf and Welling 2017

$$
E^{(k+1)} = \sigma\left((I + \mathcal{L})E^{(k)}W_1 + (\mathcal{L}E^{(k)}) \odot E^{(k)}W_2\right), \tag{2.20}
$$

$$
\mathcal{L} = D^{-\frac{1}{2}}AD^{-\frac{1}{2}} \tag{2.21}
$$

where A is the adjacency matrix and D is the diagonal degree matrix (w/ some tricks mentioned in GCN).

NGCF then concatenates the embeddings of all layers to obtain the final user and item embeddings, using the inner product to generate the prediction score.

The authors of LightGCN argue that the nodes in tasks of the original GCN paper have rich semantic features such as the title and the abstract, but in collaborative filtering, each node only has an ID. The motivation of LightGCN is very reasonable and the story is nice. The LGC (Light Graph Convolution) at layer k is defined as:

$$
e_u^{(k+1)} = \sum_{i \in \mathcal{N}_u} \frac{1}{\sqrt{|\mathcal{N}_u||\mathcal{N}_i|}} e_i^{(k)}, \tag{2.22}
$$

$$
e_i^{(k+1)} = \sum_{u \in \mathcal{N}_i} \frac{1}{\sqrt{|\mathcal{N}_u||\mathcal{N}_i|}} e_u^{(k)} \tag{2.23}
$$

The final embeddings are (learnable) weighted sum of the outputs of all layers:

$$e_u = \sum_{k=0}^{K} \alpha_k e_u^{(k)}, e_i = \sum_{k=0}^{K} \alpha_k e_i^{(k)}, \tag{2.24}$$

$$\hat{y}_{u,i} = e_u^\top e_i \tag{2.25}$$

LightGCN employs Bayesian Personalized Ranking (BPR) loss that encourages the prediction of an observed entry to behigher than its unobserved counterparts:

$$\mathcal{L} = -\sum_{u=1}^{M} \sum_{i \in \mathcal{N}_u} \sum_{j \neq \mathcal{N}_u} \ln \sigma(\hat{y}_{u,i} - \hat{y}_{u,j}) + \lambda \|E^{(0)}\|^2 \tag{2.26}$$

For user and item attribute (e.g., Female is a user attribute, sci-fi is a item attribute for a moive) interactions, there are two types of attributes interactions: inner interactions (interactions between homogeneous attributes, aka. both user or both item attributes), cross interactions (between heterogenous attributes). Existing methods do not distinguish these two types of interactions. GMCF [15] aruges that it is most effective way to explicitly model these two types of interactions separately.

[15] Su et al. 2021

Formally, user attributes and item attributes are both the set of key-value pairs (e.g., `(female, 1)`, `(age, 22)`). Each node is the embedding of the attribute $u = \text{val} \cdot e_{\text{attribute}}$. User attribute graph is a **complete** graph constructed from attributes of the user, which is same as the item attribute graph.

The inner interaction (for characteristic learning) is just the edge between two nodes in the same graph and is modeled by a MLP. After message passing, the new representation of node i is $z_i = \sum_{j \in \mathcal{N}(i)} \text{MLP}_{2d \to d}(u_i \parallel u_j)$.

The cross interaction (for node matching) is modeled by Hadamand product between the node of user graph and the node of item graph. The node matching result is the aggregation of a node in one graph and all node in the other graph: $s_i^U = \sum_{j \in V(I)} u_i^U \odot u_j^I$.

The final node representation is fused by GRU with the input sequence $[u_i, z_i, s_i]$. The final graph representations are $v_G^U = \sum_{i \in V(U)} u_i^U, v_G^I = \sum_{i \in V(I)} u_i^I$. The task is the prediction of an action (e.g., watch, like) w.r.t. a user and an item, using the inner product (graph matching) of user graph and item graph: $\hat{y} = v_G^{U\top} v_G^I$.

In overall, the motivation to distinguish two types of interactions is reasonable and gains some improved performance. However, the proposed two graphs cannot bring any structure information (i.e., the edge information) of the graph because they

are complete graphs. The fusion part (GRU over a sequence of three elements) is a unreasonable and stiff hyperparameter tuning. Besides, this work lacks the usage of the information of the relation between users and the historical interactions of the user.

3 | Bibliography

Arora, S., Li, Y., Liang, Y., Ma, T., and Risteski, A. (2018). Linear algebraic structure of word senses, with applications to polysemy. *Transactions of the Association for Computational Linguistics*, 6(0):483–495.

Brown, P. F., Della Pietra, S. A., Della Pietra, V. J., and Mercer, R. L. (1993). The mathematics of statistical machine translation: Parameter estimation. *Computational Linguistics*, 19(2):263–311.

