张量网络讲义

夏盟佶

April 19, 2020

Abstract

庚子年，新冠状病毒引起的肺炎流行，中国科学院大学也从教室授课改为网络授课。2016年首次参与高级算法课讲授，一般以幻灯片为主（2019年春季新增的多项式插值归约内容用板书讲授），幻灯片未承载所有细节。一直围绕张量网络，讲授我最熟悉的过去的前沿研究内容，所选内容只有零星部分可见于一些教科书。考虑以上，试写一份讲义，用于2020 年研究生一年级课程《高级算法设计分析》的部分课次。顺便一说，上次肺炎流行与2003年，恰好是我自己在中国科学院研究生院玉泉路园区读研究生一年级下学期的时候。

Contents

Chapter 1

张量网络定义

1.1 封闭的张量网络

用$[k]$来表示一个大小为k的有限集，例如$\{1,2,\ldots,k\}$。一个d元布尔函数$F:[2]^d\to\mathcal{C}$，在$(x_1,x_2,\ldots,x_d)$的值记为$F(x_1,x_2,\ldots,x_d)$。张量网络用图描述离散函数的结合。使用允许重边和自环的图，而不局限于简单图。图$G(V,E)$的每个点v 被赋予一个d_v元布尔函数F_v，这里d_v表示v的度。点v的d_v条边按一定的次序记为$e_{v,1},e_{v,2},\ldots,e_{v,d_v}$。张量网络的值定义为：

$$\sum_{e_1,\ldots,e_m\in[2]}\prod_{v\in V}F_v(e_{v,1},e_{v,2},\ldots,e_{v,d_v})$$

定义 (封闭的张量网络) 一个张量网络由三份要素构成：

1. 图$G(V,E)$。（$E=\{e_1,e_2,\ldots,e_m\}$。顶点v的度记为d_v。）
2. 每个顶点v被赋予一个d_v元离散函数F_v。（函数的每个变量的定义域是D。）
3. 每个顶点v的d_v条边被赋予一个次序，第i条边记为$e_{v,i}$。

它的值定义为：

$$\sum_{e_1,\ldots,e_m\in D}\prod_{v\in V}F_v(e_{v,1},e_{v,2},\ldots,e_{v,d_v})$$

用更数学家一点的符号可写为：

$$\sum_{\sigma:E\to D}\prod_{v\in V}F_v(\sigma(e_{v,1}),\sigma(e_{v,2}),\ldots,\sigma(e_{v,d_v}))$$

或

$$\sum_{\sigma:E\to D}\prod_{v\in V}F_v(\sigma|_{Neighbor(v)})$$

定义 (对称函数) 一个d元函数F，如果对任何d元置换π，都有$F(x_1,x_2,\ldots,x_d)=F(x_{\pi(1)},x_{\pi(2)},\ldots,x_{\pi(d)})$，称$F$是对称函数。

当张量网络的函数都是对称函数时，定义中的第三份要素还重要吗？

定义 (对称函数的简记法) 一个d元布尔函数F，最多只有$d+1$种函数值，通过枚举函数值记F为$[F_0,F_1,\ldots,F_d]$，其中F_i 是F 在输入是i 个1 和$d-i$ 个0时的值。

如果定义域$D=[k]$，$k>2$，可以怎样记？（提示：$k-1$维表格。$k=2$时，$[F_0,F_1,\ldots,F_d]$ 是一维的线排列。）

练习题

1. 写出一个由若干个$[0,1,0,0]$函数组成的张量网络并求值。

2. 把上题的张量网络中每个函数换成$[0,0,1,0]$并求值。与习题1的答案比较。

3. 写出一个由非对称函数组成的张量网络并求值。

定义 (计数问题框架之一：张量网络求值问题) 输入是一个张量网络，求它的值。

定义 ($\#\mathcal{F}$问题) 输入是一个所有函数都来自$\mathcal{F}$的张量网络，求它的值。

k规则图，是每个点的度都是k的图。图$G(V,E)$的一个完美匹配是一个集合E'，满足：1、$E'\subseteq E$ （即E'是一些边构成的

集合）；2、$G(V,E')$是1 规则图。

定义 (**完美匹配数目问题（#PM）**) 输入是一个图，求它的完美匹配数目。

s入t出规则图，是每个点的入度都是s出度都是t的图。有向图$G(V,E)$的一个圈覆盖是一个集合E'，满足：1、$E' \subseteq E$；2、$G(V,E')$是1入1出规则图。

定义 (**圈覆盖数目问题（#PM）**) 输入是一个图，求它的圈覆盖数目。

练习题

1. 给出一个函数集合$\mathcal{F}$，使得完美匹配数目问题就是$\#\mathcal{F}$问题。

2. 给出一个函数集合$\mathcal{F}$，使得圈覆盖数目问题就是$\#\mathcal{F}$问题。

1.2 开放的张量网络

在封闭张量网络中，函数结合成一个值，一个值可以认为是一个零元函数的k^0个函数值。开放的张量网络更一般化，函数结合成一个函数。需要一个比图更广泛的概念，除了有完整的图，还有图的局部。一个直观的例子，取一个图和它的割（cut），把割里的边从中间割开，就得到了两个图的局部。

在图的环境下，定义一种顶点和边之外的新元素半边，半边是从图的一个顶点出发的没有到另一个顶点（无向）线段。（也没有回到出发顶点，因此自环不是半边）。

定义 (**图元**) 一个图元$G(V,E,X)$由顶点集V、边集E和半边集X 构成，其中E 是一个重集，其元素是以无序点对(u,v)形式表示的边，$u,v\in V$，X也是一个重集，其元素是以无序单点组(v) 形式表示的半边，$v\in V$。E也叫作内部边集，X 也叫作外部边集。

定义 (张量网络) 一个张量网络由三份要素构成：

1. 图元$G(V,E,X)$。（顶点v的度记为d_v。$E=\{e_1,e_2,\ldots,e_m\}$。$X=\{x_1,x_2,\ldots,x_n\}$。）

2. 每个顶点v被赋予一个d_v元离散函数F_v。（函数的每个变量的定义域是D。）

3. 每个顶点v的d_v条边被赋予一个次序，第i条边记为$e_{v,i}$。

此张量网络定义了一个函数$F:D^n\to\mathcal{C}$，它的值定义为：

$$F(x_1,x_2,\ldots,x_n)=\sum_{e_1,\ldots,e_m\in D}\prod_{v\in V}F_v(e_{v,1},e_{v,2},\ldots,e_{v,d_v})$$

上面的记号，采用了计算机和程序的习惯，（内部和外部）边的符号也代表其取值。用更数学一点的符号，设$\tau:X\to D^n$是对外部边的任意一个取值，定义

$$F(\tau)=F(\tau(x_1),\tau(x_2),\ldots,\tau(x_n))=\sum_{\sigma:E\to D}\prod_{v\in V}F_v(\tau\cup\sigma|_{Neighbor(v)})$$

