清 华 大 学

综 合 论 文 训 练

题目：量子 Markov 链的周期与极限行为研究

系　　别：软件工程学院

专　　业：软件工程

姓　　名：张佳瑜

指导教师：罗贵明教授

2016 年 6 月 11 日

关于学位论文使用授权的说明

本人完全了解清华大学有关保留、使用学位论文的规定，即：学校有权保留学位论文的复印件，允许该论文被查阅和借阅；学校可以公布该论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存该论文。

(涉密的学位论文在解密后应遵守此规定)

签　名：____________ 导师签名：____________ 日　期：____________

中文摘要

量子 Markov 链是量子信息学研究中的一个重要模型，在模型检测、容错计算等领域有着重要应用。本论文研究了量子 Markov 链的周期与极限分布的性质，并给出了算法与一些应用。我们给出了非周期量子 Markov 链的定义，并证明了不可约量子 Markov 链可以唯一地分解成非周期量子 Markov 链。我们还深入研究了不可约量子 Markov 链分解的唯一性问题，给出了伪酉子空间的定义，并基于这一结果解决了量子 Markov 链的极限行为问题。进一步，我们给出了计算状态空间分解与极限行为的算法。

关键词：周期；极限行为；量子 Markov 链

ABSTRACT

Quantum Markov chain is an important model in the study of quantum information. This thesis studies the period and limit behavior of quantum Markov chains and also gives algorithms and some potential applications. We give a definition of aperiodic quantum Markov chains, and proves that an irreducible quantum Makov chain could be decomposed to aperiodic quantum Markov chain uniquely. This thesis also studies the uniqueness of irreducible quantum Markov chain decomposition and gives the definition of "pseudo unitary subspace", and use this result to solve the limit behavior problem of quantum Markov chains. Furthermore, we give the algorithms to calculate these decompositions and limit behavior.

Keywords: period; limit behavior; quantum Markov chain

目　录

主要符号对照表

Hilbert 空间	希尔伯特空间
C	复数域
$a^\dagger$	a 的共轭或共轭转置
$\|\varphi\rangle, \langle\varphi\|, \langle\phi\|\varphi\rangle$	狄拉克符号
P_S	S 上的投影算符
supp	求支撑子空间
span	求张成的子空间
$\sum$	求和
$\rho, \sigma, \cdots$	密度矩阵
$F(\rho, \sigma)$	保真度
$\\|\cdot\\|_{tr}$	迹范数
i	虚数单位
e	自然对数底数
$\mathcal{D}(S)$	S 上的密度矩阵集合
BSCC	底层强连通分支
$\mathcal{R}_{\mathcal{G}}(S)$	S 在量子 Markov 链 $\mathcal{G}$ 下的可达空间

第 1 章　引言

1.1　研究背景

量子 Markov 链是经典 Markov 链的量子扩展，在量子信息学的许多问题中均有出现。人们很早便将量子随机游走应用到量子算法设计中[1]，而量子随机游走可以看做量子 Markov 链的特殊情况。量子噪声和量子通信也有着这一模型的出现。[2][3]

在量子算法验证领域，[4] 给出了一个有不错效果的量子算法验证机制，它以量子 Markov 链和 Markov 决策过程的研究结果为基础。[5] 提出了使用量子 Markov 链和量子 Markov 链进行并行算法验证的思想。进一步，[6] 研究了量子 Markov 链的结构，并基于其结构研究了可达概率的问题。这一结果进一步扩充了量子 Markov 链在算法验证上的应用。[7] 基于量子 Markov 链的性质进一步研究了量子 Markov 决策过程。

1.2　研究现状

[1] 对量子 Markov 链的一种特殊情况：量子随机游走进行了研究。[5] 研究了量子 Markov 链的可达空间的问题。[8] 研究了双随机量子 Markov 链的极限行为问题。[6] 给出了量子 Markov 链的 BSCC 分解，并研究了可达概率的问题。这篇论文中作者提出了底部强连通分量的概念，这也是我们研究了基础。

1.3　研究问题与成果

这篇论文进一步研究了量子 Markov 链的极限行为问题，作为基础，给出了不可约子空间的周期与周期分解定理。进一步，我们给出了伪酉空间的概念，并给出了量子 Markov 链结构的详细分析。最终，我们给出了量子 Markov 链的结构、极限分解等问题的算法。

第 2 章　基础工作与背景知识

2.1　基本符号与约定

我们首先对本论文将使用的符号与约定进行解释。部分概念的含义可参见2.2节。

我们使用带有狄拉克符号的希腊字母代表纯态，如 $|\varphi\rangle$。没有狄拉克符号的希腊字母代表它们对应的密度算符，即 $\varphi = |\varphi\rangle\langle\varphi|$。

$a^\dagger$ 代表复数的共轭以及复矩阵的共轭转置。

P_S 代表 S 上的投影算符。

$\mathrm{supp}(\rho)$ 代表密度矩阵 ρ 的支撑子空间。

我们用 $\mathrm{span}(\cdots)$ 表示纯态、子空间等张成的子空间。例如，$\rho = \sum_{i=1}^{n} c_i\varphi_i$，那么 $\mathrm{supp}(\rho) = \mathrm{span}(\{|\varphi_i\rangle\}_{i=1}^{n})$。我们还会以其他形式使用这个符号，比如 $\mathrm{span}(S_1, S_2), \mathrm{span}(|\varphi\rangle)$。

我们将 $\dim(\mathrm{supp}(\rho))$ 简写为 $\dim(\rho)$，即 ρ 的支撑子空间的维数。

我们将 $\rho \in \mathcal{D}(S)$ 简写为 $\rho \in S$，其中 $\mathcal{D}(S)$ 为满足 $\mathrm{supp}(\rho) \subseteq S$ 的所有密度矩阵的集合。

2.2　量子理论基础

为便于理解，我们给出基础量子计算理论中的一些结果。本节所有结果来自于 [3]。

在量子力学中，纯态由 Hilbert 空间中的向量表示。我们在这篇论文中仅考虑有限维 Hilbert 空间，于是可以认为我们要考虑的 Hilbert 空间为 C^n。混合态由密度矩阵 $\rho \in C^{n\times n}$ 表示，它满足：

1. ρ 半正定
2. $tr(\rho) = 1$

如果空间 $H = A \otimes B$，对 H 上的一个混合态 ρ，它限制在子系统 A 和 B 上的状态用偏迹刻画，分别为 $tr_B(\rho)$ 和 $tr_A(\rho)$。

量子系统的演化由超算符表示，合法的演化过程，超算符 $\mathcal{E} : C^{n\times n} \mapsto C^{n\times n}$ 需满足：

1. $tr(\mathcal{E}(\rho)) \leq tr(\rho)$
2. $\forall\sigma, (\mathcal{E}\otimes I)(\rho\otimes\sigma)$ 半正定

如果第一个条件变成等号，我们说这个超算符是保迹的。在这篇论文中，我们只考虑保迹超算符。

任何保迹超算符均有算子和表示：$\mathcal{E} = \sum_i E_i \cdot E_i^\dagger$，并且 $\sum_i E_i^\dagger E_i = I$.

密度算子的支撑子空间 $\mathrm{supp}(\rho)$ 是一个重要的概念，它代表所有非零特征值的特征向量张成的子空间。

2.3 经典 Markov 链的结构与极限行为

我们将只列举有限维经典 Markov 链的结果。本节所有结果均可参阅 [9]。

在经典 Markov 链中，状态空间为有限集合，分布由一个概率向量表示。转移算符为一个将概率向量映射到概率向量的线性变换表示，用矩阵形式表示就是转移概率矩阵。对任意一个 Markov 链，状态空间均可以划分为暂态空间与稳态空间。从任何态开始，随着演化时间的增加，概率分布在暂态空间上的分量趋近于 0。

然后我们可以定义“不可约 Markov 链”的概念。如果任何两个状态均彼此可达，则该 Markov 链为不可约 Markov 链。任何 Markov 链的稳态空间均可以划分为一系列的不可约子空间，即使得原 Markov 链限制在这些子集合上均为不可约 Markov 链。另一个重要的性质是不可约 Markov 链必有唯一的稳定分布。

进一步，我们可以用“非周期 Markov 链”的概念进一步研究不可约 Markov 链的性质。经典 Markov 可以用图论的办法研究。对于一个不可约 Markov 链，定义所有圈的长度的最大公约数为该 Markov 链的周期。如果周期为 1，则称这个 Markov 链为非周期 Markov 链。对于周期大于 1 的 Markov 链，考虑其 p 次迭代的 Markov 链，我们发现状态空间在该 Markov 链下可以分解成一系列不可约子空间，并且这些子空间上的稳定分布在原 Markov 链的演化下连成一个圈。这样我们就得到了不可约子空间的结构，从而完成了经典 Markov 链的状态空间分解。

2.4 量子 Markov 链的概念与现有结果

本节中的所有结果均来自于 [6]。下面将对 [6] 中的部分结果进行综述，以便大家理解本论文的背景与结果

定义 2.1： 量子 Markov 链定义为有序对 $(H, \mathcal{E})$, 其中 H 是有限维 Hilbert 空间，$\mathcal{E}$ 为 H 上的保迹超算符。

对应于经典 Markov 链，概率分布由 H 上的密度矩阵代替，转移概率矩阵由超算符代替。

这一定义包含的情况足够广泛，有着广泛的应用场景。

对量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$，用 $\mathcal{G}^i$ 表示 $\mathcal{G}$ 的 i 次迭代 $(H, \mathcal{E}^i)$。其中 $\mathcal{E}^i = \mathcal{E} \circ \mathcal{E} \circ \cdots \mathcal{E}$.

对量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$，如果子空间 X 满足 $\mathcal{E}(X) = X$，我们说 X 是底部不变的。

对量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$，$S$ 是 H 的一个子空间，定义量子 Markov 链 $\mathcal{G}|S = (S, \mathcal{E}')$，其中 $\mathcal{E}'$ 为 S 上的超算符，满足 $\mathcal{E}'(\rho) = P_S \mathcal{E}(\rho) P_S$。

一个自然的问题是：如何描述量子 Markov 链的结构？量子 Markov 链是否和经典 Markov 链一样具有暂态空间，稳态空间，不可约子空间等？

2.4.1 可达空间与不可约子空间

定义 2.2： 对量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$，定义状态 ρ 的可达空间为由 $\mathrm{supp}(\rho), \mathrm{supp}(\mathcal{E}(\rho)), \mathrm{supp}(\mathcal{E}^2(\rho)) \cdots$ 张成的子空间。记为 $\mathcal{R}_{\mathcal{G}}(\rho)$.

定义 2.3： 考虑量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$. 如果 H 的子空间 S 满足 $\forall \rho \in \mathcal{D}(S), \mathcal{R}_{\mathcal{G}}(\rho) = S$，我们说 S 是 H 的一个不可约子空间。

在 [6] 中不可约子空间被叫做底层强连通分量（BSCC），定义也有所不同，但二者是等价的。为了与经典 Markov 链类比，我们将其称作不可约子空间。

可达空间与不可约子空间的性质这里略去。下面的定理是 [6] 中的重要定理：

定理 2.1： 对量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$，其状态空间 H 可以被分解成正交子空间 $B_1, B_2 \cdots B_u, T$ 的直和，其中 T 是暂态空间，B_i 是不可约子空间。

暂态空间的定义可见 [6] 下面举例说明：

例 2.1：　考虑量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$，$H = \text{span}(|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle)$，

$$\mathcal{E} = \sum_{i=1}^{5} E_i \cdot E_i^\dagger$$

其中

$$\begin{aligned}
E_1 &= \frac{1}{\sqrt{2}}(|1\rangle\langle 0+1| + |3\rangle\langle 2+3|) \\
E_2 &= \frac{1}{\sqrt{2}}(|1\rangle\langle 0-1| + |3\rangle\langle 2-3|) \\
E_3 &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0+1| + |2\rangle\langle 2+3|) \\
E_4 &= \frac{1}{\sqrt{2}}(|0\rangle\langle 0-1| + |2\rangle\langle 2-3|) \\
E_5 &= \frac{1}{10}(|0\rangle\langle 4| + |1\rangle\langle 4| + |2\rangle\langle 4| + 4\,|3\rangle\langle 4| + 9\,|4\rangle\langle 4|)
\end{aligned}$$

其中 $|i \pm j\rangle = \frac{|i\rangle \pm |j\rangle}{\sqrt{2}}$

H 的一个 BSCC 分解为 $H = B_1 \oplus B_2 \oplus T$，其中 $T = \text{span}(|4\rangle)$ 为暂态空间，$B_1 = \text{span}(|0\rangle, |1\rangle), B_2 = \text{span}(|2\rangle, |3\rangle)$ 是 $\mathcal{G}$ 的不可约子空间。

第 3 章　不可约子空间的周期与周期分解定理

3.1　介绍

经典 markov 链中对于一个 scc 有下面的结论:[9]

每个 scc 均存在一个“周期”。这个“周期”等于这个 markov 链中所有圈（cycle）的长度的最大公约数。进一步，我们可以把这个 scc 分成 p 个子集，每个子集上均可定义一个分布 π, 满足 $\pi_i P = \pi_{i+1 \mod p}$. 每个子集在 P^p 下均是 aperiod 的，aperiod 的 markov chain 的 scc 满足对任何一个分布 π 均有 $\pi P^i \to \pi_i$

对量子 markov 链 S Ying 证明了 BSCC 分解定理[6]。对每一个 BSCC 也有类似的周期的概念。首先对于量子 markov 链 $G = (H, \mathcal{E})$ 我们定义一个子空间 S 为 aperiodic BSCC，如果其满足下列条件：(1)S 是一个 BSCC(2)$\forall\, |\varphi\rangle \in S, \exists N, span(\mathcal{E}^N(\varphi)) = S$

对一个量子 markov 链 $G = (H, \mathcal{E})$, 一个 BSCC S，存在周期 p，满足: 存在密度算子 $\rho_1, \rho_2 \cdots \rho_p$, 满足：(1)$span(\rho_1), span(\rho_2) \cdots span(\rho_p)$ 的直和为 S 并且两两正交（2）$\mathcal{E}(\rho_i) = \rho_{i+1 \mod p}(3)span(\rho_i)$ 是 G^p 下的 aperiodic BSCC。

3.2　基础

3.2.1　基本符号

$\{a_i\}_n, \{a_i\}_{i=0}^{+\infty}$ 等右下角或右上角有长度等标记时代表序列而非集合。

引入 $\boxplus$ 符号：设 $\{|\varphi_i\rangle\}_n$ 为态的序列 $|\varphi_1\rangle, |\varphi_2\rangle \cdots |\varphi_n\rangle$, $\{|\chi_i\rangle\}_n$ 为态的序列 $|\chi_1\rangle, |\chi_2\rangle \cdots |\chi_n\rangle$, 记 $\alpha\{|\varphi_i\rangle\}_n \boxplus \beta\{|\chi_i\rangle\}_n = \{\alpha\, |\varphi_i\rangle + \beta\, |\chi_i\rangle\}_n$.

注意这里 $\{|\varphi_i\rangle\}_n$，$\{|\chi_i\rangle\}_n, \{\alpha\, |\varphi_i\rangle + \beta\, |\chi_i\rangle\}_n$ 都是态的序列而不是集合。$\boxplus$ 作用在两个等长的态的序列和两个系数上，得到一个新的态的序列。我们感兴趣的往往是 $span(\alpha\{|\varphi_i\rangle\}_n \boxplus \beta\{|\chi_i\rangle\}_n)$.

例 3.1：　$\{|\varphi_i\rangle\}_2 = \{|0\rangle, |1\rangle\}_2, \{|\chi_i\rangle\}_2 = \{|2\rangle, |3\rangle\}$, 那么

$$span(\frac{1}{\sqrt{2}}\{|\varphi_i\rangle\}_2 \boxplus \frac{1}{\sqrt{2}}\{|\chi_i\rangle\}_2) = span(\frac{|0\rangle + |2\rangle}{\sqrt{2}}, \frac{|1\rangle + |3\rangle}{\sqrt{2}})$$

我们也可以使用 $\boxplus$ 得到密度算子。我们引入一个符号 $\boxed{DenM}$, 用来表示密度矩阵:

$$\{c_i\}_n \boxed{DenM} \{|\varphi_i\rangle\}_n = \sum_{i=1}^{n} c_i \varphi_i$$

于是我们可以使用 $\boxed{DenM}$ 和 $\boxplus$ 定义密度算子: 设 S_1, S_2 是 H 的两个子空间, $dim(S_1) = dim(S_2) = n$, $S_1 \perp S_2$, $\{|\varphi_i\rangle\}_n$, $\{|\chi_i\rangle\}_n$ 分别是 S_1 和 S_2 的正交基, $|\alpha|^2 + |\beta|^2 = 1$, $\{c_i\}_n$ 满足 $(1)\forall i, c_i \in [0,1]$$(2)\sum_i c_i = 1$。下面是一个我们常用的定义密度矩阵的方式: $\{c_i\}_n \boxed{DenM} (\alpha\{|\varphi_i\rangle\}_n \boxplus \beta\{|\chi_i\rangle\}_n)$. 即先用 $\boxplus$ 得到一组基, 再用 $\boxed{DenM}$ 和系数得到密度矩阵。

例 3.2:

$$\{\frac{1}{2},\frac{1}{2}\}_2 \boxed{DenM} (\frac{3}{5}\{|0\rangle,|1\rangle\}_2 \boxplus \frac{4}{5}i\{|2\rangle,|3\rangle\}_2) = \frac{1}{2}(\frac{3}{5}|0\rangle+\frac{4}{5}i|2\rangle)(\frac{3}{5}\langle 0|-\frac{4}{5}i\langle 2|)+\frac{1}{2}(\frac{3}{5}|1\rangle+\frac{4}{5}i|3\rangle)(\frac{3}{5}\langle 1|-\frac{4}{5}i\langle$$

我们用 $\varphi = |\varphi\rangle\langle\varphi|$ 代表某个纯态对应的密度算子。即如果某个狄拉克符号代表纯态, 去掉括号后剩下的字母即为密度算子。

如果 $\rho = \sum_i c_i\varphi_i$, 我们用 $span(\rho) = span(\{|\varphi_i\rangle\})$ 代表密度算子张成的子空间.