Chang, J., Gao, C., Zheng, Y., Hui, Y., Niu, Y., Song, Y., Jin, D., and Li, Y. (2021). Sequential recommendation with graph neural networks. In *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '21, page 378387, New York, NY, USA. Association for Computing Machinery.

Chen, D., Bolton, J., and Manning, C. D. (2016). A thorough examination of the CNN/daily mail reading comprehension task. In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 2358–2367, Berlin, Germany. Association for Computational Linguistics.

Chen, D., Fisch, A., Weston, J., and Bordes, A. (2017). Reading Wikipedia to answer open-domain questions. In *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 1870–1879, Vancouver, Canada. Association for Computational Linguistics.

Chen, D. and Manning, C. (2014). A fast and accurate dependency parser using neural networks. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 740–750, Doha, Qatar. Association for Computational Linguistics.

Chen, T., Kornblith, S., Norouzi, M., and Hinton, G. (2020). A simple framework for contrastive learning of visual represen-

tations. In III, H. D. and Singh, A., editors, *Proceedings of the 37th International Conference on Machine Learning*, volume 119 of *Proceedings of Machine Learning Research*, pages 1597–1607. PMLR.

Cho, K., van Merriënboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, H., and Bengio, Y. (2014). Learning phrase representations using RNN encoder–decoder for statistical machine translation. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 1724–1734, Doha, Qatar. Association for Computational Linguistics.

Clark, K., Luong, M.-T., Le, Q. V., and Manning, C. D. (2020). ELECTRA: Pre-training text encoders as discriminators rather than generators. In *ICLR*.

Collobert, R. and Weston, J. (2008). A unified architecture for natural language processing: Deep neural networks with multitask learning. In *Proceedings of the 25th International Conference on Machine Learning*, ICML 08, page 160167, New York, NY, USA. Association for Computing Machinery.

Conneau, A., Schwenk, H., Barrault, L., and Lecun, Y. (2017). Very deep convolutional networks for text classification. In *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 1, Long Papers*, pages 1107–1116, Valencia, Spain. Association for Computational Linguistics.

Devlin, J., Chang, M.-W., Lee, K., and Toutanova, K. (2019). Bert: Pre-training of deep bidirectional transformers for language understanding.

Fang, H., Wang, S., Zhou, M., Ding, J., and Xie, P. (2020). Cert: Contrastive self-supervised learning for language understanding.

Gao, T., Yao, X., and Chen, D. (2021). SimCSE: Simple contrastive learning of sentence embeddings. In *Empirical Methods in Natural Language Processing (EMNLP)*.

Gehrmann, S., Deng, Y., and Rush, A. (2018). Bottom-up abstractive summarization. In *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*, pages 4098–4109, Brussels, Belgium. Association for Computational Linguistics.

Giorgi, J., Nitski, O., Wang, B., and Bader, G. (2021). DeCLUTR: Deep contrastive learning for unsupervised textual representations. In *Proceedings of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)*, pages 879–895, Online. Association for Computational Linguistics.

Glorot, X. and Bengio, Y. (2010). Understanding the difficulty of training deep feedforward neural networks. In Teh, Y. W. and Titterington, M., editors, *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*, volume 9 of *Proceedings of Machine Learning Research*, pages 249–256, Chia Laguna Resort, Sardinia, Italy. PMLR.

He, K., Fan, H., Wu, Y., Xie, S., and Girshick, R. (2020a). Momentum contrast for unsupervised visual representation learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*.

He, K., Zhang, X., Ren, S., and Sun, J. (2016). Deep residual learning for image recognition. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 770–778.

He, X., Deng, K., Wang, X., Li, Y., Zhang, Y., and Wang, M. (2020b). Lightgcn: Simplifying and powering graph convolution network for recommendation. In *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '20, page 639648, New York, NY, USA. Association for Computing Machinery.

Hochreiter, S. and Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8):1735–1780.

Huang, C.-Z. A., Vaswani, A., Uszkoreit, J., Simon, I., Hawthorne, C., Shazeer, N., Dai, A. M., Hoffman, M. D., Dinculescu, M., and Eck, D. (2019). Music transformer. In *International Conference on Learning Representations*.

Huang, E., Socher, R., Manning, C., and Ng, A. (2012). Improving word representations via global context and multiple word prototypes. In *Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pages 873–882, Jeju Island, Korea. Association for Computational Linguistics.

Huang, G., Liu, Z., v. d. Maaten, L., and Weinberger, K. Q. (2017). Densely connected convolutional networks. In *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 2261–2269.

Ioffe, S. and Szegedy, C. (2015). Batch normalization: Accelerating deep network training by reducing internal covariate shift. In *Proceedings of the 32nd International Conference on International Conference on Machine Learning - Volume 37*, ICML15, page 448456. JMLR.org.