$\tau\cup\sigma$ 赋予每条边一个值，$\tau\cup\sigma|_{Neighbor(v)}$ 表示把此赋值局限到v的邻边上。

练习题

1. 画出一个张量网络，并计算它的函数。

2. 画出一个没有内部边的张量网络，并计算它的函数。

3. 画出一个没有内部边也没有外部边的张量网络，并计算它的函数。（度自然可以为0，此时点被赋予0元函数。约定一个0元函数有唯一函数值。）

练习题

1. 搜索爱因斯坦求和约定、因子图等定义，比较与张量网络的异同。

1.3 张量网络的结合律

1.3.1 张量网络与线性代数之一：张量网络与矩阵乘法

张量网络是一些线性代数运算的推广，并且具有形象的图表示，可被直观认为是形象表示的网形代数运算。

矩阵乘法大概是最常见的，同张量网络一样采取“$\sum\prod$”方式定义的代数运算。

$$(M_{x,y})(N_{y,z}) = (T_{x,z})$$

$$T_{x,z} = \sum_y M_{x,y}N_{y,z}$$

向量和矩阵的标号对应函数的变量。向量（矩阵）有一（两）个标号，对应一（二）元函数。矩阵有两个标号，对应二元函数。

练习题

1. 写一个矩阵乘积式子，并把它转换成张量网络。即画出一个张量网络，由式子中的向量和矩阵构成，张量网络的函数对应整个矩阵乘积。

顺应矩阵的符号，约定画矩阵点时，把行标变量边向左画，把列标变量边向右画。此约定自然下放到向量。

1.3.2 矩阵乘法的结合律

本小节复习熟知的矩阵乘法结合律，为更一般的张量网络的结合律做铺垫，可以跳过。其实我们也可以选取其他运算的结合律用作铺垫，例如张量积的结合律。

α, β表示列向量。矩阵乘法结合律告诉我们$(\alpha' N)\beta = \alpha'(N\beta)$。下面证之。

证明 设$\alpha = (\alpha_x)$，$N = (N_{x,y})$，$\beta = (\beta_y)$，$T = \alpha' N$。

$$T_y = \sum_x \alpha_x N_{x,y}$$

$$T\beta = \sum_y T_y \beta_y = \sum_y (\sum_x \alpha_x N_{x,y}) \beta_y = \sum_y (\sum_x \alpha_x N_{x,y} \beta_y) = \sum_{x,y} \alpha_x N_{x,y} \beta_y$$

同理，

$$\alpha'(N\beta) = \sum_{x,y} \alpha_x N_{x,y} \beta_y$$

□

证明过程中验证了，按照矩阵乘法一步步计算，会得到$\alpha' N \beta = \sum_{x,y} \alpha_x N_{x,y} \beta_y$，右侧正好是表示$\alpha' N \beta$的张量网络的函数。

练习题

1. 在有外部边情形下，证明矩阵乘法结合律，例如$(M_{x,y})(N_{y,z})(R_{z,w})$。
2. 用张量网络定义矩阵乘法，用张量网络直接定义一列矩阵的乘积，说明这两个定义是如何融洽的。

1.3.3 张量网络的结合律

定理 $G(V,E,X)$是一个张量网络，V_1和V_2是V的一个划分，V_1和V_2自然地引出一个X 的划分X_1和X_2，自然地引出一个E 的三划分$E_1 = E \cap (V_1 \times V_1)$、$E_2 = E \cap (V_2 \times V_2)$和$E_3 = E \cap (V_1 \times V_2)$。即$E_3$是一个$V_1, V_2$一割。定义两个新的张量网络，把$E_3$ 中每一条边隔开成两条半边，自然的引出一个V_1相关的半边集合Y_1和一个V_2相关的半边集合Y_2，第一个新张量网络是$G_1(V_1, E_1, X_1 \cup Y_1)$，第二个新张量网络是$G_2(V_2, E_2, X_2 \cup Y_2)$。张量网络$G, G_1, G_2$的函数分别记为$F, F_1, F_2$。

定义张量网络H，H把$F_1(X_1, Y_1)$和$F_2(X_2, Y_2)$以类似G的方式组合称一个函数，$H(\{u_1, u_2\}, E_3, X = X_1 \cup X_2)$，$u_i$被赋予$F_i$。张量网络$H$的函数记为$F_H$。

$$F_H(X) = F(X)$$

证明

$$\begin{aligned}
F_H(X) &= \textstyle\sum_{E_3} F_1(X_1, E_3) F_2(X_2, E_3) \\
&= \textstyle\sum_{E_3} (\sum_{E_1} \prod_{v \in V_1} F_v)(\sum_{E_2} \prod_{v \in V_2} F_v) \\
&= \textstyle\sum_{E_3} \sum_{E_1} \sum_{E_2} \prod_{v \in V_1} F_v \prod_{v \in V_2} F_v) \\
&= \textstyle\sum_{E} \prod_{v \in V} F_v \\
&= F(X)
\end{aligned}$$

□

思考题

1. 如果边集E_3是空集，这一特殊情形会怎样？
2. 如果边集E_3没有构成一个割，会怎样？
3. 这个定理只讲了两个子网络G_1和G_2并列的情形，多个子网络并列会怎样？
4. 子网络G_1在分割成若干个子子网络，例如$G_{1,1}$和$G_{1,2}$，这种嵌套使用结合律的情形会怎样？

1.4 张量网络与线性代数

1.4.1 函数的矩阵表示

1.4.2 张量网络与线性代数之二：张量网络与张量积

定义

$$\mathbf{M} = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1t} \\ m_{21} & m_{22} & \dots & m_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ m_{s1} & m_{s2} & \dots & m_{st} \end{pmatrix}$$

两个矩阵$\mathbf{M}$和$\mathbf{N}$的张量积$\mathbf{M}\otimes\mathbf{N}$定义为：

$$\begin{pmatrix} m_{11}\mathbf{N} & m_{12}\mathbf{N} & \dots & m_{1t}\mathbf{N} \\ m_{21}\mathbf{N} & m_{22}\mathbf{N} & \dots & m_{1t}\mathbf{N} \\ \vdots & \vdots & \ddots & \vdots \\ m_{s1}\mathbf{N} & m_{s2}\mathbf{N} & \dots & m_{st}\mathbf{N} \end{pmatrix}$$

这是矩阵分块写法，每一块是矩阵$\mathbf{M}$的一个元素m_{xy}数乘矩阵$\mathbf{N}$。

设$\mathbf{M}=(m_{x;y})$是一个$s\times t$矩阵，$\mathbf{N}=(n_{z;w})$是一个$p\times q$矩阵，$x\in[s]$是$\mathbf{M}$的行指标，其定义域有一个自然的行次序。$\mathbf{M}\otimes\mathbf{N}$是一个$sp\times tq$矩阵。

