物理学报 Acta Physica Sinica

Chinese Physical Society

Institute of Physics, CAS

熵不确定度关系综述

李丽娟 明飞 宋学科 叶柳 王栋

Review on entropic uncertainty relations

Li Li-Juan Ming Fei Song Xue-Ke Ye Liu Wang Dong

引用信息 Citation: Acta Physica Sinica, 71, 070302 (2022) DOI: 10.7498/aps.71.20212197

在线阅读 View online: https://doi.org/10.7498/aps.71.20212197

当期内容 View table of contents: http://wulixb.iphy.ac.cn

专题: 量子计算新进展: 硬件、算法和软件

熵不确定度关系综述*

李丽娟[1)] 明飞[1)] 宋学科[1)] 叶柳[1)] 王栋[1)†]

1) (安徽大学物理与光电工程学院, 合肥 230601)

(2021 年 11 月 29 日收到; 2021 年 12 月 26 日收到修改稿)

不确定关系是量子力学的基本特征之一, 随着量子信息理论的蓬勃发展, 不确定关系更是在其中发挥着重要的作用. 特别是将熵引入来描述不确定关系之后, 不确定关系在量子信息技术中涌现出多种应用. 众所周知, 熵不确定度关系已成为几乎所有量子密码协议安全分析的核心要素. 这篇综述主要回顾不确定关系的发展历史和最新研究进展, 从 Heisenberg 提出不相容测量其结果是不能被预测伊始, 许多学者在该观点的启发下, 做了进一步的相关扩展研究, 将可观测物体与环境之间的量子关联结合起来, 对不确定关系进行各种推广从而得到更普适的数学表达式. 除此以外, 本文还重点介绍了量子存储下的熵不确定度关系及其发展, 也介绍了在某些物理系统中对应的动力学特性. 最后讨论了熵不确定度关系在量子信息领域的各种应用, 从随机数到波粒二象性再到量子密钥分发.

关键词: 熵不确定度关系, 量子存储, 量子关联

PACS: 03.65.–w, 03.67.–a, 03.67.Hk **DOI:** 10.7498/aps.71.20212197

1 引 言

量子力学颠覆了我们一直以来用经典力学的方式来研究世界运行规律的传统观念, 许多无法用经典力学理论来解释的微观现象, 量子力学都可以解释. 在量子力学领域, 不确定关系是一个极为重要的概念, 也被称作测不准关系, 它实质上反映的是微观粒子运动的基本规律, 这也是量子力学区别于经典力学的判据之一. 1927 年, Heisenberg[1] 通过对假想实验的分析首次提出不确定关系 (示意图参照图 1), 该不确定关系展示了人们无法同时准确预测一对非对易观测量的测量结果, 也就是说, 对粒子动量预测的结果准确性越高, 那么对其位置预测的准确性就越低, 反之亦然. 随后, 这个关系式由 Kennard[2] 给出了严格证明. 随着深入研究, 人们发现, 不确定关系不仅适用于位置和动量这对非对易物理量, 对于其他成对的非对易可观测量同样适用, 比如谐振子的相位与激发数、粒子的角度与轨道角动量等. 据此, 关于任意两个可观测量, Robertson[3] 提出了更为普适的不确定度不等式. 值得注意的是, 这个公式虽然普适, 但也不是量化

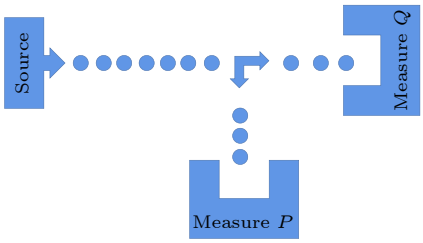

图 1 每个从粒子源发出的粒子都是用 P 或 Q 来测量的, 测量的选择是随机的. 不确定关系指出我们不能预测 P 和 Q 的测量结果

Fig. 1. Each particle emitted from the particle source is measured by P or Q, and the choice of measurement is random. The uncertainty relation indicates that we cannot predict the outcomes of both P and Q.

* 国家自然科学基金 (批准号: 12075001, 61601002, 12004006, 12175001)、安徽省自然科学基金 (批准号: 1508085QF139) 和中国科学院量子信息重点实验室开放基金 (批准号: No. KQI201701) 资助的课题.

† 通信作者. E-mail: dwang@ahu.edu.cn

不确定性的最佳不等式, 它亦有不足之处, 这点本文将在第 2 节中给出具体分析.

随着量子信息理论的不断发展, Deutsch[4] 指出标准差用来量化不确定度有它自身的局限性, 同时学者们发现标准差并不是量化不确定度的唯一方式, 所以也逐渐衍生出许多其他方式来量化不确定度. 其中, Everett[5] 和 Hirschman[6] 首次提出关于位置和动量的熵不确定度关系, 这也是第一个熵不确定度关系. 随后, 这个不确定关系被推广到任意两个非对易的可观测量. 由于 Robertson 提出的不等式下界是依赖于系统的态, 为了克服这一弊端, Deutsch[4] 利用信息熵构造了一个全新的熵不确定度不等式. 之后在 Kraus[7] 推测的启发下, Maassen 和 Uffink[8] 延续 Deutsch 的结论进而提出了一个著名的熵不确定度关系式. 除上述方式之外, 本文第 2 节将回顾多种形式的不确定关系.

通常情况下, 人们可用猜测游戏来演示不确定关系的物理意义. 在猜测游戏中 (如图 2 所示), 假设有两位观察者 Alice 和 Bob, 现在 Bob 准备了一个任意的态 ρ_A 并且将它发送给了 Alice, Alice在收到这个态之后, 随机在两个 (或多个) 测量选择中选定某一个作用在态 ρ_A 上, 并记录下测量结果, 随后 Alice 告诉 Bob 她的测量选择, Bob 的任务就是猜出 Alice 的测量结果. 不确定性原理告诉我们, 如果 Alice 做了两个不相容的测量, 那么 Bob 就无法准确地猜测出两次测量的结果, 这也正好对应了制备不确定性的概念. 而熵不确定度关系, 比如 Maassen-Uffink 关系式可以被认为是最佳猜测概率的基本约束. 这个猜测游戏引发学者继续思考: 在刚提及的游戏中, Bob 只能通过经典信息来获得关于被测粒子制备的相关信息, 若让 Bob 除经典信息外还能获取相关量子信息, 那么能否提高 Bob 对 Alice 的测量结果的猜测概率呢? 具体来说也就是如果 Bob 准备的是一个双粒子系统, 且这两个粒子之间是相互关联的, 随后 Bob 只发送了其中一个粒子给 Alice, 留下另一个粒子作为量子存储, 那么在这种情况下, Bob 就可以通过两粒子之间的关联获取量子信息, 考虑到这些, Berta 等[9] 以及 Renes 和 Boileau[10] 顺着这个思路完成了相关研究, 并提出了一种新的熵不确定度关系, 被称为量子存储下的熵不确定度关系, 随后也有许多工作在该主题下展开, 比如三体系统的熵不确定度关系, 还有各种模型下熵不确定度动力学等, 这些工作进展都将在本文的第 3 节中一一展示.

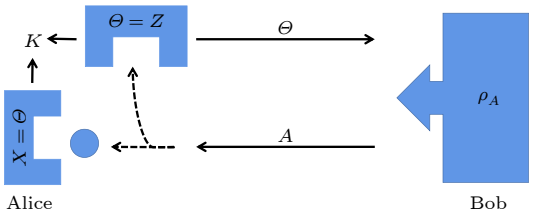

图 2 玩家 Alice 和 Bob 的猜测游戏. 首先, Bob 准备 ρ_A 并把 A 发送给 Alice. 然后, Alice 以相等的概率进行 $\mathbb{Q}$ 或 $\mathbb{R}$ 测量, 并将测量选项存储在 Θ 中. 第三, Alice 得出测量结果并将其存储在 K, 且向 Bob 透露测量选择 Θ. Bob 的任务是猜测 K (给定 Θ)

Fig. 2. A guessing game between players Alice and Bob. First, Bob prepares ρ_A and sends A to Alice. Then, Alice performs measurement $\mathbb{Q}$ or $\mathbb{R}$ with equal probability on A, and stores the measurement options in Θ. Third, Alice stores the measurement result in the K bit and tells Bob about her option Θ. Bob's task is to guess K (given Θ).

除了在理论上对不确定关系进行不断地探索之外, 量子信息理论的蓬勃发展也为不确定度关系打开了应用的大门. 目前, 不确定度关系广泛应用于包括纠缠目击、量子隐形传态、量子密码学、量子密钥分发、随机数等量子信息研究领域, 相关应用将会在第 4 节进行详细的讨论.

2 不同种类的不确定关系

不确定关系最开始是基于动量和位置提出的, 随着量子信息理论的兴起和发展, 众多学者在研究不确定关系的过程中引入标准差、熵等概念, 逐渐形成了不同种类的不确定关系分支, 本节主要考虑单个系统 A 的不确定关系, 介绍几种不同形式的不确定关系.

2.1 基于标准差的不确定关系

首先, Heisenberg[1] 提出了著名的不确定性关系, 并由 Kennard 进行了严格的证明, 它可以表示为

$$\Delta p \cdot \Delta x \geqslant \frac{\hbar}{2}, \tag{1}$$

这里的 Δx 和 Δp 分别代表位置和动量的标准差 $\Delta\tau = \sqrt{\langle\tau^2\rangle - \langle\tau\rangle^2}$ $(\tau = x, p)$, $\hbar$ 是普朗克常数. 该不确定关系指出人们无法同时确定地获得某个粒子的位置和动量的精确测量结果. 在此基础上, 对于任意两个非对易的可观测量 Q 和 R, Robertson[3] 推广得到了一个新的不等式:

$$\Delta Q \cdot \Delta R \geqslant \frac{1}{2}|\langle[Q, R]\rangle|, \tag{2}$$

这里的$[Q,R]=QR-RQ$, $\langle\tau\rangle=\langle\psi|\tau|\psi\rangle$是可观测量$\tau$在量子态$|\psi\rangle$下的期望值. 正如引言所说, (2) 式并不是完美的, 它的缺点是当系统准备的态是选取的两个可观测量的本征态时, 通过计算可知, Robertson 不等式所展现出的下界 (不等式的右侧) 就会变为零, 此时结果显得过于平庸. 也就是说这个不等式的下界依赖于系统的态. 接着 Schrödinger[11] 通过附加一个反对易子项强化 (2) 式得出:

$$\Delta Q^2\cdot\Delta R^2\geqslant\left|\frac{1}{2}\langle[Q,R]\rangle\right|^2+\left|\frac{1}{2}\langle\{Q,R\}\rangle-\langle Q\rangle\langle R\rangle\right|^2. \tag{3}$$

然而, (2) 式和 (3) 式的下界是与状态相关的. 如果系统由Q或R中的某一个本征态制备, 很容易算出来$|\langle[Q,R]\rangle|=0$, $\left|\frac{1}{2}\langle\{Q,R\}\rangle-\langle Q\rangle\langle R\rangle\right|=0$, 即 (2) 式和 (3) 式的下界为零, 这意味着在这种情况下, 用标准差来测量不确定性将变得没有意义. 随后 Maccone 和 Pati[12] 为了消除了这个缺点提出了一个新的不确定关系:

$$\Delta Q^2+\Delta R^2\geqslant\max\{\mathcal{B}_1,\mathcal{B}_2\}, \tag{4}$$

这里的$\mathcal{B}_1=\pm\mathrm{i}|\langle[Q,R]\rangle|+|\langle\psi|Q\pm\mathrm{i}R|\psi^\perp\rangle|^2$, $\mathcal{B}_2=\frac{1}{2}|\langle\psi^\perp_{Q+R}|Q+R|\psi\rangle|^2$, 态$|\psi^\perp\rangle$正交于$|\psi\rangle$. (4) 式表示的不确定关系已经在实验[13−15]上得到了验证.

2.2 基于熵的不确定关系

从技术上讲, 除了上面提到的偏差以外还有另一种有效而直接的方法来描述不确定性关系, 即熵. Everett[5] 和 Hirschman[6] 首次引入熵来描述测不准原理. 随后, Białynicki-Birula 和 Mycielski[16] 严格证明了关于位置与动量的微分熵不确定度关系:

$$h(Q)+h(R)\geqslant\log_2(e\pi), \tag{5}$$

其中h表示的是微分熵, 考虑一个由概率密度$\Gamma(q)$控制的随机变量Q, 微分熵可以表示为

$$h(Q)=-\int_{-\infty}^{\infty}\Gamma(q)\log_2\Gamma(q)\mathrm{d}q. \tag{6}$$

假设这个量属于高斯概率分布, 则满足

$$\Gamma(q)=\frac{1}{\sqrt{2\pi\Delta(Q)^2}}\exp\left[\frac{-(q-\bar{q})}{2\Delta(Q)^2}\right], \tag{7}$$

这里的$\bar{q}$表示q的平均值. 高斯概率分布在这个情况下是特别的: 对一个固定的标准差$\Delta(Q)$, (7) 式的分布形式会使得 (6) 式中的熵最大化, 这一点利用拉格朗日乘数的变分演算就可以展现出来.