如果 $span(\rho) \subseteq S_1$, 我们直接写 $\rho \in S_1$

然后: 如果 $span(\rho_1) = span(\rho_2)$, 那么 $span(\mathcal{E}(\rho_1)) = span(\mathcal{E}(\rho_2))$. 于是对于子空间 S 我们可以直接用 $\mathcal{E}(S)$ 代表某一个 $span(\rho) = S$ 在 $\mathcal{E}$ 作用下的结果, 也就是 S 在 $\mathcal{E}$ 作用下得到的子空间。

P_S 代表子空间 S 上的投影算子。

我们在这篇文章里特别定义的符号或算符列举如下:

1. $\boxplus$: 2.1 小节, 作用在两个等长的态序列和两个系数上得到一个新的态序列。
2. $\boxed{DenM}$ 由系数和态序列定义密度算子
3. MS: 作用在两个子空间上, 代表相似度
4. $MSPOS$: 作用在两个自空间上, 代表最大相似子空间
5. XD: 轨道维度函数, 作用在密度算子上得到一个正整数
6. LF: 轨道保真度函数, 作用在一个正整数和一个密度算子上得到一个实数
7. $\rho_\blacklozenge$: 我们构造出的一个密度算子。

8. MID: 作用在两个纯态上得到一维子空间，作用在两个密度算子上得到密度算子
9. $AXLE$: 作用在两个纯态上得到一维子空间，作用在两个密度算子上得到密度算子

3.2.2 基础定理

引理 3.1： 设 $S = span(\rho_1)$，则 $F(\rho_1, \rho_2) \leq \sqrt{tr(P_S\rho_2)}$，等号成立当且仅当 $\rho_1 \perp \rho_2$ 或 $\rho_1 = \frac{P_S\rho_2 P_S}{tr(P_S\rho_2)}$

3.2.3 quantum Markov chain

设 $G = (H, \mathcal{E})$ 是一个 quantum markov chain，用 G^i 表示其幂 $(H, \mathcal{E}^i)$

我们下面只考虑 $\mathcal{E}$ 为 trace-preserving operator 的情况。

3.3 周期分解定理证明

3.3.1 证明思路

各小节之间关系：1 为介绍，3,6,8,9 是证明主线，2（弱不动点态），4（相似度，保真度的性质），5（弱不动点态与相似度），7（完全最大保真度的深入性质）是证明中用到的引理，2 推 3, 3+4 推 5，3+4+5 推 6,4 推 7，3+6+7 推 8,8 推 9, 9 最后是主定理。

下面引出定理。

aperiodic BSCC 定义如下：

定义 3.1： BSCC S 是 aperiodic BSCC，如果它满足下列条件：$\forall |\varphi\rangle \in S, \exists N, span(\mathcal{E}^N(\varphi)) = S$

下面即是 BSCC 的周期分解定理，也是这一节的主定理：

定理 3.1： 一个 BSCC S, 必是下列两种类型之一:

1. aperiodic BSCC
2. 存在周期 $p \geq 2$，以及密度算子序列 $\rho_1, \rho_2 \cdots \rho_p$，满足：(1)$span(\rho_1), span(\rho_2) \cdots span(\rho_p)$ 的直和为 S 并且正交 (2) $\mathcal{E}(\rho_i) = \rho_{i+1 \bmod p}(3)span(\rho_i)$ 是 G^p 下的 aperiodic BSCC。对满足这

样条件的分解，p 和子空间维数组成的集合以及每一个维数的出现次数是唯一的.

总体来说，为了证明主定理，我们采用了这样的方法：假设我们考虑的 BSCC S 不是 aperiodic. 如果能够通过某种方法寻找到初态 ρ_1, 满足这样的性质（我们将在后面经常引用这一性质）：

$$F(\rho, \mathcal{E}^k(\rho)) = \begin{cases} 0 & \text{when } 1 \leq k < K \\ 1 & \text{when } k = K \end{cases}, \text{for some } K \geq 2 \tag{3-1}$$

那么 $\rho_1, \mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1) \cdots \mathcal{E}^{K-1}(\rho_1)$ 作为主定理中的 $\rho_1, \rho_2 \cdots \rho_p$, 几乎可以满足主定理中对分解分量的各项要求. 除了一项：$span(\rho_i)$ 在 G^K 下是 aperiodic BSCC。

以经典 Markov 链做类比。我们得到的结论与经典 Markov 链 irriducible subspace 的周期具有类似的性质。在经典中，一个非 aperiodic 的 irriducible subspace 如果周期为 p, 我们做分解时如果没有限定分解得到的分量的 aperiodic 性，我们有可能将这个 irriducible subspace 分解成 K 个子空间，$K|p$. 量子 Markov 链也有类似情况。我们这时只是找到了一个分解，但没有在 G^K 下是 aperiodic BSCC 的性质。但是我们只要有 $K \geq 2$, 就可以反复使用这个结论，得到最终的分解，使得每一个子空间都具有 aperiodic 性质。然后我们利用 aperiodic 性质证明这样的分解中的唯一性。

具体思路为：

我们在第 2 小节引入了轨道 (Orbit)(definition 2) 和弱不动点态 (weak fixed point state)(definition 3) 的概念。我们观察到的一个要点是：我们不能只关心 $\rho, \mathcal{E}(\rho) \cdots \mathcal{E}^d(\rho), d = dim(S)$. 我们如果考虑 $\{\mathcal{E}^i(\rho)\}_{i=0}^{+\infty}$, 研究序列整体的性质，可以得到很多不错的性质。$\{\mathcal{E}^i(\rho)\}_{i=0}^{+\infty}$ 就是我们定义的 ρ 的轨道 Orbit。进一步，如果一个密度算子 ρ 满足其 Orbit$\{\mathcal{E}^i(\rho)\}_{i=0}^{+\infty}$ 中存在一个收敛到 ρ 的子序列，我们称 ρ 为一个弱不动点态。正如每一个 BSCC 中都有一个不动点态，周期分解中的任意一个 ρ_i 都是弱不动点态。但弱不动点态包含的范围还要更广泛. 不动点态（fixed point state）,G^k 的不动点都是弱不动点态的特例。弱不动点态一方面具有不错的性质（lemma 3.2，以及后面第 5 小节 lemma 3.13），另一方面又足够广泛且易于构造：任何一个初态 ρ_0, 其 Orbit$\{\mathcal{E}^i(\rho_0)\}_{i=0}^{+\infty}$ 的任何一个收敛子列均收敛到一个弱不动点态 (lemma 3.3)。我们在第 3 小节将这样构造出一个弱不动

点态并利用其性质。

第 3 小节是证明主线的第一部分，我们给出了具体构造方法是：我们定义了两个函数：轨道维度函数 XD 和轨道保真度函数 LF(definition 4)。构造第一步是根据这两个量在全体密度算子上构造出一个序，然后找到这个序下的最大值。第二步是在得到序关系的最大值之后，在它的轨道上取收敛子列得到一个弱不动点态。我们把它记为 $\rho_\blacklozenge$。我们将证明对于非 aperiodic BSCC，我们就能得到周期分解当中的 ρ_1. 剩下的工作就是证明我们得到的 $\rho_\blacklozenge$ 确实满足周期分解需要的性质。

从另一个角度考虑，通过这样的构造，我们找到了一个 weak fixed point state$\rho_\blacklozenge$ 满足轨道维度函数 XD 尽量小，然后轨道保真度函数 LF 尽量大。这样构造的原因是：在第 6,8 小节的证明中，我们将充分利用我们构造出来的 XD 和 LF 在这个序关系中位于最大值这个性质。我们先在第 4，7 小节中证明一些定理，它们有可能在某些条件不满足的情况下使我们得到更小的 XD 或者更大的 LF(lemma 3.4,3.10,3.17,3.18). 换句话说，通过这些定理，我们可以由 $\rho_\blacklozenge$ 在序关系下最大的特性导出这些条件。使用这些引理我们能够对 $\rho_\blacklozenge$ 的 Orbit 给出越来越强的限制条件，最终这个序列必须满足 Eq. (1)。而在证明过程中，弱不动点态的性质是很重要的。

另一方面，在第 3 小节中，我们构造出 weak fixed point state 后，我们事实上已经得到了 Eq. (1) 中的 K 和第一行代表的正交性，但是 $\rho, \mathcal{E}^K(\rho)$ 的关系仍然未知。唯一已知的是二者非正交。而这一点是我们后面一系列论证的基础。

在第 4 小节中，我们定义了两个子空间上的算子：相似度 MS 与最大相似子空间 $MSPOS$。MS 作用在两个子空间上，结果为一个数，为分别位于两个子空间上的态的内积的模长的最大值。这个代表两个子空间之间的“最近位置的相似程度”。$MSPOS$ 也作用在两个子空间上，代表输入的两个子空间中使内积能够取到 MS 的态组成的集合。我们还定义了“完全最大相似度”，“完全最大保真度”等概念并进行了研究。第 4 小节是一些基础概念，在后面的证明中将用到这些概念。同时，这一小节的许多定义引理，比如之前的 lemma 3.10 3.12 直接用到第 6 小节的证明中。比如 lemma 3.10 将在第 6 小节的证明中应用，用来构造具有更小的 XD 的初态 ρ。lemma 3.10 应用的条件事实上只有我们研究的两个子空间非正交的条件，而这恰好是对于 $\rho, \mathcal{E}^K(\rho)$ 我们已知的性质. lemma 3.12 则给了我们增大 LF 需要的引理。这些定理在第 6 小节中应用的结果是，我

们得到了 Orbit 上的一个“完全最大保真度”的性质。完全最大保真度的密度算子可以使用这一小节的结论（lemma 3.11）用基具体地表示出来。对完全最大保真度的更深入研究留到第 7 小节。而第 7 小节的定理引理也是以这一小节的概念为基础的。

第 5 小节给出了 weak fixed point state 的一个与相似度相关的性质。我们在第 6 小节证明“完全最大保真度”的性质时将用到这一性质。

第 6 小节是证明主线，和第 3 小节衔接。在这里我们使用了第 4, 5 小节的结论证明了 $\rho, \mathcal{E}^K(\rho)$ 完全最大保真度. 证明中主要使用了 lemma 3.10，3.12，3.13.

第 7 小节：要把第 6 小节的结论推进，我们要研究 ρ_1 与 ρ_2,$\mathcal{E}(\rho_1)$ 与 $\mathcal{E}(\rho_2)$ 均完全最大保真度且保真度相等时的结论。我们这里用 $\mathcal{E}$，事实上在证明中我们考虑的是 $\mathcal{E}^K$。这一小节的主定理是 lemma 3.16。定理 3.16 是一个比较强也比较关键的引理，一方面可以应用到 fixed point state，weak fixed point state 上，也是下面几个定理的基础。我们接下来的思路是：根据已有的条件寻找使 $F(\rho, \mathcal{E}(\rho))$ 尽量大的 ρ。找到一些定理后，就可以把他们用在 $\rho_\blacklozenge$ 的 Orbit 上尝试得到更大的 LF，从而得到一些性质. 利用 3.16 及其推论我们可以从 ρ_1, ρ_2 构造出 ρ 使得 $\mathcal{E}(\rho)$ 可以以类似的方式由 $\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)$ 构造出来。进一步，我们研究了如何选取 ρ 可以尽量增大 $F(\rho, \mathcal{E}(\rho))$. 在第 8 小节的证明主线，我们应用这些结论 (lemma 3.17, 3.18)，即可利用 $\rho_\blacklozenge$ 的 LF_K 的最大性引出矛盾。而且 corollary 3.16.1，3.16.2 保证了我们的构造不影响轨道维度函数 XD 的值，并且在 $k < K$ 时轨道保真度 LF_k 已经为 0，只能更大不可能更小。

第 8 小节中，我们证明了 $\rho_\blacklozenge$ 满足 Eq. (1)。在第 6 小节中我们已经证明了完全最大保真度，于是我们可以使用第 7 小节的结论尝试找到 $F(\rho, \mathcal{E}^K(\rho))$ 更大的初态。也就是说，尝试违背 $\rho_\blacklozenge$ 在这个序结构中由 LF 的值的序带来要求。首先使用 3.17，利用 MID 算子尝试构造，最终由等号成立条件得到 Orbit 的 fidelity C cyclic 的性质。在 fidelity C cyclic 条件下，用 3.18 即可证明它们必定满足 $\exists p, \mathcal{E}^p(\rho_1) = \rho_1$, 而 $\forall i \in \{1, 2 \cdots p-1\}, \mathcal{E}^i(\rho_1) \perp \rho_1$. 同时我们使用 corollary 3.16.1，3.16.2 保证 XD 不会改变，不会影响序关系。

第 9 小节：虽然在上一小节我们得到了一个分解，但是我们还没有证明每一个分量在 G^p 下都是 aperiodic，也没有证明唯一性。因为可能存在这样的情况：本来这个 BSCC 以 6 为周期，但我们找到的是周期 2 或周期 3 的分解。但是上一节中的结论中，我们知道只要一个 BSCC 不是 aperiodic，它就一定可以根据

上一节的结论分解。于是如果得到的分解中某个子空间在 G^p 下不是 aperiodic，我们可以继续分解，直到分解中的所有子空间均为 aperiodic，然后我们证明唯一性。

3.3.2 弱不动点态的定义与基本性质

我们先给出弱不动点态（weak fixed point state）的定义，然后 lemma 3.2 和后面的 lemma 3.5 说明了 weak fixed point state 的性质，lemma 3.3 给出了如何得到一个 weak fixed point state。在第 3 小节的证明中，我们将用到 lemma 3.3 得到一个弱不动点态，并使用 lemma 3.2，3.5.5 中的性质。

定义 3.2： 对一个初态 ρ, 将密度算子序列 $\{\mathcal{E}^i(\rho)\}_{i=0}^{+\infty}$ 称作 ρ 在 $\mathcal{E}$ 下的 Orbit(轨道).

定义 3.3： 如果 ρ 满足: ρ 的 Orbit 中有一个收敛子列收敛到 ρ, 我们说 ρ 是 $G = (H, \mathcal{E})$ 的一个弱不动点态（weak fixed point state）

比如说，考虑一个酉变换，任何一个态都是其弱不动点态。即使一个初态经 U 连续作用不能最终恰好回到原来的初态，我们也可以找到一个收敛子列收敛到初态。另一方面，不动点态（fixed point state）均是弱不动点态，transient subspace 中不可能有弱不动点态，因此我们认为弱不动点态是一个比较重要的概念。而且它有很多不错的性质。这些性质将在证明中发挥重要的作用。另一方面，我们注意到我们要证明的主定理中的 ρ_1 也必然是弱不动点态。这启发我们，证明的关键可能是找到一个合适的弱不动点态 ρ_1。

引理 3.2： 如果 ρ 是 $G = (H, \mathcal{E})$ 的一个 weak fixed point state, 密度算子序列 $\{O_i\}_{i=0}^{+\infty}$ 是 ρ 的 Orbit，我们有：$F(O_i, O_{i+k})$ 在 k 固定时是不随 i 变化的常数.

weak fixed point state 除了具有 Orbit 中相等间隔的两项保真度不变的性质，还有其他的不变性：我们将在第 4 小节定义“相似度”的概念，并在第 5 小节证明 Orbit 中相等间隔的两项张成的子空间之间的相似度也不变。

弱不动点态的另一个性质是，它非常容易从任意初始态生成的 Orbit 中生成出来：

引理 3.3： ρ_0 是任意态, 如果 ρ_0 的 Orbit 中有一个子序列收敛到 ρ, 那么: ρ 是 $G = (H, \mathcal{E})$ 的一个 weak fixed point state.

事实上，我们证明主定理的第一步就是从一个以某种特定方式选定的初态生成的 Orbit 中生成出一个弱不动点态。然后我们证明这个 weak fixed point state 满足条件。在下一小节中我们将给出构造过程.

