$\mathrm{MIP}^* = \mathrm{RE}$介绍

喻良

南京大学数学系

March 11, 2021

双缝干涉

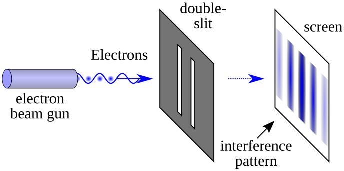

Figure: Test

from Wiki

Hilbert空间

Definition

Hilbert 空间是一个具有实或复的内积$\langle , \rangle$的向量空间，并且在距离函数$\|x-y\| = \sqrt{\langle x-y, x-y\rangle}$下是完备的。

- n–维Euclid空间$\mathbb{R}^n$下内积定义为$\langle (x_1, \cdots, x_n), (y_1, \cdots y_n)\rangle = \sum_{i\leq n} x_i y_i$，它是一个Hilbert空间。
- 复空间$\mathbb{C}^n$内积定义为$\langle (x_1, \cdots, x_n), (y_1, \cdots y_n)\rangle = \sum_{i\leq n} x_i \bar{y}_i$，它是一个Hilbert空间。

量子力学

量子力学对于双缝干涉的解释。

量子态: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 并且$|\alpha|^2 + |\beta|^2 = 1$.

例如: $|\psi\rangle = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$.

每一个量子态可以看成Hilbert空间的一个向量。

ψ的概率幅(probability amplitude)就是$|\psi|^2$。

Einstein-Podolsky-Rosen 佯谬

- 局域实在性与相对论;
- 物理理论的完备性，隐变量。

Bell不等式

令 λ为隐变量，$A(\mathbf{a},\lambda), B(\mathbf{b},\lambda): S^2\times\Lambda\to\{-1,1\}$，以及

$$C_h(\mathbf{a},\mathbf{b}) = \int_\Lambda A(\mathbf{a},\lambda)B(\mathbf{b},\lambda)p(\lambda)d\lambda.$$

那么“应该”有：

$$|C_h(\mathbf{a},\mathbf{b}) - C_h(\mathbf{a},\mathbf{c})| \le 1 + C_h(\mathbf{b},\mathbf{c})$$

Bell不等式的实验要求很苛刻，一般要求$A(\mathbf{a},\lambda) = -B(\mathbf{a},\lambda)$。

CHSH不等式

Alice测量$\mathbf{a}, \mathbf{a}'$， Bob测量$\mathbf{b}, \mathbf{b}'$.

$$|C_h(\mathbf{a}, \mathbf{b}) - C_h(\mathbf{a}, \mathbf{b}') + C_h(\mathbf{a}', \mathbf{b}') + C_h(\mathbf{a}', \mathbf{b})| \leq 2.$$

Bell实验

如果假定探测器与量子发射是随机的，那么迄今所有的实验得到的结果都与CHSH不等式相反。

量子力学下CHSH不等式右边可以达到$2\sqrt{2}$.

量子纠缠。

并不是任何两个量子的状态可以写成各自状态的乘积(张量积)：

$$\frac{\sqrt{2}}{2}|00\rangle + \frac{\sqrt{2}}{2}|11\rangle.$$

交互式证明(interactive proofs)

随机化交互式证明包含prover（无时间限制的图灵机）和verifier（多项式限制）。即对于一个集合L，verifier存在一个算法$V(z, n)$使得

- 如果$z \in L$，那么存在一个证明π使得$V(z, \pi)$输出1的概率很大.
- 如果$z \notin L$，那么对于所有的证明π，$V(z, \pi)$输出1的概率很小。

例如图非同构问题的就属于IP.

Theorem (Shamir)

$\mathrm{IP} = \mathrm{PSPACE}$.

多交互式证明(Multiprover interactive proofs)

多交互式证明包含多个prover 和一个verifier。Provers之间允许有协议但是在计算过程正不允许有通讯。 对于一个集合L，verifier存在一个算法$V(z,n)$使得

- 如果$z \in L$，那么存在一个证明π使得$V(z,\pi)$输出1的概率很大.
- 如果$z \notin L$，那么对于所有的证明π， $V(z,\pi)$输出1的概率很小。

Theorem (Babai, Fortnow, and Lund)

$\mathrm{MIP} = \mathrm{NEXT}$.