将 (7) 式代入 (6) 式来计算高斯分布的熵更直观, 代入得到:

$$h(Q)=\log_2\sqrt{2\pi e\Delta(Q)}, \tag{8}$$

又由于高斯概率分布使熵最大化, 所以对于一个一般分布的随机变量, 下面的不等式始终成立:

$$h(Q)\leqslant\log_2\sqrt{2\pi e\Delta(Q)}. \tag{9}$$

现在考虑粒子平移自由度的任意量子态, 它分别产生位置和动量的随机变量Q和P, 然后将得到的结果不等式代入到 (5) 式得出

$$\begin{aligned}&\log_2(2\pi e\Delta(Q)\Delta(R))\\ =\ &\log_2\sqrt{2\pi e\Delta(Q)^2}\log_2\sqrt{2\pi e\Delta(R)^2} &(10)\\ \geqslant\ &h(Q)+h(R) &(11)\\ \geqslant\ &\log_2(e\pi). &(12)\end{aligned}$$

最后, 结合 (10) 式和 (11) 式很容易推断出之前关于位置与动量的结果$\Delta x\cdot\Delta p\geqslant\hbar/2$.

众所周知, 香农熵[17] 在信息论中起着基础而又关键的作用, 在经典物理学领域量化了给定系统状态下的信息量. 通过引入香农熵, Deutsch[4] 提出了一个不确定关系, 写成

$$H(Q)+H(R)\geqslant2\log\left(\frac{2}{1+\sqrt{c(Q,R)}}\right), \tag{13}$$

其中, $H(Q)=-\sum_i p_q\log_2 p_q$就是香农熵的计算公式, $p_q=\mathrm{Tr}(|Q_q\rangle\langle Q_q|\rho)$是关于$Q$的测量结果$q$的概率; c是指Q和R的最大重叠量, $c=\max_{ij}\{c_{ij}\}=|\langle\psi_i^Q|\psi_j^R\rangle|^2$, $|\psi_i^Q\rangle$指代可观测量Q的本征矢, $|\psi_i^R\rangle$也是一样.

随后, 基于 Deutsch 的开创性工作, Maassen 和 Uffink[8] 遵循 Kraus 的猜想对 (13) 式进行了优化, 对任意的态ρ_A,

$$H(Q)+H(R)\geqslant\log_2\frac{1}{c(Q,R)}=:q_{MU}. \tag{14}$$

注意 (13) 式和 (14) 式中的下界都是和初态无关的, 这一点和 Robertson 提出的下界形成了对比. Korzekwa 及其团队[18] 表示, 通过考虑总的不确定性, 单比特系统的 Maassen-Uffink 不等式可以改进为

$$\begin{aligned}&H(Q)+H(R)\\ \geqslant\ &\log_2\frac{1}{c(Q,R)}+H(\rho)[2+\log_2 c(Q,R)]. &(15)\end{aligned}$$

此外, 从香农熵出发, Rényi[19] 提出一个相对更普遍的熵版本, 可以为具有高或低信息量的事件提供更大的权重. 由于其固有的数学性质, 这些不同类型的熵可以很好地应用于量子密码学和信息论. 一般来说, x 阶的 Rényi 熵定义为

$$H_x(Q)=\frac{1}{1-x}\log_2\sum_q p_q^x, \tag{16}$$

x 的范围是 $[0,\infty]$. 当 $x=1$ 时, Rényi 熵就会恢复到 Shannon 熵, Shannon 熵可以说是 Rényi 熵的一种特殊形式. Maassen 和 Uffink[8] 还指出, 从 Rényi 熵的角度出发 (14) 式会变得更普适, 对任意的 $x,y\geqslant\frac{1}{2}$ 且 $\frac{1}{x}+\frac{1}{y}=2$, 有以下关系:

$$H_x(Q)+H_y(R)\geqslant q_{MU}. \tag{17}$$

当 $x=y=1$ 时, (17) 式和 (14) 式一致, 当 $x\to\infty$, $y\to\frac{1}{2}$ 时, 可以得到另一个关于 (17) 式用最小熵和最大熵来描述的特殊例子:

$$H_{\min}(Q)+H_{\max}(R)\geqslant q_{MU}. \tag{18}$$

由于最小熵表征了正确猜测结果 Q 的概率, 因此这种类型不确定关系在量子密码学和量子信息论中应用最为广泛.

除上面说的三种熵不确定度关系外, 也有学者推导出了时间-能量熵不确定度关系[20], 比如 Rastegin[21] 通过 Pegg[22] 的方法推导出了能量-时间的熵不确定度关系.

2.3 Majorization 不确定关系

另外一种获得与熵直接相关的不确定关系的方法就是 Majorization 方法, 代替之前的概率之和, 该方法采用的是概率的乘积. 这个想法是由 Partovi[23] 首次提出, 然后由 Friedland 小组[24] 和 Puchała 小组[25] 进一步推广和发展. 现有两个半正定算子值 (positive operator-valued measures, POVM) $\mathbb{X}=\{\mathbb{X}^x\}_x$ 和 $\mathbb{Z}=\{\mathbb{Z}^z\}_z$, 用这两个测量对系统 ρ_A 进行测量, 根据玻恩定则可以得到概率分布分别为 $P_X(x)=\mathrm{Tr}(\rho_A\mathbb{X}^x)$ 和 $P_Z(z)=\mathrm{Tr}(\rho_A\mathbb{Z}^z)$. 可以用 $\boldsymbol{P}_X^{\downarrow}$ 和 $\boldsymbol{P}_Z^{\downarrow}$ 来表示相应的重新排序的向量, 方便概率按从大到小的顺序排列.

现在需要找到一个向量使得 $\boldsymbol{P}_X^{\downarrow}$ 和 $\boldsymbol{P}_Z^{\downarrow}$ 张量积最大, 也就是说需要找到一个概率分布 $\boldsymbol{\mu}=\{\mu(1),\mu(2),\cdots,\mu(|X||Z|)\}$ 使得

$$\boldsymbol{P}_X^{\downarrow}\times\boldsymbol{P}_Z^{\downarrow}\prec\boldsymbol{\mu} \tag{19}$$

对 $\forall\rho\in\mathcal{S}(\mathcal{H})$ 即希尔伯特空间都成立. 这样的关系式给乘积分布如何展开设置了一个界, 一个满足 (19) 式的概率分布 $\boldsymbol{\mu}$ 可以这样来构造, 考虑到 (19) 式中乘积分布的最大概率:

$$p_1=\boldsymbol{P}_X^{\downarrow}\cdot\boldsymbol{P}_Z^{\downarrow}=\boldsymbol{p}_{\text{guess}}(X)\cdot\boldsymbol{p}_{\text{guess}}(Z). \tag{20}$$

我们知道如果两个测量是不相容的, 那么 p_1 总是会远离 1, 因为不可能两个测量都有一个确定的结果. 举例说明, 回想一下 Deutsch 的结果, 可以得到

$$\boldsymbol{p}_{\text{guess}}(X)\cdot\boldsymbol{p}_{\text{guess}}(Z)\leqslant b^2=:\mu_1, \tag{21}$$

其中 $b=\frac{1}{2}[1+\sqrt{c}\,]$, 因此, 很明显向量 $\boldsymbol{\mu}^1=\{\mu_1,1-\mu_1,0,\cdots,\}$ 符合 (19) 式, 且构成了一个简单而不平凡的不确定关系式.

除此以外, Friedland 小组和 Puchała 小组都提到了用一套有效的方法来构造一个向量序列 $\{\boldsymbol{\mu}^k\}_{k=1}^{|X|-1}$, 形式为

$$\boldsymbol{\mu}^k=\{\mu_1,\mu_2-\mu_1,\cdots,1-\mu_{m-1},0,\cdots,0\}, \tag{22}$$

同时 $\boldsymbol{\mu}^k\prec\boldsymbol{\mu}^{k-1}$ 满足 (19) 式并且带来了一个越来越紧致的不确定关系. $\boldsymbol{\mu}^k$ 的表达式是根据 Majorization 问题给出的, 并且会随着 k 的增加而变得越来越难.

这里要说明的是, Rényi 熵的熵不确定度关系是直接由 Majorization 关系派生而来的, 这是由于 Rényi 熵是 Schur 凹的, 且具有可加性. 这代表了

$$\boldsymbol{P}_X^{\downarrow}\times\boldsymbol{P}_Z^{\downarrow}\prec\boldsymbol{\mu}\Rightarrow H_\alpha(X)+H_\alpha(Z)\geqslant H_x(V), \tag{23}$$

这里的 V 是一个根据 $\boldsymbol{\mu}$ 规律分布的随机变量, 与公式 (7) 中的 Maassen-Uffink 关系相比, (23) 式中的不确定关系具有不同性质, 因为它给出了具有相同参数的 Rényi的总和的下界. 作为一个 $x\to\infty$ 的特例, 又恢复到了 Deutsch 提出的熵不确定度关系:

$$H(Q)+H(R)\geqslant H^{\min}(Q)+H^{\min}(R) \tag{24}$$

$$\geqslant\log\frac{1}{b^2}=:q_D, \tag{25}$$

第一行的不等式是通过以 α 为参数的 Rényi 熵的单调性推出的, 若 $\alpha=1$, 再根据 (23) 式, 可以得到

$$H(X)+H(Z)\geqslant H_{\text{bin}}(b^2)=:q_{\text{majorization}}, \tag{26}$$

这里的 $H_{\text{bin}}(\Lambda)=-\Lambda\log\Lambda-(1-\Lambda)\log(1-\Lambda)$ 指二元熵.

3 量子存储下的熵不确定度关系

3.1 背 景

在开始介绍量子存储下的熵不确定度关系之前, 为了更好地理解接下来的内容, 需要先引入几个概念及他们的数学表达式, 首先 von Neumann[26] 为了描述量子体系将熵的概念推广到量子范畴, 即冯诺依曼熵, 它可以用来表征量子态的不确定度, 计算方法如下:

$$S(\boldsymbol{\rho}) = -\mathrm{Tr}(\boldsymbol{\rho}\log\boldsymbol{\rho}) = -\sum_j \lambda_j \log\lambda_j, \tag{27}$$

λ_j 代表量子态 $\boldsymbol{\rho}$ 的本征值. 对于一个双边量子态 $\boldsymbol{\rho}_{AB}$, 量子联合熵、量子条件熵以及量子互信息可以表示为

$$S(AB) = -\mathrm{Tr}(\boldsymbol{\rho}_{AB}\log\boldsymbol{\rho}_{AB}); \tag{28}$$

$$S(A|B) = S(AB) - S(B); \tag{29}$$

$$\begin{aligned} I(A:B) &= S(A) + S(B) - S(AB) \\ &= S(A) - S(A|B). \end{aligned} \tag{30}$$

接着可以利用下面的式子来计算经典关联 $C(B|A)$ 和量子失谐 $D(B|A)$:

$$C(\boldsymbol{\rho}_{AB}) = S(\boldsymbol{\rho}_B) - \min_{\{E_k^A\}} S\left(B|\{E_k^A\}\right), \tag{31}$$

$$D(B|A) = I(\boldsymbol{\rho}_{AB}) - C(B|A), \tag{32}$$

$I(\boldsymbol{\rho}_{AB})$ 表示系统态的互信息, $S(B|\{E_k^A\}) = \sum_k p_k S(\boldsymbol{\rho}_{B|E_k^A})$, 其中 $\boldsymbol{\rho}_{B|E_k^A} = \mathrm{Tr}_A(E_k^A\boldsymbol{\rho}_{AB})/p_k$ 指的是经过 POVM E_k^A 测量后的态, $p_k = \mathrm{Tr}(E_k^A\boldsymbol{\rho}_{AB})$ 表示测量结果 k 的概率.

目前为止, 上面所展现出的不确定关系都是有限制的, 他们都只允许观察者获得有限的经典信息, 前面的猜测游戏中提出的问题, 即如果 Bob 除了经典信息之外还能根据两个关联的粒子获取相关的量子信息, 是否可以提高 Bob 对 Alice 测量结果的概率呢? Renes 和 Boileau[10] 在这个问题上做出了尝试并且得到了相关的结果, 也为熵不确定度关系研究打开了一个新的局面, 他们利用两个互补的测量基 X 和 Z 得到了如下的不等式:

$$\begin{aligned} &S(X|B) + S(Z|B) \geqslant \log_2 d + S(A|B), \\ &S(X|B) + S(Z|E) \geqslant \log_2 d, \end{aligned} \tag{33}$$

d 代表 A 粒子维度, E 代表窃听者 Eve 的系统.