3.3.3 证明主线第一部分：分解的构造

下面，在证明主线中（第 3,6,8 小节），我们将设 $G = (S, \mathcal{E} = \sum_i E_i \cdot E_i^+)$ 仅包含一个 BSCC S, 而且 S 不是 aperiodic BSCC

我们做一点不严格的思考，来引出下面的证明构造。我们考虑一个 BSCC S，不是 aperiodic BSCC。我们要证明定理，我们希望能找到一个 $\rho \in S$ 满足 Eq. (1) 的条件。如果能够找到这样的 ρ, 似乎就能解决问题了。我们首先考虑只满足 $F(\rho, \mathcal{E}^p(\rho)) = 1$ 是否可以。这在处理上比较方便，但是存在问题：首先，选取 ρ 为 S 的 fixed point state，即 $\mathcal{E}(\rho) = \rho$，满足条件，但我们无法进一步研究。然后，还存在这样的情况：

假设 $H = C^3$。$\mathcal{E}$ 为这样的算符：首先将态 $|\varphi\rangle$ 在基 $|0\rangle, |1\rangle, |2\rangle$ 下作投影，然后作酉变换：$U|0\rangle = |1\rangle, U|1\rangle = |2\rangle, U|2\rangle = |0\rangle$. 我们发现对于这样的 Markov chain，我们可以直观地看出 $p = 3$, 但是如果我们取 $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$, 它满足 $F(\rho, \mathcal{E}^3(\rho)) = 1$, $F(\rho, \mathcal{E}(\rho)) = F(\rho, \mathcal{E}^2(\rho)) < 1$，但是 $\rho, \mathcal{E}(\rho), \mathcal{E}^2(\rho)$ 没有正交性。我们想到，如果对 ρ 的维数加以限制，也即取能让 $F(\rho, \mathcal{E}^p(\rho)) = 1$ 成立的维数最小的 ρ, 或许就能解决问题。这就是我们下面引入轨道维度函数 XD 的意义。

按照我们上面的思考过程，我们似乎要假定 $F(\rho, \mathcal{E}^p(\rho)) = 1$ 与维数最小，去尝试证明正交性。但其实我们做的是在已经有维数最小与正交性两个条件下去证明 $F(\rho, \mathcal{E}^p(\rho)) = 1$。这一点需要依赖于我们的构造过程，这也是我们引入轨道保真度函数 LF 的意义。我们在 XD 最小的情况下寻找使 Orbit 保真度函数 LF 尽量大的初态 ρ, 最终经过一些构造和证明我们将得到 Eq. (1). 另外，由于 p 不能被提前确定，我们需要对所有的 k 考虑 $F(\rho, \mathcal{E}^k(\rho))$

另一方面，直接定义 LF_k 为 $F(\rho, \mathcal{E}^k(\rho))$ 并不合适。我们需要考虑其 Orbit$\{\mathcal{E}^i(\rho)\}_{i=0}^{+\infty}$ 整体的性质。于是，我们有以下定义：

定义 3.4： 设 ρ 的 orbit 为 $\{O_i\}_{i=0}^{+\infty}$. 定义轨道维度函数 XD 与轨道保真度函数

LF_k:

$$XD(\rho) = max_{i \in N} dim(span(O_i))$$

$$LF_k(\rho) = \lim_{i \to +\infty} F(O_i, O_{i+k})$$

由于 $F(O_i, O_{i+k})$k 固定，i 增加时不会减小，上面的极限必然存在。故良定义得到保证。

下面是构造第一步. 首先定义一个序结构，然后通过几条引理找到这个序结构下的最大值:

定义 3.5: 在所有可能的 ρ 上按下面的比较关系定义一个序结构:

```
def compare(ρ1,ρ2):
    if XD(ρ1) < XD(ρ2):#返回值与比较结果相反
        return '>'
    if XD(ρ1) > XD(ρ2):
        return '<'
    if XD(ρ1) = XD(ρ2):
        for k in 1..n:
            if LF_k(ρ1) < LF_k(ρ2):
                return '<'
            if LF_k(ρ1) > LF_k(ρ2):
                return '>'
  return '=' #过程进行到这里说明二者相等
```

我们用 $\rho_1 \prec \rho_2, \rho_1 \sim \rho_2, \rho_1 \succ \rho_2$ 直接表示上面的比较关系返回 $<, =, >$ 的情况。

下面我们将找到一个这个序结构的最大值。换句话说，对于这样一个最大值 ρ, 任何 ρ' 均有 $\rho' \prec \rho$ 或 $\rho' \sim \rho$. 寻找最大值是构造的第一步，这个最大性将在后面的证明中发挥作用。

从上面的序结构中可以看出，我们首先要求 XD 也即和 Orbit 每一项的维数相关的量尽量小，然后要求 LF 也即和 Orbit 上的项间的保真度有关的量尽量大。XD 这里有着从各种可能的初态 ρ_1 中选出最小一个的作用，而 LF 有着将 ρ_1 构造出来的作用。具体我们将在后面看到。

我们将证明一些定理，它们有可能可以得到更小的 XD 或更大的 LF，除非 ρ 的 Orbit 满足这些定理的等号成立条件或边界条件，或者不满足某些前提。于是利用我们已知的在此序结构下的最大性，我们可以通过这些定理得到 Orbit 的越来越多的性质。通过这些性质，我们最后将会得到 LF_k 必须满足 Eq. (1). 然后我们将在第 9 小节中处理剩下的唯一性与分解得到的分量的性质等问题。

首先我们需要证明这样序结构确实存在最大值。下面的引理说明了定义的两个函数的某种连续性。

引理 3.4：

$$max_{i\in N}XD(\rho_i) \geq XD(\lim_{i\to+\infty}\rho_i)$$

$$\lim_{i\to+\infty}LF_k(\rho_i) = LF_k(\lim_{i\to+\infty}\rho_i)$$

引理 3.5： 存在" 最大的"ρ. 也就是说，存在 ρ 使得任何 ρ' 均有 $\rho' \prec \rho$ 或 $\rho' \sim \rho$

证明 我们先找使 $XD(\rho)$ 最小的初态 ρ 构成的集合。这是一个紧集 (lemma 3.4 可得). 然后选取这里具有最大 $LF_1(\rho)$ 的 ρ 的集合. 依此类推。 □

但是取到序结构的最大值只是构造的第一步。由于 XD, LF 均以极限或最大值的形式定义，$F(O_i, O_{i+k})$ 等值可能不是常数，难以研究。但是借助弱不动点态，我们可以在不影响序结构下最大性的前提下找到需要的初态。下面是构造第二步：

定义 3.6： 根据 lemma 3.5 选取一个最大的 ρ. 选取 ρ 的 Orbit 的一个收敛子列，记其极限为 $\rho_\blacklozenge$。如果有多种选取方式，任取一个。

我们将在后面的证明中一直使用这个初态。我们将在后面证明，我们找到的 $\rho_\blacklozenge$ 满足 Eq. (1) 的条件。也就是说，通过 ρ 的 Orbit，我们就找到 S 一个周期分解。

我们将在第小节最后证明这一结论。然后，我们将在第小节中给出唯一性与其他性质。

首先，为什么这样的构造能够使保真度恒定呢？因为根据 lemma 3.3，我们其实找了 $\mathcal{E}$ 的一个弱不动点。这个性质我们后面还会用到。

引理 3.6： $\rho_\blacklozenge$ 是弱不动点态。并且 $\rho_\blacklozenge$ 在序关系中具有最大性，即任何 ρ' 均有 $\rho' \prec \rho$ 或 $\rho' \sim \rho$

推论 3.1： 设 $\{O_i\}_{i=0}^{+\infty}$ 是 $\rho_\blacklozenge$ 的 Orbit, 那么 k 固定时，$F(O_i, O_{i+k})$ 为常数.

我们将在第 5 小节看到，我们构造的 $\rho_\blacklozenge$ 不但保真度为常数，“相似度”也是常数，“相似度”的概念将在下面给出。这些性质将在第 6 小节中发挥作用。

3.3.4 子空间与相似度，密度算子与保真度

这一小节的内容是后面几小节的基础。XD 是子空间的性质，LF 是密度算子的性质。我们从基本的子空间的性质开始研究，然后研究密度算子。definition 7 定义了作用在两个子空间上的相似度 MS，引理 3.7 说明了相似度在后面证明中起到的一个作用，definition 8 定义了最大相似子空间 $MSPOS$，lemma 3.8 是最大相似子空间的基本性质. 为了得到更深入的性质，我们定义了完全最大相似度的概念。然后在 lemma 3.9 中我们给出了完全最大相似度的正交基表示。具体证明在之前的稿子里有，这里省略了，来突出证明思路。定义之后有对应例子。lemma 3.10 是相似度的重要应用，将在第 6 小节的证明中用到。然后我们研究了密度算子的性质。我们重点关注在已知完全最大相似度的情况下密度算子的性质。以 lemma 3.11 为基础我们引出了完全最大保真度的概念，并在 lemma 3.12 中给出了从完全最大相似度得到完全最大保真度的重要性质。在这一小节的最后我们说明了 lemma 3.10，lemma 3.12, 完全最大保真度的概念在后面的具体应用。

然后介绍一个技巧，这个技巧最早在 lemma 3.8 中得到应用。保真度有性质：$F(\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)) \geq F(\rho_1, \rho_2)$. 结合 $MS, MSPOS$ 我们可以得到下面的思路：假设 $span(\rho_1) = S_1, span(\rho_2) = S_2$. 取 $|\varphi\rangle \in S_1, |\phi\rangle \in S_2$ 使得 $|\langle\varphi|\phi\rangle|$ 最大, 此时 $F(\varphi, \phi)$ 自然也为最大值。然而 $F(\mathcal{E}(\varphi), \mathcal{E}(\phi))$ 大于等于这个值。如果我们可以通过其他途径得到 $F(\mathcal{E}(\varphi), \mathcal{E}(\phi))$ 的限制使得它小于等于某个值，如 $span(\rho_1)$,$span(\rho_2)$ 为 BSCC，ρ_1, ρ_2 为弱不动点态, 或者给定一些条件限制 $MS(span(\rho_1), span(\rho_2))$

的上界等，我们就可以得到 $F(\mathcal{E}(\varphi),\mathcal{E}(\phi)) = F(\varphi,\phi)$. 而等号成立有往往意味着 $\mathcal{E}(\varphi),\mathcal{E}(\phi)$ 之间存在某种关系。这可以反映出 $\mathcal{E}$ 结构上的很多性质。lemma 3.8 的证明是这一方法的体现。lemma 3.16 也间接体现了这一技巧。

在这一小节中，我们将先研究子空间。先引入两个作用在子空间上的算子 $MS, MSPOS$.

定义 3.7： 对子空间 S_1, S_2 定义相似度 $MS(S_1, S_2)$ 如下:

$$MS(S_1, S_2) = max_{|\varphi\rangle\in S_1}|P_{S_2}(|\varphi\rangle)|$$

首先，MS 是良定义的。因为紧集上的连续函数必能取到最值，定义中使用 max 是合理的。然后，我们有 $MS(S_1, S_2) = MS(S_2, S_1)$。也就是说，$MS$ 是两个子空间相互之间的性质。MS 是 $|\varphi\rangle \in S_1$ 和 $|\phi\rangle \in S_2$ 的最大内积的模，表示两个子空间的“最近位置”的“相似度”。如果两个子空间正交，它们的相似度为 0. 如果两个子空间的交空间维数大于 0，那么其相似度为 1.

例 3.3： $S_1 = span(|0\rangle, |1\rangle)$, $S_2 = span(\frac{|0\rangle+|2\rangle}{\sqrt{2}}, \frac{|1\rangle+|3\rangle}{\sqrt{2}})$, $S_3 = span(\frac{|0\rangle+|2\rangle}{\sqrt{2}}, \frac{|1\rangle+|2\rangle}{\sqrt{2}})$, $S_4 = span(|2\rangle, |3\rangle)$, 那么 $MS(S_1, S_2) = MS(S_2, S_4) = \frac{1}{\sqrt{2}}$, $MS(S_1, S_3) = |\frac{\langle 0|-\langle 1|}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}| = 1$, $MS(S_2, S_3) = |\frac{\langle 0|+\langle 2|}{\sqrt{2}}\frac{|0\rangle+|2\rangle}{\sqrt{2}}| = 1$.

为什么定义“相似度”的概念呢？我们将看到，相似度具有与保真度类似的单调性：

引理 3.7： $MS(S_1, S_2) \leq MS(\mathcal{E}(S_1), \mathcal{E}(S_2))$

我们在第 5 小节有关 weak fixed point state 的性质的证明中将用到这一性质。我们后面将看到，由于弱不动点态的性质 (lemma 3.13), 我们后面小节的证明中，遇到的一般是等号成立的情况。而目前我们对等号成立的具体条件并不了解。等号成立的情况这是我们感兴趣的情况，我们下面将推出一些性质，最终得到一个将在第 6 小节的证明中用到的引理：lemma 3.10。为了研究等号成立条件下的性质，我们需要再定义一些概念。第一个问题是，$MS(S_1, S_2)$ 是 $|\varphi\rangle \in S_1$ 和 $|\phi\rangle \in S_2$ 的最大内积的模, $|\varphi\rangle$ 和 $|\phi\rangle$ 可以在什么范围内取呢?

定义 3.8： S_1, S_2 是两个子空间, 定义 S_1 内到 S_2 的最大相似子空间 $MSPOS_{S_1}(S_2)$ 为 S_1 内的态中满足 $|P_{S_2}(|\varphi\rangle)| = MS(S_1, S_2)$ 的态的集合。

我们之所以把集合叫做子空间，因为有下面的定理。

引理 3.8： $MSPOS_{S_1}(S_2)$ 为 S_1 中的子空间. 进一步，设 S_1 内到 S_2 的最大相似子空间为 S_3，S_2 内到 S_1 的最大相似子空间为 S_4，我们有:

1. $dim(S_3) = dim(S_4), MS(S_1, S_2) = MS(S_3, S_4)$
2. $MSPOS_{S_3}(S_4) = S_3, MSPOS_{S_4}(S_3) = S_4$

$MSPOS$ 的直观含义是一个子空间上可以取到对另一个子空间的“最近”(投影之模等于 MS) 的位置的集合，由引理知 $MSPOS_{S_1}(S_2)$ 得到 S_1 中的子空间, $MSPOS_{S_2}(S_1)$ 得到 S_2 中的子空间。

例 3.4： 在上面的例子中， $MSPOS_{S_1}(S_2) = S_1$， $MSPOS_{S_2}(S_1) = S_2$, $MSPOS_{S_1}(S_3) = MSPOS_{S_3}(S_1) = span(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$. 如果 $S_5 = span(\frac{|0\rangle+|1\rangle+|2\rangle+|3\rangle}{2})$, 那么

$$MSPOS_{S_1}(S_5) = span(\frac{|0\rangle + |1\rangle}{\sqrt{2}})$$
$$MSPOS_{S_5}(S_1) = span(\frac{|0\rangle + |1\rangle + |2\rangle + |3\rangle}{2})$$

进一步，引理告诉我们如果我们取 S_1 内到 S_2 的最大相似子空间为 S_3，S_2 内到 S_1 的最大相似子空间为 S_4，它们确实处在“最大”的状态。一方面，S_3, S_4 是所有能取到对另一个子空间的“最近距离”(MS) 的位置的集合，另一方面，对 S_3, S_4 再取 $MSPOS$, 它们不再变化。我们给 S_3, S_4 这种子空间取一个名字。

定义 3.9： 如果 S_1,S_2 满足 $S_1 = MSPOS_{S_1}(S_2)$, $S_2 = MSPOS_{S_2}(S_1)$ 我们说 S_1, S_2 完全最大相似度。

完全最大相似度具有下面的性质：

引理 3.9：

1. 设 S_1, S_2 完全最大相似度，记 S_1 在 $S_1 \oplus S_2$ 中的正交补为 $S_1^{\perp}$, $dim(S_1) = dim(S_1) = dim(S_1^{\perp})$ 的值为 n. 那么可以在 $S_1, S_1^{\perp}$ 中分别选取正交基 $\{|\varphi_i\rangle\}_n$,$\{|\chi_i\rangle\}_n$, 使得 $S_2 = span(C\{|\varphi_i\rangle\}_n \boxplus \sqrt{1-C^2}\{|\chi_i\rangle\}_n)$
2. 设 $\{|\varphi_i\rangle\}_n$,$\{|\chi_i\rangle\}_n$ 分别是 $S_1, S_1^{\perp}$ 的正交基, $\alpha_1, \alpha_2, \beta_1, \beta_2 \in C$ 满足 $|\alpha_1|^2+|\beta_1|^2 = |\alpha_2|^2+|\beta_2|^2 = 1$, 则 $span(\alpha_1\{|\varphi_i\rangle\}_n \boxplus \beta_1\{|\chi_i\rangle\}_n)$ 与 $span(\alpha_2\{|\varphi_i\rangle\}_n \boxplus \beta_2\{|\chi_i\rangle\}_n)$ 完全最大相似度，相似度为 $|\alpha_1^{+}\alpha_2 + \beta_1^{+}\beta_2|$.

也就是说，完全最大相似度与能在相同的基下用 $span(\boxplus)$ 形式表示是等价的。这个基表示便于一些问题的证明，将在第 7 小节的证明中用到。完全最大相似度的概念将在第 6 小节中使用，我们需要这个概念作为工具。这一小节后面的完全最大保真度的研究中也会使用这个概念。一方面完全最大相似度是完全最大保真度的必要条件，另一方面，我们将会经常在两个完全最大相似度的子空间上考虑完全最大保真度的密度算子。

前面说过，我们对 $MS(S_1, S_2) = MS(\varepsilon(S_1), \mathcal{E}(S_2))$ 的情况感兴趣。具体就是下面的定理，在第 6 小节的证明中将会用到，也是小节开始时说的技巧的体现。具体应用我们将在这一小节的最后具体说明。

引理 3.10： 量子 markov 链 $G = (H, \mathcal{E})$，子空间 S_1, S_2 满足：$MS(S_1, S_2) = MS(\mathcal{E}(S_1), \mathcal{E}(S_2)) = C$，设它们间的最大相似子空间为

$$
\begin{aligned}
B_1 &= MSPOS_{S_1}(S_2) \\
C_1 &= MSPOS_{S_2}(S_1) \\
B_2 &= MSPOS_{\mathcal{E}(S_1)}(\mathcal{E}(S_2)) \\
C_2 &= MSPOS_{\mathcal{E}(S_2)}(\mathcal{E}(S_1))
\end{aligned}
$$

我们有 $\mathcal{E}(B_1) \subseteq B_2, \mathcal{E}(C_1) \subseteq C_2$.

这个定理大体上说，如果我们有 $S_1, S_2, \mathcal{E}(S_1), \mathcal{E}(S_2)$ 并且满足一定的性质，我们可以知道 S_1, S_2 中的一个（可能）维度更小的子空间在 $\mathcal{E}$ 作用下的表现。在第 6 节中我们将使用这个定理尝试降低某个子空间的维度。

接下来研究子空间上的密度算子，在后面的证明中，我们将需要研究完全最大相似度的两个子空间上的密度算子。首先，我们有下面的定理，作为基础：

定理 3.2： 设 $S_1 = span(\rho_1), S_2 = span(\rho_2)$. 则 $F(\rho_1, \rho_2) \le MS(S_1, S_2)$. 等号成立仅当下列两种情况之一成立：

1. $\rho_1 \perp \rho_2$
2. $MS(S_1, S_2) > 0$, 此时必须有 $dim(S_1) = dim(S_2) = n$ 并且存在 S_1 的正交基 $\{|\varphi_i\rangle\}_n$, S_2 的正交基 $\{|\phi_i\rangle\}_n$, 系数 $\{c_i\}_n$ 使得 (1)$\forall i |\langle\varphi_i|\phi_i\rangle| = MS(S_1, S_2)$, (2)$\rho_1 = \sum_i c_i \varphi_i$, $\rho_2 = \sum_i c_i \phi_i$.