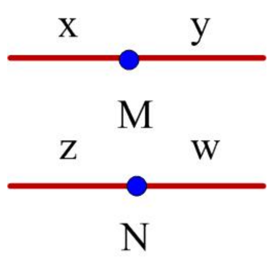
$$\mathbf{M}\otimes\mathbf{N}_{x,z;y,w}=m_{x;y}n_{z;w}$$

这里x,z表示$\mathbf{M}\otimes\mathbf{N}$的行标，它由$x\in[s]$和$z\in[p]$两个子标号联合，按照字典序排列。

$\mathbf{M}\otimes\mathbf{N}$有$stpq$个元素。回忆$\mathbf{M}$可被认定为二元函数$M:[s]\times[t]\to\mathcal{C}$, $M(x,y)=m_{x;y}$，矩阵$\mathbf{M}$以一定的次序（$[s]$和$[t]$自带的排序联合）和方式（二维表格）存储函数M的函数值。函数N类似。

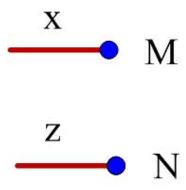
定义四元函数$MN:[s]\times[t]\times[p]\times[q]\to\mathcal{C}$, $MN(x,y,z,w)=M(x,y)N(z,w)$。$\mathbf{M}\otimes\mathbf{N}$以一定的次序和方式存储了$MN$的所有函数值。本质上，张量积就是以一定次序排列的函数乘积的函数值表。

张量网络定义之中也有函数值的乘积，利用张量网络表示张量积。



用张量网络的结合律推导出张量积的结合律。

张量积的定义也适用于向量。



思考题

1. 使用张量积的结合律作为例子解释张量网络的结合律会怎样？

1.4.3 零元函数的张量积

$$(M \otimes N) = MN$$

推论 一个无外部边的张量网络的值，是它各个连通分支的值的乘积。

证明 先用张量网络的结合律，把每个连通分支缩成点，然后零元函数的张量积。 □

练习题 使用张量网络求值问题定义证明上面的推论。

1.4.4 张量积、张量是不同的概念（与主题无关的独立小节）

张量概念是矢量概念和矩阵概念的推广，标量是零阶张量，矢量是一阶张量，矩阵（方阵）是二阶张量，而三阶张量则好比立体矩阵。用计算机的语言说，张量就是高维数组。

张量网络是描述函数的结合的，其基本元素是函数，例如，一个d元函数$F:[k]^d \to \mathcal{C}$，其实就是一个d维数组。

可以说张量网络的基本元素是，函数=高维数组=张量。张量网络的名字来自于第三种叫法。

高维数组的叫法比较直观，使人想到编程，本文将减少使用高维数组这个名字。函数容易使人想到连续函数，当想到是离散函数时，是个相对合适的名字。张量是个比较偏数学的名字，打算避免使用。

显现为高维数组或函数的张量并不抽象，但是可以把离散函数F作为线性空间的线性函数，即把$[k]$看成线性空间的基。我们熟知，从一个线性空间A到另一个线性空间B的线性映射f，在取定每个空间的基向量之后，可以对应一个矩阵M。线性映射的复合对应矩阵乘法。

待补图：向量矩阵乘法，解释成向量映射到向量

更适宜推广到高维向量的看法是，把M看成两个线性空间A和B'到标量集合$\mathcal{C}$的映射f，定义如下：

$$f(\alpha, \beta) = \alpha M \beta'$$

函数f关于两个自变量都具有线性性。在线性空间的视角下下，张量代表了多重线性函数。

待为上式补图：

对于高维张量，图：

高维张量就只能看成空间到标量的映射，而就不能看成线性空间到线性空间的函数了吗？非也，因不计划纠缠多重线性函数、对偶空间、空间张量积等概念，在下节仅给出张量如何作为线性空间到线性空间的函数的直觉。

线性空间做基变换时，其矩阵形式就发生相应的变换。（例如，矩阵相似。）以后我们将通过张量网络，利用张量网络直观的优点，直接看到多重线性函数的基变换。（不是指深层的数学概念不好，而是焉用牛刀（xueshucaiqian未熟悉到足以讲好）。）

思考题

1. 把矩阵乘法看做张量。

2. 扩展阅读：张量秩，以及矩阵乘法的张量秩和矩阵乘法的算法时间的关系。

1.4.5 函数的矩阵形式

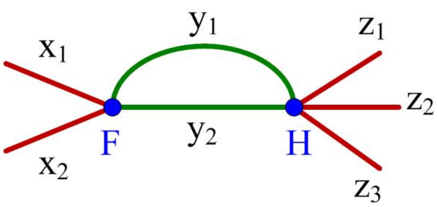
设F是一个$n+m$元布尔函数，可以任意把自变量区分成两部分，设$x_1,\ldots,x_n,y_1,\ldots,y_m$是它的输入。

对应$2^n\times 2^m$的矩阵$M=(M_{x_1\cdots x_n,y_1\cdots y_m})$，其中

$$M_{x_1\cdots x_n,y_1\cdots y_m}=F(x_1,\ldots,x_n,y_1,\ldots,y_m)。$$

若取$m=0$（或$n=0$），就成了列（或行）向量。

如下张量网络的函数可用矩阵乘法表示：



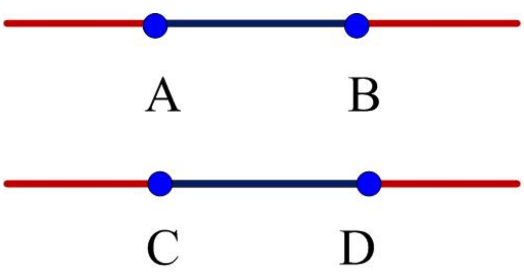
$$(F_{x_1x_2,y_1y_2})(H_{y_1y_2,z_1z_2z_3})$$