接着, Berta 等[9] 在 Renes 和 Boileau 的结论上做出了新的突破, 将 (33) 式进一步推广到了任意两个可观测量, 现在解释 Berta 等提出的不确定游戏是如何实现的. 与之前猜测游戏不同的是, 这个游戏的规则是允许 Bob 保留量子存储系统来帮助他猜测 Alice 的测量结果, 如图 3 所示. 两个游戏玩家必须事先知晓两个测量 Q 和 R, Bob 先准备一个双粒子系统态 $\boldsymbol{\rho}_{AB}$, AB 粒子相互纠缠, Bob 将粒子 B 留下, 将粒子 A 发送给 Alice, Alice随机选择对粒子 A 进行测量, 并且把自己的测量选择告诉 Bob, Bob 的任务仍然是预测 Alice 的测量结果, 此时 Bob 这里有和粒子 A 存在纠缠的量子存储粒子 B, Bob 可以通过利用他所收到的经典信息来对粒子 B 进行测量. $S(Q|B)$ 是用来衡量 Bob 关于 Alice 用可观测量 Q 的测量结果的不确定度, $S(R|B)$ 也是同样的意义. Berta 等[9] 提出了量子存储支撑下的熵不确定度关系:

$$S(Q|B) + S(R|B) \geqslant \log_2\frac{1}{c} + S(A|B), \tag{34}$$

$$S(Q|B) + S(R|E) \geqslant \log_2\frac{1}{c}, \tag{35}$$

其中, $S(A|B) = S(\boldsymbol{\rho}_{AB}) - S(\boldsymbol{\rho}_B)$ 代表测量前的态 $\boldsymbol{\rho}_{AB}$ 的条件熵, $S(Q|B) = S(\boldsymbol{\rho}_{QB}) - S(\boldsymbol{\rho}_B)$ 代表的是经过 Q 测量过后的态 $\boldsymbol{\rho}_{QB}$ 的条件熵, 可以通过如下的式子求出经过测量的态:

$$\boldsymbol{\rho}_{QB} = \sum_i (\Pi_i^Q \otimes I_B)\boldsymbol{\rho}_{AB}(\Pi_i^Q \otimes I_B), \tag{36}$$

其中 $\Pi_i^Q = |\psi_i^Q\rangle\langle\psi_i^Q|$ 是作用在子系统 A 上的测量算子, $|\psi_i^Q\rangle$ 指代可观测量 Q 的本征矢. 现在来解读 (36) 式, 当可观测量 Q 和 R 完全互补且粒子

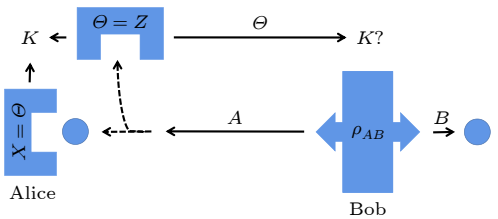

图 3 量子存储下的不确定游戏. 首先, Bob 准备态 $\boldsymbol{\rho}_{AB}$, 然后把子系统 A 发送给 Alice. 第二, Alice 对 A 进行 Q 和 R 测量, 然后向 Bob 告知测量选择 Θ. Bob 的任务是正确猜测 K

Fig. 3. The guessing game with a quantum memory system. First, Bob prepares ρ_{AB} and sends A to Alice, Then, Alice performs measurement Q or R on A, and stores the measurement options in Θ. Third, Alice tells Bob about her option Θ. Bob's task is to guess K correctly.

A 与 B 处于最大纠缠时, 通过计算可以得出此时 $c=1/d$, $S(A|B)=-\log_2 d$, 可以发现式子右边也就是下界等于 0, 也就是说, 此时 Berta 可以精准预测出 Alice 对粒子 A 执行测量 Q 和 R 的结果.

Berta 等的结果已在全光平台中得到验证[27−28], 也有人提出了利用金刚石氮空位色心体系进行验证[29]. 除这些以外, 量子存储下的熵不确定度关系在近些年也在不断发展、完善, 这些进展都会在接下来的章节中介绍.

3.2 进 展

3.1 节主要介绍了量子存储下熵不确定度关系的背景起源, 接下来展示的是近些年来量子存储下熵不确定度关系的发展方向及进程.

3.2.1 两粒子系统量子存储下的熵不确定度关系

首先在两粒子量子存储下熵不确定度关系方面, 继 Berta 之后, 许多学者也在不断进行探索, 他们发现考虑到粒子 A, B 间的量子关联, 可以得到比 (34) 式更为优化的下界, Pati 等[30] 证明了 (34) 式可以更加紧致:

$$S(Q|B)+S(R|B)\geqslant \log\frac{1}{c}+S(A|B)+\max\{0,\delta_1\}, \tag{37}$$

其中 $\delta_1=D(\boldsymbol{\rho}_{AB})-C(\boldsymbol{\rho}_{AB})$, $C(\boldsymbol{\rho}_{AB})$是经典关联, $D(\boldsymbol{\rho}_{AB})$是量子失谐[31], 数学表达式如 (31) 式和 (32) 式. 证明方程的关键是 $S(X|B)=S(X)-I(\boldsymbol{\rho}_{XB})$($X$ 表示测量 Q,R), $I(\boldsymbol{\rho}_{XB})\leqslant C(B|A)$和 $H(Q)+H(R)\geqslant q_{MU}$, 这表明当量子失谐大于经典关联时, Pati 等提出的不确定度下界较 (34) 式的下界更为收紧. 如果考虑到量子态 $\boldsymbol{\rho}_{AB}$的纯化 $|\psi_{ABC}\rangle$, 量子失谐和经典关联之间的差异遵循单配性分配[32,33]:

$$\delta_D=D(BC|A)-D(B|A)-D(C|A), \tag{38}$$

因此只有在量子态 $\boldsymbol{\rho}_{AB}$的纯化$|\psi_{ABC}\rangle$违反单配性不等式$D(BC|A)\geqslant D(B|A)+D(C|A)$时, Berta 等的不确定度下界才会被提高.

同样的, (35) 式下界也可以被优化为

$$S(Q|B)+S(R|E)\geqslant \log\frac{1}{c}+\max\{0,\delta_1'\}, \tag{39}$$

其中, $\delta_1'=C(B|A)-D(BE'|A)$, $D(BE'|A)$代表系统 A 和 BE之间的量子失谐, E指代 ABE 的纯化系统, 即 $\boldsymbol{\rho}_{ABE}=\mathrm{Tr}_{E'}(|\Psi\rangle_{ABEE'}\langle\Psi|)$.

回到 (34) 式的下界优化问题上, 2014 年, Coles 和 Piani[34] 在紧致界方面做出了突破, 他们引入 $\{c_{ij}\}$中第二大的参数c_2先推导出了新的不确定度关系式:

$$\begin{aligned}&S(Q|B)+S(R|B)\\&\geqslant \log\frac{1}{c}+\frac{1-\sqrt{c}}{2}\log\frac{c}{c_2}+S(A|B),\end{aligned} \tag{40}$$

并进一步证明了下面紧致的不确定度关系下界:

$$S(Q|B)+S(R|B)\geqslant q(\boldsymbol{\rho}_A)+S(A|B), \tag{41}$$

式中的 $q(\boldsymbol{\rho}_A)=\max\{q(\boldsymbol{\rho}_A,Q,R),q(\boldsymbol{\rho}_A,R,Q)\}$, 计算方式如下:

$$q(\boldsymbol{\rho}_A,Q,R)=\sum_j p_j^Q\log\frac{1}{\max_k c_{jk}}, \tag{42}$$

$$q(\boldsymbol{\rho}_A,R,Q)=\sum_j p_j^R\log\frac{1}{\max_k c_{jk}}, \tag{43}$$

其中$p_j^Q=\mathrm{Tr}\left(\prod_i^Q\boldsymbol{\rho}_A\right)$指 Q 的测量结果概率分布, p_j^R也是一样. 仔细观察可以发现, 如果系统 A 的维度 $d=2$, (41) 式所表示的熵不确定度关系下界和 Berta 的下界是一致的, 但是如果维度$d\geqslant q2$, (41) 式的结果可能会比 Berta 的下界更为紧致.

还可以在全套的$\boldsymbol{\rho}_A$找出最小的$q(\boldsymbol{\rho}_A)$, 也就是 $q=\min_{\boldsymbol{\rho}_A}q(\boldsymbol{\rho}_A)$, Coles 和 Piani 提出这种最小化可以通过以下步骤实现:

$$q=\max_{0\leqslant p\leqslant 1}\lambda_{\min}[\Delta(p)], \tag{44}$$

$\lambda_{\min}[\Delta(p)]$表示矩阵$\mathrm{var}\Delta(p)=p\Delta_{QR}+(1-p)\Delta_{RQ}$的最小本征值, 其中

$$\begin{aligned}\Delta_{QR}&=\sum_j\log_2\left(\frac{1}{\max_k c_{jk}}\right)\left|\psi_j^Q\right\rangle\left\langle\psi_j^Q\right|,\\ \Delta_{RQ}&=\sum_k\log_2\left(\frac{1}{\max_j c_{jk}}\right)\left|\psi_k^R\right\rangle\left\langle\psi_k^R\right|,\end{aligned} \tag{45}$$

同样, (40) 式和 (41) 式的不确定下界可以通过在不等式右侧加上额外的一项$\max\{0,\delta_1\}$而变得更为紧致.

Adabi 等[35] 以及Haseli 和Ahmadi[36] 从Holevo 量和互信息方面出发, 提出了如下表达式:

$$\begin{aligned}&S(Q|B)+S(R|B)\geqslant \log\frac{1}{c}+S(A|B)+\max\{0,\chi_2\},\\&\chi_2=I(\boldsymbol{\rho}_{AB})-I(\boldsymbol{\rho}_{QB})-I(\boldsymbol{\rho}_{RB}),\end{aligned} \tag{46}$$

其中$I(\boldsymbol{\rho}_{QB})$代表着 Bob 对 Alice 的测量 Q 可获取的信息量, $I(\boldsymbol{\rho}_{RB})$也是一样, 因此当互信息$I(\boldsymbol{\rho}_{AB})$

大于 Bob 可获取的信息之和时, (46) 式给出的下界将会比 Berta 给出的下界更为优化, 对于两粒子纯态, 经计算可得 $\delta_1=\chi_2$, 此时, (46) 式给出的下界将会和 (34) 式和 (37) 式的下界保持一致, 除此之外, Adabi 等[35] 还讨论了对 Werner 态, (46) 式的下界将会和 (37) 式的下界重合, 但是对于贝尔对角态和两量子比特 X 态, Adabi 的下界结果明显优于 (34) 式和 (37) 式的.

由 Berta 等[9] 提出的熵不确定度关系适用于两个可观测量的情况, 实际上这个关系可以被推广到更一般情况, 也就是多测量设置情况, 沿着这个想法, 不少学者也在这个方向上做出了突破[37], 下面给大家展示一些代表性的相关工作, Berta 等提出的不确定游戏中是两测量 (Q 和 R), 那么多测量的情况会是怎么样? 根据 Liu 等[38] 提出的新量子存储下熵不确定度关系, 假设这两个测量被 N 个测量 $\{M_i\}_{i=1}^N$ 所代替, 那么有:

$$\sum_{i=1}^{N}S(M_i|B)\geqslant\log\frac{1}{b}+(N-1)S(A|B), \tag{47}$$

$$b=\max_{i_N}\left\{\sum_{i_2\sim i_{N-1}}\max_{i_1}\left[c\left(\psi_{i_1}^1,\psi_{i_2}^1\right)\right]\prod_{m=2}^{N-1}c\left(\psi_{i_m}^m,\psi_{i_{m+1}}^{m+1}\right)\right\}, \tag{48}$$

其中, b 是参数, $c\left(\psi_{i_m}^m,\psi_{i_n}^n\right)=\max\limits_{i_m i_n}\left|\langle\psi_{i_m}^m|\psi_{i_n}^n\rangle\right|^2$, $\{|\psi_{i_m}^m\rangle\}$指代 M_m 的本征矢. 观察 (47) 式可以发现, 当 $N=2$, 也就是两测量时, $b=c$, $c=\max_{ij}\{c_{ij}\}$, (47) 式中下界便会恢复到和 (36) 式一样的情况. 随后将 ε 表示为测量 $\{M_i\}$ 的新顺序, 且将 $\varepsilon_{i_n}^n$ 表示为 M_m 对应的按 ε 顺序排列的本征矢, 在此基础上, Zhang 等[39] 得到了一个相对 (47) 式更为紧致的下界, 数学表达式如下:

$$\sum_{i=1}^{N}S(M_i|B)\geqslant\max_{\varepsilon}\{\ell_\varepsilon\}+(N-1)S(A|B), \tag{49}$$

式中

$$\ell_\varepsilon=-\sum_{i_N}p_{\varepsilon_{i_N}^N}\log\sum_{i_k,N\geqslant k\geqslant 1}\max_{i_1}\prod_{n=1}^{N-1}\left|\langle\varepsilon_{i_n}^n|\varepsilon_{i_{n+1}}^{n+1}\rangle\right|^2,$$

$$p_{\varepsilon_{i_N}^N}=\mathrm{Tr}\left(\left|\varepsilon_{\mathrm{i_N}}^{\mathrm{N}}\right\rangle\left\langle\varepsilon_{\mathrm{i_N}}^{\mathrm{N}}\right|\otimes\mathrm{I_B}\right)\boldsymbol{\rho}_{\mathrm{AB}}.$$

此外, 也可以利用其他方式来优化 (49) 式的下界, Dolatkhah 等[40] 采用 Adabi 等在这篇文章中一样的方法推导出

$$\sum_{i=1}^{N}S\left(M_i|B\right)\geqslant\log\frac{1}{b}+(N-1)\,S\left(A|B\right)+\max\left\{0,\chi_N\right\}, \tag{50}$$

其中 $\chi_N=(N-1)I(\boldsymbol{\rho}_{AB})-\sum_{i=1}^{N}I(\boldsymbol{\rho}_{M_iB})$, 经对比 (50) 式和 (49) 式可知, 当 $C(B|A)\leqslant I(\boldsymbol{\rho}_{M_iB})$时, (50) 式的下界相对于 (49) 式呈现的下界更优化.