这个定理是直观的。如果要让 $F(\rho_1,\rho_2)$ 在 $MS(span(\rho_1), span(\rho_2))$ 是某个定值的情况下尽可能大的话，值最大时应该满足二者的分解式中的态可以按照 $|\langle\varphi_i|\phi_i\rangle| = MS(S_1,S_2)$ 的关系对应起来.

例 3.5： $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|, \rho_2 = \frac{1}{4}(|0\rangle + |2\rangle)(\langle 0| + \langle 2|) + \frac{1}{4}(|1\rangle + |3\rangle)(\langle 1| + \langle 3|)$ 使等式成立，而 $\rho_1, \rho_3 = \frac{1}{8}(|0\rangle + |2\rangle)(\langle 0| + \langle 2|) + \frac{3}{8}(|1\rangle + |3\rangle)(\langle 1| + \langle 3|)$ 只能满足不等关系。

我们注意到，上面定理的第二个情况其实蕴含 S_1, S_2 完全最大相似度（与情况 2 中的条件 1 等价）。而且，我们还对密度矩阵的分解有要求（情况 2 中的条件 2）。也就是说，$F(\rho_1,\rho_2) = MS(span(\rho_1), span(\rho_2))$ 是比 $span(\rho_1), span(\rho_2)$ 完全最大相似度更强的要求。另一方面，如果我们给出完全最大相似度的两个子空间 S_1, S_2, 我们可以根据这个定理的等号成立条件构造出两个子空间中的密度算子 ρ_1,ρ_2 使 $F(\rho_1,\rho_2)$ 尽量大。

等号成立的情况我们将在后面遇到。我们给出下面的定义：

定义 3.10： 如果 ρ_1,ρ_2 满足 $F(\rho_1,\rho_2) = MS(span(\rho_1), span(\rho_2))$, 我们说 ρ_1,ρ_2 完全最大保真度。

例 3.6： $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|, \rho_2 = \frac{1}{4}(|0\rangle + |2\rangle)(\langle 0| + \langle 2|) + \frac{1}{4}(|1\rangle + |3\rangle)(\langle 1| + \langle 3|)$ 完全最大保真度，保真度为 $\frac{1}{\sqrt{2}}$。这也是 $span(\rho_1), span(\rho_2)$ 的相似度。而 ρ_1, $\rho_3 = \frac{1}{8}(|0\rangle + |2\rangle)(\langle 0| + \langle 2|) + \frac{3}{8}(|1\rangle + |3\rangle)(\langle 1| + \langle 3|)$ 不是完全最大保真度的，但是 $span(\rho_1), span(\rho_2)$ 完全最大相似度，相似度为 $\frac{1}{\sqrt{2}}$。

由 lemma 3.11 得出：

1. ρ_1,ρ_2 完全最大保真度，保真度为 C，那么 $span(\rho_1), span(\rho_2)$ 一定完全最大相似度，相似度为 C。
2. $F(\rho_1,\rho_2) = MS(span(\rho_1), span(\rho_2)) \Leftrightarrow \rho_1 \perp \rho_2$ 或 ρ_1,ρ_2 完全最大保真度且 $F(\rho_1,\rho_2) > 0$.

由 1 想到，我们可以先使用相似度的性质研究 $span(\rho_1), span(\rho_2)$ 的性质，如果得到了完全最大相似度的结论，我们可以通过完全最大相似度的两个子空间得到完全最大保真度的两个密度算子。完全最大保真度的基表示我们在 lemma 3.11 中已经有了。但我们后面还需要更进一步的结论即下面的引理。

引理 3.11: S_1, S_2 是 $G=(H,\mathcal{E})$ 中两个完全最大相似度的子空间, 相似度 $C>0$, $span(\mathcal{E}(S_1)) \subseteq S_2$, 那么存在两个密度算子 $\rho_1 \in S_1$, $\rho_2 \in S_2$, 满足 (1)$\mathcal{E}(\rho_1)=\rho_2$, (2)$\rho_1, \rho_2$ 完全最大保真度，保真度为 C.

证明思路: S_1, S_2 是完全最大相似度,那么我们可以使用 $span(\boxplus)$ 形式表示这两个子空间，再根据这样的表示中的基构造一个酉变换 U 把 S_2 中的态映射到 S_1 中"对应" 的态 (所谓对应是指内积的模为它们的相似度)。那么 S_1 就成了 $U\circ\mathcal{E}$ 的一个不变子空间,必有 fixed point state ρ_1。把 ρ_1 按 U 的逆变换映射回 S_2 中即得 ρ_2.

在第 6 小节的证明中，我们将会需要在两个完全最大相似度，相似度大于 0 的子空间上构造 $\rho, \mathcal{E}(\rho)$ 使得 $F(\rho,\mathcal{E}(\rho))$ 尽量大。这时可以使用这个引理。根据完全最大保真度的定义,这个引理得到的 ρ 确实使得 $F(\rho,\mathcal{E}(\rho))$ 最大.

由保真度的性质我们有 $F(\rho_1,\rho_2) \le F(\mathcal{E}(\rho_1),\mathcal{E}(\rho_2))$。在第 8 小节的证明中，我们将遇到 ρ_1, ρ_2 完全最大保真度，$\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)$ 完全最大保真度并且保真度相等的情况。我们将在第 7 小节中研究其性质。

小结与在后面的应用

我们在研究子空间与密度算子时采用了类似的过程：首先引入概念：对于子空间是“相似度”，对于密度算子是已存在的保真度。然后对于相似度，我们有 lemma 3.7，与保真度类似；我们对 lemma 3.7 等号成立的情况，有定理 3.10，而对保真度，我们研究的是在有“完全最大保真度”的条件下 $F(\rho_1,\rho_2)=F(\mathcal{E}(\rho_1),\mathcal{E}(\rho_2))>0$ 成立的情况，这部分我们将放在第 7 小节研究。

这一小节中的大部分引理定义是作为第 5 和第 7 小节的定理定义的基础, 但 3.10，3.12 会直接用到第 6 小节的证明中。在第 6 小节中我们将按照这样的方式应用这一小节中的引理（大家可以参见 Example 3.5）: 我们研究 $\rho, \mathcal{E}(\rho)$. 首先我们利用 3.10 得到 $span(\rho), span(\mathcal{E}(\rho))$ 完全最大相似度。虽然 3.10 看起来结论并没有得到某两个子空间完全最大相似度，但是在第五节证明的环境下，如果他们不是完全最大相似度的，我们可以利用 3.10 得到矛盾。然后我们可以利用 3.12，在第 5 小节证明的环境下，得到 $\rho, \mathcal{E}(\rho)$ 完全最大保真度。进一步的处理将使用第 7 小节的结论，在第 8 小节进行。我们将在后面介绍。

详细的说，在第 6 小节的证明中，我们将会需要能够构造具有更小的 $max(dim(\rho), dim(\mathcal{E}(\rho)))$ 或者更大的 $F(\rho,\mathcal{E}(\rho))$ 的定理。因为之前我们找的 $\rho_\blacklozenge$

是在 XD 尽量小，LF 尽量大的情况下构造出的，如果能够在一定条件下应用这样的定理，引出矛盾，就可以得到一些结果，比如定理应用条件不成立或某条件中等号必须取到等。减小维数就是使用 lemma 3.10. 3.10 的应用有可能减小 $max(dim(\rho), dim(\mathcal{E}(\rho)))$。导出矛盾的结果是我们得到了完全最大相似度的性质。

lemma 3.12 中找 $F(\rho, \mathcal{E}(\rho))$ 的最大值是为了试图找到与 $\rho_\blacklozenge$ 的 LF 的最大性的矛盾。我们的 3.12 其实已经解决了完全最大相似度的两个子空间上构造 ρ 来取到最大的 $F(\rho, \mathcal{E}(\rho))$ 的问题。只是第 6 小节证明中这里可能不是 $\mathcal{E}$ 而是其幂。由 $\rho_\blacklozenge$ 的 LF 的最大性我们将能够证明 $F(\rho, \mathcal{E}(\rho))$ 完全最大保真度，这也是我们将在第 6 小节得到的结论。

得到完全最大保真度后，我们将在第 7 小节中研究这一情况的进一步处理。

3.3.5 弱不动点态与相似度

前面研究了 weak fixed point state，又研究了相似度保真度等性质。这一小节只有一个定理，说明 weak fixed point state 的一个相似度的性质：

引理 3.12： 如果 ρ 是 $G = (H, \mathcal{E})$ 的一个 weak fixed point state, 密度算子序列 $\{O_i\}_{i=0}^{+\infty}$ 是 ρ 的 Orbit，设 $S_i = span(O_i)$, 我们有 $MS(S_i, S_{i+k})$ 在 k 固定时是不随 i 变化的常数.

弱不动点态对于保真度和相似度都具有这样的性质，是因为保真度和相似度具有类似的特性。一个是 lemma 3.7 与保真度性质类似。另一个是二者都具有一定程度的“连续性”。这个相似性隐含在证明中而不是直接由定理体现。

3.3.6 证明主线第二部分: 利用弱不动点态与相似度得到的结论

回忆 aperiodic BSCC 的定义。如果一个 BSCC S 不是 aperiodic BSCC，也就是说 $\exists |\varphi\rangle \in S, \forall i, dim(span(\mathcal{E}^i(\varphi))) < dim(S)$. 那么我们有 $XD(\varphi) < dim(S)$。也就是说，$\rho_\blacklozenge$ 一定不会是 S 的不动点态。

我们考虑 $\rho_\blacklozenge$ 的性质。我们已经知道 $F(O_i, O_{i+k}) = LF_k(\rho_\blacklozenge)$ 为定值。然后，我们可以假设使 $LF_k(\rho_\blacklozenge) > 0$ 的最小的 k 为 K. 于是我们的问题是，如何处理 O_i, O_{i+K} 之间的关系？我们的目标是证明 $F(O_i, O_{i+K}) = 1$. 这一节中，我们先用第 4 第 5 小节的引理证明 O_i, O_{i+K} 完全最大保真度。也就是下面的引理。

引理 3.13： S 是 $G=(S,\mathcal{E})$ 的一个 BSCC, 但不是 aperiodic BSCC. 我们根据 definition 6 得到 $\rho_\blacklozenge$, 设其 Orbit 为 $\{O_i\}_{i=0}^{+\infty}$, 那么我们有:

$$\begin{cases} \forall i \in N, O_i \perp O_{i+k} & \text{when } 1 \le k < K \\ \forall i \in N, O_i, O_{i+k}\text{完全最大保真度}, F(O_i, O_{i+K}) > 0\text{且为常数} & \text{when } k = K \end{cases}, \text{for some } K \in N$$

在证明这个引理之前，我们举几个例子，来具体说明我们这个证明的思路和之前一系列引理的来源。

例 3.7：

1. 使用前面举过的例子。假设 $H=C^3$。$\mathcal{E}$ 为这样的算符：首先将态 $|\varphi\rangle$ 在基 $|0\rangle,|1\rangle,|2\rangle$ 下作投影，然后作酉变换：$U|0\rangle=|1\rangle, U|1\rangle=|2\rangle, U|2\rangle=|0\rangle$. 我们可以直观地看出 $p=3$，全部的弱不动点态为 $c_0|0\rangle\langle 0|+c_1|1\rangle\langle 1|+c_2|2\rangle\langle 2|$。想象对这个 Markov chain 进行前面的证明过程。我们得到弱不动点态 $\rho_\blacklozenge$, 及其 Orbit, XD, LF_k 等值，我们要利用其 Orbit，尝试在某些条件不成立的情况下构造出更小 XD 或在 XD 相等情况下有更大 LF 的初态，从而产生矛盾，来证明这些条件必然成立。我们考虑一下 $\mathcal{E}$ 的在序关系下不为最大的弱不动点态的 Orbit 都有哪些特征，分别该如何处理。
   $\rho=\frac{1}{3}|0\rangle\langle 0|+\frac{2}{3}|1\rangle\langle 1|$. 设其 Orbit 为 $\{O_i\}_{i=0}^{\infty}$, $span(O_i)=S_i$. 计算得

$$O_1=\mathcal{E}(\rho)=\frac{1}{3}|1\rangle\langle 1|+\frac{2}{3}|2\rangle\langle 2|$$
$$O_2=\mathcal{E}^2(\rho)=\frac{1}{3}|2\rangle\langle 2|+\frac{2}{3}|0\rangle\langle 0|$$

   S_0,S_1 完全最大相似度，相似度为 1.$S_1=\mathcal{E}(S_0), S_2=\mathcal{E}(S_1)$ 完全最大相似度，相似度为 1. 使用 lemma 3.10，取 MSPOS 即得具有更小的态：

$$MSPOS_{S_1}(S_0)=span(|1\rangle)$$

   取 $\rho=|1\rangle\langle 1|$ 即可使 XD 更小。
2. 假设 $H=C^4$。$\mathcal{E}$ 为这样的算符：首先将态 $|\varphi\rangle$ 在基 $|0\rangle,|1\rangle,|2\rangle,|3\rangle$ 下作投影，然后作酉变换：$U|0\rangle=|1\rangle, U|1\rangle=|2\rangle, U|2\rangle=|3\rangle, U|3\rangle=|0\rangle$. 我们可以直

观地看出 $p=4$, 全部的弱不动点态为 $c_0\left|0\right\rangle\left\langle 0\right|+c_1\left|1\right\rangle\left\langle 1\right|+c_2\left|2\right\rangle\left\langle 2\right|+c_3\left|3\right\rangle\left\langle 3\right|$ 与上面的例子类似，对下面的初态 ρ, 我们考虑如何处理。

$\rho=\frac{1}{3}\left|0\right\rangle\left\langle 0\right|+\frac{2}{3}\left|2\right\rangle\left\langle 2\right|$. 设其 Orbit 为 $\{O_i\}_{i=0}^{\infty}$, $span(O_i)=S_i$. 计算得

$$
\begin{aligned}
O_1=\mathcal{E}(\rho)&=\frac{1}{3}\left|1\right\rangle\left\langle 1\right|+\frac{2}{3}\left|3\right\rangle\left\langle 3\right| \\
O_2=\mathcal{E}^2(\rho)&=\frac{1}{3}\left|2\right\rangle\left\langle 2\right|+\frac{2}{3}\left|0\right\rangle\left\langle 0\right| \\
O_3=\mathcal{E}^3(\rho)&=\frac{1}{3}\left|3\right\rangle\left\langle 3\right|+\frac{2}{3}\left|1\right\rangle\left\langle 1\right|
\end{aligned}
$$

S_0,S_1 正交.$S_1=\mathcal{E}(S_0),S_2=\mathcal{E}(S_1)$ 正交, 使用不了 lemma 3.10。又有 $S_0=S_2,S_1=S_3$, 使用 lemma 3.10 取 $MSPOS$ 得不到非平凡的结果。于是：

由于 $S_0,\mathcal{E}^2(S_0)$ 完全最大相似度，相似度为 1，根据 lemma 3.12 我们可以找到 $\rho\in S_0$ 使得 $F(\rho,\mathcal{E}^2(\rho))=MS(S_0,S_2)=1>F(O_0,O_2)$. 于是我们找到了更大的 LF_2.（LF_1 本来就是 0，不需要更大）。

证明 设 $S_i=span(O_i)$.

由于 $\rho_\blacklozenge$ 为 weak fixed point state, 根据 lemma 3.2, 3.13，$F(O_i,O_{i+K})$, $MS(S_i,S_{i+K})$ 均为只与 K 有关的定值。

选取最小的 K 使得 $F(O_i,O_{i+K})>0$。也就是说，当 $0<k<K$ 时 $LF_k=0$, $LF_K>0$. 首先，显然必须有 $K\le dim(S)$.

如果 $F(O_i,O_{i+K})=1$, 引理自动成立.

如果 $F(O_i,O_{i+K})=MS(S_i,S_{i+K})$，也就是说它们是完全最大保真度且 $F(O_i,O_{i+K})>0$(definition 10 下面的总结 (2)), 引理也自动成立.

由 theorem 3.11 $F(O_i,O_{i+K})\le MS(S_i,S_{i+K})$. 于是剩下的情况是 $F(O_i,O_{i+K})<MS(S_i,S_{i+K})$. 对于这种情况，我们将利用 $\rho_\blacklozenge$ 在序关系下最大的性质得出矛盾。

如下构造两列子空间 $\{B_i\}_{n=0}^{+\infty}$ 和 $\{C_i\}_{n=0}^{+\infty}$:

$$B_i=MSPOS_{S_i}(S_{i+K})$$

$$C_i=MSPOS_{S_{i+K}}(S_i)$$

根据 lemma3.10, $\mathcal{E}(B_i) \subseteq B_{i+1}$,$\mathcal{E}(C_i) \subseteq C_{i+1}$.

然后根据 C_i 的定义我们有 $dim(C_i) \leq dim(S_{i+K})$ 下面分类讨论是否存在 i 使得二者相等:

1. 如果 $\forall i, dim(C_i) < dim(S_{i+K})$ 成立, 任取 $\rho' \in C_0$, 将会有 $\mathcal{E}^i(\rho') \in C_i \subset S_{i+K}$, 故 $dim(\mathcal{E}^i(\rho')) < dim(S_{i+K})$, 故 $XD(\rho') < XD(\rho)$, 和 $\rho_\blacklozenge$ 在序关系下最大违背.
2. 如果 $\exists i, dim(C_i) = dim(S_{i+K})$ 那么 $\mathcal{E}^K(B_i) \in S_{i+K} = span(C_i)$. 由于 B_i 与 C_i 是完全最大相似度 (上面构造过程,lemma3.8(2) 和完全最大相似度定义)。于是根据 Lemma 3.12，我们可以找到 ρ' 满足 $\rho' \in B_i$，并且

$$F(\rho', \mathcal{E}^K(\rho')) = MS(S_i, S_{i+K}) > F(O_i, O_{i+K})$$

于是我们得到 ρ'，它有更大的 LF_K，且 XD 值不变，而 $1 \leq k < K$ 时 $LF_k(\rho_\blacklozenge)$ 已经是 0，不可能更小, 这样与 $\rho_\blacklozenge$ 的序关系下最大性违背.