遵循行（列）标的变量边画在左（右）边。

思考题

1. 矩阵转置对应什么样的张量网络变换？或者说，一个矩阵的转置矩阵怎么画？

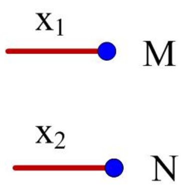
2. 利用矩阵运算写出下图张量网络的函数



$$(A\cdot B)\otimes(C\cdot D) \qquad 还是 \qquad (A\otimes C)\cdot(B\otimes D)$$

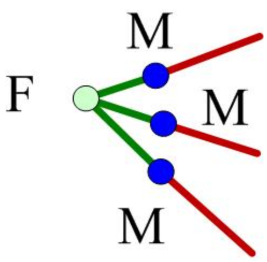
1.4.6 矩阵乘法与张量积的共同（同构）狭义情形

$$(MN')_{x_1,x_2} = M_{x_1}N_{x_2}$$



$$(M \otimes N)_{x_1,x_2} = M_{x_1}N_{x_2}$$

1.4.7 混合矩阵乘法与张量积

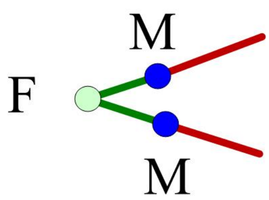


$$F \cdot M^{\otimes 3}$$

$$F \cdot M^{\otimes 2}$$

思考题

1. 回忆之前的同构：列向量乘以行向量$M \otimes N$ 与$M\ N'$，
   猜一猜$F \cdot M^{\otimes 2}$ 同构与什么？



1.4.8 张量网络与线性代数之三：张量网络与迹

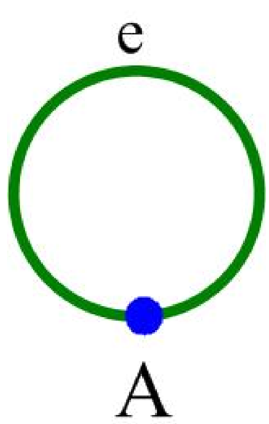


Figure 1.1: $\sum_e A_{e,e}$

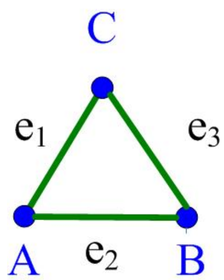
矩阵乘积的迹

$$\mathrm{trace}(ABC) = \sum_{e_1,e_2,e_3\in[d]} A_{e_1e_2}B_{e_2e_3}C_{e_3e_1}$$

思考题

1. 证明$\mathrm{trace}(ABC) = \mathrm{trace}(BCA) = \mathrm{trace}(C'B'A')$。

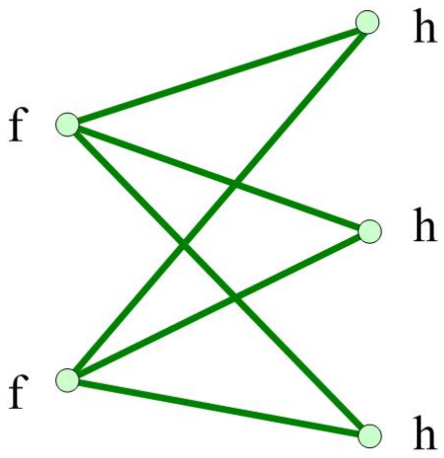
2. 给出$\mathrm{trace}(ABC)$的张量网络。用张量网络解释上式。

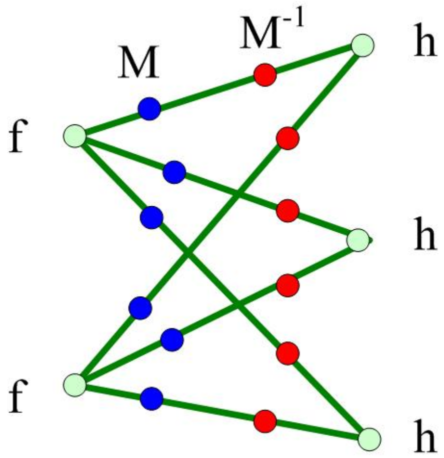


3. 扩展阅读：partial trace。

1.4.9 全息归约

$AB = AEB = AMM^{-1}B = (AM)(M^{-1}B)$。($E$是单位阵)

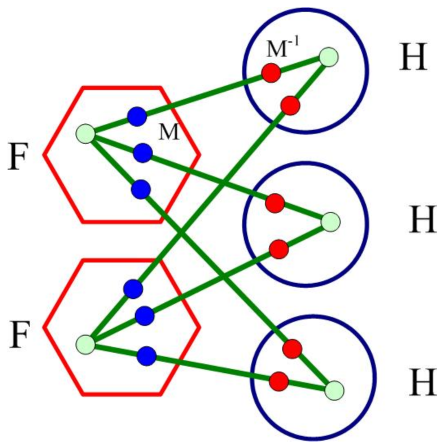




定理 (Valiant 2004) $\#\{F\}|\{H\}$和$\#\{f\}|\{h\}$在相同的图上的值相等。其中，

$$F = fM^{\otimes 3},$$

$$(M^{-1})^{\otimes 2}h = H。$$



1.4.10 模型与观点

1.4.11 变量与二元相等函数

张量网络中的边变量出现两次，例如，$\sum_e A_{e,e}$中被求和的变量e在后面式子中出现两次。

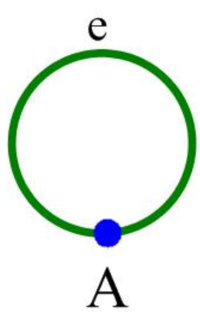


Figure 1.2: $\sum_e A_{e,e}$

考虑另外一个张量网络，它的值与trace$A$是否相等？

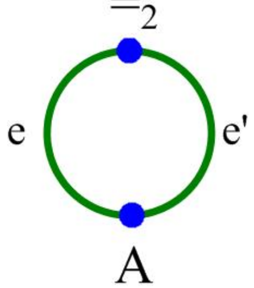


Figure 1.3: $\sum_{e,e'} A(e,e')``=_2"(e',e)$

张量网络的中的变量都恰好出现两次，本质上，边变量与点二元相等函数的功能没有区别，画图表达方式上不同而已。变量就是函数，特殊的函数而已。

若变量只出现一次，没有起到联接函数的作用；若出现k次，可以用k元相等函数模拟。

思考题

1. 上述言论中在$k=1$时是什么意思？

即便使用一个度为2的二元相等函数点，替代一条边变量，新点与其他部分的连接还是边。边，或者二元相等，是我能想到的起到关联作用的最小的最简便的独点集合。

1.4.12 与其他模型的关系

布尔门和布尔线路

概率布尔门

概率布尔门构成的概率随机布尔线路

练习题

探索概率随机布尔线路与张量网络的关系。

复数化的概率

从2入1出门到2入2出门

量子线路，结束时的状态经过测量输出答案

BQP

Post-BQP = PP （decision version of #P）

概率图模型：1、有向：贝叶斯网络；2、无向：马尔科夫随机场。（参见CMU课程10708 Probabilistic Graphical Models）

以考虑分布为主。Partition function。

练习题

了解相关概念。或者在以后遇到相关概念时，从张量网络的角度看待它们一下，看看张量网络的种种基本性质，能否给出什么观察。

1.4.13 教学内容安排

计算角度有两个对立面：易解性和难解性。易解指存在比较高效的算法，其严格对立面指不存在高效的算法，但这是一种很难证明的使用任意量词命题，常见的难解性分析使用某一计算复杂性类的困难性。困难性的证明涉及到构造归约算法。

