arXiv:2603.29896v1 [math.QA] 31 Mar 2026

超越自由情形与扭曲Kitaev模型的量子比特稳定子

Ruslan Maksimau

摘要。我们研究任意维数 d的量子位稳定子形式体系。在自由情形下，我们证明稳定子形式体系的基本定理仍然成立：若稳定子子群 H 是自由的 $\mathbb{Z}/d\mathbb{Z}$-模，且不含非平凡标量，那么受保护空间 V^H 可自然地识别为由较少个、维数相同的量子位构成的态空间，而商 $N(H)/H$ 可识别为作用于较少个量子位的泡利群。

随后，我们去掉自由性假设，并描述一般情况下由此产生的结构。在这种情况下，受保护空间可识别为量子位空间的张量积，各空间的维数可能较小；商$N(H)/H$ 则可由相应的量子比特 Pauli 群的乘积来描述，这些群的维数可能较小，并共享一个中心。我们还刻画了平移自由情形：恰好在这种情况下， $N(H)/H$ 又是一个通常的量子比特 Pauli 群。我们的方法具有代数性且统一，尤其适用于量子比特 Kitaev 模型及其平移和扭曲变体。

目录

1. 引言 1**第零部分：准备**2. 辛 $(\mathbb{Z}/d\mathbb{Z})$-模 5**第一部分：自由情形**3. 量子位的自由稳定子形式体系 10 4. 量子位的Kitaev 模型 15**第二部分：一般情形**5. 放宽自由性假设 18 6. 扭曲Kitaev模型 28 参考文献 29

1. 引言

在经典计算和量子计算中，我们都必须处理影响所处理信息的错误。为此，我们可能需要执行纠错过程。最简单的经典示例之一是重复码，其中每个比特 $b \in \{0,1\}$ 都被编码为三个相同的比特 $bbb \in \{0,1\}^3$。如果某个比特受到错误影响，所得的三元组便不再是常量，这使我们能够检测并纠正错误。这种纠错码可以描述为从 $\{0,1\}^n$ 到 $\{0,1\}^{3n}$的映射，这意味着我们用 $3n$ 个物理比特编码 n 个逻辑比特。更一般地，我们可能希望将 k 个逻辑比特编码为

n 个物理比特，这对应于映射 $\{0,1\}^k \hookrightarrow \{0,1\}^n$，以及一套用于检测和纠正错误的过程。

在量子计算中，我们使用量子比特而不是比特。量子比特态不是 $\{0,1\}$ 的元素，而是一个 2 维厄米向量空间中的元素，该空间有一组标准正交基 $|0\rangle, |1\rangle$；我们将这个空间简称为 $\mathbb{C}^2$。对于不熟悉量子力学基础知识的读者，我们请您参阅作者为工作组 [7]，所作讲座撰写的笔记，其中以面向代数学家的语言，对量子比特及相关概念作了初步介绍。

现在，如果我们想用 n 个物理量子比特来编码 k 个逻辑量子比特，这就相当于寻找一个线性映射 $(\mathbb{C}^2)^{\otimes k} \hookrightarrow (\mathbb{C}^2)^{\otimes n}$。Gottesman [4] 提出了一种构造此类线性映射的方法。下面简要回顾 Gottesman 稳定子形式体系。

设 $\mathcal{P}_n$ 为作用在 n 量子比特向量空间 $V = (\mathbb{C}^2)^{\otimes n}$ 上的 n 量子比特泡利群。对于子群 $H \subset \mathcal{P}_n$，令 $V^H = \{v \in V \mid \forall h \in H,\, h(v) = v\}$。用 $N(H)$ 表示 H 在 $\mathcal{P}_n$ 中的正规化子。

命题 (Gottesman)。设 $H \subset \mathcal{P}_n$ 是一个不含非平凡标量的任意阿贝尔子群，且 2^k 是 H 的基数。那么存在一个酉同构 $V^H \simeq (\text{复数域}^2)^{\otimes n-k}$，以及一个群同构 $N(H)/H \simeq \mathcal{P}_{n-k}$，使得 $N(H)/H$ 在 V^H 上的作用可识别为 $\mathcal{P}_{n-k}$ 在 $(\text{复数域}^2)^{\otimes n-k}$ 上的作用。

上述命题使我们能够构造形如 $(\text{复数域}^2)^{\otimes n-k} \hookrightarrow (\text{复数域}^2)^{\otimes n}$ 的有趣线性映射，并将 $(\text{复数域}^2)^{\otimes n-k}$ 上所有有趣的算子表示为 $V = (\text{复数域}^2)^{\otimes n}$ 上保持 V^H 不变的算子的限制。

现在，我们希望将这一结果推广到从量子比特（复数域^2）转向量子位（复数域^d）的情形，其中 d 是任意正整数。本文旨在为量子位的稳定子形式体系提供统一的代数表述。本文重点不在于构造新的码，而在于提供一个概念框架，使稳定子码的结构清晰明了。

我们研究作用于 $V = (\mathbb{C}^d)^{\otimes n}$ 的 n-量子比特 Pauli 群 $\mathcal{P}_n = \mathcal{P}_n^{(d)}$。上述针对量子比特的命题证明，基于在 $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ 上进行的一些辛线性代数，并将其应用于群 $\mathcal{P}_n$ 对其中心取商后得到的 $\mathbb{F}_2$-向量空间（该向量空间具有自然的辛形式）。当 $d = p$ 为素数时，很容易将 Gottesman 的结果推广到这一情形，因为此时我们可以在有限域 $\mathbb{F}_p$ 上进行研究。然而，对于一般的 d，情况就不那么简单了。我们无法使用域上的向量空间，而必须研究环 $\mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z}$ 上的模。这个环与域相去甚远，而且还含有零因子。这带来了额外的技术难题。

量子比特情形下稳定子空间 V^H 的维数公式已有定论，例如参见 [3, 定理 1]。本文提出的方法超越了维数计数，还描述了 $N(H)/H$ 在 V^H 上的诱导作用，并在统一的代数框架下将其识别为泡利型群。

在 $\mathbb{Z}_d$-模中，最简单的是自由 $\mathbb{Z}_d$-模，它们最接近域上的向量空间。（当 $d = p$ 为素数时，所有模都是自由模。）我们分两步推广 Gottesman 的结果。首先，假设 H 是自由 $\mathbb{Z}_d$-模。第二步，我们去掉“自由”这一假设，研究一般情况下 V^H 的结构以及 $N(H)/H$ 在其上的作用。

下面的定理 A 是本文在“自由”情形下的主要结果。它表明，当我们假设 H 是自由模时，Gottesman 结果显而易见的自然推广成立。

定理 A (定理 3.13)。 假设 $H \subset \mathcal{P}_n^{(d)}$是一个不含非平凡标量的交换子群，且 H 是秩为 k的自由$\mathbb{Z}_d$-模。那么存在一个酉同构 $V^H \simeq$ (复数域$^d)^{\otimes n-k}$ 以及一个群同构 $N(H)/H \simeq \mathcal{P}_{n-k}^{(d)}$，使得 $N(H)/H$ 在 V^H 上的作用与 $\mathcal{P}_{n-k}^{(d)}$在(复数域$^d)^{\otimes n-k}$上的作用相对应。

接下来，在第 4 节中，我们将说明如何将这一结果应用于量子位 Kitaev 模型 [6] 的研究。本节不包含新的结果。不过，值得注意的是，与情形 $d = 2$一样，现在可以在稳定子形式体系内以统一的方式处理 Kitaev 模型，因此其主要性质可以直接从一般框架中得出，无需采用临时论证。

接下来，我们想了解去掉“自由”这一假设后会发生什么。若 d 为奇数，令 $d = d$；若 d 为偶数，令 $d = 2d$。设 $\zeta \in$C 是一个本原 d 次单位根。对于 d 的一个正因子 d_0，令 $\mathcal{P}^{(d_0,\zeta)}{}_n$ 为由 $\mathcal{P}^{(d_0)}{}_n$ 和乘以 ζ 的算子生成的 (C^{d_0})$^{\otimes n}$ 的子群。

以下定理是本文关于“非自由”情形的主要结果。

定理 B (定理 5.28). 假设 $H \subset \mathcal{P}_n^{(d)}$ 是一个不含非平凡标量的交换子群。那么我们可以找到 d 的正因子 $d_1, d_2, \ldots, d_k$，使得下述结论成立。存在一个酉同构

$$V^H \simeq \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \ldots \otimes \mathbb{C}^{d_k}$$

以及一个群同构

$$N(H)/H \simeq \mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)}$$

使得 $N(H)/H$ 在 V^H 上的作用可识别为

$$\mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)} \quad on \quad \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \ldots \otimes \mathbb{C}^{d_k}.$$

上文中，记号 $G_1 \times_\zeta G_2$ 表示两个群的直积，其中两群中由 ζ 相乘定义的算子被视为相同。

最后，我们希望找出对“自由”这一假设的最小推广，使得定理 A 的结论仍然成立。我们引入一种平移自由群 H 的方法。由此得到以下定理。

定理 C (定理 5.31)。 设 H 是 $\mathcal{P}_n^{(d)}$ 的一个不含非平凡标量的阿贝尔子群。那么，对于某个 k，群 $N(H)/H$ 与 $\mathcal{P}_{n-k}^{(d)}$ 同构，当且仅当 H 是移位自由的。此外，在此情形下， $N(H)/H$ 在 V^H 上的作用可以与 $\mathcal{P}_{n-k}^{(d)}$ 在(复数域$^d)^{\otimes(n-k)}$ 上的作用等同，其中同构 $V^H \simeq$ (复数域$^d)^{\otimes(n-k)}$ 是酉的。

我们还定义了扭曲这一概念，它是对平移概念的轻微推广，并研究它如何改变 $N(H)/H$和 V^H的结构。最后，我们将这一概念应用于 Kitaev 模型，并引入移位 Kitaev 模型和扭曲Kitaev模型的概念。鉴于我们针对量子位的广义稳定子形式体系，对 Kitaev 模型的这类修改可以自动进行研究。这体现了这种方法的优势，也体现了将稳定子

形式体系用作通用工具，而不是为研究特定模型寻找特殊论证的理念。我们想强调，平移和扭曲并非专为 Kitaev 模型引入的修改，而是源自一般稳定子形式体系的自然构造。

本文结构如下。出于教学考虑，我们将其分为两部分：第一部分（自由情形）和第二部分（一般情形）。非自由情形的理论自然涵盖自由情形。不过，我们决定作此区分，因为不同部分可能会吸引不同的读者。

在这两部分之前，还有第零部分，研究辛 $\mathbb{Z}/d\mathbb{Z}$- 模。该部分没有新的结果，但为我们所需的一般性下关于 $\mathbb{Z}/d\mathbb{Z}$- 模的所有引理作了准备。接下来，第一部分分为第 3 节和第 4 节：第 3 节介绍自由情形下稳定子形式体系的一般定理；第 4 节则说明如何将其应用于 CSS 码和 Kitaev 环面码等例子。随后，关于一般（非自由）理论的第二部分也分为两节。在第 5 节中，我们给出非自由稳定子形式体系的一般结果。在第 6 节中，我们将这些结果应用于移位和扭曲的 Kitaev 模型。

本文面向两类不同的读者：一类是量子信息领域的研究人员，尤其是从事量子纠错和稳定子形式体系研究的人员；另一类是对底层代数结构感兴趣、但可能不太熟悉量子信息的代数学家。因此，本文的部分内容可能会回顾某一领域中已属标准的基础知识，而另一些部分对于来自另一领域的读者而言则可能显得较为简略。作者力求兼顾这两种视角，以便两类读者都能理解本文内容。在若干证明中，从代数角度来看，采用同调代数是很自然的做法；然而，我们有意避免使用这种方法，转而给出更直接的论证。

尽管这并非本文最初的目标，但这种方法足够自洽，因此文中出现的所有量子信息相关论述，均在我们的框架内予以证明，而不将文献中的知名结果当作黑箱使用。不过，我们仍会引用原始文献，以恰当地致谢相关作者。

在若干情形下，本文给出的论证为已知结果提供了更简短、更具代数性的证明，而这些结果原有的证明往往更偏向算法或计算。这反映出，一旦建立起代数框架，这些结果便会在其中自然地呈现出来，只需付出相对较少的额外努力即可得到。

例如，我们重新得到了以下已知结果：

- 从 Clifford 群到辛群的映射的满射性[5]，
- 自由辛 $\mathbb{Z}/d\mathbb{Z}$-模的拉格朗日子模的分类 [1]，
- 受保护空间的维数 V^H [3]。

从这个意义上说，本文也可作为一篇简明导论，以纯代数语言向代数学家介绍稳定子形式体系和量子纠错的若干代数方面。

第零部分：准备

2. 辛 (Z/dZ)-模

2.1. 记号与约定。 我们将 Z_d 简记为 Z/dZ。不过，有时当我们想强调它是环 Z 对理想 dZ 取商所得的商环时，使用记号 Z/dZ 会更方便。

我们先说明一下 Z_d-模这一概念。通常，当 R 是任意环时，我们说“M 是一个 R-模”，意思是 M 是一个阿贝尔群，并带有一种额外结构，即由 R 的元素进行乘法作用，且满足一些自然公理。

然而，对于 $R = \mathsf{Z}_d$，更合理的看法是：成为一个 Z_d-模并非阿贝尔群 M 的额外结构，而是其额外性质。事实上，由于每个阿贝尔群 M 都有唯一的 Z-模结构，成为 Z-模与成为阿贝尔群并无区别。现在，对于一个 Z-模 M，Z 的作用可经由 $\mathsf{Z}_d = \mathsf{Z}/d\mathsf{Z}$ 的作用分解，当且仅当理想 dZ 在 M 上的作用为零；也就是说，当且仅当M 的每个元素的阶都整除 d。因此，最终这意味着“M 是一个 Z_d-模”与“M 是一个阿贝尔群，且其每个元素的阶都整除d”并无区别。此外，对于一个 Z_d-模 M，“ M 的 Z_d-子模”与“ M 的子群”这两个概念也并无区别。

对于满足 $a \leqslant b$ 的 $a, b \in$Z，我们设定 $[a;\ b] = \{a, a+1, \ldots, b-1, b\}$。这里的意思是，对于 $a = b$，该集合只包含一个元素。对于有限集 X，用 $\#X$ 表示 X 中元素的个数。