于是唯一的可能是 $\forall i, O_i$ 和 O_{i+K} 完全最大保真度，$F(O_i, O_{i+K}) > 0$. 由 $\rho_\blacklozenge$ 是 weak fixed point state 和 lemma 3.2 知其为常数。 □

3.3.7 完全最大保真度的密度算子的进一步的性质

在前面的证明的结果中，我们现在面对的情况大致可以简单描述为:

已知 ρ_1, ρ_2 完全最大保真度，$\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)$ 完全最大保真度，$F(\rho_1, \rho_2) = F(\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)) > 0$，如何得出进一步的结论?

我们现在有 ρ_1, ρ_2 在 $\mathcal{E}$ 作用下的值。我们希望找到其他 ρ, 使得 $\mathcal{E}(\rho)$ 能够确定。我们可以先直观地想一下。由 ρ_1, ρ_2 完全最大保真度，我们可以想象夹在 ρ_1, ρ_2“中间”的一个密度算子。考虑这个算子的目的是我们要构造一个使得 $(F(\rho_1, \rho))^2 + (F(\rho_2, \rho))^2$ 最大的 ρ. 我们可以先在 Bloch 球上直观想象 ρ_1, ρ_2 均为纯态时的情况。我们在 definition 11 中对纯态引入 MID 算符使这个值最大，并在定以后给出了例子和描述。密度算子时的情况可以由纯态 MID 算符和完全最大保真度的密度算子的基表示定义。我们同样有 $(F(\rho_1, \rho))^2 + (F(\rho_2, \rho))^2$ 最大。由保真度的性质，我们将得到 $(F(\mathcal{E}(\rho_1), \mathcal{E}(\rho)))^2 + (F(\mathcal{E}(\rho_1), \mathcal{E}(\rho)))^2$ 不小于这个值。但是 $\mathcal{E}(\rho_1), \mathcal{E}(\rho_2)$ 完全最大保真度并且和 ρ_1, ρ_2 具有相等的保真度，通过考虑 $F(\mathcal{E}(\rho_1), \rho') + F(\mathcal{E}(\rho_2), \rho')$ 取到最大值的 ρ',$\mathcal{E}(\rho)$ 将可以唯一确定。也就是说，

我们只需要 $\rho_1, \mathcal{E}(\rho_1)$，$\rho_2, \mathcal{E}(\rho_2)$ 的性质，就可以得到某个新的 ρ 对应的 $\mathcal{E}(\rho)$ 的值。

更进一步地，我们可以 "递归" 地得到无穷多个 $\mathcal{E}(\rho)$ 的值。最终，我们将证明 MID 算符是 $DenM$ 表示的密度算子的特殊情况，并给出所有能够用 $\boxed{DenM}$ 算符表示的密度算子被 $\mathcal{E}$ 作用后的结果。MID 和 $AXLE$ 算符是 $\boxed{DenM}$ 能够表示的情况之一，将在下面的证明中用到。

我们将先从 MID 入手，然后给出一般的定理作为这一小节的主定理。然后我们在第 8 小节将使用这个定理的推论推进周期分解定理的证明。$MID, AXLE$ 的性质是两个特例。一般情况下，我们使用 MID 即可构造出来。但是有一种情况下 MID 是无效的。我们将给这种特殊情况起一个名字，然后针对这种情况使用 $AXLE$ 算子解决。具体为:

我们先给出两个算子 MID 与 $AXLE$. 我们先在纯态上定义它们，再把它推广到完全最大保真度的密度算子上。在纯态上定义时的性质可以直接通过几何方法证明，推广到密度算子上时需要使用第 3 小节中对于完全最大保真度的相关结果证明。然后我们把第 3 小节里常用到的 $span(\boxplus)$ 形式推广到密度算子上得到 $\boxed{DenM}(\boxplus)$ 形式的密度算子表示形式，并发现 MID 与 $AXLE$ 都是 $\boxed{DenM}(\boxplus)$ 形式的特殊情况。虽然如此，我们后面直接使用的是更方便的 $AXLE,MID$ 两个算子而不是更广泛的 $\boxed{DenM}$ 和 $\boxplus$. 然后我们证明 $\boxed{DenM}(\boxplus)$ 相关的一个性质，也是这一小节的主定理.15。MID 与 $AXLE$ 上的性质是这个主定理的特殊情况。然后我们得到了一些可以在后面应用到的定理，并定义了 fidelity$C$ cyclic 的概念方便描述。corollary 3.16.1、3.16.2, lemma 3.17, 3.18 将在第 8 小节的证明中用到。

定义 3.11:　两个纯态 $|\varphi_1\rangle, |\varphi_2\rangle$, 二者不正交, 设 $|\varphi_3\rangle$ 使得 $|\langle\varphi_1|\varphi_3\rangle|^2 + |\langle\varphi_2|\varphi_3\rangle|^2$ 最大，记这样的 $|\varphi_3\rangle$ 的集合为 $MID(|\varphi_1\rangle, |\varphi_2\rangle)$.

定义 3.12:　对两个纯态 $|\varphi_1\rangle, |\varphi_2\rangle$, $|\langle\varphi_1|\varphi_2\rangle| = C \in (0, 1)$ 定义 $AXLE(|\varphi_1\rangle, |\varphi_2\rangle)$ 为满足下述条件的纯态 $|\varphi\rangle$ 的集合:

1. $|\varphi\rangle \in span(|\varphi_1\rangle, |\varphi_2\rangle)$
2. $|\langle\varphi|\varphi_1\rangle| = |\langle\varphi|\varphi_2\rangle| = \frac{1}{\sqrt{2}}$
3. 在 $span(|\varphi_1\rangle, |\varphi_2\rangle)$ 的 Bloch 球上，从 $|\varphi_1\rangle$ 到 $|\varphi_2\rangle$ 的旋转角度在 $(0, \pi)$ 间的旋转与 $|\varphi_3\rangle$ 的位置满足左手定则

从 Bloch 球上可以直观地看到，MID 与 $AXLE$ 的值均为 $span(|\varphi_1\rangle, |\varphi_2\rangle)$ 内的

一维子空间中，也就是说除去一个无影响的相位结果为一确定的纯态。在 Bloch 球上，$MID(|\varphi_1\rangle, |\varphi_2\rangle)$ 落在两个态的中间，而 $AXLE(|\varphi_1\rangle, |\varphi_2\rangle)$ 处在与 $|\varphi_1\rangle, |\varphi_2\rangle$ 均垂直的位置上。但是这样的位置有两处，并恰好位于正交的位置上，于是需要条件（3）确定。

例 3.8： $MID(|0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}) = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, AXLE(|0\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}) = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$

MID 和 $AXLE$ 可以推广到完全最大相似度，相似度 >0 的子空间上，不过用处不大，跳过（定义这些东西可以把完全最大保真度相关的一些定理证明写得更清楚，但是本身用处不大）。下面把 MID 和 $AXLE$ 推广到完全最大保真度, 保真度 >0 的密度算子上。

定义 3.13： ρ_1, ρ_2 是两个密度算子，ρ_1, ρ_2 完全最大保真度，$\rho_1, \rho_2 > 0$，$\rho_1 = \sum_i c_i\varphi_i$, $\rho_2 = \sum_i c_i\phi_i$, $|\langle\varphi_i|\phi_i\rangle| = C$, $|\varphi_i\rangle, |\phi_i\rangle$ 分别是 $span(\rho_1), span(\rho_2)$ 的正交基, 定义 $MID(\rho_1, \rho_2) = \sum_i c_i MID(\varphi_i, \phi_i)$, 其中 $MID(\varphi_i, \phi_i)$ 为纯态 $MID(|\varphi_i\rangle, |\phi_i\rangle)$ 对应的密度算子。

定义 3.14： ρ_1, ρ_2 是两个密度算子, ρ_1, ρ_2 完全最大保真度，$F(\rho_1, \rho_2) \in (0, 1)$, 设 $\rho_1 = \sum_{i=1}^n c_i\varphi_i$, $\rho_2 = \sum_{i=1}^n c_i\phi_i$, $|\langle\varphi_i|\phi_i\rangle| = C$, $|\varphi_i\rangle, |\phi_i\rangle$ 分别是 $span(\rho_1)$, $span(\rho_2)$ 的正交基, 定义 $AXLE(\rho_1, \rho_2) = \sum_{i=1}^n c_i AXLE(\varphi_i, \phi_i)$, 其中 $AXLE(\varphi_i, \phi_i)$ 为纯态 $AXLE(|\varphi_i\rangle, |\phi_i\rangle)$ 对应的密度算子

也就是说，MID 和 $AXLE$ 两个算符作用在两个纯态上，得到一维子空间；作用在两个完全最大保真度的密度算子上，得到一个密度算子。

我们注意到，MID 和 $AXLE$ 两个算符都可以用 $\{c_i\}_n \boxed{DenM} (\alpha\{|\varphi_i\rangle\}_n \boxplus \beta\{|\chi_i\rangle\}_n)$ 的形式表达。也就是说,MID 与 $AXLE$ 都是 $\{c_i\}_n \boxed{DenM} \alpha\{|\varphi_i\rangle\}_n \boxplus \beta\{|\chi_i\rangle\}_n)$ 形式的特例，也就是下面的引理：

引理 3.14： 设 S_1, S_2 是 H 的两个子空间, $dim(S_1) = dim(S_2) = n$, $S_1 \perp S_2$, $\{|\varphi_i\rangle\}_n$, $\{|\chi_i\rangle\}_n$ 分别是 S_1 和 S_2 的正交基, 满足 (α_1, β_1) 与 (α_2, β_2) 均模长为 1 且不正交.

$$\rho_1 = \{c_i\}_n \boxed{DenM} \alpha_1\{|\varphi_i\rangle\}_n \boxplus \beta_1\{|\chi_i\rangle\}_n)$$
$$\rho_2 = \{c_i\}_n \boxed{DenM} \alpha_2\{|\varphi_i\rangle\}_n \boxplus \beta_2\{|\chi_i\rangle\}_n)$$

(也即 ρ_1,ρ_2 表达式区别仅在 α,β). 那么

1.

$$MID(\rho_1,\rho_2)=\{c_i\}_n \boxed{DenM} (\alpha_{mid}\{|\varphi_i\rangle\}_n \boxplus \beta_{mid}\{|\chi_i\rangle\}_n)$$

其中 α_{mid},β_{mid} 满足 $\alpha_{mid}|0\rangle+\beta_{mid}|1\rangle\in MID(\alpha_1|0\rangle+\beta_1 1,\alpha_2|0\rangle+\beta_2|1\rangle)$

2.

$$AXLE(\rho_1,\rho_2)=\{c_i\}_n \boxed{DenM} (\alpha_{axle}\{|\varphi_i\rangle\}_n \boxplus \beta_{axle}\{|\chi_i\rangle\}_n)$$

其中 $\alpha_{axle},\beta_{axle}$ 满足 $\alpha_{axle}|0\rangle+\beta_{axle}|1\rangle\in AXLE(\alpha_1|0\rangle+\beta_1 1,\alpha_2|0\rangle+\beta_2|1\rangle)$

例 3.9： $\{|\varphi_i\rangle\}_2=\{|0\rangle,|2\rangle\}_2$，$\{|\chi_i\rangle\}_2=\{|1\rangle,|3\rangle\}_2$，$\{|\phi\rangle\}_2=\{\frac{|0\rangle+|1\rangle}{\sqrt{2}},\frac{|2\rangle+|3\rangle}{\sqrt{2}}\}_2$，$\rho_1=\{\frac{1}{2},\frac{1}{2}\}\boxed{DenM}\{|\varphi_i\rangle\}_2)$, $\rho_3=\{\frac{1}{2},\frac{1}{2}\}_2\boxed{DenM}\{|\phi_i\rangle\}_2$ 那么有：

$$MID(\rho_1,\rho_3)=\{\frac{1}{2},\frac{1}{2}\}_2\boxed{DenM}\{\cos\frac{\pi}{8}|0\rangle+\sin\frac{\pi}{8}|1\rangle,\cos\frac{\pi}{8}|2\rangle+\sin\frac{\pi}{8}|3\rangle\}_2$$

$$AXLE(\rho_1,\rho_3)=\{\frac{1}{2},\frac{1}{2}\}_2\boxed{DenM}\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}},\frac{|2\rangle+i|3\rangle}{\sqrt{2}}\}_2$$

下面的定理是这一小节的主定理：

引理 3.15： 现有量子 markov 链 $G=(H,\mathcal{E})$. $\rho_1,\rho_2\in H$.

设 $\{|\varphi_{1i}\rangle\}_n\cup\{|\chi_{1i}\rangle\}_n$ 是 $span(\rho_1)\oplus span(\rho_2)$ 的正交基，$\{|\varphi_{2i}\rangle\}_m\cup\{|\chi_{2i}\rangle\}_m$ 是 $span(\mathcal{E}(\rho_1))\oplus span(\mathcal{E}(\rho_2))$ 的正交基，(α_1,β_1) 与 (α_2,β_2) 均模长为 1 且不正交，并且 ρ_1,ρ_2 满足

$$\rho_1=\{c_{1i}\}_n \boxed{DenM} (\alpha_1\{|\varphi_{1i}\rangle\}_n \boxplus \beta_1\{|\chi_{1i}\rangle\}_n)$$
$$\rho_2=\{c_{1i}\}_n \boxed{DenM} (\alpha_2\{|\varphi_{1i}\rangle\}_n \boxplus \beta_2\{|\chi_{1i}\rangle\}_n)$$
$$\mathcal{E}(\rho_1)=\{c_{2i}\}_m \boxed{DenM} (\alpha_1\{|\varphi_{2i}\rangle\}_m \boxplus \beta_1\{|\chi_{2i}\rangle\}_m)$$
$$\mathcal{E}(\rho_2)=\{c_{2i}\}_m \boxed{DenM} (\alpha_2\{|\varphi_{2i}\rangle\}_m \boxplus \beta_2\{|\chi_{2i}\rangle\}_m)$$

那么 $\forall\alpha,\beta,|\alpha|^2+|\beta|^2=1$, 我们有

$$\mathcal{E}(\{c_{1i}\}_n \boxed{DenM} (\alpha\{|\varphi_{1i}\rangle\}_n \boxplus \beta\{|\chi_{1i}\rangle\}_n)) = \{c_{2i}\}_m \boxed{DenM} \alpha\{|\varphi_{2i}\rangle\}_m \boxplus \beta\{|\chi_{2i}\rangle\}_m)$$

上面的表达式意味着，ρ_1,ρ_2 完全最大保真度, $\mathcal{E}(\rho_1),\mathcal{E}(\rho_2)$ 完全最大保真度，它们的保真度相等且大于 0，具体为 $C=|\alpha_1^+\alpha_2+\beta_1^+\beta_2|$. 我们给 ρ_1,ρ_2 所在的子空间找了一组基 $\{|\varphi_{1i}\rangle\}_n\cup\{|\chi_{1i}\rangle\}_n$, 给 $span(\mathcal{E}(\rho_1))\oplus span(\mathcal{E}(\rho_2))$ 找了一组基 $\{|\varphi_{2i}\rangle\}_m\cup\{|\chi_{2i}\rangle\}_m$, 并且我们找到的基恰好能够以相同的系数 α_i,β_i 表示 ρ_i 和 $\mathcal{E}(\rho_i)$. 在这种情况下，我们能够得出定理的结论。
par 定理证明依赖于引理 2.1，3.11 和 MID 算符。即：先通过其他方法证明下面的推论 1，具体是用 lemma 2.1 和 lemma 3.11，利用 3.11 的等号成立条件唯一确定结果。然后用这个结论证明主定理。另一方面，推论 1 和 2 也是主定理的特殊情况。也就是说，这里的定理 3.16 和 corollary 3.16.1 虽然强度差别很大，但有一种“强度相等”的关系，我们可以先证明较弱的命题，再证明一般性的命题。

下面举几个主定理应用的例子。

例 3.10：　1. 如果

$$\mathcal{E}(|0\rangle\langle 0|)=|2\rangle\langle 2|$$
$$\mathcal{E}(\frac{1}{2}(|0\rangle+|1\rangle)(\langle 0|+\langle 1|))=\frac{1}{2}(|2\rangle+|3\rangle)(\langle 2|+\langle 3|)$$

那么 $\forall\alpha,\beta,|\alpha|^2+|\beta|^2=1$, 我们有

$$\mathcal{E}((\alpha|0\rangle+\beta|1\rangle)(\alpha^+\langle 0|+\beta^+\langle 1|))=(\alpha|2\rangle+\beta|3\rangle)(\alpha^+\langle 2|+\beta^+\langle 3|)$$

2. 如果（这样对齐方便阅读）：

$$\begin{aligned}\rho_1 &= \frac{1}{2}|0+2\rangle\langle 0+2| &&+\frac{1}{2}|1\rangle\langle 1|\\ \rho_2 &= \frac{1}{2}|0\rangle\langle 0| &&+\frac{1}{2}|1+3\rangle\langle 1+3|\end{aligned}$$

$$\mathcal{E}(\rho_1) = \rho_2 = \frac{1}{2}\left|0\right\rangle\left\langle 0\right| + \frac{1}{2}\left|1+3\right\rangle\left\langle 1+3\right|$$
$$\mathcal{E}(\rho_2) = \frac{1}{2}\frac{\left|0\right\rangle + i\left|2\right\rangle}{\sqrt{2}}\frac{\left\langle 0\right| - i\left\langle 2\right|}{\sqrt{2}} + \frac{1}{2}\left|3\right\rangle\left\langle 3\right|$$

那么有 $\forall\alpha,\beta,|\alpha|^2+|\beta|^2=1$,

$$\mathcal{E}(\frac{1}{2}(\alpha\left|0+2\right\rangle+\beta\left|0-2\right\rangle)(\alpha^+\left\langle 0+2\right|+\beta^+\left\langle 0-2\right|)+\frac{1}{2}(\alpha\left|1\right\rangle+\beta\left|3\right\rangle)(\alpha^+\left\langle 1\right|+\beta^+\left\langle 3\right|))$$
$$=\frac{1}{2}(\alpha\left|0\right\rangle+i\beta\left|2\right\rangle)(\alpha^+\left\langle 0\right|-i\beta^+\left\langle 2\right|)+\frac{1}{2}(\alpha\left|1+3\right\rangle+\beta\left|1-3\right\rangle)(\alpha^+\left\langle 1+3\right|+\beta^+\left\langle 1-3\right|)$$

其中 $\left|i+j\right\rangle = \frac{\left|i\right\rangle+\left|j\right\rangle}{\sqrt{2}}, \left|i-j\right\rangle = \frac{\left|i\right\rangle-\left|j\right\rangle}{\sqrt{2}}$

由于 MID 和 $AXLE$ 两个算符都可以用 $\{c_i\}_n \boxed{DenM} (\alpha\{|\varphi_i\rangle\}_n \boxplus \beta\{|\chi_i\rangle\}_n)$ 形式表达, 借助引理 3.15，我们有:

推论 3.2: 如果 ρ_1,ρ_2 完全最大保真度, $\mathcal{E}(\rho_1),\mathcal{E}(\rho_2)$ 完全最大保真度, 它们的保真度相等且大于 0，那么 $\mathcal{E}(MID(\rho_1,\rho_2)) = MID(\mathcal{E}(\rho_1),\mathcal{E}(\rho_2))$

推论 3.3: 如果 ρ_1,ρ_2 完全最大保真度, $\mathcal{E}(\rho_1),\mathcal{E}(\rho_2)$ 完全最大保真度, 它们的保真度相等且大于 0, 那么 $\mathcal{E}(AXLE(\rho_1,\rho_2)) = AXLE(\mathcal{E}(\rho_1),\mathcal{E}(\rho_2))$

这两个定理将在第 8 小节的证明中用到.