本部分课程关注张量网络求值问题，将从计算角度，侧重概念、性质、算法，轻困难性证明，方法上侧重通过深刻理解基础属性，带动具体问题上的具体分析，大致安排如下内容：

以张量网络概念为核心介绍定义与性质。

1、介绍一些计数问题的多项式时间算法。

2、难解性方面，几乎仅介绍多项式插值归约方法。

3、透过张量网络的（全息归约以外）基本性质，直观地理解的一些结论。（散布于各章，例如本章的各个连通分支的值的乘积。）

4、全息归约最常见的应用是证明困难性，但本讲义搜集了多个非证明困难性的例子。（不少例子是作者在十多年研究中积攒的，碰巧遇到的可以使用全息归约重新认知的已知结论，属于原创的重复性证明。估计这份搜集是独一份。当然，这份搜集也不完整，有一个MCMC算法，可以看做在到Hardmard基下进行随机行走。作者偏科于严格计数问题，听研究近似计数同行提过此问题。）

5、讲解完美匹配数目问题的方方面面。

Chapter 2

满足约束解数目问题（#CSP）

上一章结束时，我们看到张量网络中的每个变量出现两次。本章介绍变量出现次数不受限的对应问题。先从判定版本看起。

2.1 约束可满足问题（CSP）

3CNF公式

$$\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$$

其中每个子句$C_i = l_{i,1} \vee l_{i,2} \vee l_{i,3}$，是3元或函数，作用在3个文字上。每个文字，是某个变量x_j 或者$\neg x_j$。

SAT=satisfiability

定义 (3SAT问题) 输入是一个3CNF公式φ，φ是关于布尔变量集$X = \{x_1, x_2, \ldots, x_n\}$的，问是否存在一个变量的赋值$\pi : \{x_1, x_2, \ldots, x_n\} \to \{0, 1\}$，使得$\pi$满足$\varphi$，即$\varphi(\pi) = 1$（也记做即$\pi \models \varphi$）。

公式φ的每一个子句是一个关于变量的约束。π满足φ，就是满足每一个约束。

在3SAT问题问题中，每个约束来自8种形式之一，从$x \vee y \vee z$，到$\neg x \vee \neg y \vee \neg z$。

定义 (2SAT问题) 输入是n个布尔变量构成的集合$X = \{x_1, x_2, \ldots, x_n\}$上的一个2CNF公式$\varphi$，问是否存在一个变量的赋值$\pi : \{x_1, x_2, \ldots, x_n\} \to \{0, 1\}$，使得$\pi$满足$\varphi$，即$\varphi(\pi) = 1$（也记做即$\pi \models \varphi$）。

公式φ的每一个子句是一个关于变量的约束。π满足φ，就是满足每一个约束。

在2SAT问题问题中，每个约束来自4种形式之一，$x \vee y$，$x \vee \neg y$，$\neg x \vee y$，$\neg x \vee \neg y$。

不难看出3SAT问题和2SAT问题，可以统一到一个框架下定义。设$\mathcal{F}$是一个函数集合，定义对应的约束可满足问题CSP($\mathcal{F}$)，

定义 (**约束可满足性问题**CSP($\mathcal{F}$)) 输入是一些形式来自$\mathcal{F}$ 的约束R_j，每个R_j作用于布尔变量$x_1, x_2, \ldots, x_n$中的若干个，问是否存在一个变量的赋值$\pi : \{x_1, x_2, \ldots, x_n\} \to \{0, 1\}$，使得$\pi$满足每一个约束$R_j$。

CSP问题，就是通过规定可用作变量的约束的函数集合$\mathcal{F}$，定义的对应可满足性问题CSP($\mathcal{F}$)。

当$\mathcal{F}$变动时，CSP($\mathcal{F}$)就构成一个判定问题集合。如此一来，就可以研究$\mathcal{F}$ 如何决定CSP($\mathcal{F}$) 的计算复杂性。

练习题

1. 参考张量网络$\sum\prod$的定义方式，给3SAT一个$\bigvee\bigwedge$定义方式，把定义方式调整成$\bigvee\prod$，并推广到一般的CSP 问题。

2. 给定一个CSP问题的一个输入I，I有变量集合$X = \{x_1, x_2, \ldots, x_n\}$和约束集合$R = \{r_1, \ldots, r_m\}$，把约束作用于变量的关联性描述成一个二部图$G(X, R, E)$。

思考题

1. 把上面练习题中的二部图$G(X, R, E)$，扩展定义出一个张量网络。此张量网络和原来CSP问题的值有什么关系？

2.2 判定问题的难解性的判定标准之一：NP困难性

关于一个问题集合的中每个问题的计算复杂性结论，恰好有两种情况时，就称之为二分定理。二分定理把问题分成易解和难解两类。判定问题或者关系，都是值域为{0,1}的函数。判定问题的分类标准经常分别是多项式时间可计算和NP困难。（当然，严格来说，所谓两种情况，需要类似P≠NP之类的假设，否则就成了一种情况。）上节提到的2SAT 问题是多项式时间可计算的，3SAT问题是NP困难的。

一个计算问题（即关系或者函数）$F(X)$ 多项式时间可计算，指存在多项式时间算法，即存在计算它的图灵机使得：计算步数作为输入长度的函数，有一个多项式函数上界。

多项式时间可计算概念也用用于二元关系$R(X,Y)$ ，此时，输入长度是$|X,Y|$。

对一个二元关系$R(X,Y)$ 的两个变量X和Y，如果存在一个多项式P，使得如果有$R(X,Y) = 1 \Rightarrow |Y| \leq P(|X|)$，则称$|Y|$被$|X|$ 多项式限定的。

NP是一个判定问题集合，$F(X)$ 在NP中，当且仅当存在多项式时间可计算的$|Y|$被$|X|$多项式限定的二元关系$R(X,Y)$ 使得：$F(X) = [\exists Y, R(X,Y) = 1]$。

归约概念类似于编程中的函数调用。A 到B 的一个归约算法θ，是一个计算函数A 的算法，算法可以直接使用函数B，每次使用函数B 时，只计做A 的一个时间步（不把计算B 所需的时间计入A的计算时间）。如果存在一个A 到B 的多项式时间的归约算法，称A 多项式时间归约到B。

归约具有传递性。

多一归约：

对A的任一输入I，$A(I) = B(\theta(I))$。

图灵归约：暂略。

定义 (NP**困难性**) 如果NP里的任何一个问题A都可以多项式时间归约到某个问题B，则称B是NP困难的。

定理 (Cook-Levin, Karp) 3SAT 是NP困难的。

定理证明概述。

1. 计算过程，可以被布尔线路描述；因而计算结果0或1，可以等同于它的值。

   计算过程的表格，第一行记录I 和起始状态q_0，第i 行记录时刻i的带子内容和状态。第$i+1$行根据转移函数机械的取决于第i行。

2. 线路的大小，被I的长度和时间函数所限制。

3. 根据第一条，$R(X,Y)$ 的计算过程，可以转化为一个布尔线路C，线路的输入门X,Y，设线路的其他门是Z。

   进而可以转化为一个3SAT公式$\varphi(X,Y,Z), \exists Z, \varphi(X,Y,Z) = 1$当且仅当$C(X,Y)=1$。

4. 回顾NP的定义，任取NP里的一个问题A，则存在多项式时间可以计算的二元关系R，$A(I) = [\exists Y, R(I,Y) = 1]$。$\exists Y, R(I,Y) = 1$ 当且仅当$\exists Y, C(I,Y) = 1$ 当且仅当$\exists Y, \exists Z, \varphi(I,Y,Z) = 1$。

5. A到B的归约算法θ，就是上一条的从I 机械化计算到$\varphi(I,Y,Z)$。$\varphi(I,Y,Z)$做为Y和Z的公式，是可满足的，当且仅当$\exists Y, \exists Z, \varphi(I,Y,Z) = 1$。

$\mathcal{F}$ is a set of relations in Boolean variables.