Kim, Y. (2014). Convolutional neural networks for sentence classification. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 1746–1751, Doha, Qatar. Association for Computational Linguistics.

Kim, Y., Jernite, Y., Sontag, D., and Rush, A. M. (2016). Character-aware neural language models. In *Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence*, AAAI'16, page 27412749. AAAI Press.

Kingma, D. P. and Ba, J. (2014). Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980*.

Kipf, T. N. and Welling, M. (2017). Semi-supervised classification with graph convolutional networks. In *International Conference on Learning Representations (ICLR)*.

Lee, K., He, L., Lewis, M., and Zettlemoyer, L. (2017). End-to-end neural coreference resolution. In *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, pages 188–197, Copenhagen, Denmark. Association for Computational Linguistics.

Luong, M.-T. and Manning, C. D. (2016). Achieving open vocabulary neural machine translation with hybrid word-character models.

Luong, M.-T., Socher, R., and Manning, C. D. (2013). Better word representations with recursive neural networks for morphology. In *Proceedings of the Seventeenth Conference on Computational Natural Language Learning*, pages 104–113.

McCann, B., Bradbury, J., Xiong, C., and Socher, R. (2017). Learned in translation: Contextualized word vectors. In Guyon, I., Luxburg, U. V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., and Garnett, R., editors, *NeurIPS*, volume 30.

Meng, Y., Xiong, C., Bajaj, P., Tiwary, S., Bennett, P., Han, J., and Song, X. (2021). Coco-lm: Correcting and contrasting text sequences for language model pretraining.

Mikolov, T., Sutskever, I., Chen, K., Corrado, G. S., and Dean, J. (2013). Distributed representations of words and phrases and their compositionality. In Burges, C. J. C., Bottou, L., Welling, M., Ghahramani, Z., and Weinberger, K. Q., editors, *NeurIPS*, pages 3111–3119.

Nivre, J. (2003). An efficient algorithm for projective dependency parsing. In *Proceedings of the Eighth International Conference on Parsing Technologies*, pages 149–160, Nancy, France.

Parmar, N., Vaswani, A., Uszkoreit, J., Kaiser, L., Shazeer, N., Ku, A., and Tran, D. (2018). Image transformer. In Dy, J. and Krause, A., editors, *Proceedings of the 35th International Conference on Machine Learning*, volume 80 of *Proceedings of Machine Learning Research*, pages 4055–4064. PMLR.

Pascanu, R., Mikolov, T., and Bengio, Y. (2013). On the difficulty of training recurrent neural networks. In *Proceedings of the 30th International Conference on International Conference on Machine Learning - Volume 28*, ICML13, page III1310III1318. JMLR.org.

Paulus, R., Xiong, C., and Socher, R. (2018). A deep reinforced model for abstractive summarization. In *International Conference on Learning Representations*.

Pennington, J., Socher, R., and Manning, C. (2014). Glove: Global vectors for word representation. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, pages 1532–1543, Doha, Qatar. Association for Computational Linguistics.

Peters, M. E., Ammar, W., Bhagavatula, C., and Power, R. (2017). Semi-supervised sequence tagging with bidirectional language models. In *ACL (1)*, pages 1756–1765.

Peters, M. E., Neumann, M., Iyyer, M., Gardner, M., Clark, C., Lee, K., and Zettlemoyer, L. (2018). Deep contextualized word representations. In *NAACL*, pages 2227–2237.

Rohde, D. L., Gonnerman, L. M., and Plaut, D. C. (2005). An improved model of semantic similarity based on lexical co-occurrence.

See, A., Liu, P. J., and Manning, C. D. (2017). Get to the point: Summarization with pointer-generator networks. In *ACL (1)*, pages 1073–1083.

Seo, M., Kembhavi, A., Farhadi, A., and Hajishirzi, H. (2016). Bidirectional attention flow for machine comprehension.

Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., and Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, 15:1929–1958.

Su, Y., Zhang, R., M. Erfani, S., and Gan, J. (2021). Neural graph matching based collaborative filtering. In *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '21, page 849858, New York, NY, USA. Association for Computing Machinery.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L. u., and Polosukhin, I. (2017). Attention is all you need. In *NeurIPS*, volume 30.

Wang, T. and Isola, P. (2020). Understanding contrastive representation learning through alignment and uniformity on the hypersphere. In *International Conference on Machine Learning*, pages 9929–9939. PMLR.

Wang, X., He, X., Wang, M., Feng, F., and Chua, T.-S. (2019). Neural graph collaborative filtering. In *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR'19, page 165174, New York, NY, USA. Association for Computing Machinery.