除此以外, 利用 Pati 等紧致下界的方法思路, 也有学者推导出了在没有量子存储器的情况下多测量的熵不确定度关系[38]:

$$\sum_{i=1}^{N}S\left(M_i\right)\geqslant\log\frac{1}{b}+(N-1)\,S\left(A\right), \tag{51}$$

可以得到

$$\begin{aligned}\sum_{i=1}^{N}S(M_i|B)&=\sum_{i=1}^{N}S(M_i)-\sum_{i=1}^{N}I(\boldsymbol{\rho}_{M_iB})\\&\geqslant\sum_{i=1}^{N}S(M_i)-NC(B|A)\\&\geqslant\log\frac{1}{b}+(N-1)S(A)-NC(B|A)\\&=\log\frac{1}{b}+(N-1)\,S\left(A|B\right)\\&\quad+(N-1)\,D\left(B|A\right)-C\left(B|A\right).\end{aligned} \tag{52}$$

将 (52) 式进行整合简化, 可以得到一个比 Liu 等的下界 ((47) 式) 更为紧致的下界, 表示如下:

$$\sum_{i=1}^{N}S\left(M_i|B\right)\geqslant\log\frac{1}{b}+(N-1)\,S\left(A|B\right)+\max\left\{0,\delta_N\right\}, \tag{53}$$

这里的 $\delta_N=(N-1)\,D\left(B|A\right)-C\left(B|A\right)$.

Hu 和 Fan[41] 从另外的角度来分析量子存储下的熵不确定度关系, 他们从 Berta 等提出的结论 ((34) 式) 出发, 将不确定游戏推广到了这样情况, 现有 N 个玩家共享量子态 $\boldsymbol{\rho}_{AB_1B_2\cdots B_{N-1}}$, 所有玩家都知道这个态的具体形式除了, 玩家 Alice, 那么玩家 $B_1B_2\cdots B_{N-1}$ 之间禁止交流, 他们的任务就是预测出 Alice 作用在粒子 A 上的测量结果, 依赖于冯诺依曼熵的强次加性和条件熵的次加性[42], 可以得到:

$$\sum_{i=1}^{N}S(A|B_i)\geqslant 0, \tag{54}$$

从 (54) 式联系到上面的游戏情况, 可以这样理解,

Alice 对粒子 A 的测量结果不能被其余玩家 $B_1B_2\cdots B_{N-1}$ 同时准确预测, 从这个角度分析得出的 (54) 式被认定为是不同种的不确定关系.

3.2.2 三粒子系统量子存储下的熵不确定度关系

2009 年 Renes 和 Boileau[10] 给出了三粒子系统中量子存储下熵不确定度关系的具体形式:

$$S(X|B)+S(Z|C)\geqslant \log_2\frac{1}{c}=:q_{MU}, \tag{55}$$

这里可以用单配性游戏来解释. 如图 4 所示, 假设现在有一个输出三粒子系统态 $\boldsymbol{\rho}_{ABC}$ 的发射源, 现将子系统 A, B 和 C 分别发送给 Alice, Bob 和 Charlie 三人, 接着, Alice 对系统 A 进行 X 或 Z测量, 如果选择 X 测量, 将选择告诉 Bob, Bob的任务就是以最小的不确定性猜出测量结果. 同样, 如果选择 Z 测量, 将选择告诉 Charlie, Charlie需要以最小的不确定性猜出对应的测量结果, 在这个游戏里, 玩家 Bob 和 Charlie 与玩家 Alice 是对手, 在 Alice 得到测量结果 K 并将测量选择告知 Bob 和 Charlie 后, 只有在这两个玩家同时猜出结果为 K 时, 他们两个才算赢了玩家 Alice. 但是从 (55) 式可以看出, 由于测量选择 X 和 Z 的互补性, Bob 和 Charlie 对猜测结果的不确定性是一种此起彼伏的关系, 即如果在玩家 Alice 测量选择为 X 时, Bob 准确地猜测出了结果为 K, 那么 Charlie就无法在 Alice 测量

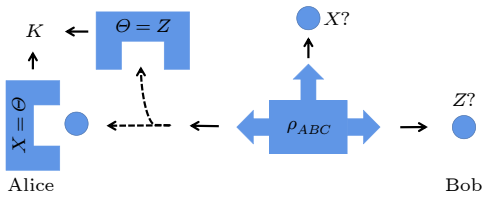

图 4 三粒子量子存储器设置图. 首先, 粒子源准备 $\boldsymbol{\rho}_{ABC}$, 并将 A 发送给 Alice, B 发送给 Bob, C 给 Charlie. 接着, Alice 在 A 上进行 X 或 Z 测量, 然后在已经给 Bob 粒子 B 的情况下, 询问 Bob 关于 Alice 的 X 测量结果的不确定性, 在已经给 Charlie 粒子 C 的情况下询问 Charlie 有关 Alice 的 Z 测量结果的不确定性. 只有他们两个同时猜出结果 K 这个游戏才能算 Bob 和 Charlie 胜利

Fig. 4. The tripartite quantum memory setup. First, the particle source prepares $\boldsymbol{\rho}_{ABC}$, and sends A to Alice, B to Bob, and C to Charlie. Next, Alice performs measurement X or Z on A, and asks Bob about the uncertainty of Alice's X measurement outcome, ask Charlie about the uncertainty of Alice's Z measurement outcome. Only both of them guessed that the output is K, the game can be considered a victory for Bob and Charlie.

选择为 Z 时, 正确猜测到结果为 K, 反之亦然.

对于 Renes 的结论, 会发现它的下界在两个可观测量确定下来后就是一个常量, 这是有一定的局限性. 于此, Ming 等[43] 在 Renes 和 Boileau 的结论基础上, 得到了一个更为优化的下界, 具体形式如下:

$$S(X|B)+S(Z|C)\geqslant q_{MU}+\max\{0,\Delta\}, \tag{56}$$

其中, $\Delta=q_{MU}+2S(\boldsymbol{\rho}_A)-[I(A:B)+I(A:C)]+[I(Z;B)+I(X;C)]-H(X)$中, $I(A:B)$是互信息, $I(X;C)=S(\boldsymbol{\rho}^B)-\sum_i p_iS(\rho_i^B)$是 Holevo 量, 它代表的是 Bob 对于 Alice 测量结果可获取信息的上界, Alice 对粒子 A 进行 X 测量, 得到第 i 次的测量结果对应的概率为 $p_i=\mathrm{Tr}_{\mathrm{AB}}\left(\prod_i^A\boldsymbol{\rho}_{AB}\prod_i^A\right)$, 此时粒子 B 对应的量子态为 $\rho_i^B=\frac{1}{p_i}\mathrm{Tr}\left(\prod_i^A\boldsymbol{\rho}_{AB}\prod_i^A\right)$. $H(X)$ 代表的是对 A 粒子执行测量 X 的香农熵, $H(Z)$也是同样的意义, 推导过程如下: 他们利用两粒子存储下的熵不确定度关系

$$S(X|B)+S(Z|B)\geqslant S(A|B)+q_{MU}, \tag{57}$$

$$S(X|C)+S(Z|C)\geqslant S(A|C)+q_{MU}, \tag{58}$$

将两式结合便可得到一个新的不等式

$$S(X|B)+S(Z|C)\geqslant 2q_{MU}+S(A|B)+S(A|C) \tag{59}$$

$$-S(Z|B)-S(X|C). \tag{60}$$

再将 $S(A)=I(A:B)+S(A|B)$, $S(A)=I(A:C)+S(A|C)$, $H(Z)=I(Z;B)+S(Z|B)$和$H(X)=I(X;C)+S(X|C)$整理, 即可推出 Ming 等的结果. 值得注意的是, 在几个特殊的情况下 Δ可以被简化: 1) 当可观测量 X 和 Z 是完全互补且子系统 A 是最大混合态时, 比如 GHZ 态; 2) 当可观测量是泡利测量即 σ_x,σ_z测量, 子系统又是非相干态时, 例如 GHZ 类态、广义的 W 态和 Werner 类态; 在这两种情况下都可以得到 $H(X)+H(Z)=S(\boldsymbol{\rho}^A)+q_{MU}$, 那么 Δ 可以被简化为 $\Delta=S(\boldsymbol{\rho}_A)-[I(A:B)+I(A:C)]+I(Z;B)+I(X;C)$.

随后, Dolatkhah 等[44] 在 Ming 等[43] 的工作基础上提出了新的下界, 形式如下:

$$S(X|B)+S(Z|C)\geqslant q_{MU}+\frac{S(A|B)+S(A|C)}{2}+\max\{0,\delta\}, \tag{61}$$

这里的 $\delta=\dfrac{I(A:B)+I(A:C)}{2}-[I(X:B)+I(Z:C)]$,

与 Ming 等的下界相比, 该下界在广义 W 态及混合三量子比特态中明显更为紧致, 如图 5 所示.

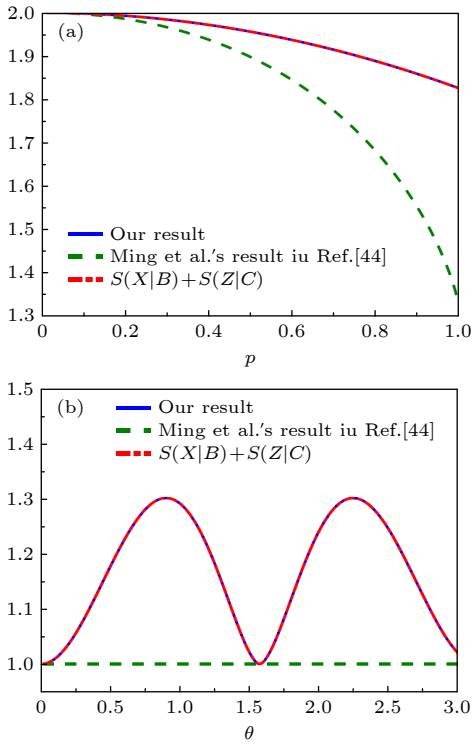

图 5 这两张图引用自参考文献 [44] 中的第三, 四幅图, 图片展示了 Ming 等的结果 (图上的 Ref. [45] 就是本文参考文献 [43]) 和 Dolatkhah 等结果的对比, 这里选取的测量是泡利测量: $X=\sigma_x, Z=\sigma_z$. 图中蓝线是式 (61) 左式, 红线对应右式, 重合表明对应的量子态、界与不确定度重合. (a) 广义 W 态量子存储下的熵不确定度及下界的图像. (b) 混合三比特态量子存储下的熵不确定度及下界的图像

Fig. 5. These two pictures are quoted in the third and fourth pictures in the reference [44].The picture shows the comparison of the results of Ming et al. (Ref. [45] on the picture is the reference [43] in this text) and Dolatkhah et al.. The measurement selected here is the Pauli measurement: $X=\sigma_x, Z=\sigma_z$. The blue line in the figure is the left side of the formula (61), and the red line corresponds to the right side. Their overlap indicates the corresponding quantum state, and the bounds coincide with the uncertainty. (a) Different lower bounds of the tripartite quantum-memory-assisted entropic uncertainty relation (QMA-EUR) for the generalized W state; (b) Different lower bounds of the tripartite QMA-EUR for symmetric family of mixed three-qubit states.