定理 (Schaefer, STOC 1978) Given a constraint set $\mathcal{F}$, the problem CSP($\mathcal{F}$) is in P, if $\mathcal{F}$ satisfies one of the conditions below, and CSP($\mathcal{F}$) is otherwise NP-complete.

- $\mathcal{F}$ is 0-valid (1-valid).
- $\mathcal{F}$ is weakly positive (weakly negative). (Horn SAT)
- $\mathcal{F}$ is affine. (A system of linear equations)
- $\mathcal{F}$ is bijunctive. (2SAT)

2.3 计数问题的难解性的判定标准

判定问题3SAT，对应一个计数问题#3SAT。

定义 (#3SAT问题) 输入是一个3CNF公式φ，φ是关于布尔变量集$X = \{x_1, x_2, \ldots, x_n\}$的，问存在多少个赋值$\pi : \{x_1, x_2, \ldots, x_n\} \to \{0, 1\}$，使得$\pi$满足$\varphi$。

练习题

1. 给出从3SAT到#3SAT的归约。
2. 说明#3SAT是NP难的。（提示：归约具有传递性。）

回忆：

定义 (约束可满足问题CSP($\mathcal{F}$)) 输入是一些形式来自$\mathcal{F}$的约束R_j，每个R_j是作用于布尔变量$x_1, x_2, \ldots, x_n$中的若干个

的，问是否存在一个变量的赋值$\pi:\{x_1,x_2,\ldots,x_n\}\to\{0,1\}$，使得$\pi$满足所有约束$R_j$，即问

$$\bigvee_{\pi:\{x_1,x_2,\ldots,x_n\}\to\{0,1\}}\prod_j R_j(\pi|_{\text{inputs of }R_j})$$

。

自然地存在一个计数问题框架#CSP：

定义 (**满足约束解数目问题（#CSP）**) 输入是一些形式来自$\mathcal{F}$ 的约束R_j，每个R_j是作用于布尔变量$x_1,x_2,\ldots,x_n$中的若干个的，问存在多少个赋值$\pi:\{x_1,x_2,\ldots,x_n\}\to\{0,1\}$，使得$\pi$满足所有约束$R_j$，即问

$$\sum_{\pi:\{x_1,x_2,\ldots,x_n\}\to\{0,1\}}\prod_j R_j(\pi|_{\text{inputs of }R_j})$$

。

练习题

1. 给定一个#CSP问题的一个输入I，I有变量集合$X=\{x_1,x_2,\ldots,x_n\}$和约束集合$R=\{r_1,\ldots,r_m\}$，把约束作用于变量的关联性描述成一个二部图$G(X,R,E)$。

2. 把上面练习题中的二部图$G(X,R,E)$，扩展定义出一个张量网络。此张量网络和原来#CSP问题的值有什么关系？

在CSP 框架下$\mathcal{F}$ 是约束可用的关系集合。在#CSP框架下，既然使用了$\prod_j R_j$，可以自然把$\mathcal{F}$推广到一般的函数集合。

当$\mathcal{F}$变动时，#CSP($\mathcal{F}$)就构成一个判定问题集合。如此一来，就可以研究$\mathcal{F}$ 如何决定#CSP($\mathcal{F}$) 的计算复杂性。

先仍然使用P（多项式时间可计算）和NP困难作为#CSP($\mathcal{F}$)的二分定理划分标准。把之前CSP($\mathcal{F}$)的二分定理，直接推广成关于#CSP($\mathcal{F}$)的二分定理会出现什么问题？

当$\mathcal{F}$是仿射的，CSP($\mathcal{F}$)有多项式时间算法，#CSP($\mathcal{F}$)也有多项式时间算法；$2SAT$有多项式时间算法，但我们不知

道$\#2SAT$的多项式时间算法。

3SAT已经是NP困难的，#3SAT貌似提供了更多的信息，是否应该得到一个比NP困难性“更难”的计算复杂性结论？

Valiant在1979年给出了计数问题的难解性标准#P困难性。（我们会继续感觉到计数复杂性方面的结论，与判定问题的理论方面的相平行。但结果方面，互不具备完全的容纳性。分三种情况来：1.判定和计数都有多项式时间算法（计数版的算法可以推出判定版的）；2. 判定是多项式时间的，计数是#P困难的（结论互不包含，不相及）；3. 判定和计数都是难解的（结论互不包含。计数版是证明“更强”的问题的“更难”的困难性）。况且还不论计数问题的值域不限于0,1。）

回忆：

NP是一个判定问题（关系）集合，$F(X)$ 在NP中，当且仅当存在多项式时间可计算的$|Y|$被$|X|$多项式限定的二元关系$R(X,Y)$ 使得：$F(X) = [\exists Y, R(X,Y) = 1]$。

定义 (#P) #P是一个判定问题（关系）集合，$F(X)$ 在#P中，当且仅当存在多项式时间可计算的$|Y|$被$|X|$多项式限定的二元关系$R(X,Y)$ 使得：$F(X) = |\{Y : R(X,Y) = 1\}|$。

定义 (#P**困难性**) 如果#P里的任何一个问题A都可以归约到某个问题B，则称B是#P困难的。

#P困难性给#3SAT提供了更精确更匹配的复杂性刻画。

定理 #3SAT 是#P困难的。

证明与“3SAT 是NP困难的”类似：建立计算表格与布尔线路的对应，然后转化成布尔公式。

$\mathcal{F}$ is a set of relations in Boolean variables.

定理 (Creignou, Hermann, I& C 1996) Given a constraint set $\mathcal{F}$, the problem #CSP($\mathcal{F}$) is in P, if $\mathcal{F}$ contains only affine relations, and CSP($\mathcal{F}$) is otherwise #P-complete.