对于 Z_d-模 M 中的若干元素 $e_1, e_2, \ldots, e_n$，我们用 $\langle e_1, e_2, \ldots, e_n\rangle$ 表示由它们生成的子模（即所有 Z_d-线性组合）。回顾一下，若 $(e_1, \ldots, e_n)$ 是 M 的一组基，则要求 $M = \langle e_1, \ldots, e_n\rangle$，并且对于任意关系 $\sum_{i=1}^n \lambda_i e_i = 0$，若 $\lambda_i \in$ 属于 Z_d，则必有 $\lambda_1 = \cdots = \lambda_n = 0$。若一个 Z_d-模有一组基，则称其为自由。（本文只讨论有限 Z_d-模。）

为简便起见，我们常用同一个符号表示整数 $a \in$Z 及其在 Z_d 中的像。书写分数时，我们始终表示在 Z 中进行除法（只有整除时才有定义）；有时随后会将结果视为 Z_d 中的一个元素。例如，对于 d 的一个因子 a，我们可以写作 $\frac{d}{a} \in \mathsf{Z}_d$，表示先在 Z 中将 d 除以 a，然后再将所得结果的像视为 Z_d 中的元素。

2.2. 自由 Z_d-模。 下面的命题回顾有限 Z_d-模的著名分类。

命题 2.1。 设 N 是一个有限的 $\mathbb{Z}_d$-模。那么存在唯一的正整数元组 $(d_1, d_2, \ldots, d_n)$ 使得 $1 < d_1 \mid d_2 \mid \ldots \mid d_n \mid d$，且使得 $N \simeq \bigoplus_{r=1}^n \mathbb{Z}_{d_r}$。

以下命题称为史密斯标准形，它描述了有限秩自由 Z_d-模的子模。

命题 2.2。 假设 M 是秩为 n 的自由 $\mathbb{Z}_d$-模，且 N 是 M的子模。那么存在正整数 $a_1, a_2, \ldots, a_n$ 以及 M 的一个 $\mathbb{Z}_d$-基$e_1, e_2, \ldots, e_n$，使得 $a_1 \mid a_2 \mid a_3 \mid \ldots \mid a_n \mid d$，并且 N由 $a_1e_1, a_2e_2, \ldots, a_ne_n$生成。

注意，在上述命题中，某些 a_k 可以为 d。此时我们得到 $a_k e_k = 0$。

推论 2.3。 如果有限自由$\mathbb{Z}_d$-模 M 的子模 N 是自由的，那么 N 是 M 的直因子（即，对某个子模 $N' \subset M$，有 $M = N \oplus N'$）。此外，这样的每个补模 N' 也都是自由的。

证明。 考虑 N 的史密斯标准形。当且仅当存在一个指标 $k \in [0;\ n]$，使得若 $1 \leqslant i \leqslant k$ 则 $a_i = 1$，且若 $k < i \leqslant n$ 则 $a_i = d$ 时，子模 N 才是 Z_d 上的自由模。在这种情况下，显然 N 是一个直因子。此外，每个补模都同构于商模 M/N，显然它是自由的。□

推论 2.4。 若 N 是有限自由$\mathbb{Z}_d$-模 M 的自由子模，则 N 的每个基都可以补充为 M 的一个基。

证明。 这由上面的推论立即得出。 □

2.3. **交错形式**。

定义 2.5。 设 M 是一个 Z_d-模。设 ϕ: $M \times M \to \mathsf{Z}_d$ 是一个映射。若 ϕ 是一个交错形式，则称其为交错形式，当且仅当它是 Z_d-双线性的，并满足 $\phi(m, m) = 0$ 对每个 $m \in M$ 都成立。我们称 Z_d-子模 $Ker\phi = \{m_0 \in M | \forall m \in M, \phi(m_0, m) = 0\}$ 为形式的核。

注记 2.6。 注意，交错形式自动满足性质$\phi(m_1, m_2) = -\phi(m_2, m_1)$，其中 $m_1, m_2 \in M$。

设 M 是一个 Z_d-模。记 M^* 为其对偶 Z_d-模 $\mathrm{Hom}_{\mathbb{Z}_d}(M, \mathsf{Z}_d)$。

引理 2.7。 假设 M 是一个有限$\mathbb{Z}_d$-模，且 N 是一个子模。那么自然映射 $M^* \to N^*$ 是满射。

证明。 首先假设 M 是一个自由的 Z_d-模。由史密斯标准形（命题 2.2）可立即得出结论。

一般而言，我们可以将 M 嵌入有限自由 Z_d-模 M中。于是包含映射$N \subset M \subset M$给出 $M^* \to M^* \to N^*$.。由于 M是自由的，映射 $M^* \to N^*$是满射，因此映射 $M^* \to N^*$也是满射。□

引理 2.8。 设 M是有限的$\mathbb{Z}_d$-模。设 ϕ: $M \times M \to \mathbb{Z}_d$是一个交错形式。那么以下命题等价。

(a) 我们有核$\phi = \{0\}$。(b) 映射 $M \to M^*$, $m \mapsto \phi(m, \bullet)$ 是双射。

证明。 显然，条件（a）等价于（b）中映射的单射性。然而，由于 M 和 M^* 是基数相同的有限集，该映射的单射性与双射性并无区别。□

从现在起，我们始终假设 Z_d-模 M 是有限的。

定义 2.9. 对于有限 Z_d-模上的交错形式 ϕ，如果满足上述等价条件（a）和（b），则称其为辛 形式。我们只对有限模（此时这些条件等价）使用这一术语。我们也可以简单地说“（M，ϕ）是辛的”，意为“M 是一个具有辛形式 ϕ的有限 Z_d-模”。

固定 M 上的辛形式 ϕ。对于子模 $N \subset M$，我们定义 $N^{\perp} = \{m \in M | \forall n \in N,\ \phi(m,\ n) = 0\}$。

引理 2.10。我们有 $\#N^{\perp} = \#M\,\#N$。

证明。根据引理 2.7，态射 $M^* \to N^*$ 是满射。若通过辛形式 ϕ 将 M 与 M^* 等同，则此态射的核为 $N^{\perp}$。这意味着 $\#N^{\perp} = \#M^*\,\#N^* = \#M\,\#N$。□

推论 2.11. 我们有 $(N^{\perp})^{\perp} = N$。

证明。显然有 $N \subset (N^{\perp})^{\perp}$。然而，由基数的原因，这个包含映射必须是等式。□

定义 2.12。设 d_0 为 d 的一个正整数因子。初等辛 Z_d-模 S_{d_0} 是 Z_d-模 $\mathsf{Z}_{d_0} \oplus \mathsf{Z}_{d_0}$，配备辛形式 $\phi\colon (\mathsf{Z}_{d_0} \oplus \mathsf{Z}_{d_0}) \times (\mathsf{Z}_{d_0} \oplus \mathsf{Z}_{d_0}) \to \mathsf{Z}_d$，其定义为 $\phi((1,0),(0,1)) = d/d_0$。

如果 $(M_1,\ \phi_1)$ 和 $(M_2,\ \phi_2)$ 是两个带有交错形式的 Z_d-模，那么我们可以将它们的（正交）直和 $(M_1 \oplus M_2,\ \phi_1 \oplus \phi_2)$ 定义为 Z_d-模 $M_1 \oplus M_2$，并赋予交错形式 $\phi = \phi_1 \oplus \phi_2$，其定义为 $\phi((m_1,\ m_2),\ (m_1',\ m_2')) = \phi_1(m_1,\ m_1') + \phi_2(m_2,\ m_2')$。当我们使用记号 S_{d_0} 时，我们约定其上的辛形式是固定的。于是，我们可以讨论形如 S_{d_0} 的辛模的直和（并且约定所考虑的辛形式是通过直和得到的辛形式）。

引理 2.13。对于每个非零辛 $(M,\ \phi)$，我们都可以找到正整数 d_1、d_2、…、d_k，使得 $1 < d_1 \mid d_2 \mid d_3 \mid \ldots \mid d_k \mid d$，并且存在一个保持辛形式的 $M \simeq S_{d_1} \oplus S_{d_2} \oplus \ldots \oplus S_{d_k}$ 同构，该同构作用于 $\mathbb{Z}_d$-模。

证明。设 m 是 M 中一个阶最大的元素，并设 a 是它的阶。

根据引理 2.7，我们可以将每个从 $\langle m\rangle$ 到 M 的 Z_d-线性形式延拓，然后（利用 $M \simeq M^*$）可以找到 $m' \in M$，使得 $\phi(m',\ m) = \frac{d}{a}$。由于 m 的阶 a 是最大的，m' 的阶也同样是 a（由于 $\phi(m',\ m) = \frac{d}{a}$，它不可能小于 a）。

令 $N = \langle m,\ m'\rangle$ 为由 m 和 m' 生成的 M 的 Z_d-子模。由 N 的构造可知，我们有 $N^{\perp} \cap N = \{0\}$。然而，根据引理 2.10，由于 $\#N \cdot \#N^{\perp} = \#M$，我们得到 $M = N \oplus N^{\perp}$。

我们有 $N \simeq S_a$。由于 M 中元素的最大阶为 a，所有其他阶都必须是 a 的因子。特别地，$N^{\perp}$ 中所有元素的阶都是 a 的因子。然后我们只需对 $N^{\perp}$ 应用归纳法，便得到 $N^{\perp}$ 同构于若干个 $S_{a'}$ 的直和，其中 a' 是 a 的因子（并且这些 a' 可以按线性顺序排列，使得每个 a' 都整除下一个）。□

推论 2.14 (拉格朗日分解)。假设 (M, ϕ) 是辛的。那么我们可以找到一个 $\mathbb{Z}_d$-模 L，使得存在 $\mathbb{Z}_d$-模的同构 $M \simeq L \oplus L^*$，在此同构下，形式 ϕ 呈现如下：

$$((l_1, l_1'), (l_2, l_2')) \mapsto l_1'(l_2) - l_2'(l_1).$$

证明。对于初等辛模 S_{d_0}，该结论显然成立。因此，对于这类模的直和，该结论也自动成立。进而，由引理 2.13 可知，这对所有辛模都成立。□

2.4. **自由辛模**。

引理 2.15。 假设 M 是有限的，且 ϕ 是交错的。那么，以下两个条件等价。

(a) M 是自由的，且 ϕ是辛的。*(b)* 存在 M的一组基$(e_1, \ldots, e_n, f_1, \ldots, f_n)$，使得对于所有 $i, j \in [1; n]$，都有 $\phi(e_i, e_j) = \phi(f_i, f_j) = 0$, $\phi(e_i, f_j) = \delta_{i,j}$，其中$\delta_{i,j}$ 是克罗内克δ。

证明。 $(b) \implies (a)$显然。下面证明$(a) \implies (b)$。假设 M 是自由的，且 ϕ 是辛的。那么由引理 2.13 可得 $M \simeq S_{d_1} \oplus S_{d_2} \oplus \ldots \oplus S_{d_n}$。然而，模 M只有在 $d_1 = d_2 = \ldots = d_n = d$的情况下才可能是自由的（由命题 2.1 中 $d_1, d_2, \ldots, d_n$的唯一性）。此时，我们得到一组具有预期形式的基。□

定义 2.16。 我们称 $(e_1, \ldots, e_n, f_1, \ldots, f_n)$ 为自由辛 Z_d-模 M 的辛基，如果它是满足引理 2.15 (b) 中条件的基。

从上文引入的术语来看，对于带有交错形式 ϕ 的有限 M，自由且为辛模等价于存在辛基。从现在起，我们假设 M 是秩为 $2n$ 、带有辛形式 ϕ 的有限自由 Z_d-模。

定义 2.17。 设 N 是 M 的一个 Z_d-子模。

(a) 若 N 满足 $N \subset N^\perp$（也就是说，ϕ 在 N 上的限制为零），我们称 N 为各向同性的。

(b) 若 N 满足 $N = N^\perp$（也就是说，N 是各向同性的，且不能包含于严格更大的各向同性子模中；根据引理 2.10，这也等价于“N 是基数为 $\sqrt{\#M}$ 的各向同性子模”），我们称 N 为拉格朗日的。

(c) 我们称 N为辛子模，如果 $N \cap N^\perp = \{0\}$（也就是说，ϕ 在 N 上的限制仍然是辛形式）。

注 2.18。 另外请注意，根据引理 2.10，条件 $N \cap N^\perp = \{0\}$等价于 $M = N + N^\perp$，进而也等价于 $M = N \oplus N^\perp$。特别地，每个辛子模都有一个正交补，而该正交补也是辛子模。

引理 2.19。 设 M 是一个带有辛形式 ϕ的有限自由$\mathbb{Z}_d$-模。假设 L是 M的一个自由各向同性子模。那么， L 的每个基$(e_1, \ldots, e_k)$ 都可以扩充为 M的一个辛基$(e_1, \ldots, e_n, f_1, \ldots, f_n)$。

证明。根据引理 2.7，映射 $M^* \to L^*$ 是满射。于是，同构 $M \simeq M^*$ 使我们能够将 L^* 中的 Z_d-线性形式提升为 M 中的元素。由此我们可以构造元素 f_1、……、$f_k \in M$，使得 $\phi(e_i, f_j) = \delta_{i,j}$。元素 $(e_1$、……、e_k、f_1、……、$f_k)$ 显然是 Z_d-线性无关的（要看出这一点，只需将 $\phi(e_i, \bullet)$ 和 $\phi(f_i, \bullet)$ 应用于一个线性组合）。此外，我们可以假设所有 f_i 两两正交；否则，可以将 e_i 的适当线性组合加到每个 f_j 上。我们已经证明，元素 $(e_1$、……、e_k、f_1、……、$f_k)$ 构成 M 的子模 M_1 的辛基。

我们有 $M = M_1 \oplus M_1^\perp$。现在，根据推论 2.3， $M_1^\perp$也是自由的。由于 $M_1^\perp$是自由的辛模，我们可以找到$M_1^\perp$的一组辛基（e_{k+1}，…，e_n，f_{k+1}，…，f_n）。

□

如果没有“自由”这一假设，对于任意各向同性子模，就不存在引理 2.19 中那样的良好形式。不过，至少对于拉格朗日子模，这个问题可以解决，正如 [1, 定理 7]所示。