回到我们一直关心的问题：我们已经知道 ρ_1,ρ_2 完全最大保真度, $\mathcal{E}(\rho_1),\mathcal{E}(\rho_2)$ 完全最大保真度, 它们的保真度相等且大于 0, 也就是说我们已经有 $F(\rho_1,\rho_2) = F(\mathcal{E}(\rho_1),\mathcal{E}(\rho_2)) = C > 0$, 我们如何构造一个 ρ 使得 $F(\rho,\mathcal{E}(\rho)) > C$ 呢?

我们将通过 MID 与 $AXLE$ 来构造。换句话说, 我们在 corollary 3.16.1,3.16.2 中得到了 $\mathcal{E}(\rho_4) = \rho_5$ 形式的结论，我们要进一步考虑 $F(\rho_4,\rho_5)$. 下面我们的结果告诉我们确实可以以某种形式得到类似 $F(\rho_4,\rho_5) > C$ 的结论。为了方便表达，首先引入一个概念。

定义 3.15: 如果 $\{|\varphi_i\rangle\}_n$ 满足:

1. $\forall i, |\varphi_i\rangle \in span(|\varphi_1\rangle, |\varphi_2\rangle)$
2. $\forall i = 1,2\cdots n-2, |\varphi_{i+1}\rangle \in MID(|\varphi_i\rangle, |\varphi_{i+2}\rangle)$

我们说 $\{|\varphi_i\rangle\}_n$ 是 fidelity C cyclic, 其中 $C = |\langle\varphi_1|\varphi_2\rangle| \in (0,1]$

例 3.11： $\{\cos\frac{n\pi}{6}|0\rangle + \sin\frac{n\pi}{6}|1\rangle\}_{n=1}^{10}$ 是 fidelity $\frac{\sqrt{3}}{2}$ cyclic. 如果 $\rho_1 = \rho_2 = \rho_3$, 那么 $\{\rho_i\}_3$ 是 fidelity 1 cyclic。

对于纯态来说，fidelity $\cos\theta$ cyclic 意味着在一个 Bloch 球上沿着某个大圆旋转，每次旋转 2θ 角。某两个相邻的态的 $AXLE$ 就是旋转轴。进一步，如果 $\{|\varphi_i\rangle\}_n$ 是 fidelity C cyclic，那么 $\forall i = 1, 2\cdots n-2, AXLE(|\varphi_i\rangle, |\varphi_{i+1}\rangle) = AXLE(|\varphi_{i+1}\rangle, |\varphi_{i+2}\rangle)$.

定义 3.16： 定义 $\{\rho_i\}_n$ 是 fidelity C cyclic 的，如果满足：存在系数 $\{c_j\}_{j=1}^m$, $\{\rho_i\}_n$ 每一项均满足分解 $\rho_i = \{c_j\}_{j=1}^m\{|\varphi_{ij}\rangle\}_{j=1}^m$, 并且 $\forall j, \{|\varphi_{ij}\rangle\}_{i=1}^n$ 是 fidelity C cyclic.

例 3.12： 设 $\rho_1 = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$,$\rho_2 = \frac{1}{2}(|0+2\rangle\langle 0+2| + |1+3\rangle\langle 1+3|)$,$\rho_3 = \frac{1}{2}(|2\rangle\langle 2| + |3\rangle\langle 3|)$, 则 $\{\rho_i\}_3$ 为 fidelity $\frac{1}{\sqrt{2}}$ cyclic.

引理 3.16： 如果 ρ_1, ρ_2 完全最大保真度，ρ_2, ρ_3 完全最大保真度，$F(\rho_1, \rho_2) = F(\rho_2, \rho_3) > 0$, 那么

$$F(MID(\rho_1, \rho_2), MID(\rho_2, \rho_3)) \geq C$$

等号成立当且仅当 ρ_1, ρ_2, ρ_3 是 fidelity C cyclic.

也就是说，当 $\rho_1, \mathcal{E}(\rho_1)$ 完全最大保真度，$\mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1)$ 完全最大保真度，$\rho_1, \mathcal{E}(\rho_1) = \mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1) = C > 0$, 但是 $\rho_1, \mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1)$ 不是 fidelity C cyclic 的时候，我们可以构造出 $\rho_4 = MID(\rho_1, \mathcal{E}(\rho_1))$, $\rho_5 = MID(\mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1))$ 满足 (1)$\mathcal{E}(\rho_4) = \rho_5$(根据 corollary 3.16.1)(2)$F(\rho_4, \mathcal{E}(\rho_4)) > C$（根据 lemma 3.17）. 当 $\rho_1, \mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1)$ 是 fidelity C cyclic 的时候，我们可以使用下面的定理。

引理 3.17： 如果 $\{\rho_i\}_n$ 是 fidelity C cyclic，$C \in (0,1)$, 那么 $\forall i, AXLE(\rho_i, \rho_{i+1}) = AXLE(\rho_{i+1}, \rho_{i+2})$.

也就是说，当 $\rho_1, \mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1)$ 是 fidelity $C > 0$ cyclic 的时候，我们可以构造出 $\rho_4 = AXLE(\rho_1, \mathcal{E}(\rho_1))$, $\rho_5 = AXLE(\mathcal{E}(\rho_1), \mathcal{E}^2(\rho_1))$ 满足: (1)$\mathcal{E}(\rho_4) = \rho_5$(根据 corollary 3.16.2)(2)$F(\rho_4, \mathcal{E}(\rho_4)) = 1$（根据 lemma 3.18）.

这些定理将在第 8 小节的证明中用到。在第 8 小节的证明前，我们整理一下这一小节的内容，说明一下如何通过第 6 小节的结论和这一小节的结果推出第 8 小节。在第六小节中我们已经得到了完全最大保真度的结果，而这一小节的定理全是在完全最大保真度的情况下研究的。我们将用 lemma 3.17，corollary 3.16.1 处理不是 fidelity cyclic 的情况，用 lemma 3.18，corollary 3.16.2 处理 fidelity cyclic 的情况。lemma 3.17, 3.18 使我们构造出具有更大 $F(\rho, \mathcal{E}^K(\rho))$ 的 ρ, 从而得到更大的轨道保真度 LF. corollary 3.16.1，3.16.2 使我们在构造更大 LF 的过程中能够保持轨道维度函数 XD 不变，不会对序（definition 5）产生额外的影响。

3.3.8 证明主线第三部分：周期分解的存在性

引理 3.18： 那么前面构造出的 $\rho_\blacklozenge$ 满足 Eq. (1)

$$F(\rho, \mathcal{E}^k(\rho)) = \begin{cases} 0 & \text{when } 1 \le k < K \\ 1 & \text{when } k = K \end{cases}, \text{for some } K \ge 2$$

证明 设 $\rho_\blacklozenge$ 的 Orbit 为 $\{O_i\}_{i=0}^{+\infty}$.

首先由 lemma 3.6 及 corollary 3.6.1 我们可以得到 $\rho_\blacklozenge$ 是 weak fixed point state 并且 $\exists K$，$\forall 0 < k < K, LF_k(\rho_\blacklozenge) = 0, LF_K(\rho_\blacklozenge) = C > 0$ 并且 $\forall i, O_i, O_{i+K}$ 完全最大保真度.

首先我们能得到 $\forall i_0 \in \{0, 1 \cdots K-1\}, O_{i_0}$ 在 $\mathcal{E}^K$ 下的 Orbit 一定是 fidelity C cyclic.

否则的话, 如果对某个 i_0, O_{i_0} 在 $\mathcal{E}^K$ 下的轨道即 $\{O_{Ki+i_0}\}_{i=0}^{+\infty}$ 不是 fidelity C cyclic，取 $\rho' = MID(O_{Ki+i_0}, O_{Ki+K+i_0})$, ρ' 将有更大的轨道保真度 LF_k（Lemma 3.17）, 并且轨道维度 XD 值不变（corollary 3.16.1 简单推出), 与 lemma 3.6 矛盾. 因此 $\forall i_0 = 0, 1 \cdots K-1, O_{i_0}$ 在 $\mathcal{E}^K$ 下的 Orbit 一定是 fidelity C cyclic.

进一步，如果 $C < 1$，取 $\rho' = AXLE(O_1, O_{K+1})$. 根据 corollary 3.16.2 我们知道:

$$\mathcal{E}(\rho') = AXLE(O_2, O_{K+2})$$
$$\mathcal{E}^2(\rho') = AXLE(O_3, O_{K+3})$$
$$\cdots$$

$$\mathcal{E}^K(\rho') = AXLE(O_{K+1}, O_{2K+1}) = AXLE(O_1, O_{K+1}) = \rho'(\text{lemma 3.18})$$

于是我们得到 $C = 1$.

然后，由于它不是 aperiodic，我们有 $K > 1$. 这就完成了证明。 □

引理 3.19： 一个 BSCC S, 必是下列两种类型之一:

1. aperiodic BSCC
2. 存在周期 $k \geq 2$，满足：存在密度算子 $\rho_1, \rho_2 \cdots \rho_k$，满足：(1)$span(\rho_1), span(\rho_2) \cdots span(\rho_k)$ 的直和为 S 并且两两正交（2）$\mathcal{E}(\rho_i) = \rho_{i+1 \mod k}$

证明 实质上和 lemma 3.19 是同一件事。引理 3.19 的证明是在 BSCC S 非 aperiodic 的前提下进行的。如果这个子空间不是 aperiodic 的，根据 lemma 3.19 有 Eq. (1) 成立，而 $F(\rho_1, \rho_2) = 0 \Leftrightarrow \rho_1 \perp \rho_2$, $F(\rho_1, \rho_2) = 1 \Leftrightarrow \rho_1 = \rho_2$, 故选取 $\rho_1 = \rho_\blacklozenge$ 即可。由 BSCC 性质知 $span(\rho_1), span(\rho_2) \cdots span(\rho_k)$ 的直和必为 S。 □

3.3.9 证明主线第四部分：最大分解与其唯一性

从 lemma 3.20 开始，证明主定理。lemma 3.20 和主定理相比，缺少唯一性与每个分量在 G^K 下 aperiodic 的性质。这是因为虽然我们找到了一个分解，但不一定是最大分解。就是说，可能 BSCC 是周期 6 的，但我们找到的是周期 2 或 3 的分解。

但是 theorem 3.20 可以使我们能够把非 aperiodic 的 BSCC 分解成 $K \geq 2$ 个子空间。如果得到的子空间在 G^K 不是 aperiodic，在 G^K 下继续分解即可。唯一性的证明需要研究 aperiodic BSCC 在 G^i 下的性质。

定理 3.3： S 是 G 的一个 aperiodic BSCC, 则有如下结论

1. $\exists N \forall |\varphi\rangle \in S, \forall n > N span(\mathcal{E}^n(\varphi)) = S$
2. $\forall i$,S 是 G^i 的一个 aperiodic BSCC

第一条调换了 $\exists, \forall$ 两个符号的位置，形式上更强。这个暂时用不到。第二条有用。下面开始证明主定理，theorem 3.1。

证明 (Proof of theorem 3.1) theorem 3.1 和已证明的 lemma 3.20 比较，我们没有证明每一个分量在 G^p 下都是 aperiod 的，也没有证明唯一性。于是剩下的就是找到一个最大分解，并证明唯一性。假设 S 不是 aperiodic BSCC。根据 lemma 3.20，分解成 $\{\rho_i\}_K$。不妨假设 ρ_1 在 $\mathcal{E}^K$ 下不是 aperiodic BSCC。我们可以在 $\mathcal{E}^K$ 下继续应用 lemma 3.20 分解。假设 $\rho_{11}, \cdots \rho_{1m}$ 是 S_1 在 G^K 下的分解得到的密度矩阵。由 $F(\mathcal{E}^K(\rho_{1i}), \mathcal{E}^K(\rho_{1j})) = 0$ 我们知道 $\forall k, F(\mathcal{E}^k(\rho_{1i}), \mathcal{E}^k(\rho_{1j})) = 0$. 我们可以得到 $\forall k, 1 \le k \le K, \{\mathcal{E}^k(\rho_{1i})\}_{i=1}^m$ 是 S_k 在 $\mathcal{E}^K$ 下的分解。易知我们可以将 S 分解成 mK 个子空间, 满足周期分解的要求（1）（2），由 $mK > K$, 不断重复最终分解必然会满足定理中的要求（3）即 aperiod 的要求。

于是剩下唯一性。假设我们可以得到两种不同的分解，先假设二者有着不同的 p. 设为 p_1, p_2. 考虑 $G^{p_1 p_2}$ 的 BSCC 分解。由 theorem 3.21 性质 2 我们得到两个不同的 BSCC 分解，矛盾。故 $p_1 = p_2$. 然后考虑 G^{p_1} 易得维数的唯一性。 □

3.4 进一步的结论

前面主定理中的唯一性事实上比较弱。我们有更强的定理：设 S 可以按主定理分解得到 $\{\rho_i\}_p$，$\{\rho_i\}_p$ 及其线性组合是其全部的弱不动点。也就是说，满足主定理的分解对一个 BSCC 有且仅有一种。证明需要在主定理的基础上进行。先假设有两个主定理条件下的分解，导出矛盾，然后证明上面说的结论。

第 4 章　周期分解的强唯一性与不可约量子 Markov 链极限行为

4.1　介绍

尽管我们已经证明了和经典情形类似的定理，但是这个定理中的唯一性并不令人满意。这一节中我们将证明周期分解的强唯一性。我们将找到不可约子空间中的所有弱不动点态，并用它证明周期分解是唯一的。接着我们将研究不可约量子 Markov 链中的极限行为问题。

4.2　非周期量子 Markov 链的极限行为

作为基础，我们首先研究不可约 Markov 链的极限行为。

引理 4.1：　如果 S 是一个非周期子空间，那么对 $|\varphi\rangle \in S$，$\lim_{i\to+\infty} \mathcal{E}^i(\varphi) = \rho$，其中 ρ 是 S 的稳定分布。

证明 因为

$$\exists N, \forall\, |\varphi\rangle \in S, \mathrm{supp}(\mathcal{E}^N(\varphi)) = S$$

我们有

$$\exists N, \delta > 0, \forall \sigma \in S, \mathcal{E}^N(\sigma) = \delta\rho + (1-\delta)\sigma'$$

所以 $\forall\, |\varphi\rangle \in S$,

$$\begin{aligned}
\lim_{i\to+\infty} \mathcal{E}^i(\varphi) &= \lim_{i\to+\infty} \mathcal{E}^r(\mathcal{E}^{pN}(\varphi)) \quad (t = \lfloor \frac{i}{N} \rfloor, i = tN + r) \\
&= \lim_{i\to+\infty} \mathcal{E}^r((\delta + \delta(1-\delta) + \cdots + \delta(1-\delta)^{t-1}(\rho) + (1-\delta)^t\sigma) \quad (t = \lfloor \frac{i}{N} \rfloor, i = tN + r) \\
&= \lim_{i\to+\infty} ((1-(1-\delta)^t)\rho + (1-\delta)^t\sigma') \quad (t = \lfloor \frac{i}{N} \rfloor, i = tN + r) \\
&= \rho
\end{aligned}$$