虽然2SAT是多项式时间的，但是#2SAT是困难的，实际上是#P困难的。

类似的问题还有环数目问题。一个有向图有没有环是多项式时间的，但一个有向图有多少个环是NP困难的，也是#P困难的？我们把一个已知的NP困难问题，一个有向图有没有哈密尔顿环，归约到有多少个环。

- n表示输入图G的顶点数。

  构造图G'，原图G的每条边，被替换成一个$O(m)$大小但有2^m通过方式的构件。

- 如果G有长为n的环，一个G的长n的环对应G'的$(2^m)^n$个环，因此G'至少有$(2^m)^n$个环。

- 如果G没有长为n的环，G的一个环对应G'的至多$(2^m)^{n-1}$个环（比前一条的数字亏了一个2^m个因子）。

- G至多有$n^{2(n-1)}$个环，因此G'至多有$n^{2(n-1)} \cdot (2^m)^{n-1}$个环。

  （G至多有n^2条边，一个长$n-1$的环，要依次选择$n-1$次边。）

- 取一个合适的多项式大小的m，使得$2^m > n^{2(n-1)} = 2^{2(n-1)\log n}$，以便于区分两种情况。

- 完成了从是否存在哈密尔顿环问题到环数目的归约。

以后或许会在“多项式插值归约”一章看到，实际上，我们也可以把#P难问题，哈密尔顿环数目问题，归约到环数目问题上。

2.4 复数值域的满足约束解数目问题

布尔定义域的#CSP问题二分定理

- $\{0,1\}$值域
  只有一类问题有多项式时间算法，其他都是#P难的。
  一类：仿射关系。

- 非负实数值域
  两类：pure affine和product type

- 复数值域
  两类：$\mathcal{A}$ 和 $\mathcal{P}$(即product type的定义自然推广到复数值域)

2.4.1 #CSP($\mathcal{A}$)

定义 ($\mathcal{A}$) 一个函数$F:\{0,1\}^n \to \mathbb{C}$ 在集合$\mathcal{A}$中，当且仅当它可以写成如下形式：

$$\chi_{(AX=C)} \cdot i^{P(x_1,x_2,\ldots,x_n)}$$

其中，$X=(x_1,x_2,\ldots,x_n)$是F的输入，在第一个因子$\chi_{(AX=C)}$中，我们把X看成整数模2的加法和乘法构成的域运算意义下的向量，是$AX=C$ 的解空间（$\{0,1\}^n$ 的仿射子空间）的指示函数，而在第二个因子中，输入变量之间只是整数运算，没（木）有模2，$P(x_1,x_2,\ldots,x_n)$ 是一个二次整系数多项式，满足所有交错二次项的系数是偶数。

看待函数$\chi_{(AX=C)}$时，我们把自变量X看做取值于一个大小为2的有限域上的n维向量空间，$AX=C$方程组里所使用的线性运算都是 mod 2 意义下的运算。

$P(x_1,x_2,\ldots,x_n)$是一个整系数多项式，$x_j \in \{0,1\}$，使用整数加法乘法运算。

要求P的最高次数是2，二次项只有两种情况：x_ix_j和x_i^2。

因为$x_j \in \{0,1\}$，所以$x_j^2=x_j$，实际上第二种情况会退化成一次项。

第一种情况叫做交错二次项。

要求交错二次项的系数是偶数。

例如：$3x_1 + 2x_2 + 2x_1x_3 + 4x_2x_3$。

因为P作为i的指数出现，$i^P = i^{P \mod 4}$。

定理 $\#CSP(\mathcal{A})$有多项式时间算法。

证明 需展示如何在多项式时间内计算

$$\sum_{x_j \in \{0,1\}, j=1,\ldots,n} \chi_{(AX=C)} i^{P(x_1,x_2,\ldots,x_n)}$$

我们归纳地减少变量数目，从而从2^n项求和，降低到不多于2^{n-1}项求和。

1. $AX = C$自由变量少于n个，有非自由变量。

   设$AX = C$的自由变量是$x_1, \ldots, x_r$，方程组等价于$x_{r+1} = L_{r+1}(X')$,..., $x_n = L_n(X') (\mod 2)$，其中$X' = (x_1, \ldots, x_r, 1)$。

   把这些表达式带入要计算的求和式，得到：

   $$\sum_{x_j \in \{0,1\}, j=1,\ldots,r} i^{P(x_1,x_2,\ldots,x_r,L_{r+1}(X'),\ldots,L_n(X'))}$$

   接下来只需把指数整理成符合$\mathcal{A}$要求的形式。

   - 如果P里有一个单项式是一次项cx_j, $j > r$，那么应当被替换为$c(L_j(X') \mod 2)$，贡献的因子是$i^{c(L_j(X') \mod 2)}$。把$L_j(X')$看成整数上的线性运算表达式，假如直接使用，得到的因子是$i^{cL_j(X')} = i^{c(L_j(X') \mod 4)}$，当$L_j(X') \mod 4 = 0 or 1$时也是对的，但当当$L_j(X') \mod 4 = 2 or 3$时是错的。

     可以验证如果我们使用$L_j(X')^2$，就会得到$i^{cL_j(X')^2} = i^{c(L_j(X')^2 \mod 4)} = i^{c(L_j(X') \mod 2)}$。

     而且$L_j(X')^2$的交错项系数是偶数，满足要求。

   - 如果有交错项$2cx_jx_{j'}$，替换成$2cL_j(X')L_{j'}(X')$即可。

     原因是$i^{2cL_j(X')L_{j'}(X')} = (-1)^{cL_j(X')L_{j'}(X')} = (-1)^{c(L_j(X') \mod 2)(L_{j'}(X') \mod 2)} = (-1)^{cx_jx_{j'}} = i^{2cx_jx_{j'}}$。

2. $\chi \equiv 1$

$$\sum_{x_j \in \{0,1\}, j=1,\ldots,n} i^{P(x_1,x_2,\ldots,x_n)} = \sum_{x_2,\ldots,x_n} \sum_{x_1} i^{P(x_1,x_2,\ldots,x_n)}$$

- x_1的一次项系数是偶数。提取含$2x_1$的项的公因子。

$$\sum_{x_2,\ldots,x_n} \sum_{x_1} i^{2x_1 L(X')+P'(x_2,\ldots,x_n)} = \sum_{x_2,\ldots,x_n} (i^{P'(x_2,\ldots,x_n)} \sum_{x_1} (-1)^{x_1 L(X')})$$

  其中，$X' = (x_2, \ldots, x_n, 1)$。

$$\sum_{x_1} (-1)^{x_1 L(X')} = 1 + (-1)^{L(X')} = 2\chi_{(L(X')=0 \mod 2)}$$

- x_1的一次项系数是奇数。保留一个x_1，提取公因子。

$$\sum_{x_2,\ldots,x_n} (i^{P'(x_2,\ldots,x_n)} \sum_{x_1} (-1)^{x_1 L(X')} i^{x_1})$$

  记$\psi(X) = (-1)^{x_1 L(X')} i^{x_1}$。

  当$L(X') = 0 \mod 2$时，$\psi(1, x_2, \ldots, x_n) = i\psi(0, x_2, \ldots, x_n)$；

  当$L(X') = 1 \mod 2$时，$\psi(1, x_2, \ldots, x_n) = -i\psi(0, x_2, \ldots, x_n)$。

  由此两种情况，可以验证：

$$\sum_{x_1} (-1)^{x_1 L(X')} i^{x_1} = \sum_{x_1} \psi(X) = (1+i) i^{3L^2(X')}$$