命题 2.20. 假设 $L \subset M$ 是拉格朗日的。那么存在 M 的辛基 $(e_1, \dots, e_n, f_1, \dots, f_n)$ 以及正整数 $d_1, d_2, \dots, d_n$，使得 $d_1 \mid d_2 \mid d_3 \mid \dots \mid d_n \mid d \mid d_1^2$，且 $L = \langle d_1 e_1, d_2 e_2, \dots, d_n e_n, \frac{d}{d_1} f_1, \frac{d}{d_2} f_2, \dots, \frac{d}{d_n} f_n \rangle$。

注记 2.21. 由引理 2.19 可知，如果拉格朗日 L 是自由的，那么在上述命题中，我们可以取 $d_1 = d_2 = \dots = d_n = d$，此时 $(f_1, \dots, f_n)$ 是 L 的一组基。

对于初等自由辛 Z_d-模 $S_d = \mathsf{Z}_d \oplus \mathsf{Z}_d$，手工描述拉格朗日子模很容易。

引理 2.22. N 中的每个各向同性子模都具有形式 $N = \langle ae, bf \rangle$，其中存在 S_d 的某个辛基 (e, f) 以及某些正整数 a, b，使得 $d \mid ab$ 且 $b \mid a$。特别地，S_d 的每个拉格朗日子模 L 都具有形式 $L = \langle ae, \frac{d}{a} f \rangle$，其中 a 是满足 $a \mid d \mid a^2$ 的正整数。

证明. 令 m 为 N 中的一个最大阶元素，令 c 为其阶。记作 $d = ac$。由于模 S_d 是自由的，我们可以写成 $m = ae$，其中 $e \in S_d$ 为某个元素。按照引理 2.13 证明中的相同论证，我们可以构造一个元素 $f \in S_d$，使得 $\phi(e, f) = 1$。于是 (e, f) 是 S_d 的一个辛基。

令 b 为满足 $bf \in N$ 的最小正整数。显然有 $d \mid ab$ 且 $b \mid a$。我们来证明 $N = \langle ae, bf \rangle$。

假设我们有 $xe + yf \in N$ 以及一些整数 x，y。由于 $xe + yf$ 的阶整除 c，因此有 $c(xe + yf) = 0$，从而 $d \mid cx$，这意味着 $a \mid x$。于是我们有 $xe \in N$，因此 $yf \in N$，这意味着 $b \mid y$。所以我们有 $xe + yf \in \langle ae, bf \rangle$。□

[1]中命题 2.20 的证明是算法性的。为保持一致，我们倾向于将其改写为另一种形式，并给出一个更直接的模论证明。

命题 2.23。 假设 $L \subset M$ 是拉格朗日的。那么我们可以选择 $M = M_1 \oplus M_2 \oplus \dots \oplus M_n$ 这一 M 的分解，使其成为自由辛子模的正交直和，且每个子模的维数为 2（即每个因子都同构于 S_d），并且对每个 $r \in [1; n]$，子模 $L \cap M_r \subset M_r$ 都是 M_r 中的拉格朗日子模（于是由基数的原因，我们自动有 $L = \oplus_{r=1}^{n} L \cap M_r$）。

证明。令 m 为 L 中的一个最大阶元素，并令 a 为它的阶。记 $d = ab$。由于模 M 是自由的，我们可以写成 $m = be$，其中 $e \in M$。按照引理 2.13 证明中的相同论证，我们可以构造一个元素 $f \in M$，使得 $\phi(e, f) = 1$。

由于 $\phi(e, f) = 1$，元素 e 和 f 显然是 Z_d-线性无关的。因此，由 e 和 f 生成的 M 的子模 $N = \langle e, f \rangle$ 是自由辛模。

我们断言 $af \in L$ 成立。事实上，由于 L 中元素的阶都是 a 的因子，对每个 $l \in L$，都有 $\phi(f, l) \in b\mathsf{Z}/d\mathsf{Z} \subset \mathsf{Z}/d\mathsf{Z} = \mathsf{Z}_d$，于是对每个 $l \in L$，都有 $\phi(af, l) = 0$。这表明 $af \in L^{\perp} = L$。

我们看到 $L \cap N$ 包含 $\langle be, af \rangle$，它是 N 的拉格朗日子空间。因此，由于 $L \cap N$ 是各向同性的，我们必有等式 $L \cap N = \langle be, af \rangle$。

现在我们声称 $L = (L \cap N) \oplus (L \cap N^{\perp})$。取 $l \in L$，并考虑分解 $l = l_1 + l_2$，使得 $l_1 \in N$ 且 $l_2 \in N^{\perp}$。由于 $L \cap N$ 是 N中的一个拉格朗日子空间，我们有 $(L \cap N)^{\perp} \cap N = L \cap N$。另一方面，我们知道 $l_1 = l - l_2 \in (L \cap N)^{\perp} \cap N$，因此 l_1 必定是 L的一个元素。于是，$l_2 = l - l_1$ 也必定是 L的一个元素。因此，我们有 $l = l_1 + l_2$，其中 $l_1 \in N \cap L$且 $l_2 \in L \cap N^{\perp}$。这表明 $L = (L \cap N) \oplus (L \cap N^{\perp})$。

由于基数的原因，子模 $L \cap N^{\perp} \subset N^{\perp}$是拉格朗日的。现在只需对带有拉格朗日子模 $L \cap N^{\perp}$的自由辛模 $N^{\perp}$ 应用归纳法。□

第一部分：自由情形

3. 量子位的自由稳定子形式体系

处理阿贝尔群时，我们通常将其视为 Z-模或 Z_d-模。在这种情况下，我们使用加法记号，并用 0 表示单位元。处理一般群（通常是非交换群）时，我们使用乘法记号，并用 1 表示单位元。如果恒等元是恒等线性算子，我们也可以用 I代替 1。例如，泡利群 $\mathcal{P}_n$ 的单位元记作 I。

例如，泡利群 $\mathcal{P}_n$ 不是交换的，因此我们对其使用乘法记号。然而，泡利群模其中心的商 $\mathcal{P}_n/\langle\zeta\rangle$ 是交换的。我们将其视为一个（辛）Z_d-模 F_n，并对 F_n 使用加法记号。对于不含非平凡标量的交换子群 $H \subset \mathcal{P}_n$，子群 H 与其在 F_n 中的像同构。不过，我们对其本身使用乘法记号，对它在 F_n中的像使用加法记号。

3.1. 量子位。 量子比特在数学上由向量空间 C^2 及作用于其上的两个矩阵描述：

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

它们满足 $X^2 = Z^2 = I$和 $XZ = -ZX$。注意，(I, X, Z, XZ) 是 $\mathsf{End}(\mathsf{C}^2)$ 的一组基。

现在，量子位将这一概念推广。设 d 为正整数（当 $d = 2$ 时，我们就得到量子比特）。记

$$\bar{d} = \begin{cases} d & \text{if } d \text{ is odd,} \\ 2d & \text{if } d \text{ is even.} \end{cases}$$

设 ζ 为 1 的 $\bar{d}$ 次本原单位根，并令 $\xi = \zeta^2$。那么 ξ 是 1 的 d 次本原单位根。考虑向量空间 C^d，以及作用于其上的以下两个矩阵：

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \xi & 0 & \cdots & 0 \\ 0 & 0 & \xi^2 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \xi^{d-1} \end{pmatrix}.$$

可以用以下方式来理解这一点。向量空间 C^d 的一组基是 $\{v_i, i \in \mathsf{Z}_d\}$，并且我们有 $X(v_i) = v_{i+1}$ 和 $Z(v_i) = \xi^i v_i$。那么

很容易看出它们满足 $X^d = Z^d = I$ 和 $ZX = \xi XZ$。此外，集合 $\{X^a Z^b \mid a, b \in \mathbb{Z}_d\}$ 是 End($\mathbb{C}^d$) 的一组基。

3.2. **量子比特 Pauli 群**。

定义 3.1. 单个量子比特的泡利群 是由 X 、 Z 以及作用为乘以 ζ的算子生成的子群 $\mathcal{P}_1 \subset GL(\mathbb{C}^d)$。（为简便起见，我们也将泡利群中的这个元素记作 ζ。）

不过，当我们考虑群代数 $\mathbb{C}\mathcal{P}_1$时， ζ 的记号可能会令人困惑。在这种情况下，我们可以给 $\zeta_{\mathcal{P}_1}$ 和 $\zeta_{\mathbb{C}}$ 加上下标，以区分泡利群中的元素与域 $\mathbb{C}$ 中的元素。

注 3.2. 算子 $ZXZ^{-1}X^{-1}$ 在 $\mathbb{C}^d$ 上的作用是乘以 ξ。因此，看起来只用 ξ 而不用 ζ 来定义泡利群或许更自然。通常加入 ζ 的原因之一是，若不加入它，命题 3.11 中的满射性就不成立，见注 3.12。这样做的另一个原因将在本文后文中阐明：届时我们会从海森堡扩张的角度考察泡利群。若不加入 ζ，泡利群将不满足定义 5.2 中的（c）。

注记 3.3。第 3.1 节末尾关于基的陈述可以加强为以下代数同构：

$$\mathbb{C}\mathcal{P}_1/(\zeta_{\mathcal{P}_1} - \zeta_{\mathbb{C}}) \simeq \mathrm{End}(\mathbb{C}^d).$$

设 n 为正整数。现在我们给出这一概念对 n个量子位的推广。令 $V = (\mathbb{C}^d)^{\otimes n}$。对于 $r \in [1;\ n]$，用 X_r 和 Z_r 表示作用于第 r个量子位上的算子 X 和Z，换言之，我们有

$$X_r = I^{\otimes r-1} \otimes X \otimes I^{\otimes n-r}, \quad Z_r = I^{\otimes r-1} \otimes Z \otimes I^{\otimes n-r}.$$

定义 3.4。（针对 n 个量子位的）泡利群 是子群 $\mathcal{P}_n \subset GL((\mathbb{C}^d)^{\otimes n})$，由 X_r 和 Z_r（其中 $r \in [1;\ n]$）以及按 ζ相乘的算子生成。（滥用记号，我们也将此算子记为 ζ。）

注记 3.5。由于 End$((\mathbb{C}^d)^{\otimes n}) \simeq$ End$(\mathbb{C}^d)^{\otimes n}$，代数 End$((\mathbb{C}^d)^{\otimes n})$具有以下基

$$\{X_1^{a_1} Z_1^{b_1} \dots X_n^{a_n} Z_n^{b_n},\ a_r, b_r \in [0; d-1]\}.$$

另一方面，我们有

$$\mathcal{P}_n = \{\zeta^c X_1^{a_1} Z_1^{b_1} \dots X_n^{a_n} Z_n^{b_n},\ a_r, b_r \in [0; d-1], c \in [0; \bar{d}-1]\}. \tag{3.1}$$

这立即表明我们有一个代数同构

$$\mathbb{C}\mathcal{P}_n/(\zeta_{\mathcal{P}_n} - \zeta_{\mathbb{C}}) \simeq \mathrm{End}((\mathbb{C}^d)^{\otimes n}).$$

推论 3.6。群 $\mathcal{P}_n$ 可按如下方式通过生成元与关系定义。生成元为 $Z_1, \dots, Z_n, X_1, \dots, X_n, \zeta$，关系为

$$\zeta^{\bar{d}} = 1, \qquad X_k\zeta = \zeta X_k, \qquad Z_k\zeta = \zeta Z_k, \qquad X_kX_r = X_rX_k, \qquad Z_kZ_r = Z_rZ_k,$$

$$X_kZ_r = Z_rX_k \ (\text{if } r \neq k), \qquad X_kZ_k = \zeta^2 Z_kX_k, \qquad X_k^d = 1, \qquad Z_k^d = 1.$$

证明。 将由上述生成元与关系生成的群记作 $\mathcal{P}'_n$ 。由于所有这些关系在泡利群中都成立，因此存在一个群同态 $\mathcal{P}'_n \to \mathcal{P}_n$ ，它将生成元映射到同名元素。由于$\mathcal{P}_n$ 由 Z_1、 . . . 、 Z_n， X_1、 . . . 、 X_n， ζ 生成，因此该同态是满射。

我们来检查单射性。显然，利用这些关系，我们可以将 $\mathcal{P}'_n$ 的每个元素写成 $\zeta^c X_1^{a_1} Z_1^{b_1} \dots X_n^{a_n} Z_n^{b_n}$，其中 a_r， $b_r \in [0;\ d-1]$ 和 $c \in [0;\ \bar{d}-1]$。然而，根据注 3.5，这些元素都映射到 $\mathcal{P}_n$ 中不同的元素。这就说明了单射性。

□

3.3. **量子位 Clifford 群**。

定义 3.7。 量子位 *Clifford* 群 Cl_n 是泡利群$\mathcal{P}_n$ 在酉群 U((复数域^d)$^{\otimes n}$) 中的正规化子，再对标量取商。

注 3.8。 下面给出量子信息文献中更常见的 Clifford 群定义。不过，正如第 5.3 节所解释的，Clifford 群 Cl_n 不过是固定 ζ 的 $\mathcal{P}_n$ 的自同构群 Aut$_\zeta$($\mathcal{P}_n$)。

设 F_n 是一个以 (z_1、 ..... 、 z_n、 x_1、 ..... 、 x_n) 为基的自由 $2n$ 维 $\mathbb{Z}_d$-模。泡利群 $\mathcal{P}_n$ 中的任意两个元素相乘后相差一个 ξ 的幂，这意味着对由 ζ 生成的子群 $\langle\zeta\rangle$ 取商后，该群变为交换群。此外，商群中每个元素的阶都是 d 的因数，因此该商群可视为一个 $\mathbb{Z}_d$-模。我们得到以下显然的引理。

引理3.9. 我们有以下 $Z\mathbb{Z}_d$-模同构

$$\mathcal{P}_n/\langle\zeta\rangle \simeq F_n, \qquad Z_r \mapsto z_r,\, X_r \mapsto x_r.$$

记 τ 为自然同态 τ: $\mathcal{P}_n \to F_n$ ，其定义为将商映射 $\mathcal{P}_n \to \mathcal{P}_n/\langle\zeta\rangle$ 与上述同构复合得到。考虑辛形式 ϕ: $F_n \times F_n \to \mathbb{Z}_d$ ，定义为

$$\phi(z_i, z_j) = \phi(x_i, x_j) = 0, \qquad \phi(z_i, x_j) = -\phi(x_j, z_i) = \delta_{i,j},$$