3.3 熵不确定度关系动力学

仅仅分析熵不确定度关系本身是远远不够的, 对于熵不确定度关系的研究应该落实到具体的量子系统中来, 所以本节主要介绍熵不确定度关系在各类量子系统中的动力学演化.

3.3.1 马尔科夫和非马尔科夫噪声

从实际的角度出发, 量子系统通常是开放系统, 开放系统 [45] 退相干效应会或多或少地影响不确定度的大小. 从这个意义上说, 在量子测量中, 了解环境如何影响不确定性的大小变得不可或缺和至关重要. 到目前为止, 在各种环境噪声下的量子存储下熵不确定度关系的研究方面已经做了大量的工作. 一般来说, 环境的类型可以分为马尔科夫和非马尔科夫环境. 如果一个系统的信息以单向的方式从系统流向环境, 没有信息回流, 就说环境是马尔可夫的; 相反, 如果存储在中心系统中的信息是在系统和环境之间双向流动的, 也就是存在信息回流的情况, 则称该环境为非马尔可夫环境.

我们小组 [46] 在研究了在没有量子存储器的情况下, 当一个量子比特经历马尔科夫和非马尔科夫的交叉时, 熵不确定性的动力学. 该系统由一个两能级原子与一个复合环境 (一个单模腔和一个多层级热库) 耦合而成. 通过研究发现, 腔体与热库相对较强的耦合强度可以减少不确定性. 即原子与腔之间相对较强的耦合强度是产生非马尔科夫的原因, 而弱耦合强度则会导致马尔可夫性. 原子腔耦合强度越强, 信息就会回流到原子中, 具体表现为测量不确定度的振荡. 值得注意的是, 当原子腔的耦合强度较强于临界耦合强度时, 不确定度在测得的不确定度的范围内振荡, 当原子腔耦合强度小于临界耦合强度时, 不确定性不断减小, 并在长时间限制内达到下界.

随后, 在马尔科夫和非马尔科夫交叉的情况下讨论了由两个独立耦合到结构玻色子储层的原子组成的中心系统中量子存储下的熵不确定度关系 [47], 该不确定关系由两个独立耦合到结构玻色子储层的原子组成. 量子记忆辅助熵不确定性的动力学在马尔可夫和非马尔可夫制度中非常独特. 强烈的非马尔可夫性会导致测量不确定度和下限的大幅度和长周期振荡. 然而, 对于马尔可夫制度, 不确定性和下限会随着时间的推移先增加然后减少到一个固定值. 此外, 还有一些工作 [48–50] 来观察受非马尔可夫性影响的熵的不确定性的动力学特征.

3.3.2 几种特定的系统中的熵不确定度关系动力学

弯曲时空下系统, Feng 等 [51] 在 2015 年首次观测到在 Schwarzschild 黑洞框架中的量子存储下

的熵不确定度关系, 这个 Schwarzschild 黑洞被认为是提供弯曲时空的一个. 研究可以发现, 霍金辐射可以对不确定性下界进行重要修正. 对于自由落体的观察者与其拥有与待测量子子系统初始相关的量子存储器的静态合体之间的不确定性博弈, 因此源于霍金辐射的信息丢失不可避免地导致不确定性量的增加. 熵不确定性对黑洞的质量、量子存储器的模式频率以及观察者与黑洞表面的距离很敏感. 此外, 为了显示其结果的普遍性, 将熵不确定度与其他不确定度测量, 即 Aharonov-Anandan 时间- 能量不确定度进行了比较.

考虑到两个静态玩家之间的不确定性博弈, Alice 持有的测量系统 A 和 Bob 充当量子存储器的 B 通常可以通过一对两能级原子与黑洞外波动的无质量量子标量场相互作用来模拟. 经过模拟可以注意到复合系统最终会达到平衡. 事实上, 子系统 A 的量子信息是通过它们之间产生的纠缠来传递并存储在量子存储器中的. 值得注意的是, 可以通过 $S(A|B)<0$ 纠缠被目击到.

最近, Huang 等 [52] 研究了在 Schwarzschild 黑洞表面附近, 有自旋和无自旋的 Dirac 场方向的熵不确定度关系, 证明了其边界可以用 Holevo 量重写. 结果表明, 与互信息相比, Holevo 下界比更紧致. 此外, 当量子存储器离开黑洞时, 不确定性和所提议的下界之间的差异不变, 并且不依赖于黑洞的任何属性. 此外, 已经有学者 [53–55] 研究了在 Garfinkle-Horowitz-Strominger 背景下用于 Dirac 粒子膨胀黑洞量子存储下的熵不确定度关系.

我们还关注了自旋链系统中的熵不确定度关系, Heisenberg 自旋链也有许多分类, 一维 Heisenberg 的 XYZ 链哈密顿量可以表示为

$$H=\frac{1}{2}\sum_{k=1}^{n}\left(J_x\sigma_k^x\sigma_{k+1}^x+J_y\sigma_k^y\sigma_{k+1}^y+J_z\sigma_k^z\sigma_{k+1}^z\right), \tag{62}$$

$\sigma_k^\gamma(\gamma=x,y,z)$ 指代 k 位置的泡利算符, J_γ 是关于自旋-自旋相互作用的实际耦合强度. 如果 $J_z=0$, 且 $J_x=J_y$, 相应的 Heisenberg 链称为 XX 模型. 第一个将量子存储下熵不确定度关系应用到两比特 XX 自旋模型的是 Huang 等 [56]. 他们的结果表明, 两个自旋量子位之间的耦合系数越大越会降低不确定度, 对于相对较大的耦合系数, 熵不确定度甚至会达到零. 随后, 在其他 Heisenberg 自旋链模型和具有 Dzyaloshinski-Moriya (DM) 相互作用的 Heisenberg 模型中, 也有一些关于量子存储下熵不确定度关系的研究 [57–59].

此外, 团队还探讨了在非均匀磁场中一般海森伯 XYZ 模型中熵不确定度与量子关联之间的关系 [13]. 值得注意的是, 我们得到一个有趣的结果, (55) 式中表示的下界可以改写为

$$\begin{aligned}U_R&=S(\boldsymbol{\rho}_{AB})-S(\boldsymbol{\rho}_B)+\log_2\frac{1}{c}\\&=\log_2\frac{1}{c}+\min_{\{\pi_i^B\}}[S_{\{\pi_i^B\}}(\boldsymbol{\rho}_{A|B})]-D(\boldsymbol{\rho}_{AB}),\end{aligned} \tag{63}$$

从 (63) 式中可以发现, 下界与量子关联 $D(\boldsymbol{\rho}_{AB})$ 是成反关联的. 此外, Zheng 等 [60] 和 Huang 等 [61] 还研究了系统的纠缠与下界之间的关系, Heisenberg 模型中具有 DM 相互作用的熵不确定度的紧密性. Ming 等 [62] 比较了 DM 相互作用的不同部分对降低熵不确定度的影响, 并且发现不确定关系的下界与量子相干密切相关, 但不完全依赖于量子相干. Yang 等 [63] 也研究了具有 DM 相互作用的一般 Heisenberg XYZ 模型的熵不确定度的动力学特性. Zhang 等 [64] 和 Shi 等 [65] 研究了高维 Heisenberg 模型量子存储下熵不确定度关系, 最近 Li 等 [66] 及 Ju 等 [67] 研究了自旋混合链中的熵不确定度关系. 除了上面说的两种系统, 还有非惯性坐标系 [68]、金刚石中的单氮空位中心 [29]、中微子 [69,70]等系统中熵不确定度关系的演化.

实际上在现实量子信息处理中, 任何量子系统都不可避免地会与周围环境相互作用, 从而导致退相干或耗散, 这也会对不确定性产生影响 [71], 考虑到这一点, 在执行量子任务时需要有效地抑制退相干. 而为了获得更精确的测量结果, 一些研究人员致力于追求利用各种操作如非坍缩操作 [72–75]、过滤操作 [76,77]、非厄米操作 [78–81] 等对熵不确定度进行调控.

4 不确定关系在实际中的应用

4.1 量子隐形传态

(34) 式中量子存储下的熵不确定度关系也可以用来识别非经典隐形传态 [82] 的信道状态. 基于平均隐形传态的保真度

$$F_{\rm av}=\frac{1}{2}+\frac{1}{6}{\rm Tr}\sqrt{\boldsymbol{T}^\dagger\boldsymbol{T}}, \tag{64}$$

是局部酉不变的事实, 同时任意两量子比特态是局

部么正的, 几何上表明, 与没有量子记忆存储下的情况相比, 任意对应于 Berta 等提出的不确定下界改进的态 $\boldsymbol{\rho}_{AB}$ 对于量子隐形传态来说更有用. 也就是说, 当一个人观察到一个负的条件熵 $S(A|B)$ 时, 可以确定保真度能超越经典极限 2/3.

4.2 导引不等式

在 1935 由 Schrödinger[83] 首先强调, 导引是一种与纠缠相关的双量子系统的现象 (尽管不完全相同). 考虑有两个参与者 Alice 和 Bob 两方的远程实验室范例, 他们俩各自掌握着子系统 A 或 B. 导引表示一个子系统 A 的测量选择可能导致另一个子系统 B 上的不同状态集合. 并不是所有的量子态都是可导引的, 举个例子, 可分离态就是不可导引的. 此外只要是违反贝尔不等式的态都是可导引的, 贝尔不等式是根据局部隐变量模型推出的. Wiseman 等[84] 将可导引的概念形式化为那些不允许局域隐态模型 (LHS) 的态 $\boldsymbol{\rho}_{AB}$, LHS 模型可以这样来解释, 系统 B 有一个局部量子态, 它与系统 A 上的任意可观测物经典地相关. 这种形式化的描述使得研究人员推导出了导引不等式, 与贝尔不等式类似.

Walborn 等[85] 和 Schneeloch 等[86] 展示了如何利用熵不确定性关系来推导导引不等式. 如果 B 有一个局部隐态, 那么它的测量概率必须服从单系统的不确定性关系, 即使它们是以 A 的测量结果为条件的. 更准确地说, LHS 模型意味着 A 和 B 上的离散可观测量 X_A, X_B 的联合概率分布为

$$P(X_A,X_B)=\sum_{\lambda}P(\Lambda=\lambda)P(X_A|\Lambda=\lambda)P_Q(X_B|\Lambda=\lambda), \quad (65)$$

这里 Λ 是决定 Bob 的局部状态的隐变量, λ 是这个变量可以取的一个特定值, 而 $P_Q(X_B|\Lambda=\lambda)$ 上的下标 Q 强调了概率分布来自于单个量子态. 然后得到

$$H(X_B|X_A)\geqslant H(X_B|X_A\Lambda) \quad (66)$$

$$=\sum_{\lambda}P(\Lambda=\lambda)H(X_B|X_A\Lambda=\lambda) \quad (67)$$

$$=\sum_{\lambda}P(\Lambda=\lambda)H(X_B|\Lambda=\lambda), \quad (68)$$

这里的 $H(X_B|X_A\Lambda=\lambda)$ 可以被解读为以 X_A 为条件, 以 $\Lambda=\lambda$ 为条件的 X_B 的熵. 因此, 对于两个在 B 上的可观测量 X_B 和 Z_B 和其他两个在 A 上的可观测量 X_A 和 Z_A, 可以得到

$$H(X_B|X_A)+H(Z_B|Z_A)\geqslant\sum_{\lambda}P(\Lambda=\lambda)[H(X_B|\Lambda=\lambda)+H(Z_B|\Lambda=\lambda)]. \quad (69)$$

将其与 Maassen-Uffink 的不确定度关系 (31) 式相结合, 得到如下的导引不等式[86]:

$$H(X_B|X_A)+H(Z_B|Z_A)\geqslant q_{MU}, \quad (70)$$

其中, q_{MU} 对应着 Bob 的可观测量, 任何允许 LHS 模型的状态 $\boldsymbol{\rho}_{AB}$ 必须满足 (70) 式. 因此, (70) 式的实验违反可以构成导引的演示. 对于连续变量, 也可以推导出类似的导引不等式[85].

Zhen 等[87] 通过局域不确定原理证明了 EPR (Einstein-Podolsky-Rosen) 导引. 他们指出如果下面的不等式被违背, 那么就说明两比特态 $\boldsymbol{\rho}_{AB}$ 是可导引的 (A 可以导引 B), 不等式如下:

$$\sum_i\delta^2(\alpha_iA_i+B_i)\geqslant C_B, \quad (71)$$

其中, $\delta^2(M)=\langle M^2\rangle-\langle M\rangle^2$, $C_B=\min_{\boldsymbol{\rho}_B}\sum_i\delta^2(B_i)$, $\{\alpha_i\}$ 均为实数.