  因此，

$$\sum_{x_2,\ldots,x_n} (i^{P'(x_2,\ldots,x_n)} \sum_{x_1} (-1)^{x_1 L(X')} i^{x_1}) = \sum_{x_2,\ldots,x_n} (i^{P'(x_2,\ldots,x_n)})(1+i) i^{3L^2(X')}$$

$\square$

记

$$F = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

#CSP($\{F\}$)问题的一个实例，是一些F应用到变量$x_1, \ldots, x_n$。

这个实例对应图G，$V_G = \{x_1, \ldots, x_n\}$，$(x_j, x_k) \in E_G$当且仅当实例中有约束$F(x_j, x_k)$。

考虑被赋值1的顶点形成的子图H。如果H有奇（偶）数条边，所有约束的乘积是-1（resp. 1）。

#CSP($\{F\}$)(G)=图G的偶数条边的这种子图数目$-$奇数条边的子图数目。

推论：图G的偶数条边的子图数目是多项式时间可以计算的。

2.4.2 #CSP与张量网络

回忆：

练习题

1. 给定一个#CSP问题的一个输入I，I有变量集合$X = \{x_1, x_2, \ldots, x_n\}$和约束集合$R = \{r_1, \ldots, r_m\}$，把约束作用于变量的关联性描述成一个二部图$G(X, R, E)$。

2. 把上面练习题中的二部图$G(X, R, E)$，扩展定义出一个张量网络。此张量网络和原来#CSP问题的值有什么关系？

定理 #CSP($\mathcal{F}$)等价于#$\mathcal{F}|\{=_1, =_2, \ldots, =_d, \ldots\}$ 等价于#$\mathcal{F} \cup \{=_1, =_2, \ldots, =_d, \ldots\}$。

练习题

1. 证明$\{=_1, =_2, \ldots, =_d, \ldots\} \subset \mathcal{A}$。

推论 #$\mathcal{A}$ 有多项式时间算法。

Clifford门是由以下三种门（通过一种比开放张量网络狭隘的方式）生成的门。

1.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

2.

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

3.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

练习题

1. 证明H、P、CNOT都在$\mathcal{A}$中。

推论　Clifford门构成的张量网络（以及量子线路）有多项式时间算法。

思考题

通过学习论文“Clifford Gates in the Holant Framework”了解Clifford门与集合$\mathcal{A}$的关系。

Jin-Yi Cai, Heng Guo, Tyson Williams: Clifford gates in the Holant framework. Theor. Comput. Sci. 745: 163-171 (2018)

2.4.3 #CSP($\mathcal{P}$)

先看一种简单情形：取一些一元函数F_i，定义$F(x_1, x_2, \ldots, x_n) = F_1(x_1)F_2(x_2)\cdots F_n(x_n)$。

#CSP($\{F\}$)的算法？

$$\sum_{x_1, x_2, \ldots, x_n \in \{0,1\}} F(x_1, x_2, \ldots, x_n) = \prod_{j=1}^{n} (F_j(0) + F_j(1))$$

定义 (**集合**$\mathcal{E}$)　一个n元函数F在集合$\mathcal{E}$，当且仅当它在除某互补串对α和$\bar{\alpha}$之外的输入上值都是0。

严格定义：$F \in \mathcal{E}$当且仅当存在$\alpha \in \{0,1\}^n$，

$\forall X, X \notin \{\alpha, \bar{\alpha}\} \Rightarrow F(X) = 0$。

$\{\alpha,\bar{\alpha}\}$是一个一维仿射子空间，即只有一个自由变量的。

任意取定$\mathcal{E}$中一个函数F，一个变量赋值若要得到非0函数值，它对的一个自变量的赋值，决定了它对其他自变量的赋值。即一个自由变量的值，决定其他非自由变量的值。

性质 #CSP($\mathcal{P}$)有多项式时间算法。

定义 (集合$\mathcal{P}$) 一个函数$\mathcal{P}$在中当且仅当能表示成$\mathcal{E}$中函数的乘积。

定理 #CSP($\mathcal{P}$)有多项式时间算法。

2.4.4 难解性证明p略

2.5 图同态数目问题

一个图$G(V_G,E_G)$到图$H(V_H,E_H)$的同态，是一个从V_G到V_H的映射ψ，满足对任意$e=(u,v)\in E_G$，$(\psi(u),\psi(v))\in E_H$。

定义 (到图H的同态数目问题) 输入图是G，问G到H的同态数目。

图H的边关系是一个二元关系$H: V\times V\to\{0,1\}$。

练习题

1. 证明到图H的同态数目问题，就是#CSP($\{H\}$)问题。

#CSP($\{H\}$)问题中，H可以从一个二元关系自然地推广到一个二元函数，推广后对应“到H的同态权重和问题”。

图同态数目问题也有二分定理。简单介绍一个易解类。

如果H的每个连通分支对应的矩阵的秩为1，那么#CSP($\{H\}$)问题有多项式时间算法。

因为H秩为1, 设$H=ab'$。

思考题

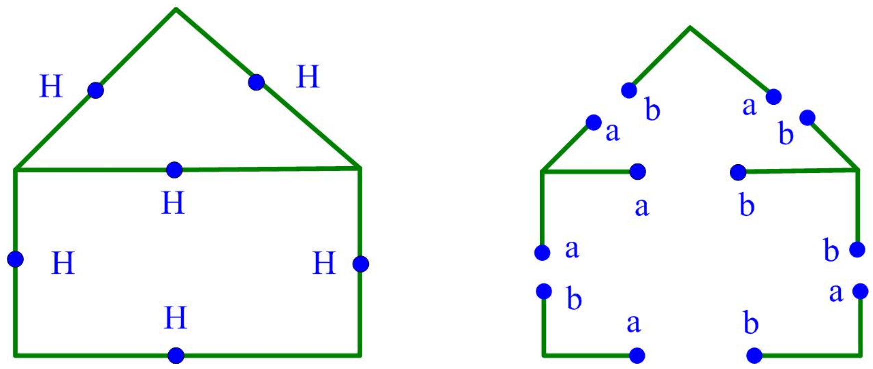


Figure 2.1: 作为输入的张量网络的两种等价形式

作为本章结尾的思考题：如何在一个#CSP问题中模拟两个一元函数$[1,0]$和$[0,1]$？

注：目前已知的证明方法，未在讲义中介绍过。来自文献：Martin E. Dyer, Leslie Ann Goldberg, Mark Jerrum: The Complexity of Weighted Boolean CSP. SIAM J. Comput. 38(5): 1970-1986 (2009)，见section 2.3 pinning。

Bibliography

[1] text