其中 $\delta_{i,\ j}$ 是克罗内克δ。以下引理显然成立。

引理 3.10。 对于 $x, y \in \mathcal{P}_n$ ， 我们有 $xy = \xi^{\phi(\tau(x),\tau(y))} yx$。

上述引理表明，即使对 $\mathcal{P}_n$ 取商 $\langle\zeta\rangle$ 后使群变得交换，辛形式仍保留了取商之前对易关系的全部信息。

设 Φ 是 $\mathcal{P}_n$ 的一个自同构，它由 Clifford 群中某个元素的共轭作用导出。若对于 x 有 $xy = \xi^a yx$ ， $y \in \mathcal{P}_n$ ，那么我们也有Φ(x)Φ(y) $= \xi^a$Φ(y)Φ(x)。这意味着，鉴于引理 3.10， Cl_n 通过共轭在 $\mathcal{P}_n/\langle\zeta\rangle \simeq F_n$ 上的作用保持辛形式 ϕ。特别地，我们得到一个群同态 $Cl_n \to Sp(F_n,\ \phi)$。

命题 3.11。 上述同态 $Cl_n \to Sp(F_n, \phi)$ 是满射。

证明。 这可由 [5, §IIC] 得出。更具体地说，他们声称，每个满足条件 [5, (10)] 的 $C \in Sp(F_n,\ \phi)$ 和 h ，都可以提升为 Cl_n 的一个元素，该元素在 $Sp(F_n,\ \phi)$ 中的像为 C。对 h 的条件仅仅是奇偶条件，因此对于每个 C ，都存在这样的元素 h。

这一事实在更一般情形下的另一种证明将在第 5 节给出（见注 5.23）。□

备注 3.12。泡利群的定义中额外加入了元素 ζ。我们来说明，如果不加入它，上述命题中的满射性为何会失效。取 $n=1$和 $d=2$。设想我们定义泡利群时没有加入 ζ（在 $d=2$ 的情形下，它就是 $i\in$C），并假设我们根据较小的泡利群定义 Clifford 群。那么泡利群包含 $\pm ZX$（其阶为 4），但不包含 $\pm iZX$（其阶为 2）。$Sp(F_1,\ \phi)$ 中由 $z_1\mapsto z_1+x_1, x_1\mapsto x_1$ 给出的辛映射不在修改后的 Clifford 群的像中，因为出于阶数的原因，不可能通过共轭 X 得到 $\pm ZX$。

3.4. **自由稳定子形式体系**。对于子群 $H\subset\mathcal{P}_n$，令 $V^H=\{v\in V|\forall h\in H,\ \ h(v)=v\}$ 为 V 中 H 的稳定子子空间。用 $N(H)$ 表示 $\mathcal{P}_n$ 中 H 的正规化子。

定理 3.13。设 H 是满足以下两个条件的阿贝尔子群：

$$H\cap\{\zeta^a,a\in\mathbb{Z}\}=\{I\}. \tag{3.2}$$

$$H\simeq\mathbb{Z}_d^k \text{ for } k\in\mathbb{Z}_{\geqslant 0}. \tag{3.3}$$

于是我们有以下结论。

我们有 $k\leqslant n$，并且存在一个从 V^H 到(复数域$^d)^{\otimes n-k}$ 的酉同构，使得 $N(H)/H$ 的作用与 $\mathcal{P}_{n-k}$ 在(复数域$^d)^{\otimes n-k}$上的作用相对应。

在证明定理之前，我们先做一些准备。

注 3.14。对于每个满足 (3.2) 的交换子群 $H\subset\mathcal{P}_n$，其正规化子与其中心化子相同。此外，对于 $x\in\mathcal{P}_n$，$\mathcal{P}_n$ 中 xHx^{-1} 的中心化子必为 $xN(H)x^{-1}$。但由于 xHx^{-1} 和 H 的元素至多相差 ξ的幂次，因此它们的中心化子必定相同。于是我们有$xN(H)x^{-1}=N(H)$。这意味着 $N(H)$是 $\mathcal{P}_n$的正规子群。

此外，由于映射 τ: $\mathcal{P}_n\to F_n$ 的核由标量构成，根据 (3.2)，复合映射 $H\to\mathcal{P}_n\to F_n$ 是单射。因此，H 与 $\tau(H)$同构。这尤其意味着，H 只能包含阶整除 d的元素。¯（而 $\mathcal{P}_n$ 本身包含阶为 d的元素。）由此可将 H 视为 Z_d-模。

命题 3.15。若子群 $H\subset\mathcal{P}_n$ 满足定理 *3.13* 中的条件，则 $k\leqslant n$ 和 H 可通过 ***Clifford*** 群 Cl_n 中的某个元素共轭到由 $Z_1,\ldots,Z_k$生成的 $\mathcal{P}_n$ 的子群。

证明。根据 (3.2)，群 H 与其像 $\tau(H)$同构（见注 3.14）。接下来，条件 (3.3)意味着 $\tau(H)$是 F_n 的一个秩为 k的自由 Z_d-子模。此外，根据引理 3.10，由于 H 是交换的，子模 $\tau(H)\subset F_n$ 按照定义 2.17 的含义是各向同性的。

现在，根据引理 2.19，我们有 $k\leqslant n$，并且可以找到一个元素 $\beta\in Sp(F_n,\ \phi)$，使得 $\beta(\tau(H))=\langle z_1,\ z_2,\ \ldots,\ z_k\rangle$。根据命题 3.11，元素 $\beta\in Sp(F_n,\ \phi)$ 可以提升为一个元素 $\hat{}\ \beta\in Cl_n$，从而得到 $\tau(\hat{}\beta H\hat{}\beta^{-1})=\langle z_1,\ z_2,\ \ldots,\ z_k\rangle$。这意味着 $\hat{}\ \beta H\hat{}\beta^{-1}$有一组形如 $\{\xi^{a_1}Z_1,\xi^{a_2}Z_2,\ldots,\xi^{a_k}Z_k\}$的生成元，其中 $a_1,\ldots,\ a_k$为整数。现在，我们还可以用 $X_1^{a_1}X_2^{a_2}\ldots X_k^{a_k}$共轭所得子群，从而得到由 $Z_1,\ Z_2,\ldots,\ Z_k$生成的子群。□

注记 3.16。 上面的命题可能会让人觉得，所有基于自由群 H 的码都是平凡的。然而，还应考虑以下一点。研究一个码的纠错性质时，考虑长度函数 ℓ很重要：$\mathcal{P}_n \to \mathbb{Z}_{\geqslant 0}$ 定义为表示式 (3.1) 中满足 a_i 或 b_i 非零的指标 i的数量。该长度函数在 Cl_n的作用下并不保持不变，因此，将 H 共轭为由 Z-算子生成的子群，并不能保持该码的纠错性质。若要使该码能够纠正许多错误，则要求 $N(H) \setminus H$ 中的元素具有足够大的长度。

定理 *3.13* 的证明。 鉴于命题 3.15，只需证明在 H 由 $Z_1, \dots, Z_k$生成的情形下定理成立。由于泡利群中 H 的正规化子$N(H)$与中心化子相同（见注 3.14），由引理 3.10 可知，当且仅当 $\tau(x) \in \langle z_1, z_2, \dots, z_k\rangle^\perp = \langle z_1, z_2, \dots, z_n, x_{k+1}, \dots, x_n\rangle$时，$x \in N(H)$成立。这意味着 $N(H)$由 $\zeta, Z_1, \dots, Z_n, X_{k+1}, \dots, X_n$生成。

向量空间 V^H 是子空间 $v_0^{\otimes k} \otimes (\text{复数域}^d)^{\otimes n-k} \subset (\text{复数域}^d)^{\otimes n}$，并且可自然地识别为 $(\text{复数域}^d)^{\otimes n-k}$。 $N(H)/H$ 在 V^H 上的作用由 $\zeta, Z_{k+1}, \dots, Z_n, X_{k+1}, \dots, X_n$生成。在此识别下，它们恰好是泡利群 $\mathcal{P}_{n-k}$ 作用于 $(\text{复数域}^d)^{\otimes n-k}$时的生成元。

□

3.5. **特征子空间**。设 $H \subset \mathcal{P}_n$ 如定理 3.13 中所述。由于 H中元素的阶整除 d，我们可以将群 $\mathrm{Hom}(H, \mathbb{Z}_d)$、$\mathrm{Hom}(H, \mu_d)$ 和 $\mathrm{Hom}(H, \mathbb{C}^*)$ 视为同一个群，并将它们统称为 H^*。设$V = \bigoplus_{\chi \in H^*} V_\chi$ 是 V 按 H的公共特征子空间作直和分解，其中对$\chi \in H^* = \mathrm{Hom}(H, \mathbb{C}^*)$，令 $V_\chi = \{v \in V \mid \forall h \in H,\, h \cdot v = \chi(h)v\}$。

于是，对每个 $x \in \mathcal{P}_n$ 和 $\chi \in H^*$，都有 $x(V_\chi) = V_{\chi'}$，其中某个 $\chi' \in H^*$ 满足该式。这给出了 $\mathcal{P}_n$ 在 H^*上的作用。此外，受保护空间 V^H 与 $V_{\mathbb{1}}$相同，其中 $\mathbb{1} \in H^*$ 是平凡特征标。

注 3.17。 显然，同一 $\mathcal{P}_n$-轨道中 χ的所有特征子空间 V_χ 维数都相同。因此，满足 $\dim V^H = \text{维数}\, V \# H^*$ 等价于 $\mathcal{P}_n$作用在 H^*上的传递性。

命题 3.18。 $\mathcal{P}_n$ 在 H^* 上的作用是传递的。特别地，所有向量空间 V_χ 的维数都相同。

证明。 根据注 3.17，只需验证 $\dim V^H = \text{维数}\, V \# H^*$。由定理 3.13， V^H 的维数为 d^{n-k}，因此这成立。□

注 3.19。 我们在上文根据受保护空间的维数推导出了传递性。不过，我们将在第 5.3 节看到，即使不作“自由”这一假设，传递性依然成立。但在那里，我们将注 3.17 中的推理顺序倒置：先利用海森堡扩张理论推导出传递性，再根据传递性推导出受保护空间的维数。

根据上述命题，每个特征子空间 V_χ 都具有如下形式

$$V_\chi = x(V^H) = V^{xHx^{-1}}$$

对于某个 $x \in \mathcal{P}_n$。此外， $\mathbb{1} \in H^*$ 在 $\mathcal{P}_n$ 中的稳定子是 $N(H)$。由于 $V_\chi = x(V_{\mathbb{1}})$， χ 的稳定子是 $xN(H)x^{-1} = N(H)$，因为 $N(H)$ 是正规子群。

因此，对于每个特征子空间 V_χ，泡利群中保持该子空间不变的元素集合恰好是 $N(H)$。

引理 3.20。 假设 $\chi \in H^*$ 和 $x \in \mathcal{P}_n$。那么我们有以下等价关系：

$$x(V_\chi) \subset V_\chi \Leftrightarrow x(V^H) \subset V^H \Leftrightarrow x \in N(H).$$

4. 量子位的 Kitaev 模型

4.1. CSS 码。 泡利群有两个特殊的阿贝尔子群：由 $Z_1, Z_2, \ldots, Z_n$ 生成的子群$\mathcal{P}_n^Z$，以及由 $X_1, X_2, \ldots, X_n$生成的子群 $\mathcal{P}_n^X$。此外，同态 τ: $\mathcal{P}_n \to F_n$ 诱导了 $\mathcal{P}_n^Z$ 和 $\mathcal{P}_n^X$与 F_n的拉格朗日子模 $\langle z_1, z_2, \ldots, z_n\rangle$ 和 $\langle x_1, x_2, \ldots, x_n\rangle$ 之间的同构。

当我们谈到 CSS 码时，指的是取一个具有特定形式的阿贝尔子群$H \subset \mathcal{P}_n$：$H = H^Z \cdot H^X$，其中 H^Z 是 $\mathcal{P}_n^Z$ 的子群，H^X 是 $\mathcal{P}_n^X$的子群，并且 H^Z 与 H^X 彼此对易。此外，显然，以这种方式选取 H^Z 和 H^X，等价于选取彼此正交的子模：$\langle z_1, z_2, \ldots, z_n\rangle$ 和 $\langle x_1, x_2, \ldots, x_n\rangle$。

下面的引理显然。

引理 4.1。 群 $H = H^Z \cdot H^X$ 自动满足 (3.2)。此外，若H^X 和 H^Z 满足 (3.3)，则 H 满足 (3.3)。

特别地，这意味着若 H^X 和 H^Z 满足 (3.3)，则我们可以对 H应用定理 3.13。

4.2. 模型的构造。 我们在此描述 Kitaev 模型 [6]的量子多能级版本。它可视为一般构造 [6, §5], 的特例 $G = \mathbb{Z}/d\mathbb{Z}$；当$d = 2$时，它还原了 [6, §2] 中的原始量子比特模型。不过需要注意的是，转向 $G = \mathbb{Z}/d\mathbb{Z}$ 时需要固定特定的约定，我们选择这些约定是为了使模型与我们的代数框架兼容。

设 $\Gamma = (S, E)$ 是一个有限有向图，其中 S 是顶点集， E 是箭集。设 $\Sigma = \Sigma_g$ 是一个亏格为$g \in \mathbb{Z}_{\geqslant 0}$的可定向紧曲面。假设图 Γ 嵌入于 Σ 中（即，曲面 Σ 是一个 CW 复形，其 1-骨架为 Γ）。用 F 表示面集（即， $\Sigma\backslash\Gamma$的连通分支）。注意，该图 Γ 由构造可知是连通的。

我们在图的每条有向边上放置一个量子比特。描述该系统的希尔伯特空间为 $V = (\mathbb{C}^d)^{\otimes \# E}$. 对于每个顶点 $s \in S$ 和每个面 $f \in F$，我们定义一个顶点算子 A_s: $V \to V$和一个面算子 B_f: $V \to V$，如下所示。