4.3 随机数

随机数是许多日常信息处理任务中的关键资源, 应用范围之广可以从在线赌博到科学模拟和密码学, 因为计算机被设定来执行确定性操作, 所以随机数是一种稀缺资源. 经典物理是确定性的, 换句话来说, 如果观察者对物理学系统的初始状态和在该系统上进行的操作有充分的了解, 那么从原理上来说, 实验的每一个结果都可以被准确地预测, 而伪随机的研究试图规避这个问题[88].

量子力学固有的不确定性不允许人们去考虑随机性更强的概念, 即在信息领域层面上来说, 随机数是安全的. 形式上, 想生成一个随机变量 L 可以均匀分布在设定长度 l 上的所有位串 $\{0,1\}^l$ 上. 此外, 我们还希望这个随机变量独立于观察者可能拥有的任何边信息包括用于计算 L 的过程和任何用来准备 L 的随机种子. 经典量子积态

$$\pi_{LE}=\frac{1}{2^l}\sum_{i=1}^{2^l}|i\rangle\langle i|_L\otimes\pi_E, \quad (72)$$

描述了独立于其环境或边信息 E 的 l 位均匀随机数. 通常我们最期待的结果就是接近这个态, 也就

是说如果

$$\left\| \boldsymbol{\rho}_{LE} - \frac{1}{2^l}\sum_{i=1}^{2^l} |i\rangle\langle i|_L \otimes \boldsymbol{\rho}_E \right\|_{\mathrm{Tr}} \leqslant \delta, \tag{73}$$

那么可以说 $\boldsymbol{\rho}_{LE}$ 描述了一个 L 是 δ 接近 l 位均匀随机数且独立于 E 的态, 这里的 $\|\cdot\|_{\mathrm{Tr}}$ 代表迹范数. 这个界意味着 L 有超过 $\frac{1}{2}(1+\delta)$ 的概率不能够从一个均匀且独立的随机变量中被区分开来. 这个观点是通用可组合安全框架的核心[89,90], 也保证了满足此属性的密钥可以安全地用于任何需要秘钥的加密协议.

熵不确定度关系可以帮助我们实现真正的随机数. 因为他们表明了量子测量产生的随机变量是不确定的. 然而, 为了提取近似均匀和独立的随机数, 还需要一个额外的步骤, 也是接下来要介绍的.

先讨论条件最小熵的现实意义. 最小熵在密码学中的重要性部分归功于剩余哈希原理 (leftover hashing lemma)[91–93], 该原理指出, 存在一个函数族 $\{f_s\}_s$ ($f_s:\chi\to[2^l]$), 叫做哈希函数, 这样, 当初始的最小熵足够大时, 通过应用含有均匀随机选择的种子 S 的函数 f_s 得到的随机变量 $L=f_S(X)$ 接近均匀随机数, 且与 S 无关.

更正式地来说, Renner[94] 和 König[95] 展示了量子情况下的结果. 对于任意 $H_{\min}(X|E)\geqslant k$ 的经典量子态

$$\boldsymbol{\rho}_{XE} = \sum_x P_X(x)|x\rangle\langle x|_X \otimes \boldsymbol{\rho}_E^x\,, \tag{74}$$

都存在一组哈希函数. 经过应用函数 f_s 之后的经典-量子-经典态 $\boldsymbol{\rho}_{LES}$ 为

$$\boldsymbol{\rho}_{LES} = \sum_{s,x}\frac{P_X(x)}{|S|}|f_S(x)\rangle\langle f_S(x)|_L \otimes \boldsymbol{\rho}_E^x \otimes |s\rangle\langle s|_S, \tag{75}$$

它描述的是一个态中的 L 是 δ 接近 l 位均匀随机数且独立于 E 和 S, 这里的 $\delta = 2^{\frac{(l-k)}{2}}$.

在计算机科学中, 对环境 E 是平凡的特殊例子进行了广泛的讨论. 由于哈希是一个经典的进程, 人可能认为边信息的物理性质是非相关的, 且一个经典处理就足够了, 事实上, 这在一般情况下是不会成立的. 举个例子, 如果某些提取器的输入侧信息被存储在量子存储器中, 那么它们的输出可能是部分已知的, 同时, 相同的输出几乎一致地限制了任意经典边信息, 具体例子见 Gavinsky 等[96] 的文章.

通过考虑 $\varepsilon-$smooth 最小熵 (记为 $H_{\min}^{\varepsilon}(X|E)$, 其中 $\varepsilon>2$)的变化, 可以对这一结果进行推广, 这是通过最大化状态的最小熵来定义的, 这些态处在围绕态 $\boldsymbol{\rho}$ 周围半径为 ε 的球中. 推广后的剩余哈希引理[94,97,98] 断言, 存在一个函数族 $\{f_s\}_s$, 使得对任意 $H_{\min}^{\varepsilon}(X|E)\geqslant k$ 的态 $\boldsymbol{\rho}_{XE}$, 发现 $L=f_S(x)$ 是 $\delta+\varepsilon$ 接近 l 位均匀随机数且独立于 E 和 S, 这里的 δ 和(75)式中定义的一样. 推广后的结果在以下情况下是紧致的, 即如果 $L=f_S(x)$ 对任意的函数族 $\{f_s\}_s$ 都是 ε 接近均匀随机数且独立于 E 和 S, 那么就可以得到 $H_{\min}^{\varepsilon'}(X|E)\geqslant l$, 这里的 $\varepsilon'=\sqrt{2\varepsilon}$. 由于这个紧密性结果, 有理由说, 平滑最小熵描述了 (至少近似地) 与其环境 E 相关的随机源 X 中可以提取多少均匀随机数.

实际上, 如果可以得出 $H_{\min}^{\varepsilon}(X|E)$很大, 那么验证了属于量子随机数. 原则上来说, 所有涉及量子存储的熵不确定度关系都适用于这项任务, 只要可以验证熵的下界. 三体不确定关系特别适合这个任务, 下面量子密钥分发的安全性取决于做出这种估计的能力. 举个例子, Vallone 等[99]专门研究了最大熵和最小熵的不确定关系

$$H_{\min}(X|B)+H_{\max}(Z|C)\geqslant q_{MU}, \tag{76}$$

从而得出

$$H_{\min}(X|E)_{\boldsymbol{\rho}}\geqslant \log_2 d - H_{\max}(Z), \tag{77}$$

这里的 X 和 Z 是 d 维希尔伯特空间中相互无偏基测量, E 是被测系统的环境, 最大熵 $H_{\max}(Z)=H_{1/2}(Z)$可以通过统计学检验估算得出, 导致了对 $H_{\min}(X|E)$ 充满信心. 正如讨论的那样, 剩余哈希引理允许从 X 中提取均匀随机数.

Miller 和 Shi[100] 推导出了基于熵差的下界, 而不是条件熵, 假设 X 和 Z 是在一个量子比特上互补的二元测量, 那么下面的关系式始终成立:

$$H_\alpha(XB)_{\boldsymbol{\rho}} - H_\alpha(B)\geqslant q(\alpha,\delta)\quad \alpha\in(1,2], \tag{78}$$

这里的 δ 是由下面的等式得出的:

$$\mathrm{Tr}\left[\left\langle Z^0\right|\boldsymbol{\rho}_{AB}\left|Z^0\right\rangle^{\alpha}\right] = \delta\mathrm{Tr}\left[\boldsymbol{\rho}_B^{\alpha}\right], \tag{79}$$

q 是满足 $\lim\limits_{\alpha\to1} q(\alpha,\delta)=1-2h(\delta)$ 的函数. 然后继续使用这个结果来限定 smooth 最小熵, 并继续应用到广义剩余哈希引理上.

4.4 波粒二象性

波粒二象性是指单个量子系统既可以表现出波的行为, 也可以表现出粒子性行为的基本概念, 无法设计出能够同时显示两种行为的干涉仪. 这一观点先被 Feynman 定性地讨论了, 随后 Wooter 和 Zurek[101]、Jaeger 等[102]、Englert[103] 和 Bergou[104] 及其他学者 [105] 将其进行了定量的讨论, 这些学者都是证明了广为人知的波粒二象性关系不等式的人. 然后在 Mach–Zehnder 干涉仪下, 推导了单光子的一些相关关系. 在所有的这些情况下, 粒子性行为与已知的光子传输路径相关, 当有人改变了一对干涉仪臂之间的相对相位时, 波行为和在特定输出模式下探测光子的概率中看到的振荡有关, 将 which-path 可观测量表示为 $Z=\{|0\rangle\langle 0|,|1\rangle\langle 1|\}$, 粒子性行为可以通过路径可预测性 $P=2p_{\text{guess}}(Z)-1$ 来量化, 路径可预测性和精准猜测路径的概率 $p_{\text{guess}}(Z)$ 有关. 波行为是由边缘可见度来量化的:

$$\nu=\frac{p_0^{\max}-p_0^{\min}}{p_0^{\max}+p_0^{\min}},$$
$$p_0^{\max}:=\max_{\phi}p_0;\quad p_0^{\min}:=\min_{\phi}p_0, \tag{80}$$

这里的 p_0 是指光子被 D_0 探测到的概率, 可以在图 6 中看到. Wootter 和 Zurek[101] 证明了

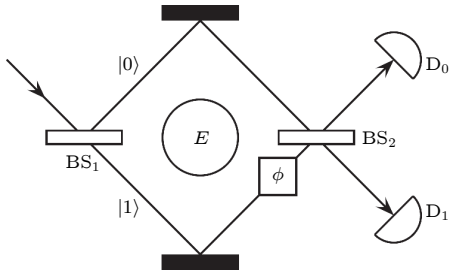

图 6 这张图引用自参考文献 [105] 中的第 18 幅图, 展示的是一个 Mach-Zehnder 单光子干涉仪. 一个光子撞击分束器, 然后通过 Z 的基态 $|0\rangle,|1\rangle$ 标记这两个可能的路径, 光子可能与干涉仪内部的某个环境 E 相互作用. 然后将一个相位 ϕ 应用于下路径, 再将这两个路径在第二个波束分束器上重新组合. 最后在 D_0 或 D_1 处检测到光子

Fig. 6. This picture is from the 18 th picture in the reference [105]. The picture shows a Mach-Zehnder single photon interferometer. A photon hits the beam splitter, and then we pass the ground state of Z ($|0\rangle,|1\rangle$) to mark these two possible paths. The photon may be related to an environment in the interferometer E Interaction. Then apply a phase ϕ to the lower path, and then recombine the two paths on the second beam splitter. Finally, a photon is detected at D_0 or D_1.

$$P^2+\nu^2\leqslant 1, \tag{81}$$

即 $P=1$ 时, $\nu=0$ (也就是说, 完全的粒子性行为就意味着没有波行为), 反之亦然.

更一般地, 假设光子与干涉仪内部的某个环境系统 E 相互作用. 测量 E 可能揭示一些比如说关于光子路径的一些信息, 所以很自然地考虑路径的可分辨性

$$\mathcal{D}=2p_{\text{guess}}(Z|E)-1. \tag{82}$$

Jaeger 等 [102] 和 Englert[103] 证明了 (81) 式的加强版本, 即:

$$\mathcal{D}^2+\nu^2\leqslant 1. \tag{83}$$

像 (81) 式和 (83) 式的波粒二象性关系概念上经常被认为不同于不确定关系, 尽管这点一直以来都存在争论. 如 Dürr 和 Rempe[106] 以及 Busch 和 Shilladay[107] 发现某些波粒二象性关系与 Robertson 涉及标准差的不确定度关系之间存在联系. Coles 等 [108] 表示 (81) 式和 (83) 式以及其他一些波粒二象性关系实际上是伪装的熵不确定度关系. 特别地, 它们对应于 (76) 式中最小和最大熵不确定度关系, 应用于互补量子位可观测量. 即 (81) 式等价于不确定度关系

$$H_{\min}(Z)+\min_{W\in XY}H_{\max}(W)\geqslant 1, \tag{84}$$

其中 $\min\limits_{W\in XY}$ 对应于最小化 Bloch 球 x-y 平面上的所有可观测量. 同样地, (83) 式等价于不确定关系

$$H_{\min}(Z|E)+\min_{W\in XY}H_{\max}(W)\geqslant 1. \tag{85}$$

这将波粒二象性原理与熵测不准原理统一起来, 说明前者是后者的一个特例.

自然地, 其他熵可以用来代替最小和最大熵, 虽然人们可能无法得到与波粒二象性关系的精确对等关系, 但概念意义可能是相似的. Bosyk 等 [109] 采用了用其他熵来替代最大最小熵的方法, 他利用的是包含了 Rényi 熵的不确定关系. Vaccaro[110] 根据互信息采用香农熵来表示波粒二象性关系. 此外, 还补充了一个概念, 即波和粒子的行为分别与对称性和非对称性有关. Englert等 [111] 还考虑了具有两条以上路径的干涉仪的波和粒子行为的熵测量.