我们用$\mathrm{MIP}(n,i)$表示n个provers以及i个回合。

Theorem (Feige and Lovasz)

$\mathrm{MIP} = \mathrm{MIP}(2,1)$

非局域博弈(1)

给定$(x, y) \in n \times n$，$(a, b) \in k \times k$，概率分布$\mu : n \times n \to [0, 1]$，估值函数$D(x, y, a, b) \in \{0, 1\}$，一个集合$\Lambda$及其概率测度$\nu$，以及对应每一个$\lambda \in \Lambda$的函数$A^\lambda, B^\lambda : n \to k$，定义

$$p_{abxy} = \nu(\{\lambda \mid A^\lambda(x) = a \wedge B^\lambda(y) = b\});$$

以及

$$val(g) = \sup_p \sum_{(x,y)\in n\times n} \mu(x, y) \sum_{(a,b)\in k\times k} D(a, b, x, y) p_{abxy}.$$

，这里g编码p以及D. 注意p是$[0, 1]^{n^2 k^2}$的一个凸子集。

非局域博弈（2）

把p看成一个证明π。

$\mathrm{MIP}(2,1)$可以看成一个非局域的博弈。如果有一个证明π大概率接收z，那么$val(z)$值比较大(例如$\geq \frac{2}{3}$)；否则每一个证明π都是小概率接收z，那么$val(z)$很小（例如$\leq \frac{1}{3}$）。

MIP*

在MIP中，如果我们允许Provers之间存在“纠缠”，就得到了MIP*。相应地：

$$val^*(g) = \sup_p \sum_{(x,y)\in n\times n} \mu(x,y) \sum_{(a,b)\in k\times k} D(a,b,x,y) p_{abxy}.$$

其中p为纠缠态的概率分布。从而p在MIP*的取值范围比MIP要大因而$val^*(g) \geq val(g)$.

CHSH不等式重访

考虑$n = k = 2$，μ为一致概率，$D(a, b, x, y) = 1 \leftrightarrow a \oplus b = x \wedge y$。

那么 $val^*(g) = \frac{2+\sqrt{2}}{4} > \frac{3}{4} = val(g)$。

$\mathrm{MIP}^* = \mathrm{RE}$

Theorem (Ji, Natarajan, Vidick, Wright and Yuen)

存在一个多项式可计算的函数f使得对于任意的e

- $f(e)$编码一个MIP^*;
- $e \in \mathcal{H}$当且仅当$val^*(f(e)) = 1$, $e \notin \mathcal{H}$当且仅当 $val^*(f(e)) \leq \frac{1}{2}$.

von Neumann 代数

固定一个复Hilbert空间H，令$\mathcal{B}(H)$为H上囿界线性算子的集合。在$\mathcal{B}(H)$上有算子$*$。它是一个C^*-代数(Banach代数+$*$算子).

von Neumann 代数 A是$\mathcal{B}(H)$的子代数使得A是弱拓扑下的闭集。

有限维von Neumann 代数同构于有限维的复方阵。

$p \in A$称为一个投射(projection)，如果$p^2 = p = p^*$.

Factors

Definition

一个von Neumann 代数 A是factor，如果A的中心N(是A的子代数)只包含单位元与复数的乘积。即$N = \{c \cdot 1 \mid c \in \mathbb{C}\}$.

Trace

Definition

对于von Neumann 代数A，A上一个trace是一个线性函子$tr : A \to \mathbb{C}$使得

- $tr(1) = 1$;
- $tr(a^* a) \geq 0$;
- $tr(ab) = tr(ba)$;
- $tr(x) = 0 \leftrightarrow x = 0$;
- 对于任意一簇正交投射$\{p_i\}_{i \in I}$，$tr(\vee_{i \in I} p_i) = \sum_{i \in I} tr(p_i)$.

Π_1-factor

Definition

Π_1-factor是一个无穷维并且具有trace的factor.