顶点算子 A_s 对每个放置在进入顶点 s的有向边上的量子比特施加 X，并对每个放置在离开顶点 s的有向边上的量子比特施加 X^{-1}。面算子 B_f 对每个放置在面 f 位于有向边右侧的有向边上的量子比特施加 Z，并对每个放置在面 f 位于有向边左侧的有向边上的量子比特施加 Z^{-1}。

$$X^{-1} \xrightarrow[Z]{Z^{-1}} X$$

注 4.2. 注意，有一个对合 ψ: 复数域$^d \to$ 复数域^d， $v_i \mapsto v_{-i}$。它满足$X\psi = \psi X^{-1}$ 和 $Z\psi = \psi Z^{-1}$。这意味着，当

我们反转图中的一条箭头，并同时对相应的量子比特应用 ψ 时，模型不会发生变化。

（$\#S+\#F$）算子 A_s 对于 $s\in S$ 以及 B_f 对于 $f\in F$ 是对易的。它们还满足

$$\prod_{s\in S} A_s = I, \qquad \prod_{f\in F} B_f = I, \qquad A_s^d = B_f^d = I.$$

现在取 $n = \#E$，并考虑由算子 A_s 对于 $s\in S$ 以及 B_f 对于 $f\in F$ 生成的泡利群的子群 H。

引理 4.3。上述定义的子群 H 满足条件（3.3），其中 $k = \#S+\#F-2$。

证明。群 H 显然具有第 4.1 节中所述的形式 $H = H^Z\cdot H^X$。只需验证 H^Z 是秩为 $\#F-1$ 的自由 Z_d-模，并且 H^X 是秩为 $\#S-1$ 的自由 Z_d-模。

我们来证明：如果对某个 $s_0\in S$ 移除一个 A_{s_0}，那么剩余的算子 $\{A_s, s\in S\backslash\{s_0\}\}$ 构成 Z_d-模 H^X 的一组基。假设我们有一个形式为 $\prod_{s\in S} A_s^{a_s} = I$ 的关系，其中 a_s 为某些整数。左侧的乘积作用在箭头 $e\in E$ 上的量子比特时，当箭头从 s_1 指向 s_2 时，其作用为 $X^{a_{s_1}-a_{s_2}}$。由于图是连通的，这说明算子 $\prod_{s\in S} A_s^{a_s}$ 只有在所有 a_s 模 d 同余时才可能是恒等元。这表明，一旦移除 A_{s_0}，剩余的 A_s 在 Z_d 上没有关系。

同样的论证适用于 B_f，从而证明 H^Z 是秩为 $\#F-1$ 的自由 Z_d-模。□

4.3. **受保护空间**。考虑受保护空间 V^H。第 3.4 节中发展的理论适用于它。其维数可由定理 3.13 推得：它等于

$$d^{n-k} = d^{\#E-\#S-\#F+2} = d^{2g}.$$

不过，也可以不使用稳定子形式体系，而通过下面明确的同调论证来计算（这与 [2] 中的论证很接近）。

命题 4.4。我们有 维数 $V^H = d^{2g}$。

证明。考虑胞腔上链复形

$$\mathcal{C}^0 \xrightarrow{d^0} \mathcal{C}^1 \xrightarrow{d^1} \mathcal{C}^2$$

关于 Z_d 的 Σ。我们有

- $\mathcal{C}^0 = \mathsf{Z}_d$ 线性组合，系数取自 S 中的元素，
- $\mathcal{C}^1 = \mathsf{Z}_d$ 线性组合，系数取自 E 中的元素，
- $\mathcal{C}^2 = \mathsf{Z}_d$ 线性组合，系数取自 F 中的元素。

V 的最显然的一组基由 $\mathcal{C}^1$ 给出。$\bigcap_{f\in F}\mathrm{Ker}(B_f - I)\subset V$ 的基是 $Z^1\subset\mathcal{C}^1$，它是这组基的子集，其中 $Z^1 = \mathrm{Ker}(d^1)$。最后，来自 A_s 的条件表明，某些基元素必须具有相同的系数。因此，V^H 的一组基为 $Z^1/B^1 = H^1(\Sigma,\ \mathsf{Z}_d)\simeq \mathsf{Z}_d^{2g}$，其中 $B^1 = \mathrm{Im}(d^0)$。□

注记 4.5。Kitaev 模型中 $V^H = V_{\mathbb{1}}$ 的维数也可以用一种更基础的计算方法求得。不借助稳定子

形式体系，我们可以看出，对特征集合 的作用具有传递性。事实上，将特征 $\chi \in H^*$ 描述为电荷构型（见第4.4节），并考察路径算子（见第4.5节）对特征集合的作用时，这种传递性就显而易见了。一旦知道所有特征子空间的维数相同，我们便可推出受保护空间 V^H 的维数为 维数$V\#H^*$。

4.4. 特征子空间的描述。我们可以分解为公共特征子空间的直和： $V = \bigoplus_{\chi \in H^*} V_\chi$。受保护空间 V^H 是其中一个 V_χ。

下面给出每个 χ的组合描述。设想每个顶点 $s \in S$ 都可以包含若干个基本电荷 e 的副本（约定拥有 d 个电荷 e等同于没有电荷，因此电荷按模 d计算）。类似地，我们设想每个面都可以包含若干个磁荷 m 的副本（同样按模 d计算）。

现在，我们将每个 χ 解释为一种电荷分布。固定 χ，并取 $v \in V_\chi$、$v \neq 0$。如果我们有 $A_s v = \xi^p v$ 和 $B_f v = \xi^q v$，那么就说在 s 处有 p 个基本电荷 e （或者简单地说，在 s处有电荷 $p{\cdot}e$），并且在 f 处有 q 个基本磁荷 m （或者简单地说，在 f 处有磁荷 $q \cdot m$ ）。此外，电荷构型必须满足总电荷与总磁荷模 d为零。

4.5. 路径算子。对于图中从顶点 s_1 到顶点s_2 的每条路径 t （路径的方向为从 s_1 到 s_2，但不要求该方向与此前选定的图的方向一致），我们按如下方式构造路径算子 $S^Z(t)$： $V \to V$。如果所选路径方向与图中相应边的方向一致，我们就在路径上的所有量子位上施加 Z；否则施加 Z^{-1}。

类似地，对于从面 f_1 到面 f_2的每条对偶路径 t （即对偶图中的路径，其中面与顶点互换），我们按如下方式构造路径算子$S^X(t)$： $V \to V$。对于路径所穿过的边，若其方向指向路径右侧，就在这些边上的所有量子位上施加 X；若指向左侧，则施加 X^{-1}。

下面来看这些算子如何改变特征空间。注意， $S^Z(t)$与所有 A_s 和 B_f 对易，唯独不与 A_{s_1} 和 A_{s_2}对易。这意味着，当我们有 $S^Z(t) \cdot V_\chi \subset V_{\chi'}$时，构型 χ 和 χ' 除了在 s_1 和 s_2 处之外，荷都相同。此外，我们看到路径算子将一个荷 $-e$ 从 s_1 移动到 s_2。

类似地，我们看到，对于对偶路径 t: $f_1 \to f_2$，路径算子 $S^X(t)$ 会将磁荷 $-m$从 f_1 移至 f_2。

注 4.6. 由于路径算子在 H^* 个 χ上具有传递作用，所有向量空间 V_χ 的维数都相同。这使得我们可以用另一种方式计算 V^H的维数。 V的总维数为 $d^{\#E}$，而可能的 χ的数量为 $d^{\#S+\#F-2}$。于是，每个 V_χ 的维数为 $d^{\#E-\#S-\#F+2} = d^{2g}$。

如果 Σ 是一个球面（$g = 0$），那么每个 V_χ 都是一维的。从物理上讲，这意味着电荷构型完全决定了系统的物理态。对于更高的亏格（$g > 0$），特征子空间 V_χ 是简并的（维数大于一）。这意味着电荷构型并不能决定物理系统的状态，并且还存在额外的内部自由度。

备注 4.7。 取一个向量 $v \in V^H$。取两条不同的路径 t, t'： $s_1 \to s_2$，它们具有相同的起点和终点。那么，只要路径 t 和 t' 同伦（对于 $g = 0$而言，这总是成立），我们就有 $S^Z(t) \cdot v = S^Z(t') \cdot v$。然而，对于 $g > 0$，一个不同伦于恒等元的环路（闭合路径）可以将向量 $v \in V^H$映射为 V^H中的另一个元素。

现在取一个向量 $v \in V_\chi$。那么，当路径 t和 t' 以一种不经过磁荷的方式同伦时，我们有 $S^Z(t) \cdot v = S^Z(t') \cdot v$。然而，如果同伦经过磁荷，那么 $S^Z(t)\cdot v$ 和 $S^Z(t')\cdot v$ 相差一个幂次为 ξ 的因子，该幂次取决于磁荷。

特别地，当一个 e-粒子顺时针绕一个 m-粒子移动时，系统的状态会乘上相位因子 ξ。

4.6. **正规化子**。 正如我们在第 3.5 节中所见，泡利群中保持每个特征子空间 V_χ 不变的元素集合都相同，且等于 $N(H)$。让我们来计算它。

命题 4.8。 群 $N(H)$ 由 ζ、与环路（闭路径） t 相关联的算子 $S^Z(t)$ 以及与对偶环路（闭对偶路径） t'相关联的算子 $S^X(t')$ 生成。

证明。 元素 $x \in \mathcal{P}_n$ 具有形式 $\zeta^c \prod_{e\in E} Z_e^{a_e} X_e^{b_e}$，其中 c, a_e, $b_e \in \mathbb{Z}$。 x 与顶点算子 A_s 对易这一事实对 a_e施加了条件，而 x 与面算子 B_f 对易这一事实则对 b_e施加了条件。

我们先来看 a_e。它们在图 Γ上定义了一个取值于 $\mathbb{Z}_d$的流，其中箭头 e 上的值为 a_e 模 d。 x 与顶点算子 A_s 对易这一条件，恰好表示在顶点 s处，流入流之和等于流出流之和。换句话说，这个流是无散流。根据图论中的一个标准结论，每个无散流都可以表示为若干个支撑在圈上的流之和。这说明 x 的 Z部分可以写成与环路 t相关联的算子 $S^Z(t)$的乘积。

类似地，系数 b_e 在对偶图上定义了一个取值于 $\mathbb{Z}_d$的流，而 x 与每个面算子 B_f 对易这一条件，恰好表示这个对偶流是无散流。因此， x 的 X部分可以写成与对偶环路 t'相关联的算子 $S^X(t')$的乘积。

□

第二部分：一般情形

5. 放宽自由性假设

5.1.**海森堡扩张**。 本节介绍一些关于海森堡群的常见概念。不过，由于我们希望海森堡群是有限的，并且与泡利群有恰当的关系（引理 5.17），因此采用了一些特定约定。我们的定义使用了由¯群 $\mu_{\bar{d}}$ 扩张得到的中心扩张，其中 d是单位根。定义 5.2 中的公理（c）并非完全标准。加入该公理，是因为我们希望得到唯一性（命题 5.5）、由生成元与关系给出的精确表示（引理 5.7），以及与泡利群的恰当关系（引理 5.17）。

定义 5.1。对于有限 Z_d-模 M，如果 $M=\langle y_1,y_2,\ldots,y_t\rangle$，并且对每个 $\lambda_1,\ldots,\lambda_t\in$，$\mathsf{Z}_d$ 中关系 $\lambda_1y_1+\lambda_2y_2+\ldots+\lambda_ty_t=0$ 都蕴含 $\lambda_1y_1=\lambda_2y_2=\ldots=\lambda_ty_t=0$，则称 $(y_1,y_2,\ldots,y_t)$ 是 M 的拟基。（此条件意味着这些元素之间的唯一关系来自它们各自的阶。）

如果 $(y_1,y_2,\ldots,y_t)$ 是 M 的拟基，且 d_k 是 y_k 的阶，那么每个元素 $m\in M$ 都能唯一地写成 $m=\sum_{k=1}^{t}\mu_ky_k$，其中 $\mu_k\in\mathsf{Z}_{d_k}$。根据命题 2.1，每个有限 Z_d-模都有拟基。

定义 5.2。设 M 是一个有限生成的 Z_d-模。设 $\phi\colon M\times M\to\mathsf{Z}_d$ 是一个交错的（见定义 2.5）Z_d-线性形式。若群 G 满足以下公理，我们称其为 (M,ϕ) 的海森堡扩张。

(a) 存在一个满射群同态 $\tau\colon G\to M$，其核同构于由 d 次单位根构成的群 $\mu_{\bar{d}}$。(b) 对每个 $g,h\in G$，都有 $gh=\xi^{\phi(\tau(g),\tau(h))}hg$。$(c)$ 阿贝尔群 M 的每个元素在 G 中都有一个阶相同的原像。

取 M 的一个拟基 $(y_1,\ y_2,\ \ldots\ldots,\ y_t)$，并用 d_k 表示 y_k 的阶。考虑由以下生成元与关系定义的群 G。G 的生成元为 $Y_1,\ \ldots\ldots,\ Y_t$、ζ，其关系为

$$\zeta^{\bar{d}}=1,\qquad Y_k\zeta=\zeta Y_k,\qquad Y_kY_r=\zeta^{2\phi(y_k,y_r)}Y_rY_k, \tag{5.1}$$

$$Y_k^{d_k}=1, \tag{5.2}$$

其中 $k,\ r\in[1;\ t]$。

引理 5.3。 G 的每个元素都可以唯一地写成如下形式

$$\zeta^aY_1^{a_1}\ldots Y_t^{a_t},\qquad a\in[0;\bar{d}-1],a_k\in[0;d_k-1]. \tag{5.3}$$

证明。从关系可以容易地看出，G 的每个元素都可以写成这样的形式，但其唯一性并不明显（最微妙之处在于要证明元素 $\zeta\in G$ 的阶仍为 d，而不是更小的阶）。为证明唯一性，我们构造 G 的一个表示，使得这种形式的元素作用为不同的算子。