4.5 量子密钥分发

密钥分发方案的目标是让诚实的两方通过公共通道进行通信, 以使密钥不被任何潜在的对手窃

取, 从而达成共享密钥的协议. 传统上, 试图共享密钥的两个诚实方被称为 Alice 和 Bob, 而窃听者被称为 Eve. 通过简单的对称论证, 很明显, 如果只考虑经典信息, 密钥分配是不可能的, 因为 Eve 会听到所有 Alice 对 Bob 的沟通, 在协议的任意点上, 她至少和 Bob 拥有同样多的关于 Alice 密钥的信息, 如果 Bob 知道 Alice 的密钥, 那么 Eve 也知道. Bennett 等 [112] 首先提出量子密钥分配, 随后由 Ekert[113] 提出了更优化方案 [114]. 由于非复制和非克隆的量子信息特征 [115], 当 Alice 和 Bob 共享密钥并通过量子信道进行通信时, 对称性的论点就不再适用了. 简单地说, 不管窃听者什么时候与信道进行相互作用, 对粒子进行测量, 她的行为都会不可避免地在量子通信过程中产生噪声. 因此, 他们能够检测并立即终止协议.

这里先介绍一种简单的协议, 采用的是删节版的 Ekert[113] 协议. 首先准备工作: Alice 和 Bob 使用公共信道共享一个最大纠缠的双量子位态. Eve 可以与信道进行连续的相互作用. 然后测量: 他们随机同意 (使用公共通道), 在基 $Z=\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ 或 $X=\{|+\rangle\langle +|, |-\rangle\langle -|\}$ 进行, 并在此基底上测量各自的量子比特 (这两个步骤重复了很多次). 参数评估: Alice 会公布她的测量结果. 如果双方的测量结果在大多数回合中都是一致的, 就可以得出结论, 双方之间关联存在一些保密性, 然后继续改正错误并提取一个密钥. 如果没有, Alice, Bob 双方就中止协议.

针对一般性攻击的量子密钥分发安全性首先由 Mayers[116], Biham 等 [117], Lo 和 Chau[118] 以及 Shor 和 Preskill[119] 正式建立. 在所有这些安全性讨论中, 互补性或不确定原理以某种形式被调用来论证如果 Alice 和 Bob 在一个基础上测量的量子比特有很大的一致性, 那么 Eve 关于在互补基础上测量的比特的信息必然是低的.

熵不确定度关系首次被 Cerf 等 [120] 和 Grosshans 等 [121] 用于这方面. 特别是 Koashi 利用 Maassen-Uffink 关系建立了安全性. 然而, 熵不确定性与量子存储器之间的关系提供了一个更直接的途径来 QKD 的安全性参数进行形式化描述, 如下所示. 这里遵循 Berta 等 [9] 提出的论点. 首先要注意, 在准备步骤中, 窃听者可能会干扰, 因此没有人知道在准备步骤完成后, Alice 和 Bob 是否确实共享最大纠缠态. 然而, 在不失一般性的前提下, 可以假设 Alice, Bob 和 Eve 在制备步骤后共享一个任意态 $\boldsymbol{\rho}_{ABE}$, 其中 A 和 B 是量子位, E 是 Eve 持有的任意量子系统. 设 Θ 是一个处于完全混合状态的二进制寄存器, 它决定了量子位是在基 X 还是基 Z 中被测量, 并用 Y 表示 Alice 测量的输出. 就可以得到 $H(Y|B\Theta)=\frac{1}{2}[H(X|B)+H(Z|B)]$ 和 $H(Y|E\Theta)=\frac{1}{2}[H(X|E)+H(Z|E)]$. 因此, 可以将具有量子存储器的三体熵不确定度原理写为

$$H(Y|E\Theta)+H(Y|B\Theta)\geqslant q_{MU}=1, \tag{86}$$

$q_{MU}=1$ 是基于测量基 X 和 Z 得出的. 在对 Alice 量子位进行测量后, 对态 $\boldsymbol{\rho}_{Y\Theta BE}$ 进行熵的计算. 接着再对 B 进行测量, 这会产生一个 Y 中的估算 $\hat{Y}$, 再根据数据处理不等式可以得出 $H(Y|B\Theta)\leqslant H(Y|\hat{Y})$, 因此总结得出 $H(Y|E\Theta)\geqslant 1-H(Y|\hat{Y})$. 这就保证了只要条件熵 $H(Y|\hat{Y})$ 很小, Eve 对于 Alice 测量结果的不确定度 (就 von Neumann 熵而言) 就会很大. 这就是安全准则的量化表达.

除上述应用外, 还有许多其他重要的应用, 比如两方密码学 [122–124]、纠缠目击 [125,126] 等, 还有熵不确定度关系与量子相干 [127–130]、量子纠缠 [131]、失谐 [30–32, 132] 等之间的联系.

5 结论与展望

本文从海森伯测不准原理出发, 追溯了熵不确定度关系的历史, 讨论了海森伯不确定原理和它的各类衍生关系式及其最新进展. 首先从标准差、熵和优化方法的角度回顾了不确定关系, 接着又着重介绍了量子存储下熵不确定度关系的发展, 这些关系与许多量子信息处理任务直接相关. 许多学者仍在探索不确定关系, 各种新的工具不断被拿来并试图推出新的不确定关系. 如 Majorization 方法, 用 Majorization 方法来度量不确定度仍有很大的发展前景; 关于量子存储下熵不确定度关系, Dupuis 等 [123] 在 2015 年建立了推导不确定关系的元定理. 但据了解, 并不是所有体系推出的不确定关系都很紧致, 因此也需要进一步改善加强.

本文提到的各种技术应用如量子密钥分发等为获得更精细的熵不确定度关系提供了动力. 例如, 要证明涉及两次以上测量的量子密钥分发协议的安全性, 就需要新的熵不确定度关系, 即允许量子存储和多次测量的熵不确定度关系. 这是一个需

要更多研究的重要前沿领域. 与设备无关的随机数, 即证明从不可信的设备获得的随机数是另一种新兴应用, 熵不确定度关系在这方面应该是很有潜力的.

对于熵的不确定度关系, 除了对各种技术应用有着推进作用, 它还让人们对基础物理学有了更深的了解. 如熵的不确定度关系使不确定原理与波粒二象性原理统一起来. 将熵不确定度关系应用于干涉仪, 很可能成为量化波粒二象性的一个自然框架, 同样, 量子基础的一个热门话题是测量不确定性. 也可以将制备不确定度的概念与可逆性测量相结合[133], 相应的熵不确定度关系在 IBM[134] 量子实验上测试成功, 不确定关系在实验研究方面也有着相当多的进展[135–137]. 除上述以外, 熵不确定度关系可能在凝聚态物理的相变研究[138,139]中发挥作用, 也在狭义和广义相对论的背景下[140,141]进行了研究. 鉴于量子信息在宇宙学中[142]扮演着越来越重要的角色, 希望在未来, 熵不确定度关系在宇宙学等相关背景下有着进一步的发展. 期待不确定度在未来得到更多的关注, 在学者们的共同努力下取得一些新的成果.

参考文献

[1] Heisenberg W 1927 *Z. Phys.* **43** 172
[2] Kennard E H 1927 *Z. Phys.* **44** 326
[3] Robertson H P 1929 *Phys. Rev.* **34** 163
[4] Deutsch D 1983 *Phys. Rev. Lett.* **50** 631
[5] Everett H 1957 *Rev. Mod. Phys.* **29** 454
[6] Hirschman I I 1957 *Am. J. Math.* **79** 152
[7] Kraus K 1987 *Phys. Rev. D* **35** 3070
[8] Maassen H, Uffink J 1988 *Phys. Rev. Lett.* **60** 1103
[9] Berta M, Christandl M, Colbeck R, Renes J M, Renner R 2010 *Nat. Phys.* **6** 659
[10] Renes J, Boileau J C 2009 *Phys. Rev. Lett.* **103** 020402
[11] Schrödinger E 1930 *Physikalisch-Mathematische Klasse* **14** 296
[12] Maccone L, Pati A K 2014 *Phys. Rev. Lett.* **113** 260401
[13] Wang K K, Zhan X, Bian Z H, Li J, Zhang Y S, Xue P 2016 *Phys. Rev. A* **93** 052108
[14] Xiao L, Wang K, Zhan X, Bian Z, Li J, Zhang Y, Xue P, Pati A K 2017 *Opt. Express* **25** 17904
[15] Fan B, Wang K K, Xiao L, Xue P 2018 *Phys. Rev. A* **98** 032118
[16] Białynicki-Birula I, Mycielski J 1975 *Commun. Math. Phys.* **44** 129
[17] Shannon C 1948 *Bell Syst. Tech. J.* **27** 379
[18] Korzekwa K, Lostaglio M, Jennings D, Rudolph T 2014 *Phys. Rev. A* **89** 042122
[19] Rényi A 1961 *Proceedings of the 4th Berkeley Symposiumon Mathematical Statistics and Probability* (Vol. 1) (Berkeley: University of California Press) pp547–561
[20] Dodonov V V, Dodonov A V 2015 *Phys. Scr.* **90** 074049
[21] Rastegin A E 2019 *Ann. Phys.* **531** 1800466
[22] Pegg D T 1998 *Phys. Rev. A* **58** 4307
[23] Partovi M H 2011 *Phys. Rev. A* **84** 052117
[24] Friedland S, Gheorghiu V, Gour G 2013 *Phys. Rev. Lett.* **111** 230401
[25] Puchała Z, Rudnicki Ł, Życzkowski K 2013 *J. Phys. A* **46** 272002
[26] Nielsen M A, Chuang I L (translated by Zheng D Z and Zhao Q C) 2005 *Quantum Computation and Quantum Information* (Beijing: Tsinghua University Press) pp155–157
[27] Li C F, Xu J S, Xu X Y, Li K, Guo G C 2011 *Nat. Phys.* **7** 752
[28] Prevedel R, Hamel D R, Colbeck R, Fisher K, Resch K J 2011 *Nat. Phys.* **7** 757
[29] Xu Z Y, Zhu S Q, Yang W L 2012 *Appl. Phys. Lett.* **101** 244105
[30] Pati A K, Wilde M M, Usha Devi A R, Rajagopal A K, Sudha 2012 *Phys. Rev. A* **86** 042105
[31] Ollivier H, Zurek W H 2001 *Phys. Rev. Lett.* **88** 017901
[32] Hu M L, Fan H 2013 *Phys. Rev. A* **88** 014105
[33] Bera M N, Prabhu R, Sen (De) A, Sen U 2012 *Phys. Rev. A* **86** 012319
[34] Coles P J, Piani M 2014 *Phys. Rev. A* **89** 022112
[35] Adabi F, Salimi S, Haseli S 2016 *Phys. Rev. A* **93** 062123
[36] Haseli S, Ahmadi F 2019 *Eur. Phys. J. D* **73** 65
[37] Xie B F, Ming F, Wang D, Ye L, Chen J L 2021 *Phys. Rev. A* **104** 062204
[38] Liu S, Mu L Z, Fan H 2015 *Phys. Rev. A* **91** 042133
[39] Zhang J, Zhang Y, Yu C S 2015 *Sci. Rep.* **5** 11701
[40] Dolatkhah H, Haseli S, Salimi S, Khorashad A S 2019 *Quantum Inf. Process.* **18** 13
[41] Hu M L, Fan H 2013 *Phys. Rev. A* **87** 022314
[42] Nielsen M A, Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[43] Ming F, Wang D, Fan X G, Shi W N, Ye L, Chen J L 2020 *Phys. Rev. A* **102** 012206
[44] Dolatkhah H, Haseli S, Salimi S, Khorashad A S 2020 *Phys. Rev. A* **102** 052227
[45] Yao Y B, Wang D, Ming F, Ye L 2020 *J. Phys. B: At. Mol. Opt. Phys.* **53** 035501
[46] Wang D, Ming F, Huang A J, Sun W Y, Shi J D, Ye L 2017 *Sci. Rep.* **7** 1066
[47] Wang D, Shi W N, Ming F, Hoehn R D, Sun W Y, Ye L, Kais S 2018 *Quantum Inf. Process.* **17** 335
[48] Chen M N, Wang D, Ye L 2019 *Phys. Lett. A* **383** 977
[49] Karpat G, Piilo J, Maniscalco S 2015 *EPL* **111** 50006
[50] Chen P F, Ye L, Wang D 2019 *Eur. Phys. J. D* **73** 108
[51] Feng J, Zhang Y Z, Gould M D, Fan H 2015 *Phys. Lett. B* **743** 198
[52] Huang J L, Shu F W, Xiao Y L, Yung M H 2018 *Eur. Phys. J. C* **78** 545
[53] Zhang Z Y, Liu J M, Hu Z F, Wang Y Z 2018 *Ann. Phys.* **530** 1800208
[54] Ming F, Wang D, Ye L 2019 *Ann. Phys.* **531** 1900014
[55] Wang D, Shi W N, Hoehn R D, Ming F, Sun W Y, Kais S, Ye L 2018 *Ann. Phys.* **530** 1800080
[56] Huang A J, Wang D, Wang J M, Shi J D, Sun W Y, Ye L 2017 *Quantum Inf. Process.* **16** 204
[57] Wang D, Ming F, Huang A J, Sun W Y, Ye L 2017 *Laser Phys. Lett.* **14** 095204
[58] Ming F, Wang D, Shi W N, Huang A J, Sun W Y, Ye L