□

4.3 弱不动点态的进一步的性质

我们的目标是找到不可约子空间中的所有弱不动点态。在这一节中我们将看到弱不动点的更多性质。

我们目前对弱不动点态的理解还很少，我们甚至不知道它是否具有可加性。首先，我们需要下面的定义。

定义 4.1： 假设 ρ，σ 是两个弱不动点态，它们的轨道是 $\{O_i\}_{i=0}^{+\infty}, \{Q_i\}_{i=1}^{+\infty}$。如果存在一列整数 $\{i_j\}_{j=1}^{+\infty}$ 使得 $\{O_{i_j}\}_{j=1}^{+\infty}, \{Q_{i_j}\}_{j=1}^{+\infty}$ 收敛到 ρ, σ，我们说 ρ, σ 是同步收敛的弱不动点态。

在周期分解定理的帮助下我们不难证明同步收敛的性质：

引理 4.2：

1. 如果 ρ, σ 是同步收敛的弱不动点态，它们的轨道分别为 $\{O_i\}_{i=0}^{+\infty}$，$\{Q_i\}_{i=1}^{+\infty}$，则
   (a) $F(O_i, Q_i)$ 对于 i 恒定。
   (b) $MS(\mathrm{supp}(O_i), \mathrm{supp}(Q_i))$ 对于 i 恒定。
2. 如果 ρ 是 $\mathcal{G}$ 的弱不动点态，则它一定是 $\mathcal{G}^i$ 的弱不动点态。
3. 假设 $\rho_1, \rho_2 \cdots \rho_p$ 是不可约子空间的周期分解中的密度算子，σ 是一个弱不动点态，那么 $\forall i$, ρ_i 和 σ 同步收敛。

为了找到不可约子空间中的所有弱不动点态，一个自然的想法是把周期分解中的弱不动点态作为基，尝试证明所有的弱不动点态均可以由这些弱不动点态表达。作为基础，我们证明了下面的引理：

引理 4.3： 对量子 Markov 链 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$，假设 S 是非周期子空间，ρ_0 是 S 的稳定分布。如果 σ 是一个弱不动点态，ρ_0 和 σ 不正交，那么存在一个弱不动点态 $\rho_2 \in \mathrm{supp}(\sigma)$ 与 ρ_0 完全最大保真度。进一步，$\exists c_1 > 0$ 使得 $\sigma = c_1\rho_2 + (1 - c_1)\rho_3$，并且 ρ_3 是一个弱不动点态，并满足 $MS(\mathrm{supp}(\rho_3), \mathrm{supp}(\rho_0)) < MS(\mathrm{supp}(\sigma), \mathrm{supp}(\rho_0))$，并且 ρ_2, ρ_3 同步收敛。

下面我们引入极小弱不动点态的概念。

定义 4.2： 如果一个弱不动点态 ρ 满足：不存在弱不动点态 σ 使得 $\mathrm{supp}(\sigma) \subset \mathrm{supp}(\rho)$，我们说 ρ 是一个极小弱不动点态。

引理 4.4: 1. 假设 $\rho_1, \rho_2 \cdots \rho_p$ 是不可约子空间的周期分解，ρ 是极小弱不动点态，对所有的 i，ρ 与 ρ_i 完全最大保真度。

2. 考虑量子 Markov 链 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$，$\sigma$ 是一个弱不动点态，则 σ 可以被写作 $\sigma = c_1\sigma_1 + c_2\sigma_2 + \cdots + c_m\sigma_m$，其中每一个 σ_m 均为极小弱不动点态

所以为了找到不可约子空间中所有的弱不动点态，我们只需找到所有的极小弱不动点态。我们将看到，不可约子空间的周期分解给出了所有的极小弱不动点态。

引理 4.5: 假设 S 是 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$ 的不可约子空间，其周期分解为 $\rho_1, \rho_2 \cdots \rho_p$。假设 $\sigma \in S$ 是一个极小弱不动点态，那么 $XD(\sigma) = XD(\rho_1), LF_k(\sigma) = 0(k < p)$, $LF_p(\sigma) = 1$。

推论 4.1: 假设 S 是 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$ 的不可约子空间，周期为 p，$\sigma \in S$ 是一个极小弱不动点态，那么 $\sigma, \mathcal{E}(\sigma), \cdots \mathcal{E}^{p-1}(\sigma)$ 是 S 的一个周期分解。

于是我们的下一步是要证明不存在两个不同的周期分解。

4.4 完全最大保真度的密度算子的进一步性质

我们这一节的目标是引入一些工具证明不可约子空间的周期分解是唯一的。

引理 4.6: 考虑量子 Markov 链 $\mathcal{G} = (\mathcal{H}, \mathcal{E} = \sum_{i=1}^{k} E_i \cdot E_i^\dagger)$。设

$$\rho_1 = \{c_i\}_n \boxed{DenM}\, \mathfrak{s}_1 \tag{4-1}$$

$$\rho_2 = \{c_i\}_n \boxed{DenM}\, \mathfrak{s}_2 \tag{4-2}$$

$$\mathcal{E}(\rho_1) = \{d_i\}_n \boxed{DenM}\, \mathfrak{s}_1' \tag{4-3}$$

$$\mathcal{E}(\rho_2) = \{d_i\}_n \boxed{DenM}\, \mathfrak{s}_2' \tag{4-4}$$

$\mathfrak{s}_1, \mathfrak{s}_2$ 完全最大相似度，$\mathfrak{s}_1', \mathfrak{s}_2'$ 完全最大相似度，相似度相等，那么

1. $\forall \mathfrak{s} \in \mathfrak{H}_1, \mathcal{E}(\{c_i\}_n \boxed{DenM}\, (\alpha\mathfrak{s}_1 \boxplus \beta\mathfrak{s}_2)) = \{d_i\}_n \boxed{DenM}\, (\alpha\mathfrak{s}_1' \boxplus \beta\mathfrak{s}_2')$.
2. $\forall i$, E_i coexists with $\mathfrak{s}_1, \mathfrak{s}_2 \mapsto \mathfrak{s}_1', \mathfrak{s}_2'$.

引理 4.7： 考虑量子 Markov 链 $\mathcal{G} = (\mathcal{H}, \mathcal{E} = \sum_i E_i \cdot E_i^\dagger)$。如果酉矩阵 $U \neq e^{i\theta} I$: $H \to H$ 满足 $[U, E_i] = 0$ 对所有 i 成立，那么 H 不是一个不可约子空间。

我们的目标是在 S 有两个周期分解的情况下构造出这样的一个 U。

引理 4.8： 假设 $\rho_1, \rho_2 \cdots \rho_p, \sigma_1, \sigma_2 \cdots \sigma_p$ 是 S 的两个周期分解，ρ_i, σ_i 完全最大保真度且保真度不为0, 则我们可以分解为 $\rho_i = \{c_j\}_i \boxed{DenM} \mathfrak{s}_i, \sigma_i = \{c_j\}_i \boxed{DenM} \mathfrak{s}'_i$ 使得 $\forall i$, $\mathfrak{s}_i$ 和 $\mathfrak{s}'_i$ 完全最大相似度且相似度为固定值 $C > 0$ 并且 $\bigcup_i \mathfrak{s}_i, \bigcup_i \mathfrak{s}'_i$ 是 S 的两组基。

引理 4.9： 如果 S 有两个不同的周期分解，则存在 S 上的酉矩阵 $U \neq e^{i\theta} I$ 满足 $\forall i, [U, E_i] = 0$

然后我们可以证明周期分解的唯一性：

定理 4.1： 不可约子空间只有一个周期分解，如果我们将周期分解的轮换看做同一个周期分解。

4.5 不可约 Markov 链的极限行为

首先，我们要找到不可约子空间中的所有弱不动点态。

定理 4.2： 假设不可约子空间的周期分解中的密度矩阵为 $\rho_1, \rho_2 \cdots \rho_p$，那么 $\rho_1, \rho_2 \cdots \rho_p$ 为这个不可约子空间的全部极小弱不动点态。进一步，所有的弱不动点态可以表示为 $c_1\rho_1 + c_2\rho_2 + \cdots + c_p\rho_p$，其中 $\sum_{i=1}^p c_i = 1$。

接下来，我们给出不可约子空间的极限分布的定理：

定理 4.3： 假设 S 是一个不可约子空间，$S_1, S_2 \cdots S_p$ 是周期分解，对应的密度算子为 $\rho_1, \rho_2 \cdots \rho_p$。对初态 $\sigma \in S$，记 $tr(P_{S_i}(\sigma))$ 为 p_i，则 $\lim_{k\to+\infty} \mathcal{E}^{kp+i_0}(\sigma) = \sum_{i=1}^k p_i \rho_{i+i_0 \mod p}$

第 5 章　一般量子 Markov 链的结构与极限行为

5.1　伪酉子空间

定义 5.1：　考虑 $\mathcal{G} = (H, \mathcal{E} = \sum_i E_i \cdot E_i^\dagger)$，我们说一个子空间 S 是一个伪酉子空间，如果 S 存在不可约子空间分解 $B_1, B_2, \cdots B_n$，并有序列 $\mathfrak{s}_1, \mathfrak{s}_2 \cdots \mathfrak{s}_n$，模为 1 的复数 $\mathrm{e}^{\mathrm{i}\theta_1}, \mathrm{e}^{\mathrm{i}\theta_2} \cdots \mathrm{e}^{\mathrm{i}\theta_n}$ 满足：

1. $\forall i, \mathfrak{s}_i$ 是 B_i 的正交基
2. $\forall i, E_i$ 与基 $\mathfrak{s}_1, \mathfrak{s}_2 \cdots \mathfrak{s}_n \mapsto \mathrm{e}^{\mathrm{i}\theta_1}\mathfrak{s}_1, \mathrm{e}^{\mathrm{i}\theta_2}\mathfrak{s}_2 \cdots \mathrm{e}^{\mathrm{i}\theta_n}\mathfrak{s}_n$ 协调

如果 S 是伪酉子空间并且 $S' \supseteq S \Rightarrow S' = S$，我们说 S 是极大伪酉子空间。

然后，我们给出伪酉子空间的极限行为。

5.2　弱不动点态的进一步性质

引理 5.1：　假设 ρ 是极小弱不动点态，S 是不可约子空间，周期分解为 $S_1, S_2 \cdots S_p$, 对应弱不动点态为 $\rho_1, \rho_2 \cdots \rho_p, tr(P_{S_1}\rho) > 0$，那么

1. $\dim(\mathrm{span}(\mathcal{E}^{kp+i}(\rho))) = \dim(\rho_i)$.
2. $\forall i, \mathcal{E}^i(\rho)$ 是极小弱不动点态

引理 5.2：　如果 ρ 是 $\mathcal{G} = (H, \mathcal{E})$ 的极小弱不动点态，则 $\forall \sigma \in \mathrm{supp}(\rho)$, $\lim_{i\to+\infty} \|\mathcal{E}^i(\sigma) - \mathcal{E}^i(\rho)\|_{tr} = 0$

推论 5.1：　如果 ρ_1, ρ_2 是两个同步收敛的极小弱不动点态，则它们完全最大保真度。

推论 5.2：　假设 ρ 是 $S_1 \oplus S_2 \cdots S_m$ 中的极小弱不动点态，S_i 是不可约子空间，$tr(P_{S_i}\rho) > 0$ 对所有 i 成立那么 $\frac{P_{S_1\oplus S_2 \cdots \oplus S_{m-1}} \rho P_{S_1\oplus S_2 \cdots \oplus S_{m-1}}}{tr(P_{S_1\oplus S_2 \cdots \oplus S_{m-1}} \rho)}$ 是 $S_1 \oplus S_2 \cdots \oplus S_{m-1}$ 中的弱不动点态。

5.3 主定理与证明

下面引入主定理。

首先，我们考虑只有两个非周期子空间的情况。

引理 5.3： 考虑量子 Markov 链 $\mathcal{G} = (S_1 \oplus S_2, \mathcal{E})$，$S_1, S_2$ 是 $\mathcal{G}$ 的两个非周期子空间，其不动点态分别为 ρ_1, ρ_2，σ 是不同于 ρ_1, ρ_2 的极小弱不动点态，S_1, S_2 满足 $\forall |\varphi\rangle \in S_i, span(\mathcal{E}(\varphi)) = S_i$ 假设 ρ_1, ρ_2, σ 可以被写作

$$\rho_1 = \{c_i\}_{i=1}^n \boxed{DenM} \mathfrak{s}_1$$

$$\rho_2 = \{c_i\}_{i=1}^n \boxed{DenM} \mathfrak{s}_2$$

$$\sigma = \{c_i\}_{i=1}^n \boxed{DenM} \alpha\mathfrak{s}_1 \boxplus \beta\mathfrak{s}_2$$

则 $\mathcal{E}(\sigma)$ 可以被写作

$$\mathcal{E}(\sigma) = \{c_i\}_{i=1}^n \boxed{DenM} \alpha'\mathfrak{s}_1 \boxplus \beta'\mathfrak{s}_2$$

下面的引理在前一个引理的基础上更进了一步。

引理 5.4： 设 S_1, S_2 是 $\mathcal{G}$ 的非周期子空间，则下列两条之一成立

1. 对所有极小弱不动点态 $\rho \in S_1 \oplus S_2$ 都有 $\rho \in S_1$ 或 $\rho \in S_2$
2. 存在正交基 $\mathfrak{s}_1$ of S_1，$\mathfrak{s}_2$ of S_2，模为 1 的复数 $e^{i\theta_1}, e^{i\theta_2}$ 使得 $\mathcal{E}$ 对应于基 $\mathfrak{s}_1, \mathfrak{s}_2 \mapsto e^{i\theta_1}\mathfrak{s}_1, e^{i\theta_2}\mathfrak{s}_2$ 伪酉。

下面让我们考虑一个较为复杂的情况：两个一般的不可约子空间。

引理 5.5： 设 S_1, S_2 是 $\mathcal{G}$ 的不可约子空间，则下列两条之一成立

1. 对所有极小弱不动点态 $\rho \in S_1 \oplus S_2$ 都有 $\rho \in S_1$ 或 $\rho \in S_2$
2. 存在正交基 $\mathfrak{s}_1$ of S_1，$\mathfrak{s}_2$ of S_2，模为 1 的复数 $e^{i\theta_1}, e^{i\theta_2}$ 使得 $\mathcal{E}$ 对应于基 $\mathfrak{s}_1, \mathfrak{s}_2 \mapsto e^{i\theta_1}\mathfrak{s}_1, e^{i\theta_2}\mathfrak{s}_2$ 伪酉。

上面的定理相当于归纳假设。下面的几个定理给出了归纳过程需要的引理。

引理 5.6: 设 ρ 是 $S_1 \oplus S_2 \cdots S_m$ 中的极小弱不动点态，S_i 是不可约子空间，$tr(P_{S_i}\rho) > 0$ 对所有的 i 成立，则 $\frac{P_{S_1\oplus S_2\cdots\oplus S_{m-1}}\rho P_{S_1\oplus S_2\cdots\oplus S_{m-1}}}{tr(P_{S_1\oplus S_2\cdots\oplus S_{m-1}}\rho)}$ 是 $S_1 \oplus S_2 \cdots \oplus S_{m-1}$ 中的极小弱不动点态。

引理 5.7: 设 ρ 是 $S_1 \oplus S_2 \cdots S_m$ 中的极小弱不动点态，S_i 是不可约子空间，如果 $S_1 \oplus S_2 \cdots \oplus S_{m-1}$ 和 $S_2 \oplus S_3 \cdots \oplus S_m$ 均伪酉，那么 $S_1 \oplus S_2 \cdots \oplus S_m$ 伪酉。

引理 5.8: 假设 ρ 是 $S_1 \oplus S_2 \cdots S_m$ 中的极小弱不动点态，S_i 是不可约子空间，$tr(P_{S_i}\rho) > 0$ 对所有的 i 成立，那么 $S_1 \oplus S_2 \cdots S_m$ 伪酉。

推论 5.3: 如果 S_1, S_2 是两个极大伪酉空间，$S_1 \oplus S_2$ 中的所有极小弱不动点态满足 $\rho \in S_1$ 或 $\rho \in S_2$.

下面给出这一节的主定理。其中第一条来自 [6]。

定理 5.1: 考虑量子 Markov 链 $\mathcal{G} = (H, \mathcal{E})$.

1. 首先，H 可以被唯一分解为暂态子空间 T 和稳态子空间 R
2. 然后，稳态子空间 R 可以被唯一分解为正交的伪酉空间，每一个极小弱不动点态均落在某一个伪酉空间中。
3. 然后，每一个伪酉空间 S 可以被分解为 $\mathcal{E}|S = \mathcal{E}_{monomer} \boxplus^{\mathfrak{s}\to\mathfrak{S}} \mathfrak{U}$ 其中 span($\mathfrak{s}$) 是 $\mathcal{E}_{monomer}$ 的不可约子空间
4. 最后，每一个不可约子空间均有周期分解。

下面的引理给出了超算符的稳态空间的极限行为的关键定理。暂态行为情况比较复杂，暂时没有合适的方法研究。

命题 5.1: 考虑量子 Markov 链 $(H, \mathcal{E})$ 的稳态空间 R 可以被分解为伪酉空间 $E_1 \oplus E_2 \oplus \cdots E_u$，初态 $|\varphi\rangle = \sqrt{c_1}\,|\varphi_1\rangle + \sqrt{c_2}\,|\varphi_2\rangle + \cdots \sqrt{c_u}\,|\varphi_u\rangle$，其中 $|\varphi_i\rangle \in E_i$ 那么 $\lim_{i\to+\infty} \|\mathcal{E}^i(\varphi) - \sum_{j=1}^{u} c_j \mathcal{E}^i(\varphi_j)\|_{tr} = 0$

第 6 章　结论

我们研究了不可约子空间的周期分解，并研究了量子 Markov 链的极限分布问题。我们还给出了相应的算法。这些算法可能能够用在量子计算机的程序的安全性检测上，并有可能成为量子算法及量子计算其他问题的工具。

插图索引

表格索引

公式索引

参考文献

[1] Ambainis A. Quantum walks and their algorithmic applications. International Journal of Quantum Information, 2003, 1

[2] Gardiner C, Zoller P. Quantum Noise: A Handbook of Markovian and Non-Markovian Quantum Stochastic Methods with Applications to Quantum Optics. Heidelberg: Springer, 2004

[3] Nielson M A, Chuang I L. Quantum Computation and Quantum Information. Cambrige: Cambrige University Press, 2000

[4] Liu T, Li Y, Wang S, et al. A theorem prover for quantum hoare logic and its applications.