显然，对于给定的交错形式 ϕ，我们可以找到一个 Z_d-双线性形式 ϕ_0，使得对每个 $m_1,\ m_2\in M$，都有 $\phi(m_1,\ m_2)=\phi_0(m_1,\ m_2)-\phi_0(m_2,\ m_1)$。（例如，可以取 ϕ_0，使得当 $k<r$ 时 $\phi_0(y_k,\ y_r)=\phi(y_k,\ y_r)$，且当 $k>r$ 时 $\phi_0(y_k,\ y_r)=0$。）考虑具有基 $\{v_m,\ m\in M\}$ 的复向量空间 C^M。我们考虑 C^M 上由下式给出的算子 $Y_1',\ \ldots\ldots,\ Y_t'$

$$Y_k'\cdot v_m=\xi^{\phi_0(y_k,m)}v_{y_k+m}.$$

并且，滥用记号，我们用 ζ 和 ξ 表示在复数域 M 上分别乘以复标量 ζ 和 ξ 的算子。

算子 Y_1'、……、Y_t'、ζ 满足关系 (5.1)，但可能不满足 (5.2)，因为 $Y'^{d_k}_k$ 可能是 ζ 的某个幂，而它不一定等于 1。不过，我们可以通过将算子 Y_k' 乘以适当的单位根来解决这个问题。这样既能满足关系 (5.2)，又不会破坏关系 (5.1)。于是，我们得到 G 在向量空间复数域 M 上的一个表示。从这个表示显然可知，形式如 (5.3) 的元素在该表示下的作用各不相同。□

引理 5.4. 上面的群 G 是 (M,ϕ) 的海森堡扩张。

证明。根据引理 5.3，元素 $\zeta \in G$ 的阶为 d。因此，群 G 含有一个由 ζ 生成且与 $\mu_{\bar{d}}$ 同构的子群。根据引理 5.3，G 对该子群取商后与阿贝尔群 M 同构。这说明定义 5.2 中的条件 (a) 成立。条件 (b) 由 (5.1) 立即得出。

下面证明 (c)。考虑一个元素 $m = \sum_{k=1}^{t} a_k y_k$，满足 $a_k \in [0;\ d_k - 1]$。m 的阶是满足以下条件的最小正整数 a：对每个 k，都有 $d_k \mid a a_k$。现在，我们要在 G 中找出 m 的一个阶为 a 的提升。令 $g = Y_1^{a_1} Y_2^{a_2} \dots Y_t^{a_t}$。那么，$g^a$ 等于 $Y_1^{a a_1} Y_2^{a a_2} \dots Y_t^{a a_t} = 1$ 乘以

$$\xi^{\sum_{k>r} \frac{a(a-1)}{2} a_k a_r \phi(y_k, y_r)}. \tag{5.4}$$

由于 y_k 的阶为 d_k，我们有 $\phi(y_k, y_r) \in \frac{d}{d_k}\mathbb{Z}_d$。于是 $a a_k \phi(y_k, y_r) \in d_k \frac{d}{d_k}\mathbb{Z}_d$，因此 $a a_k \phi(y_k, y_r) = 0$ 属于 $\mathbb{Z}_d$。那么，若 a 为奇数，$\frac{a-1}{2}$ 是一个整数，且 $\frac{a(a-1)}{2} a_k a_r \phi(y_k, y_r) = 0$ 属于 $\mathbb{Z}_d$，所以 (5.4) 等于 1，从而得到 $g^a = 1$。然而，当 a 为偶数时（这只有在 d 为偶数时才可能），数 $\frac{a-1}{2}$ 是一个半整数，因此得到 $\frac{a(a-1)}{2} a_k a_r \phi(y_k, y_r) \in \frac{d}{2}\mathbb{Z}_d$。于是 (5.4) 可能等于 1 或 -1，因此 $g^a = \pm 1$。在 $g^a = -1$ 的情况下，元素 g 的阶为 $2a$ 而不是 a；不过，我们可以通过将 g 乘以 $\zeta^{d/a}$ 来解决这个问题。

□

命题 5.5. 对于两个海森堡扩张 $\tau\colon G \to M$ 和 $\tau'\colon G' \to M$，存在一个（不一定唯一的）群同构 $\iota\colon G \to G'$，使得 $\tau' \circ \iota = \tau$。

证明. 只需证明当 $\tau\colon G \to M$ 是由 (5.1)、(5.2) 定义的 (M, ϕ) 的海森堡扩张时，结论成立。

设 $\tau'\colon G' \to M$ 是另一个海森堡扩张。设 $Y_k' \in G'$ 是 G' 中 y_k 的一个提升，且具有相同的阶。根据定义 5.2，元素 $Y_1', \dots, Y_t'$ 必须满足关系 (5.1)、(5.2)。于是存在一个群同态 $\iota\colon G \to G'$，将 Y_k 映到 Y_k'，并将 $\zeta \in G$ 映到 $\zeta \in G'$。因此我们自动得到 $\tau' \circ \iota = \tau$。

我们来验证 ι 是同构。由于 G 和 G' 的基数相同，只需验证 ι 的单射性。但由于我们有 $\tau' \circ \iota = \tau$，只有 $\ker \tau = \mu_{\bar{d}}$ 中的元素才可能属于 ι 的核。但由于 ι 将 ζ 映到 ζ，ι 的核是平凡的。□

定义 5.6。记 $Heis(M, \phi)$ 为 (M, ϕ) 的海森堡扩张（该群在同构意义下唯一）。当形式 ϕ 从上下文中显然时，我们有时简写为 $Heis(M)$。

命题 5.5 的证明蕴含如下结论。

引理 5.7. 设 $(y_1, y_2, \dots, y_t)$ 是 M 的任意拟基。取这些元素在 $Heis(M, \phi)$ 中的提升 $Y_1, Y_2, \dots, Y_t$，且阶与原元素相同。则 $Y_1, \dots, Y_t, \zeta$ 生成群 $Heis(M, \phi)$，并且 (5.1)、(5.2) 是全部关系。

引理 5.8. 对于每个辛自同构 $\psi \in Sp(M, \phi)$，都存在 Ψ 的自同构，使得 $Heis(M, \phi)$ 满足 $\psi \circ \tau = \tau \circ \Psi$ 和 $\Psi(\zeta) = \zeta$。

证明。任取一个 M 的拟基 $y_1, \dots, y_t$。那么，ψ 将该拟基映射为另一个拟基 $(y_1', \dots, y_t')$，且元素的阶相同。我们可以将这个拟基提升为元素 $Y_1, \dots, Y_t \in Heis(M, \phi)$（阶相同），并且我们可以

类似地将第二个拟基提升为 $Y_1', \ldots, Y_t' \in Heis(M, \phi)$。根据引理 5.7，元素 $Y_1, \ldots, Y_t, \zeta$ 生成 $Heis(M, \phi)$，并且满足与 $Y_1', \ldots, Y_t', \zeta$ 完全相同的关系。于是我们可以找到 $Heis(M, \phi)$ 的一个自同构，它将 Y_k 映射到 Y_k'，其中 $k \in [1; t]$。□

反过来，由定义 5.2（b）可知，ζ 不变的 $Heis(M, \phi)$ 的每个自同构都会（通过 $M \simeq Heis(M, \phi)/\mu_{\bar{d}}$ ）诱导出 (M, ϕ) 的一个辛自同构。因此，我们得到一个满射群同态 $\mathrm{Aut}_\zeta(Heis(M, \phi)) \to Sp(M, \phi)$，其中 Aut_ζ 表示完整自同构群 Aut 中由固定 ζ 的自同构组成的子群。

5.2. **ζ-群**。

定义 5.9。 对于一个含有元素 ζ 的有限群 G，若 ζ 是 G 中阶为 d 的中心元素，则称 (G, ζ) 为 ζ-群（或者在 ζ 明确时，简称 G 为 ζ-群）。若可能产生混淆，我们有时会将 ζ_G 写作 $\bar{}$，以便将元素 $\zeta_G \in G$ 与复数域 $\mathbb{C}$ 中的本原 d 次单位根 $\zeta_{\mathbb{C}} \in$ 区分开来。

根据定义，ζ-群包含一个与 $\mu_{\bar{d}}$ 同构的子群，该子群由 ζ 生成。

定义 5.10。 对于一个 ζ-群 (G, ζ)，记 $\mathrm{Aut}_\zeta(G)$ 为完整自同构群 $\mathrm{Aut}(G)$ 的子群，它由固定 ζ 的自同构组成。

定义 5.11。 我们称 V 是 ζ-群 G 的一个 ζ-表示，如果 V 是 G 的一个表示（在复数域上），且元素 $\zeta_G \in G$ 以标量 $\zeta_{\mathbb{C}}$ 作用。

换句话说，G 的一个 ζ-表示无非是群代数的以下商的一个表示：复数域$G/(\zeta_G - \zeta_{\mathbb{C}})$。

定义 5.12。 对于两个 ζ-群 G_1 和 G_2，我们将它们的 ζ-积 $G_1 \times_\zeta G_2$ 定义为直积 $G_1 \times G_2$ 对应于将 ζ_{G_1} 与 ζ_{G_2} 视为相同元素的关系所得的商。

显然，如果我们有 G_1 的一个 ζ-表示 V_1，以及 G_2 的一个 ζ-表示 V_2，那么张量积 $V_1 \otimes V_2$ 具有 $G_1 \times_\zeta G_2$ 的一个 ζ-表示的结构。此外，如果这些表示 V_1 和 V_2 是不可约的，那么 $G_1 \times_\zeta G_2$ 的表示 $V_1 \otimes V_2$ 也是不可约的。

定义 5.13。 如果一个 ζ-群 (G, ζ) 具有唯一的（在同构意义下）不可约 ζ-表示，则称其为（作为 ζ-群的）单群。

若 V 是 (G, ζ) 的唯一不可约 ζ-表示，则有代数同构 $\mathbb{C}G/(\zeta_G - \zeta_{\mathbb{C}}) \simeq \mathrm{End}(V)$（因为每个复数域上的有限维单代数都同构于 $\mathrm{End}(V)$，其中 V 是其唯一不可约表示 V）。

引理 5.14。 两个单 ζ-群的 ζ-直积是单的。

证明。 设 G_1 和 G_2 是两个单 ζ-群。众所周知，通常的直积 $G_1 \times G_2$ 的不可约表示具有 $V_1 \otimes V_2$ 的形式。此外，$G_1 \times G_2$ 的这种表示 $V_1 \otimes V_2$ 是 $G_1 \times_\zeta G_2$ 的 ζ-表示，当且仅当 V_1 和 V_2 分别是 G_1 和 G_2 的 ζ-表示。

现在，若 V_1 是 G_1 的唯一 ζ-表示，且 V_2 是 G_2的唯一 ζ-表示，那么 $V_1 \otimes V_2$ 就是 $G_1 \times_\zeta G_2$ 的唯一 ζ-表示。□

假设 (G, ζ) 是一个单群，令 V 为它的不可约表示。

引理 5.15。 自然同态 $G \to GL(V)$ 是单射。

证明。 这可由代数同构 $\mathbb{C}G/(\zeta_G - \zeta_{\mathbb{C}}) \simeq \mathrm{End}(V)$ 得出。 □

由于 G 的表示 V 不可约， V 上存在唯一（相差一个标量）的 G-不变（厄米）标量积。特别地，根据上述引理，我们可以将 G 视为酉群 $U(V)$ 的子群。

引理 5.16. 群 G 中每个固定 ζ 的自同构，都是由 $U(V)$ 中某个元素的共轭所诱导的。

证明. 设 $\psi\colon G \to G$ 是 G 的一个固定 ζ 的自同构。记 ρ 为 G 到 $GL(V)$ 的包含映射。令 $\rho' = \rho\circ\psi$。向量空间 V 上有两种 G-表示结构：通常的表示结构（由 ρ 给出）和扭曲的表示结构（由ρ'给出）。两者都是不可约的 ζ-表示。然而，由于 ζ-群 G 的表示在同构意义下唯一，它们必定同构，即存在一个线性映射 $f\colon V \to V$，使得 $\rho' = f \circ \rho \circ f^{-1}$。此外，由于 V 上的 G-不变标量积相差一个标量唯一，我们可以将 f 乘以一个标量，从而得到 $U(V)$ 中的一个元素。由此可见，G 的自同构 ψ 是由 f 的共轭给出的。□

5.3. $(, \phi)$ 在辛(M, ϕ)中的描述。 我们来描述所有辛 (M, ϕ) 对应的群 $Heis(M, \phi)$。首先假设 M 是自由且辛的。

引理 5.17。 假设 M 是秩为 $2n$ 的自由有限 $\mathbb{Z}_d$-模，且 ϕ 是辛的。那么 $Heis(M, \phi)$ 同构于泡利群 $\mathcal{P}_n$。

证明。 取 M 的一个辛基 $(e_1, \dots, e_n, f_1, \dots, f_n)$。令 $Z_1, \dots, Z_n, X_1, \dots, X_n$ 为该基中各元素在 $Heis(M, \phi)$ 中的提升（阶相同，为 d）。根据引理 5.7，群 $Heis(M, \phi)$ 由生成元 $X_1, \dots, X_n, Z_1, \dots, Z_n, \zeta$ 以及以下关系定义：

$$\zeta^{\bar{d}} = 1, \qquad X_k\zeta = \zeta X_k, \qquad Z_k\zeta = \zeta Z_k, \qquad X_kX_r = X_rX_k, \qquad Z_kZ_r = Z_rZ_k,$$
$$X_kZ_r = Z_rX_k \ (\text{if } r \neq k), \qquad X_kZ_k = \zeta^2 Z_kX_k, \qquad X_k^d = 1, \qquad Z_k^d = 1.$$

这恰好是 $\mathcal{P}_n$ 的生成元与关系集合，见推论 3.6。

□

现在我们去掉 M 是自由模这一假设。

引理 5.18. 设 M_1 和 M_2 是两个有限的 $\mathbb{Z}_d$-模，分别带有交错形式 ϕ_1 和 ϕ_2。考虑 $\mathbb{Z}_d$-模 $M_1 \oplus M_2$ 及其诱导形式 $\phi_1 \oplus \phi_2$ （使两个直因子彼此正交）。则有 $Heis(M_1 \oplus M_2, \phi_1 \oplus \phi_2) \simeq Heis(M_1, \phi_1) \times_\zeta Heis(M_2, \phi_2)$。