超穷Π_1-factor

对于$\{M_{2^n}(\mathbb{C})\}_{n\in\omega}$定义嵌入$X \mapsto \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}$。令$\mathcal{R}$为这些嵌入诱导的inductive limit.

Theorem

$\mathcal{R}$可嵌入任何 Π_1-factor.

Definition

固定一个ω上非主超滤$\mathcal{U}$，定义$\mathcal{R}^\omega = \bigoplus_{n\in\omega}\mathcal{R}/c_\omega(\mathcal{R})$，其中

- $\bigoplus_{n\in\omega}\mathcal{R} = \{f \mid f:\omega\to\mathcal{R} \wedge \sup_n ||f(n)|| < \infty\}$;
- $c_\omega(\mathcal{R}) = \{f \mid f:\omega\to\mathcal{R} \wedge \lim_\omega \sqrt{tr(f(n)^* f(n))} = 0\}$

定义中$\lim_\omega \sqrt{tr(f(n)^* f(n))} = 0$是指对于所有的$\epsilon > 0$，存在一个$A \in \mathcal{U}$使得$\forall n \in A(\sqrt{tr(f(n)^* f(n))} < \epsilon)$.

Connes embedding problem

Question (Connes)

是否每一个可分的II_1-factor都可嵌入 $\mathcal{R}^\omega$.

注意CEP独立于超滤的选择。

Theorem (Ji, Natarajan, Vidick, Wright and Yuen)

No.

$*$-代数语言

固定一个von Newmann 代数A，一个$p(\vec{x})$是一个$*$算子形成的多项式。令$\mathcal{F}$为一个多项式集合使得$p \in \mathcal{F}$，则对于任何von Newmann 代数A，$p(A_1^n) \subseteq A_1$（A_1是A的单位球。）

$\mathcal{L} = \mathcal{F} \cup \{d, tr_r, tr_i\}$。其中$d = \sqrt{tr((x-y)^*(x-y))}$，$tr_r$为实部，$tr_i$为虚部。

$\forall$解释为sup，$\exists$解释为inf，$\neg\varphi$解释为$1 \dot{-} \varphi = \max\{1-\varphi, 0\}$，以及$\varphi \to \psi$解释为$\psi \dot{-} \varphi$.

连续逻辑的公式

原子公式：与经典逻辑一致。
无量词公式：形式为$f(\overrightarrow{\varphi})$，其中$f$为是一个$\mathbb{R}^m$到$\mathbb{R}$的连续函数。
一般的公式形式为$\overrightarrow{Q(x)}\varphi(\overrightarrow{x})$，其中$Q(x)$或者是$\forall x$或者是$\exists x$.

推演规则是：$\varphi \leq \psi + \varphi \dot{-} \psi$.

一些结论

Theorem (Farah, Hart, Lupini, Pederson, Sheman, Yaacov, ...)

- 哥德尔完全性定理成立;
- Los定理;
- Π_1-factor可递归公理化;
- “可证明”是一个递归可枚举集合。

连续逻辑的模型论

对于任意一个公式$\varphi(\overrightarrow{x})$， von Newmann 代数$A$以及$A$中$\overrightarrow{a}$，$\varphi(\overrightarrow{a})$是一个实数。

$A \models \varphi(\overrightarrow{a})$定义为$\varphi(\overrightarrow{a}) = 0$.

$\forall$-理论和Σ-理论

Definition

- $\mathrm{Th}_\forall(A) = \{\varphi \mid A \models \varphi \wedge \varphi$是$\Pi_1$句子$\}$;
- $\mathrm{Th}_\Sigma(A) = \{\varphi \mid A \models \varphi \wedge \varphi$是$\Sigma_1$句子$\}$。

$\mathrm{Th}_\forall(A)$可以看成从句子到实数的函数。因此如果A是B的子代数，则$\mathrm{Th}_\forall(A) \leq \mathrm{Th}_\forall(B)$。
因此如果A是Π_1-factor，那么$\mathrm{Th}_\forall(\mathcal{R}^\omega) = \mathrm{Th}_\forall(\mathcal{R}) \leq \mathrm{Th}_\forall(A)$.