[5] Yu N, Ying M. Reachability and termination analysis of concurrent quantum programs. Proceedings of the 23rd International Conference on Concurrency Theory (CONCUR), volume 7454 of *LNCS*. Springer, 2012. 69–83

[6] Ying S, Feng Y, Yu N, et al. Reachability probabilities of quantum markov chains. Proceedings of the 24rd International Conference on Concurrency Theory (CONCUR), volume 8052 of *LNCS*. Springer, 2013. 334–348

[7] Ying S, Ying M. Reachability analysis of quantum markov decision processes.

[8] Liu C, Petulante N. On limit distributions of quantum markov chain. International Journal of Mathematics and Mathematical Sciences, 2011.

[9] 程玮琪. 马尔可夫链：模型，算法及应用. 北京: 清华大学出版社, 2015

致　谢

感谢清华大学的罗贵明老师、悉尼科技大学的应明生老师、应圣钢学长对我的指导。感谢数学系的仇泽民同学帮我解决了一个问题。

声　明

本人郑重声明：所呈交的学位论文，是本人在导师指导下，独立进行研究工作所取得的成果。尽我所知，除文中已经注明引用的内容外，本学位论文的研究成果不包含任何他人享有著作权的内容。对本论文所涉及的研究工作做出贡献的其他个人和集体，均已在文中以明确方式标明。

签　名：____________ 日　期：____________

附录 A　外文资料的调研阅读报告或书面翻译

量子 **Markov** 链的可达概率

摘要：这篇论文研究了量子 Markov 链（qMC）三种类型的长程行为，即可达性，重复可达性，持续可达性。作为铺垫，我们引入了 qMC 的底层强连通分量（BSCC）的概念，并且给出了一个寻找 qMC 状态空间的 BSCC 分解的方法。作为主要成果，论文给出了几个计算 qMC 的可达性，重复可达概率与一致可达概率的算法，并分析了它们的复杂度。

A.1　介绍

量子系统的验证问题在量子物理，量子通信，量子计算中有出现。比如说，验证问题被物理学家看做量子模拟的主要短期目标。一些有效的量子密码协议的验证技术最近被开发出来，基于量子进程代数或者量子模型检测。另一方面，一些验证量子程序的方法也被提出，包括量子最弱预条件，或者量子 Floyd-Hoare 逻辑。

一个量子 Markov 链（qMC）是 Markov 链的量子扩展，大致地说，状态空间是一个 Hilbert 空间，MC 的转移概率矩阵被超算符代替，他是开放量子系统的离散时间演化的数学形式。qMC 在物理中已经被广泛用作量子噪声的数学模型。一类特殊的 qMC，量子游走，已经被成功用在量子算法的设计与分析上。最近，一些作者引入了一个并发量子程序的模型，模型用 qMC 作为 Hart-Sharir-Pnueli 的 Markov 链的概率并发程序的量子扩展。这篇论文考虑 qMC 的验证问题。

可达性分析在经典与概率系统的验证与模型检测上均处于中心地位。量子系统的模型检测首先是被物理学家以量子控制的角度进行研究，但它们只考虑了在单步演化下可达的状态。在中，qMC 的可达性被考虑了，它被用在了并发量子程序的终止检测上。然而，中研究的可达性可以被看做定性的可达性，因为算法只能计算可达空间，但可达概率没有被研究。这篇论文是的延伸，目的是研究 qMC 的定量的可达性分析。更精确地，这篇论文的目标是给出计算可达性，重复可达性，持续可达性的（经典）算法。

经典 MC 的可达性分析技术依赖于图可达性问题的算法，特别是找到 MC 导出的图的底层强连通分量。这些算法从 1970 年早期就被图算法群体深入地研究了，可以被直接应用到 MC 的可达性分析上。然而，我们没有 qMC 的对应算法，只能从头开始。所以，为了研究 qMC 的可达性分析，我们引入了 BSCC 的概念，并开发了一个寻找 qMC 的 BSCC 分解的算法。有趣的是，经典与量子情况的 BSCC 分解有一些必要的不同。比如说，qMC 的 BSCC 分解不一定是唯一的。而且，寻找 BSCC 的经典算法如深度优先搜索不能直接被应用到 qMC 上。相反地，寻找 qMC 的 BSCC 需要非常不同的想法，依赖于超算符的矩阵表示和矩阵算符算法。处理量子 BSCC 的主要挑战是保持量子系统的线性代数结构，这在经典情况中不存在。我们相信这些量子 BSCC 的结果有独立的意义。

这篇论文如下组织。预备知识在第二节。特别地我们重复了 qMC 的概念并定义了 qMC 的图结构。qMC 的 BSCC 的概念在第三节，同时我们还给出了用超算符的不动点刻画 BSCC 和检查一个子空间是否是 BSCC 的算法。在第 4 节中我们给出了暂态子空间的概念并且证明了 qMC 的空间可以被分解成暂态子空间和一系列 BSCC 的直和。进一步，我们证明了尽管这一分解不是唯一的，它的分量的维数是确定的。特别地，我们给出了一个构造 qMC 的 BSCC 的算法。借助第 3,4 节的准备，我们在第 5 节中研究了 qMC 的可达性，并给出了一个计算可达概率的算法。计算重复可达概率和一致可达概率的算法在第 6 节。第 7 节是简要介绍。

A.2 量子 Markov 链和其图论结构

A.2.1 量子理论基础

为了方便读者，我们复习量子理论的一些基本概念。细节可参照。量子系统的状态空间是一个 Hilbert 空间。在这篇论文中，我们只考虑有限维 Hilbert 空间 $\mathcal{H}$，即一个有内积的复向量空间。两个向量 $|\phi\rangle, |\varphi\rangle \in \mathcal{H}$ 的内积记作 $\langle\phi|\varphi\rangle$。一个纯量子态是一个归一化向量 $|\phi\rangle \in \mathcal{H}$，满足 $\langle\phi|\phi\rangle = 1$。我们说两个向量 $|\phi\rangle$ 和 $|\varphi\rangle$ 是正交的，如果 $\langle\phi|\varphi\rangle = 0$，记作 $|\phi\rangle \perp |\varphi\rangle$。一个荤太用一个密度矩阵表示，即 $\mathcal{H}$ 中的一个半正定算子 ρ，满足 $tr(\rho) = 1$。或者等价地，一个半正定迹为一的 $n \times n$ 矩阵，其中 $\dim \mathcal{H} = n$。特别地，对每一个纯态 $|\psi\rangle$，我们有对应的密度矩阵 $\psi = \langle\psi|\,|\psi\rangle$。为了简化，我们经常交替使用纯态 $|\psi\rangle$ 和密度矩阵 ψ。一

个正算符 ρ 被称作部分密度矩阵如果有 $tr(\rho) \leq 1$。$\mathcal{H}$ 上的部分密度算子被记为 $\mathcal{D}(\mathcal{H})$。一个部分密度算符 ρ 的支撑 $\mathrm{supp}(\rho)$ 定义为由其非零特征值的特征向量张成的子空间。$\mathcal{H}$ 上所有的线性算子，也就是所有满足 $d = \dim\mathcal{H}$ 的 $d \times d$ 矩阵记作 $\mathcal{B}(\mathcal{H})$。

对 $\mathcal{H}$ 上的任何向量集合 V，我们用 $\mathfrak{span}\, V$ 表示 V 章程的 $\mathcal{H}$ 的子空间。也就是说，他包含所有 V 中的向量的有限线性组合。一个算子 P 被称作 X 上的投影如果它满足对所有 $|\phi\rangle \in X$ 有 $P|\phi\rangle = |\phi\rangle$，对所有 $|\phi\rangle \in X^{\perp}$ 有 $P|\phi\rangle = 0$。我们把 X 上的投影算子记作 P_X。根据量子测量理论，对任何密度矩阵 ρ，$tr(P_X\rho)$ 是混合态 ρ 在子空间 X 上的概率。设 $\{X_k\}$ 是 $\mathcal{H}$ 的一族子空间，它们的合并定义为

$$\bigvee_k X_k = \mathfrak{span}(\bigcup_k X_k)$$

特别地，我们用 $X \vee Y$ 代表两个子空间 X 和 Y 的合并。容易看出 $\bigvee_k X_k$ 是最小的包含所有 X_k 的 $\mathcal{H}$ 的子空间。

联合量子系统用张量积表示。如果一个量子系统由 $\mathcal{H}_1$ 和 $\mathcal{H}_2$ 两个子系统组成，它的状态空间是 $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$，它是由向量 $|\phi_1\rangle|\phi_2\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$ 张成的子空间，其中 $|\phi_1\rangle \in \mathcal{H}_1$，$|\phi_2\rangle \in \mathcal{H}_2$。对任何 $\mathcal{H}_1$ 上的算子 A_1，$\mathcal{H}_2$ 上的算子 A_2，它们的张量积 $A_1 \otimes A_2$ 被定义为 $(A_1 \otimes A_2)(|phi_1\rangle|\phi_2\rangle) = (A_1|\phi_1\rangle|\phi_1\rangle) \otimes (A_2|\phi_2\rangle)$ 对所有 $|\phi_1\rangle \in \mathcal{H}_1$，$|\phi_2\rangle \in \mathcal{H}_2$ 成立，并满足线性性。

封闭量子系统的演化由酉算子表示，即一个 $\mathcal{H}$ 上的酉算子 U 满足 $U^{\dagger}U = UU^{\dagger} = I$，其中 I 是 $\mathcal{H}$ 上的恒等算符。一个纯态 $|\phi\rangle$ 在演化之后变成 $U|\phi\rangle$，一个混态变成 $U\rho U^{\dagger}$。开放量子系统的演化由超算子表示，即一个 $\mathcal{H}$ 上的线性算子空间上的线性映射，满足下列条件：

1. $tr(\mathcal{E}(\rho)) \leq tr(\rho)$ 对所有 $\rho \in \mathcal{D}(\mathcal{H})$ 成立，等号成立代表保迹的 $\mathcal{E}$；
2. 完全正：对任何额外的 Hilbert 空间 $\mathcal{H}_R$，$(I_R \otimes \mathcal{E})(A)$ 在 A 为 $\mathcal{H}_R \otimes \mathcal{H}$ 上的正算子的情况下为正，其中 $\mathcal{H}_R$ 为 $\mathcal{H}_R$ 上的线性算子空间上的恒等映射。

在这篇论文中，我们只考虑保迹超算子。每个超算子都有 Kraus 算子和表示：$\mathcal{E} = \sum_i E_i \cdot E_i^{\dagger}$，或者具体地说，

$$\mathcal{E}(\rho) = \sum E_i \rho E_i^{\dagger}$$

对所有 $\rho \in \mathcal{D}(\mathcal{H})$ 成立，其中 E_i 是 $\mathcal{H}$ 上的算子，$\sum_i E_i^\dagger E_i = I$

。

A.2.2 量子 Markov 链

现在我们准备好引入量子 Markov 链的概念。回忆量子 Markov 链是一个有序对 (S, P)，其中 S 是状态的有限集合，P 是转移概率矩阵，即一个映射 $S \times S \to [0, 1]$ 满足 $\sum_{t \in S} P(s, t) = 1$ 对任何 $s \in S$ 成立，其中 $P(s, t)$ 是从 s 到 t 的概率。一个量子 Markov 链是一个 Markov 链的量子推广，其中 Markov 链的状态空间用 Hilbert 空间代替，转移矩阵由超算符代替。

定义 A.1: 量子 Markov 链是有序对 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$，其中 $\mathcal{H}$ 是有限维 Hilbert 空间，$\mathcal{E}$ 是 $\mathcal{H}$ 上的超算符。

量子 Markov 链的行为可以如下描述：如果目前进程在混态 ρ 中，下一步他将在状态 $\mathcal{E}(\rho)$。ρ 与 $\mathcal{E}(\rho)$ 均可以用统计系综表示：

$$\rho = \sum_i p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|, \mathcal{E}(\rho) = \sum_j q_j \left|\psi_j\right\rangle \left\langle\psi_j\right|$$

其中 $p_i, q_j \geq 0$ 对所有 i, j 成立，并且 $\sum_i p_i = \sum_j q_j = 1$。所以，超算符 $\mathcal{E}$ 可以被理解成转移系综 $\{(p_i, |\phi_i\rangle)\}$ 到 $\{(q_j, |\psi_j\rangle)\}$ 的变换。这样看来，量子 Markov 链是 Markov 链的推广。

A.2.3 量子 Markov 链中的图

量子 Markov 链下有一个自然的图结构。这可以通过引入相邻结构清楚地看到。首先，我们引入一个辅助记号。$\mathcal{H}$ 的子空间 X 在超算符 $\mathcal{E}$ 下的像定义为

$$\mathcal{E}(X) = \vee_{|\psi\rangle \in X} \operatorname{supp}(\mathcal{E}(\psi))$$

直观上，$\mathcal{E}(X)$ 是 X 里的态在 $\mathcal{E}$ 下的像张成的子空间。

定义 A.2: 设 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$ 是一个量子 Markov 链，$|\varphi\rangle$ 和 $|\psi\rangle$ 是 $\mathcal{H}$ 上的纯态，ρ，σ 是 $\mathcal{H}$ 上的混态。则

1. 如果 $|\varphi\rangle \in \mathcal{E}(X_\psi)$，则 $|\varphi\rangle$ 与 $|\phi\rangle$ 在 $\mathcal{G}$ 中相邻，记为 $|\psi\rangle \to |\varphi\rangle$。

2. 如果 $|\varphi\rangle \in \mathcal{E}(\mathrm{supp}(\rho))$，则 $|\varphi\rangle$ 与 ρ 相邻。记为 $\rho \to |\varphi\rangle$。
3. 如果 $\mathrm{supp}(\sigma) \subseteq \mathcal{E}(\mathrm{supp}(\rho))$，则 σ 与 ρ 相邻. 记为 $\rho \to \sigma$。

定义 A.3： 1. 一个量子 Markov 链中相邻的密度算子序列 $\pi = \rho_0 \to \rho_1 \to \rho_2 \cdots \rho_n$ 被称作 $\mathcal{G}$ 中一条 ρ_0 到 ρ_n 的道路，其长度为 $|\pi| = n$。
2. 对任何密度算子 ρ 和 σ，如果有一条 ρ 到 σ 的道路，我们说 σ 在 $\mathcal{G}$ 中是从 ρ 可达的。

定义 A.4： 设 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$ 是一个量子 Markov 链。对任何 $\rho \in \mathcal{D}(\mathcal{H})$，它在 $\mathcal{G}$ 中的可达空间为

$$\mathcal{R}_{\mathcal{G}}(\rho) = \mathfrak{span}\{|\psi\rangle \in \mathcal{H} : |\psi\rangle \text{ is reachable from } \rho in \mathcal{G}\}$$

下面的引理对我们后面的讨论非常有用。

引理 A.1： 1.（可达性的传递性）对任何 $\rho, \sigma \in \mathcal{D}(\mathcal{H})$，如果 $\mathrm{supp}(\rho) \subseteq \mathcal{R}_{\mathcal{G}}(\sigma)$，那么 $\mathcal{R}_{\mathcal{G}}(\rho) \subseteq \mathcal{R}_{\mathcal{G}}(\sigma)$
2. 如果 $d = dim\mathcal{H}$，那么对任何 $\rho \in \mathcal{D}(\mathcal{H})$，我们有

$$\mathcal{R}_{\mathcal{G}}(\rho) = \bigvee_{i=1}^{d-1} \mathrm{supp}(\mathcal{E}^i(\rho))$$

A.3 底部强连通分量

A.3.1 基本定义

底部强连通分量的概念在模型检测 Markov 链中扮演重要角色。在这一节中，我们把这个概念扩展到量子情形。我们首先引入一个辅助记号。设 X 是一个 Hilbert 空间的一个子空间。设 $\mathcal{E}$ 是 $\mathcal{H}$ 上的一个超算符。$\mathcal{E}$ 限制在 X 上的限制定义为超算符 $\mathcal{E}|_X$：

$$\mathcal{E}|_X(\rho) = P_X \mathcal{E}(\rho) P_X$$

A.4 状态空间分解

一个经典 Markov 链中的状态是暂态如果有非零概率使得这个过程永不返回该态。一个广为人知的结果是一个状态是稳态当且仅当它属于某个底部强连通分量。这一节的目标是证明这个结果的量子推广。

定义 A.5： 对量子 Markov 链 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$，一个子空间 $X \subseteq \mathcal{H}$ 是暂态，如果

$$\lim_{k\to+\infty} tr(P_X \mathcal{E}^k(\rho)) = 0$$

为了给暂态子空间一个刻画，我们需要超算符 $\mathcal{E}$ 的近似平均的概念：

$$\mathcal{E}_\infty = \lim_{N\to\infty} \frac{1}{N} \sum_{n-1}^{N} \mathcal{E}^n$$

定理 A.1： 对量子 Markov 链 $\mathcal{G} = (\mathcal{H}, \mathcal{E})$，$\mathcal{E}_\infty$ 可以被分解成正交 BSCC 的直和。

A.5 结论

我们引入量子 Markov 链的 BSCC 的概念，然后研究了 qMC 的 BSCC 分解。这是我们能够给出计算重复可达概率和持续可达概率。这些算法可以用来验证物理系统的安全性和生动性，在未来量子计算机的研究中有应用。

References

书面翻译对应的原文索引

[1] Shenggang Ying, Yuan Feng, Nengkun Yu, Mingsheng Ying, Reachability Probabilities of Quantum Markov Chains