证明。 根据定义， $Heis(M_1 \oplus M_2, \phi_1 \oplus \phi_2)$ 是一个在同构意义下唯一的群，带有一个到 $M_1 \oplus M_2$ 的同态，并满足定义 5.2 中的性质（a）、（b）、（c）。另一方面，同态 $Heis(M_1, \phi_1) \to M_1$ 和 $Heis(M_2, \phi_2) \to M_2$ 诱导出一个同态 $Heis(M_1, \phi_1) \times_\zeta Heis(M_2, \phi_2) \to M_1 \oplus M_2$。我们只需验证它满足（$a$）、（$b$）、（$c$）。性质（$a$）和（$b$）显然成立。下面验证（$c$）。

取 $(m_1, m_2) \in M_1 \oplus M_2$。我们知道，存在 m_1 的一个提升 $Y_1 \in Heis(M_1, \phi_1)$，以及 m_2 的一个提升 $Y_2 \in Heis(M_2, \phi_2)$，且二者的阶相同；分别记这些阶为 a_1 和 a_2。于是，(m_1, m_2) 在 $M_1 \oplus M_2$ 中的阶为 $\mathrm{lcm}(a_1, a_2)$。然而，元素 Y_1 和 Y_2 在 $Heis(M_1, \phi_1) \times_\zeta Heis(M_2, \phi_2)$ 中的像彼此可交换，因此它们乘积的阶也为 $\mathrm{lcm}(a_1, a_2)$。□

根据引理 2.13，每个辛 M 都同构于若干初等辛模 $M \simeq S_{d_1} \oplus S_{d_2} \oplus \ldots \oplus S_{d_k}$ 的直和。（若希望这样的表示唯一，我们还可以额外假设 $1 < d_1 \mid d_2 \mid \cdots \mid d_k$。不过，我们不作此假设，因为下文所述的一切在不作此假设时同样成立。）因此，鉴于引理 5.18，只需确定初等辛 Z_d-模 S_{d_0} 的海森堡扩张与 $d_0 \mid d$ 的关系。

我们来理解 $Heis(S_{d_0})$。令 $\mathcal{P}^{(d_0)}{}_n \subset GL((\text{复数域}^{d_0})^{\otimes n})$ 为维数为 d_0 的 n 量子位的泡利群。（如果 $d_0 = d$，我们可以去掉上标。）用 $_{\mathcal{P}^{(d_0,\zeta)}{}_n}$ 表示由 $\mathcal{P}^{(d_0)}{}_n$ 的作用所对应的算子以及乘以本原 $\bar{d}$ 次单位根 ζ 所生成的 $GL((\text{复数域}^{d_0})^{\otimes n})$的子群。（注意，群 $\mathcal{P}^{(d_0)}{}_n$ 本身只包含 d_0次单位根。）对于 $d = d_0$，显然有 $\mathcal{P}_n^{(d,\zeta)} = \mathcal{P}_n^{(d)} = \mathcal{P}_n$。

引理 5.19。我们有 $Heis(S_{d_0}) \simeq \mathcal{P}^{(d_0,\zeta)}{}_1$.

证明。根据引理 5.4，群 $Heis(S_{d_0})$ 由生成元 (X, Z, ζ) 及以下关系定义

$$\zeta^{\bar{d}} = 1, \qquad ZX = \zeta^{2\frac{d}{d_0}} XZ, \qquad X^{d_0} = Z^{d_0} = 1.$$

我们在此认出了泡利群 $\mathcal{P}^{(d_0)}{}_1$，并额外加入了 $\bar{d}$ 次单位根 ζ。

□

现在，结合引理 5.18 和引理 5.19，我们得到如下结果。

命题 5.20。如果我们有 $M \simeq \bigoplus_{r=1}^k S_{d_r}$，那么

$$Heis(M, \phi) \simeq \mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)}.$$

还要注意，显然我们有

$$\mathcal{P}_n^{(d_0,\zeta)} \simeq \mathcal{P}_1^{(d_0,\zeta)} \times_\zeta \mathcal{P}_1^{(d_0,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_0,\zeta)} \quad (n \text{ times}).$$

现在，我们指出，ζ-群 $Heis(S_{d_0}) \simeq \mathcal{P}^{(d_0,\zeta)}{}_1$ 显然是一个单 ζ-群，因为我们有 $\mathbb{C}\mathcal{P}^{(d_0,\zeta)}{}_1 \quad /(\zeta_{\mathcal{P}} - \zeta_{\mathbb{C}}) \simeq \mathrm{End}(\mathbb{C}^{d_0})$，因此 $\mathbb{C}^{d_0}$ 是唯一的单 ζ-表示。然后，根据引理 5.18 和引理 5.14，我们得到如下结果。

引理 5.21。如果 (M, ϕ) 是辛的，那么 ζ-群 $Heis(M, \phi)$ 是单群。如果 $M \simeq \bigoplus_{r=1}^k S_{d_r}$，那么其唯一的单 ζ-表示

$$Heis(M, \phi) \simeq \mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)}$$

是 $\text{复数域}^{d_1} \otimes \text{复数域}^{d_2} \otimes \ldots \otimes \text{复数域}^{d_k}$。

注记 5.22。如果 d_1 和 d_2 是正整数，使得 $d_1 d_2 \mid d$ 和 $gcd(d_1, d_2) = 1$，那么根据中国剩余定理可得 $S_{d_1 d_2} \simeq S_{d_1} \oplus S_{d_2}$。利用引理 5.18 和引理 5.19，我们将其转化到泡利群的层面：

$$\mathcal{P}_1^{(d_1 d_2,\zeta)} \simeq \mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)}. \tag{5.5}$$

现在，即使 $d_1, d_2, \ldots, d_k$ in $\mathcal{P}^{(d_1,\zeta)}{}_1 \times_\zeta \mathcal{P}^{(d_2,\zeta)}{}_1 \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)}$ 是 d的任意正因子，我们也总能将每个 d_r 分解为素数幂，再将因子重新分组（使用 (5.5)），从而得到形如 $\mathcal{P}^{(d_1,\zeta)}{}_1 \quad \times_\zeta {}_{\mathcal{P}^{(d_2,\zeta)}{}_1} \quad \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)}$ 的表达式，其中 $d_1 \mid d_2 \mid \ldots \mid d_k$。

注 5.23. 假设 M 是秩为 $2n$的自由辛群。那么，正如我们在引理 5.17 中所见，$Heis(M,\phi)$ 与泡利群 $\mathcal{P}_n$同构。因此，引理 5.8、引理 5.16 和引理 5.21 可给出命题 3.11 的另一种证明。

引理 5.24. 若(M,ϕ) 是辛的，且 V 是 $Heis(M,\phi)$的唯一简单 ζ-表示，则有 $\#Heis(M,\phi) = \bar{d}\cdot$(维数 $V)^2$。

证明. 这由 C$Heis(M,\phi)/(\zeta_{Heis(M,\phi)}-\zeta_{\mathbb{C}}) \simeq \mathrm{End}(V)$ 同构可得。

□

5.4. $N(H)/H$**的描述**。

引理 5.25. 设 $\tau\colon G \to M$ 是 (M,ϕ)的海森堡扩张。那么，对于任意 $\mathbb{Z}_{\bar{d}}$-子模 N（等价地，对于任意子群），其原像$\tau^{-1}(N)$ 是 N的海森堡扩张（配备 ϕ的限制）。

证明. 该命题立即由从 $\tau^{-1}(N)$ 到 N 的同态显然满足定义 5.2 中的公理这一事实得出。
□

定理 5.26. 设 H 是 $\mathcal{P}_n$ 的一个交换子群，满足(3.2)。那么，$N(H)/H$同构于 $\tau(H)^{\perp}/\tau(H)$ 的海森堡扩张（其形式由 F_n上的辛形式 ϕ 诱导）。

证明。 由于 $N(H)$ 与 $\mathcal{P}_n$ 中 H 的中心化子相同，见注 3.14，因此元素 $g \in \mathcal{P}_n$ 与 H 对易，当且仅当其像 $\tau(g)$ 与 $\tau(H)$ 正交。换言之，我们得到 $N(H)$ 是 $\tau(H)^{\perp}$ 关于 τ 的原像。现在，考虑同态 $N(H)/H \to \tau(H)^{\perp}/\tau(H)$。我们来检验它是否满足定义 5.2 中的公理。公理 (b) 显然成立。我们来检验 (a) 和 (c)。

$N(H)/H \to \tau(H)^{\perp}/\tau(H)$ 的核同构于 $\tau^{-1}(\tau(H))/H$。然而， $\tau^{-1}(\tau(H))$ 由 $\mathcal{P}_n$ 的子群 H 和 $\mu_{\bar{d}}$ 生成，并且由 (3.2) 可知，这两个子群的交是平凡的。因此，$N(H)/H \to \tau(H)^{\perp}/\tau(H)$ 的核同构于 $\mu_{\bar{d}}$，这就证明了 (a)。

现在来检验（c）。设 m 是 $\tau(H)^{\perp}$的一个元素。设 a、 b 为正整数，使得 ab 是 $m \in \tau(H)^{\perp}$ 的阶，而 a 是 m 在 $\bar{m} \in \tau(H)^{\perp}/\tau(H)$ 下的像的阶。设 $g \in N(H)$ 是 $\tau^{-1}(m)$ 中阶为 ab 的一个元素。

我们有 $\tau(g^a) \in \tau(H)$，这意味着存在某个 $\omega \in \mu_{\bar{d}}$，使得 $g^a \in \omega H$。另一方面，我们有 $g^{ab} = 1$，且 $g^{ab} = (g^a)^b \in \omega^b H$。由（3.2）可知，必有 $\omega^b = 1$，即 ω 必须是一个 b 次单位根。因此，对于某个 $c \in$ ，我们可以将 $\omega = \xi^{c\frac{d}{b}}$ 写成这样，其中 $c \in$ 属于 $\mathbb{Z}$。另一方面， ab 是 d 的一个约数。考虑 $g' = \xi^{-c\frac{d}{ab}} g$。于是我们有 $g'^a = \xi^{-c\frac{d}{b}} g^a \in \omega^{-1}\omega H = H$。这表明我们找到了 $\bar{m}$ 的一个提升 $\bar{g'}$，且二者的阶相同 a。□

以下引理已在 [3, 定理 1] 中证明。不过，我们采用研究海森堡群的方法给出另一种证明。

引理 5.27. 设 $H \subset \mathcal{P}_n$ 是满足 (3.2) 的交换子群，则有 维数 $V^H =$ 维数 $V \# H$。

证明。 由于我们有群同构 $\mu_d \simeq \mathbb{Z}_d$，群 $H^* = \mathrm{Hom}(H,\mathbb{Z}_d)$ 可与特征群 $\mathrm{Hom}(H,\mathbb{C}^*) = \mathrm{Hom}(H,\mu_d)$ 等同。令$V = \bigoplus_{\chi\in H^*} V_\chi$ 为 H的公共特征子空间分解。那么 V^H 是对应于平凡特征标 χ的V_χ 。

群 $\mathcal{P}_n$ 在集合 $H^* \simeq \tau(H)^*$ 上的作用为 $(h \cdot \chi)(m) = \chi(m) - \phi(\tau(h)\ m)$，其中 $h \in \mathcal{P}_n$, $\chi \in \tau(H)^*$, $m \in \tau(H)$。对于此作用，我们有 $h(V_\chi) = V_{h\cdot\chi}$。特别地， h 在 V_χ 和 $V_{h\cdot\chi}$之间诱导出一个线性同构。

我们看到，对于同一轨道中的两个特征 χ_1 和 χ_2，存在一个线性同构 $V_{\chi_1} \simeq V_{\chi_2}$。因此，要证明维数公式，只需证明该作用具有传递性；这样我们便有 $\dim V^H = \dim V/\#H^*$。

我们来证明这一传递性。为此，需要证明每个特征都属于平凡特征标的轨道，而平凡特征标由 $\mathrm{Hom}(\tau(H), \mathbb{Z}_d)$ 中的零映射表示。因此，我们需要证明，对于每个 $\chi \in \tau(H)^*$，都能找到 $h \in \mathcal{P}_n$，使得 $\chi = \phi(\tau(h)\ \bullet)$。这由引理 2.7 应用于 $M = F_n$ 和 $N = \tau(H)$ 得出。□

由于根据推论 2.11，我们有 $(\tau(H)^\perp)^\perp = \tau(H)$，因此带有诱导交错形式的 $\mathbb{Z}_d$-模 $\tau(H)^\perp/\tau(H)$ 是辛的。于是，根据命题 5.20，群 $Heis(\tau(H)^\perp/\tau(H))$ 同构于如下形式的群

$$\mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)},$$

另见注 5.22。

定理 5.28。 存在一个酉同构

$$V^H \simeq \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \ldots \otimes \mathbb{C}^{d_k}$$

使得群同构

$$N(H)/H \simeq Heis(\tau(H)^\perp/\tau(H)) \simeq \mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)}$$

定理 *5.26* 中的群同构将 $N(H)/H$ 对 V^H 的作用与以下作用相交织：

$$\mathcal{P}_1^{(d_1,\zeta)} \times_\zeta \mathcal{P}_1^{(d_2,\zeta)} \times_\zeta \ldots \times_\zeta \mathcal{P}_1^{(d_k,\zeta)} \quad on \quad \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \ldots \otimes \mathbb{C}^{d_k}.$$

证明。 由引理 5.21，这个群是一个 ζ-群中的单群，且其唯一的不可约 ζ-表示为 $V_0 = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \otimes \ldots \otimes \mathbb{C}^{d_k}$。于是由引理 5.24，我们有

$$\dim V_0 = \sqrt{\frac{\#Heis(\tau(H)^\perp/\tau(H))}{\bar{d}}}.$$

另一方面，由引理 5.27，表示 V^H of$N(H)/H$ 的维数满足

$$\dim(V^H) = \frac{\dim V}{\#H}.$$

为了将 V^H 与 $V_0 =$ 复数域$^{d_1} \otimes$ 复数域$^{d_2} \otimes \ldots \otimes$ 复数域^{d_k} 识别，我们只需证明它们具有相同的维数。我们有 $\#(\tau(H)^\perp) = \#F_n\#H$，于是

$$\#(\tau(H)^\perp/\tau(H)) = \frac{\#F_n}{(\#H)^2} = \frac{d^{2n}}{(\#H)^2}.$$

于是我们得到

$$\dim V_0 = \sqrt{\frac{\#Heis(\tau(H)^\perp/\tau(H))}{\bar{d}}} = \sqrt{\#(\tau(H)^\perp/\tau(H))} = \sqrt{\frac{d^{2n}}{(\#H)^2}} = \frac{d^n}{\#H} = \dim V^H.$$