Lemma

如果A是可分的tracial von Nuewmann代数，并且$\mathrm{Th}_\forall(A) \leq \mathrm{Th}_\forall(\mathcal{R})$，那么$A$是可嵌入$\mathcal{R}^\omega$的。

因此CEP成立当且仅当对于每一个Π_1-factor，$\mathrm{Th}_\forall(A) = \mathrm{Th}_\forall(\mathcal{R})$

可计算分析

Definition

- 一个实数r是可计算的，如果存在一个算法可以用有理数任意逼近r。
- 一个函数$f:\mathbb{R}\to\mathbb{R}$是可计算的，如果存在一个算法使得对于任意的实数$r$，可以用有理数任意逼近$f(r)$。

CEP v. s. 可计算性（1）

令T为Π_1-factor的公理化。有完备性以及以上的讨论，我们知道对于Π_1或者Σ_1语句φ， $T \vdash \varphi$当且仅当$\mathcal{R} \models \varphi$.

Theorem (Goldbring and Hart)

CEP 当且仅当对每一个Π_1 tracial von Newmann 代数，$\mathrm{Th}_\forall(A)$是递归的。

Proof.

如果CEP，那么由上讨论，对于任意Π_1句子φ，为了判定$A \models \varphi$，我们只需要判定$T \vdash \varphi$或者它的"否定". 因此这是一个可计算的过程。 $\square$

CEP v. s. 可计算性（2）

Proof.

如果CEP不成立，则存在A不可嵌入$\mathcal{R}$。因此存在$\epsilon > 0$，$a \in A$，$N \in \mathbb{N}$使得在$\mathcal{R}$中，

$$\exists x(\max_{\mathrm{d}(p) \le N} \max\{|tr_r(p(x)) - tr_r(p(z))|, |tr_i(p(x)) - tr_i(p(z))|\} > \epsilon).$$

令公式$\sigma_{N,A,a,\epsilon}$为以上表达式去掉$> \epsilon$. 对于$t \in [0,1]$，
令$A_t = t\mathcal{R} \oplus (1-t)A$。则$tr^t = t \cdot tr^{\mathcal{R}} + (1-t) \cdot tr^A$.
则$\sigma^{A_0}_{N,A,a,\epsilon} = 0$并且$\sigma^{A_1}_{N,A,a,\epsilon} > 0$.
因此$\{\mathrm{Th}(A_t) \mid t \in [0,1]\}$不可数因而存在不可计算的。 □

CEP v. s. 可计算性（3）

Theorem (Goldbring and Hart)

如果$\mathrm{Th}_\forall(\mathcal{R})$是递归的，那么$\{(e, val^*(e))\}_e$是递归的。

Proof.

首先注意存在一个递归枚举的Π_1公式集合$\{\psi_e(x)\}_e$ 使得$val^*(e) = (\forall x \psi_e(x))^{\mathcal{R}}$. 因为$(\psi_e(x))^{\mathcal{R}}$是Lipshitz函数并且常量为1，因此可以被距离函数$d(x, X)$逼近。但是距离函数可以被一个可计算的Π_1公式序列$\varphi_n(x)$逼近，因此$val^*(e) = (\forall x \psi_e(x))^{\mathcal{R}}$的计算转化为计算$\Pi_1$公式在$\mathcal{R}$中的值。因为$\mathrm{Th}_\forall(\mathcal{R})$是递归的，那么$\{(e, val^*(e))\}_e$必然是递归的。 □

阅读材料

1. The Feynman Lectures on Physics, Volume III
2. $\mathrm{MIP}^* = \mathrm{RE}$, Zhengfeng Ji and Anand Natarajan and Thomas Vidick and John Wright and Henry Yuen, 2020.
3. Quantum Computation and Quantum Information, Michael A. Nielsen and Isaac L. Chuang.
4. Computability and the Connes Embedding Problem, Isaac Goldbring and Bradd Hart.
5. The universal theory of the hyperfinite II_1 factor is not computable, Isaac Goldbring and Bradd Hart.