2018 *Quantum Inf. Process.* **17** 89
[59] Wang D, Huang A J, Ming F, Sun W Y, Lu H P, Liu C C, Ye L 2017 *Laser Phys. Lett.* **14** 065203
[60] Zheng X, Zhang G F 2017 *Quantum Inf. Process.* **16** 1
[61] Huang Z M 2018 *Laser Phys. Lett.* **15** 025203
[62] Ming F, Wang D, Shi W N, Huang A J, Du M M, Sun W Y, Ye L 2018 *Quantum Inf. Process.* **17** 267
[63] Yang Y Y, Sun W Y, Shi W N, Ming F, Wang D, Ye L 2019 *Front. Phys.* **14** 31601
[64] Zhang Z Y, Wei D X, Liu J M 2018 *Laser Phys. Lett.* **15** 065207
[65] Shi W N, Ming F, Wang D, Ye L 2019 *Quantum Inf. Process.* **18** 70
[66] Li L J, Ming F, Shi W N, Ye L, Wang D 2021 *Physica E* **133** 114802
[67] Ju F H, Zhang Z Y, Liu J M 2020 *Commun. Theor. Phys.* **72** 125102
[68] Wang D, Ming F, Huang A J, Sun W Y, Shi J D, Ye L 2017 *Laser Phys. Lett.* **14** 055205
[69] Wang D, Ming F, Song X K, Ye L, Chen J L 2020 *Eur. Phys. J. C* **80** 800
[70] Li L J, Ming F, Song X K, Ye L, Wang D 2021 *Eur. Phys. J. C* **81** 728
[71] Ming F, Wang D, Huang A J, Sun W Y, Ye L 2018 *Quantum Inf. Process.* **17** 9
[72] Zhang Y L, Fang M F, Kang G D, Zhou Q P 2018 *Quantum Inf. Process.* **17** 62
[73] Chen P F, Sun W Y, Ming F, Huang A J, Wang D, Ye L 2019 *Laser Phys. Lett.* **15** 015206
[74] Haseil S, Dolatkhah H, Salimi S, Khorashad A S 2019 *Laser Phys. Lett.* **16** 045207
[75] Guo Y N, Fang M F, Tian Q L, Li Z D, Zeng K 2018 *Laser Phys. Lett.* **15** 105205
[76] Su Q, Al-Amri M, Davidovich L, Suhail Zubairy M 2010 *Phys. Rev. A* **82** 052323
[77] Huang A J, Shi J D, Wang D, Ye L 2017 *Quantum Inf. Process.* **16** 46
[78] Bender C M, Boettcher S 1988 *Phys. Rev. Lett.* **80** 5243
[79] Shi W N, Wang D, Sun W Y, Ming F, Huang A J, Ye L 2018 *Laser Phys. Lett.* **15** 075202
[80] Yu M, Fang M F 2017 *Quantum Inf. Process.* **16** 213
[81] Adabi F, Haseli S, Salimi S 2016 *EPL* **115** 60004
[82] Hu M L, Fan H 2012 *Phys. Rev. A* **86** 032338
[83] Schrödinger E 1935 *Math. Proc. Cambridge Philos. Soc.* **31** 555
[84] Wiseman H M, Jones S J, Doherty A C 2007 *Phys. Rev. Lett.* **98** 140402
[85] Walborn S P, Salles A, Gomes R M, Toscano F, Souto Ribeiro P H 2011 *Phys. Rev. Lett.* **106** 130402
[86] Schneeloch J, Broadbent C J, Walborn S P, Cavalcanti E G, Howell J C 2013 *Phys. Rev. A* **87** 062103
[87] Zhen Y Z, Zheng Y L, Cao W F, Li L, Chen Z B, Liu N L, Chen K 2016 *Phys. Rev. A* **93** 012108
[88] Vadhan S P 2012 *Found. Trends Theor. Comput. Sci.* **7** 1
[89] Canetti R 2001 *Proc. IEEE Symposium on Foundations of Computer Science 2001* Newport Beach, CA, USA, October 8–11, 2001 p136–145
[90] Unruh D 2010 *Proceedings of 29th Annual International Conference on Theory and Applications of Cryptographic Techniques* France, May 30–June 03, 2010 pp486–505
[91] Mclnnes J 1987 *Technical Report* 194/87, Department of Computer Science, University of Toronto
[92] Impagliazzo R, Levin L A, Luby M 1989 *Proceedings of ACM STOC 1989* Washington, Seattle, USA, May 14–17, 1989 pp12–24
[93] Impagliazzo R, Zuckerman D 1989 *Proceedings of the 30th Annual Symp On Foundations of Computer Science* Research Triangle Park, North Carolina, USA, October 30-November 01, 1989 pp248–253
[94] Renner R 2005 *Ph.D. Dissertation* (Zurich: ETH)
[95] Renner R, König R 2005 *Proceedings of the 2nd Theory of Cryptography Conference* Cambridge, England, February 10–12, 2005 pp407–425
[96] Gavinsky D, Kempe J, Kerenidis I, Raz R, de Wolf R 2009 *SIAM J. Comput.* **38** 1695
[97] Tomamichel M, Renner R 2011 *Phys. Rev. Lett.* **106** 110506
[98] Tomamichel M, Schaffner C, Smith A, Renner R 2011 *IEEE Trans. Inf. Theory* **57** 5524
[99] Vallone G, Marangon D G, Tomasin M, Villoresi P 2014 *Phys. Rev. A* **90** 052327
[100] Miller C A, Shi Y 2014 *Proceedings of ACM STOC 2014* New York, USA, May 31–June 03 2014 pp417–426
[101] Wootters W, Zurek W H 1979 *Phys. Rev. D* **19** 473
[102] Jaeger G, Shimony A, Vaidman L 1995 *Phys. Rev. A* **51** 54
[103] Englert B G 1996 *Phys. Rev. Lett.* **77** 2154
[104] Englert B G, Bergou J A 2000 *Opt. Commun.* **179** 337
[105] Coles P J, Berta M, Tomamichel M, Wehner S 2017 *Rev. Mod. Phys.* **89** 015002
[106] Dürr S, Rempe G 2000 *Am. J. Phys.* **68** 1021
[107] Busch P, Shilladay C 2006 *Phys. Rep.* **435** 1
[108] Coles P J, Kaniewski J, Wehner S 2014 *Nat. Commun.* **5** 5814
[109] Bosyk G M, Portesi M, Holik F, Plastino A 2013 *Phys. Scr.* **87** 065002
[110] Vaccaro J A 2011 *Proc. R. Soc. A* **468** 1065
[111] Englert B G, Kaszlikowski D, Kwek L C, Chee W H 2008 *Int. J. Quantum Inf.* **06** 129
[112] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing 1984* Bangalore, India, December 10–12 1984 pp175–179
[113] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[114] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dusek M, Lütkenhaus N, Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[115] Wootters W K, Zurek W H 1982 *Nature* **299** 802
[116] Mayers D 1996 *Collection in Lecture Notes in Computer Science* (Springer, New York) p343
[117] Biham E, Boyer M, Boykin P O, Mor T, Roychowdhury V 2006 *J. Cryptol.* **19** 381
[118] Lo H K, Chau H F 1999 *Science* **283** 2050
[119] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[120] Cerf N J, Bourennane M, Karlsson A, Gisin N 2002 *Phys. Rev. Lett.* **88** 127902
[121] Grosshans F, Cerf N J 2004 *Phys. Rev. Lett.* **92** 047905
[122] Koashi M 2006 *J. Phys. Conf. Ser.* **36** 98
[123] Dupuis F, Fawzi O, Wehner S 2015 *IEEE Trans. Inf. Theory* **61** 1093
[124] König R, Wehner S, Wullschleger J 2012 *IEEE Trans. Inf. Theory* **58** 1962
[125] Gühne O, Tóth G 2009 *Phys. Rep.* **474** 1
[126] Horodecki R, Horodecki P, Horodecki M, Horodecki K 2009 *Rev. Mod. Phys.* **81** 865
[127] Baumgratz T, Cramer M, Plenio M B 2014 *Phys. Rev. Lett.* **113** 140401
[128] Coles P J, Yu L, Gheorghiu V, Griffiths R 2011 *Phys. Rev. A* **83** 062338

[129] Luo S L 2005 *Theor. Math. Phys.* **143** 681
[130] Yang Y Y, Ye L, Wang D 2020 *Ann. Phys.* **532** 2000062
[131] Cao Y, Wang D, Fan X G, Ming F, Wang Z Y, Ye L 2021 *Commun. Theor. Phys.* **73** 015101
[132] Ming F, Song X K, Ling J J, Ye L, Wang D 2020 *Eur. Phys. J. C* **80** 275
[133] Berta M, Wehner S, Wilde M M 2016 *New J. Phys.* **18** 073004
[134] IBM 2016 "IBM Quantum Experience."
[135] Ma W C, Ma Z H, Wang H Y, Chen Z H, Liu Y, Kong F, Li Z K, Peng X H, Shi M J, Shi F Z, Fei S M, Du J F 2016 *Phys. Rev. Lett.* **116** 160405
[136] Ringbauer M, Biggerstaff D N, Broome M A, Fedrizzi A, Branciard C, White A G 2014 *Phys. Rev. Lett.* **112** 020401
[137] Zhou F, Yan L L, Gong S J, Ma Z H, He J Z, Xiong T P, Chen L, Yang W L, Feng M, Vedral V 2016 *Sci. Adv.* **2** e1600578
[138] Romera E, Calixto M 2015 *J. Phys. Condens. Matter* **27** 175003
[139] Xiong S J, Sun Z, Liu J M 2020 *Laser Phys. Lett.* **17** 095203
[140] Feng J, Zhang Y Z, Gould M D, Fan H 2013 *Phys. Lett. B* **726** 527
[141] Jia L, Tian Z, Jing J 2015 *Ann. Phys.* **353** 37
[142] Hayden P, Preskill J 2007 *J. High Energy Phys.* **09** 120

SPECIAL TOPIC—Recent advances in hardware, algorithms and software of quantum computers

Review on entropic uncertainty relations*

Li Li-Juan [1)] Ming Fei [1)] Song Xue-Ke [1)] Ye Liu [1)] Wang Dong [1)†]

1) (*School of Physics and Optoelectronics Engineering*, *Anhui University*, *Hefei* 230601, *China*)

(Received 29 November 2021; revised manuscript received 26 December 2021)

Abstract

The Heisenberg uncertainty principle is one of the characteristics of quantum mechanics. With the vigorous development of quantum information theory, uncertain relations have gradually played an important role in it. In particular, in order to solved the shortcomings of the concept in the initial formulation of the uncertainty principle, we brought entropy into the uncertainty relation, after that, the entropic uncertainty relation has exploited the advantages to the full in various applications. As we all know the entropic uncertainty relation has became the core element of the security analysis of almost all quantum cryptographic protocols. This review mainly introduces development history and latest progress of uncertain relations. After Heisenberg's argument that incompatible measurement results are impossible to predict, many scholars, inspired by this viewpoint, have made further relevant investigations. They combined the quantum correlation between the observable object and its environment, and carried out various generalizations of the uncertainty relation to obtain more general formulas. In addition, it also focuses on the entropy uncertainty relationship and quantum-memory-assisted entropic uncertainty relation, and the dynamic characteristics of uncertainty in some physical systems. Finally, various applications of the entropy uncertainty relationship in the field of quantum information are discussed, from randomnesss to wave-particle duality to quantum key distribution.

Keywords: entopic uncertainty relation, quantum memory, quantum correlation

PACS: 03.65.–w, 03.67.–a, 03.67.Hk **DOI:** 10.7498/aps.71.20212197

* Project supported by the National Natural Science Foundation of China (Grant Nos. 12075001, 61601002, 12004006, 12175001), the Natural Science Foundation of Anhui Province, China (Grant No. 1508085QF139), and the Fund from CAS Key Laboratory of Quantum Information (Grant No. KQI201701).

† Corresponding author. E-mail: dwang@ahu.edu.cn