根据不变标量积在相差一个标量的意义下唯一，表示的同构 $V^H \simeq V_0$ 可以选为酉的。□

5.5. **移位自由子群**。 我们在定理 3.13 中看到，若阿贝尔子群 $H \subset \mathcal{P}_n$ 满足 (3.2) 和 (3.3)，则 $N(H)/H$ 在 V^H 上的作用可与 $\mathcal{P}_{n-k}$ 在 (复数域^d)$^{\otimes(n-k)}$ 上的作用等同。我们在定理 5.26 和定理 5.28 中看到，若去掉自由性假设 (3.3)，则某些量子位可以降为维数较小的量子位。若能确定自由性条件 (3.3) 的最优替代条件，使定理 3.13 的结论仍成立（即不会发生这种降维），将会很有帮助。

设 $H' \subset \mathcal{P}_n$ 是满足 (3.2) 和 (3.3) 的阿贝尔子群。于是我们可以找到 F_n 的一个辛基 $(e_1, \dots, e_n, f_1, \dots, f_n)$，使得 $(e_1, \dots, e_k)$ 是 $\tau(H')$ 的一个 Z_d-基，其中 k 满足 $\#H' = d^k$。根据引理 5.7，该基可以提升为元素 $Z'_1, \dots, Z'_n, X'_1, \dots, X'_n$，它们恰好满足推论 3.6 中泡利群标准生成元的关系（事实上，我们可以通过一个自同构将它们映射到标准生成元，见引理 5.8 的证明），并且 $H' = \langle Z'_1, Z'_2, \dots, Z'_k \rangle$。

定义 5.29. 我们称群 H 是 H' 的一种平移，如果存在一些正整数 $(a_1, a_2, \dots, a_k)$，它们整除 d，使得

$$H = \langle {Z'}_1^{a_1}, {Z'}_2^{a_2}, \dots, {Z'}_k^{a_k}, {X'}_1^{d/a_1}, \dots, {X'}_k^{d/a_k} \rangle$$

（对于某种辛基 $(e_1, \dots, e_n, f_1, \dots, f_n)$ 以及上述提升 $Z'_1, \dots, Z'_n, X'_1, \dots, X'_n$）。我们称这种形式的群 H 为移位自由群。

注记 5.30. 鉴于命题 2.20 和命题 2.23，“移位自由”的条件无非就是“$\tau(H)$ 是 F_n 的一个自由辛 Z_d-子模中的拉格朗日子群”。

定理 5.31. 设 H 是 $\mathcal{P}_n$ 的一个满足 (3.2) 的阿贝尔子群。那么，群 $N(H)/H$ 同构于某个 k，当且仅当 H 是移位自由的。此外，在此情形下，$N(H)/H$ 对 V^H 的作用可与 $\mathcal{P}_{n-k}$ 对 (复数域^d)$^{\otimes(n-k)}$ 的作用等同，其中同构 $V^H \simeq$ (复数域^d)$^{\otimes(n-k)}$ 是酉的。

证明。 我们首先证明，当 H 是移位自由时，有 $N(H)/H \simeq \mathcal{P}_{n-k}$。We have

$$H = \langle {Z'}_1^{a_1}, {Z'}_2^{a_2}, \dots, {Z'}_k^{a_k}, {X'}_1^{d/a_1}, \dots, {X'}_k^{d/a_k} \rangle$$

Then

$$\tau(H) = \langle a_1 e_1, \dots, a_k e_k, \frac{d}{a_1} f_1, \dots, \frac{d}{a_k} f_k \rangle$$

因此

$$\tau(H)^\perp = \langle a_1 e_1, \dots, a_k e_k, e_{k+1}, \dots, e_n, \frac{d}{a_1} f_1, \dots, \frac{d}{a_k} f_k, f_{k+1}, \dots, f_n \rangle.$$

我们看到，$\tau(H)^\perp/\tau(H)$ 是一个秩为 $2(n-k)$ 的自由辛 Z_d-模。于是，根据定理 5.26 和命题 5.20，有 $N(H)/H \simeq \mathcal{P}_{n-k}$。

现在假设 $N(H)/H \simeq \mathcal{P}_{n-k}$，并证明 H 是移位自由的。这个群同构意味着，$\tau(H)^\perp/\tau(H)$ 是一个秩为 $2(n-k)$ 的自由 Z_d-模。设 $e_{k+1}, \dots, e_n, f_{k+1}, \dots, f_n \in \tau(H)^\perp$ 是 $\tau(H)^\perp/\tau(H)$ 的某个辛基中各元素的提升。则 $N := \langle e_{k+1}, \dots, e_n, f_{k+1}, \dots, f_n \rangle$ 是 F_n 的一个秩为 $2(n-k)$ 的自由辛子模。然后，根据注 2.18，$N^\perp$ 也是秩为 $2k$ 的自由辛子模。

由于我们有 $(\tau(H)^\perp)^\perp = \tau(H)$，因此 $\tau(H)$ 是 $\tau(H)^\perp$ 中与 $\tau(H)^\perp$ 的所有元素正交的极大子模。现在，由于我们有 $\tau(H)^\perp = \tau(H) \oplus N$，因此

$\tau(H)$ 是 $N^\perp$ 的极大各向同性子模。因此， $\tau(H)$ 是 $N^\perp$ 中的拉格朗日子模。于是 H 是移位自由的，参见注 5.30。

表示的识别由不可约 ζ-表示的唯一性自动得出。□

5.6. **扭曲自由子群**。 我们引入扭曲这一概念，它是平移概念的推广。粗略地说，扭曲是一种带有缺陷的平移：平移时，我们会丢失所平移对象的一部分。

定义 5.32. 设 H' 如第 5.5 节所述。若存在正整数 $a_1, \dots, a_k, b_1, \dots, b_k$， 使得对每个 $r \in [1$都有 $d \mid a_r b_r; k]$， 并且满足

$$H = \langle {Z'}_1^{a_1}, {Z'}_2^{a_2}, \dots, {Z'}_k^{a_k}, {X'_1}^{b_1}, \dots, {X'_k}^{b_k} \rangle$$

对于 F_n 的一组辛基$(e_1, \dots, e_n, f_1, \dots, f_n)$的某种选取，以及将该基提升到 $\mathcal{P}_n$所得的一组提升 $Z'_1, \dots, Z'_n,\ X'_1, \dots, X'_n$ 的某种选取。

注记 5.33. 等价地（根据引理2.22），若存在一个正交分解 $F_n \simeq S_d^{\oplus n}$ ，将 H 分解为 n 个初等自由辛 Z_d-模 S_d 的副本，并且对每个 $r \in [1; k]$ ，都存在各向同性子模 $N_r \subset S_d$ ，使得 H 是扭曲自由的

$$\tau(H) = N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

在特殊情形 $a_r b_r = d$ 对所有 r 都成立时，每个 N_r 都是对应的 S_d 副本中的拉格朗日子模，此时我们便得到平移的概念。

对每个 $r \in [1; k]$， 令

$$c_r = \frac{a_r b_r}{d}.$$

在移位情形下，有 $a_r b_r = d$，因此 $c_r = 1$。然而在扭曲情形下，整数 c_r 衡量了缺陷。更准确地说，对于第 r 个块，有$N_r^\perp / N_r \simeq S_{c_r}$，因此

$$\tau(H)^\perp / \tau(H) \simeq S_{c_1} \oplus S_{c_2} \oplus \cdots \oplus S_{c_k} \oplus S_d^{\oplus(n-k)}.$$

因此，我们得到

$$N(H)/H \simeq \mathcal{P}_1^{(c_1,\zeta)} \times_\zeta \mathcal{P}_1^{(c_2,\zeta)} \times_\zeta \cdots \times_\zeta \mathcal{P}_1^{(c_k,\zeta)} \times_\zeta \mathcal{P}_{n-k},$$

and

$$V^H \simeq \mathbb{C}^{c_1} \otimes \mathbb{C}^{c_2} \otimes \cdots \otimes \mathbb{C}^{c_k} \otimes (\mathbb{C}^d)^{\otimes(n-k)}.$$

因此，与移位情形相比，扭曲自由子群会在受保护空间中产生维数为 c_1, ..., c_k 的额外较小量子位。当所有 $c_r = 1$ 时，这些额外因子便消失，我们就恢复了通常的移位自由图景。

例 5.34。考虑一个维数为 8 的量子比特（$n = 1,\ d = 8$）。设 H 是由 X^4 和 Z^4 生成的 $\mathcal{P}_1^{(8)}$ 子群。这个群是由 Z 生成的子群的一个扭曲。于是我们有 $V^H \simeq \mathsf{C}^2,$, 并且 $N(H)/H$ 同构于附加了一个 16 次单位根的单量子比特泡利群。这个例子展示了如何在一个维数为 8 的量子比特中编码一个量子比特。

6. 扭曲Kitaev模型

在 Kitaev 模型（第 4.2 节）中，子群 $H \subset \mathcal{P}_{\#E}$ 是构造为由形如 A_s、$s \in S$ 和 B_f、$f \in F$ 的算子生成的群（但我们可以从生成元集合中去掉一个 A_{s_0} 和一个 B_{f_0} ）。另一方面，平移和扭曲的概念是在第 5.5 节和第 5.6 节中引入的。我们想看看这些概念在 Kitaev 模型中的一些应用示例。

6.1. 完全移位。 固定 s_0，$s_1 \in S$，并固定一条从 s_0 到 s_1的路径 t。考虑对群 H作如下修改。我们将由 A_s、$s \in S\backslash\{s_0, s_1\}$、$B_f$、$f \in F$以及（为补偿移除的 A_{s_1}和A_{s_0}）路径算子 $S^Z(t)$生成的群记为 H。

新特征 $\chi \in H^*$ 的组合描述如下。我们仍然有所有顶点（ s_0 和 s_1除外）上的电荷概念，也仍然有面上的磁荷概念（总电荷模 d为零）。此外，现在我们有了 t上的流这一概念：$s_0 \to s_1$，其取值属于 $\mathbb{Z}_d$。换句话说，我们创建了从 s_0到 s_1 的流这一概念，但因此失去了 s_0 和 s_1 本身上的荷的概念。

我们可以通过移除 $A_{s_0}, A_{s_1}, \ldots, A_{s_u}$，并为某些 t_1: $s_0 \to s_1$,t_2: $s_0 \to s_2$, …, t_u: $s_0 \to s_u$ 添加路径算子 $S^Z(t_1)$ $S^Z(t_2) \ldots, S^Z(t_u)$，来自然地推广这一构造。这样一来，我们失去了在 $s_0, s_1, \ldots, s_u$ 处定义荷的概念，但获得了这些选定顶点之间定义流的概念。

由于我们处于“移位自由”的情形，新的受保护空间 V^H 仍具有 $(\mathbb{C}^d)^{\otimes 2g}$ 的形式。

6.2. 部分移位。 我们可以对上面的例子进行推广。固定一个由正整数 a 和 b 构成的分解 $d = ab$，再固定顶点 s_0, s_1 以及一条路径 t: $s_0 \to s_1$。接下来考虑如下构造。我们移除A_{s_0} 和A_{s_1}，但添加 $A_{s_1}^a$ （也可以添加 $A_{s_0}^a$，这不会改变任何东西，因为 $\prod_{s \in S} A_s = I$），并添加路径算子 $S^Z(t)^b$ 的幂。现在，在特征空间的组合描述中，我们有 s_0 与 s_1 之间的流（取值于 $b\mathbb{Z}/d\mathbb{Z} \subset \mathbb{Z}/d\mathbb{Z} = \mathbb{Z}_d$），而 s_0 和 s_1 处模 d 的旧荷不再有定义，但 s_0 和 s_1 处模 b 的荷仍然有定义。这看起来很自然，因为流能被 b 整除，所以荷至少仍可模 b 定义。

我们可以自然地推广这一构造。固定如上例中的 $s_0, s_1, \ldots, s_u$ 和 $t_1, t_2, \ldots, t_u$，并固定 $d = a_1 b_1 = a_2 b_2 = \ldots = a_u b_u$。移除 $A_{s_0}, A_{s_1}, \ldots, A_{s_u}$，但添加 $A_{s_1}^{a_1}, \ldots, A_{s_u}^{a_u}$ 以及路径算子 $S^Z(t_1)^{b_1}, S^Z(t_2)^{b_2}, \ldots, S^Z(t_u)^{b_u}$，其中取某些 t_1: $s_0 \to s_1$, t_2: $s_0 \to s_2$, …, t_u: $s_0 \to s_u$。于是，对于 $r \in [1; u]$，我们得到一个概念：从 s_0 到 s_r、取值于 $b_r\mathbb{Z}/d\mathbb{Z}$ 的流；而 s_r 处的荷则仅定义到模 b_r。

由于我们处于“移位自由”的情形，新的受保护空间 V^H 仍具有形式 $(\mathbb{C}^d)^{\otimes 2g}$。

6.3. 扭曲情形。 现在我们可以考虑一种与前一个例子相似的情形，但不再假设 $d = a_r b_r$，只假设 $d \mid a_r b_r$。设 $c_r = \frac{a_r b_r}{d}$。此时，从 s_0 到 s_r 的流取值于$b_r\mathbb{Z}/d\mathbb{Z}$，而 s_r 处的荷定义在模 $\frac{b_r}{c_r} = \frac{d}{a_r}$ 意义下。由于现在我们处于扭曲情形，而非移位情形，新的受保护空间为 $V^H \simeq (\mathbb{C}^d)^{\otimes 2g} \otimes \mathbb{C}^{c_1} \otimes \ldots \otimes \mathbb{C}^{c_u}$。

参考文献

[1] O. Albouy。矩阵约化与拉格朗日子模。 *arXiv* 预印本 *arXiv:0809 1059*，2008。。[2] M. H. Freedman 和 D. A. Meyer。射影平面与平面量子码。 计算数学基础，1(3):325–332，2001。[3] V. Gheorghiu。量子比特稳定子群的标准形式。《物理快报*A*》，378 509，2014 5 6 505(-): – 。[4] D. