**韩淑婷周报**

### 十七、第十七次2019年4月12日

## 论文方面

Verification of binarized neural networks via inter-neuron factoring

通过内部神经元分解验证二元神经网络（BNN）。我们减少对硬件验证的使用，对BNN的验证可以通过考虑同一层神经元之间的计算来实现更大的可扩展性。通过证明找到最佳因式分解的NP硬度以及PTAS近似性的硬度，我们设计了多项式时间搜索试探法来生成分解因式。总体框架允许将验证技术应用于具有数千个神经元和输入的嵌入式设备的中等大小的BNN。二值神经网络是更传统的前馈人工神经网络的一种潜在更高效的选择。主要特征是训练后的权重、输入、中间信号、输出、激活约束都是二进制值。因此，前向传播仅依赖于位级算术。由于BNN在图像识别的标准数据集（例如MNIST，CIFAR-10和SVHN）上也表现出良好的性能，因此，它们是当前基于嵌入式应用的神经网络基于浮点的神经网络实现方案的一种有吸引力且节能的替代方案。本文的结构：第2节定义了BNN的基本概念和概念。 第3节介绍了我们的验证工作流程，其中包括计数单位的分解（第3.2节）。 我们在第4节中用验证程序总结了实验结果，在第5节中将我们的结果与文献中的相关工作进行了比较，最后在第6节中给出了最后的评论和展望。附录中列出了定理的证明。

## 神经网络

神经网络是机器学习中的一种模型，是一种模仿动物神经网络行为特征，进行分布式并行信息处理的算法数学模型。这种网络依靠系统的复杂程度，通过调整内部大量节点之间相互连接的关系，从而达到处理信息的目的。

前馈神经网络：层与层链接

这是实际应用中最常见的神经网络类型。第一层是输入，最后一层是输出。如果有多个隐藏层，我们称之为“深度”神经网络。他们计算出一系列改变样本相似性的变换。各层神经元的活动是前一层活动的非线性函数。

循环网络：每层之间节点有连接

循环网络在他们的连接图中定向了循环，这意味着你可以按照箭头回到你开始的地方。他们可以有复杂的动态，使其很难训练。他们更具有生物真实性。循环网络的目的使用来处理序列数据。在传统的神经网络模型中，是从输入层到隐含层再到输出层，层与层之间是全连接的，每层之间的节点是无连接的，但是这种普通的神经网络对于很多问题却无能无力，例如，你要预测句子的下一个单词是什么，一般需要用到前面的单词，因为一个句子中前后单词并不是独立的。循环神经网路，即一个序列当前的输出与前面的输出也有关。具体的表现形式为网络会对前面的信息进行记忆并应用于当前输出的计算中，即隐藏层之间的节点不再无连接而是有连接的，并且隐藏层的输入不仅包括输入层的输出还包括上一时刻隐藏层的输出。

对称连接网络：单元之间连接对称

对称连接网络有点像循环网络，但是单元之间的连接是对称的（它们在两个方向上权重相同）。比起循环网络，对称连接网络更容易分析。这个网络中有更多的限制，因为它们遵守能量函数定律。没有隐藏单元的对称连接网络被称为“Hopfield 网络”。有隐藏单元的对称连接的网络被称为玻尔兹曼机。

CNN卷积神经网络与普通神经网络的区别在于，卷积神经网络包含了一个由卷积层和子采样层构成的特征抽取器。在卷积神经网络的卷积层中，一个神经元只与部分邻层神经元连接。在CNN的一个卷积层中，通常包含若干个特征平面(Feature Map)，每个特征平面由一些矩形排列的的神经元组成，同一特征平面的神经元共享权值，这里共享的权值就是卷积核。卷积核一般以随机小数矩阵的形式初始化，在网络的训练过程中卷积核将学习得到合理的权值。共享权值（卷积核）带来的直接好处是减少网络各层之间的连接，同时又降低了过拟合的风险。子采样也叫做池化（pooling），通常有均值子采样（mean pooling）和最大值子采样（max pooling）两种形式。子采样可以看作一种特殊的卷积过程。卷积和子采样大大简化了模型复杂度，减少了模型的参数。卷积神经网络由三部分构成。第一部分是输入层。第二部分由n个卷积层和池化层的组合组成。第三部分由一个全连结的多层感知机分类器构成。

RNN循环神经网路，即一个序列当前的输出与前面的输出也有关。具体的表现为网络会对前面的信息进行记忆并应用于当前输出的计算中，即隐藏层之间的节点不再无连接而是有连接的，并且隐藏层的输入不仅包括输入层的输出还包括上一时刻隐藏层的输出。理论上，RNN能够对任何长度的序列数据进行处理。

玻尔兹曼机和递归神经网络相比，区别如下：1、递归神经网络本质是一个学习函数，因此有输入和输出层的概念，而玻尔兹曼机的用处在于学习一组数据的“内在表示”，因此其没有输出层的概念。2、递归神经网络各节点链接为有向环，而玻尔兹曼机各节点连接成无向完全图。RBM受限玻尔兹曼机加入了限制，将完全图变成了二分图。即由一个显层和一个隐层构成，显层与隐层的神经元之间为双向全连接。在RBM中，任意两个相连的神经元之间有一个权值w表示其连接强度，每个神经元自身有一个偏置系数b（对显层神经元）和c（对隐层神经元）来表示其自身权重。

DBN是一个概率生成模型，与传统的判别模型的神经网络相对，生成模型是建立一个观察数据和标签之间的联合分布，对P(Observation|Label)和 P(Label|Observation)都做了评估，而判别模型仅仅而已评估了后者，也就是P(Label|Observation)。DBN由多个限制玻尔兹曼机（Restricted Boltzmann Machines）层组成，一个典型的神经网络类型如图所示。这些网络被“限制”为一个可视层和一个隐层，层间存在连接，但层内的单元间不存在连接。隐层单元被训练去捕捉在可视层表现出来的高阶数据的相关性。

GAN生成对抗网络的目标在于生成，我们传统的网络结构往往都是判别模型，即判断一个样本的真实性。而生成模型能够根据所提供的样本生成类似的新样本，注意这些样本是由计算机学习而来的。GAN一般由生成模型网络和判别模型网络组成。生成模型 G 捕捉样本数据的分布，用服从某一分布（均匀分布，高斯分布等）的噪声 z 生成一个类似真实训练数据的样本，追求效果是越像真实样本越好；判别模型 D 是一个二分类器，估计一个样本来自于训练数据（而非生成数据）的概率，如果样本来自于真实的训练数据，D 输出大概率，否则，D 输出小概率。在训练的过程中固定一方，更新另一方的网络权重，交替迭代，在这个过程中，双方都极力优化自己的网络，从而形成竞争对抗，直到双方达到一个动态的平衡（纳什均衡），此时生成模型 G 恢复了训练数据的分布（造出了和真实数据一模一样的样本），判别模型再也判别不出来结果，准确率为 50%。