老师，助教们，大家好，我是王浩宇，请允许我向大家介绍一下我们小组的项目，一个通过机器学习实现的聊天机器人。

======================= 背景部分 ============================

现如今，我们可以很容易地访问网络上对话的 “大数据”，能够让机器学习如何回复，这将极大地促进我们在人类和计算机之间建立数据驱动的、开放的对话系统。

具体来说，对话系统大致可分为两种：任务导向型对话系统和非任务导向型对话系统。我们的聊天机器人就是一种非任务对话系统。非任务导向的对话系统与人类交互，提供合理的回复和娱乐消遣功能，通常情况下主要集中在开放的领域与人交谈。

深度学习已成为对话系统的一项基本技术。值得注意的是，目前的模型远非完美。尽管取得了很大成就，但仍然有不少问题需要克服，分别是：快速适应问题、深度理解问题、评价困难和隐私保护问题。这里我们详细说明隐私保护问题，目前广泛应用的对话系统，服务于越来越多的人。我们必须要注意的是，用户使用的是同一个对话助手。通过互动、理解和推理的学习能力，对话助手可以无意中存储一些较为敏感的信息。因此，在构建更好的对话机制时，保护用户的隐私是非常重要的。

======================= 工作部分 ============================

为了实现我们的聊天机器人，我们主要翻看了两篇文献，第一篇是《Attention is all you need》 创新点在于抛弃了之前传统的encoder-decoder模型必须结合cnn或者rnn的固有模式，只用 attention，可谓大道至简。文章的主要目的是在减少计算量和提高并行效率的同时不损害最终的实验结果，创新之处在于提出了两个新的Attention机制，分别叫做 Scaled DotProduct Attention 和 Multi-Head Attention.

第二篇是《A Structured Self-attentive Sentence Embedding》，文章的主要创新之处是使用矩阵来表示句子的embedding，矩阵中的每一行通过self-attention机制来表示提取句子不同的关键信息。文章也提出一种self-attention的方法来替换max和 mean pooling操作，文章中最让人眼前一亮的是通过attention将句子转化为多个vector来提取句子中不同的部分，用一个matrix来表示句子embedding。

这是我们的参考资料。

======================= 实现部分 ============================

具体到我们的实现，我们的聊天机器人是一个基于baseline调参之后的RNN 神经网络，但我们同时也设计了一个 Transformer，Transformer分为四个步骤，分别是词向量化、编码流程、解码流程、输出预测值。

第一步是词向量化，这在 data/dailydialog 中已提供相应的词向量的映射，我们并不需要特别的实现，但究其原理，即将句子中的每一个词映射为一个向量，两者之间一一对应，原理如图所示。

第二步是编码流程，得到句子矩阵之后，我们将其送入编码器 Encoder 进行编码。这里，我们会用到 attention 策略，编码器 Encoder 整体流程如图所示。

第三步是解码流程，解码层的输入来自于两处，如下图所示，一部分输入来自于编码组件的输出，这部分是直接输入到解码器中的编码-解码attention子层中的，编码-解码attention中的Key和Value就来自于这部分输入；另一部分则是将模型已经翻译出来的部分句子重新输入到解码层的self-attention中。

第四步是输出预测值，我们通过解码组件可以得到一个向量，向量的每一个维度都代表目标语言单词库中的一个单词，对向量做softmax后，向量中该维度的值越大，代表对应单词的概率越大，输出概率最大的单词作为翻译结果。

下面是我们的具体代码细节，我们为代码做了注释，并基本按照理论进行实现。我们有Encoder 编码器、Multi-head attention 机制、还有负责表示位置 Position Encoding机制，更加详细的内容可以看我们在代码文件中的实现。

======================= 评估部分 ============================

这些是我们对模型做出的评估：对于BIEU来说，随着 n\_layers 的增加，聊天机器人的 BLEU 评分增加，但在 n\_layers 大于 3 之后，BLEU 随着层数的增加而降低，这可能是由于层数增加时的过拟合导致的；随着 学习率 的增加，聊天机器的 BLUE 呈现波动下降；这可能是因为 学习率增加会使训练更加难以收敛，从而导致无法达到最优解，让 BLEU 评分下降。在峰值下， BLEU 评分大于 baseline，符合测试需求。

对于学习时间来说，随着 n\_layers 层数的增加，学习时间呈线性增长的趋势，这符合我们的直觉，因为训练过程中的计算量也是呈比例增大的；随着 learning rate 的增加，学习时间呈现波动上升的趋势。

随着测试轮数的增加，BLUE 评分先升后降；随着迭代次数的增加，train\_loss 曲线趋近收敛至 3 。

这是我们的实际跑出来的聊天结果，如图所示，不论是 最佳 BLEU 还是 baseline，生成的回答均不令人满意，究其原因，可能是 RNN 模型本身效果并不可靠，我们应当采用更加强大的 BERT 和 Transformer 等。

======================= 动机部分 ============================

我们在之前提到过，隐私问题是当前一个需要克服的问题，这里我们小组的同学们思考过后，提出了我们自己的想法。这里我们以姓名为例，基于HanLP、人名语料库、名人语料库等。我们首先用HanLP对句子进行分词，并将这些单词转化成相应的词向量。我们在训练集中寻找和语料库匹配度较高的词向量，将这些向量替换成相应的虚拟的人名，例如张三、李四等。名人可能是对话中包含的重要信息，对于名人语料库中的姓名来说，如果识别，我们并不将其替换，只是保留他们。

======================= 分配部分 ============================

我们的工作是这样分配的。感谢老师、助教们的聆听，以上就是我们展示的内容。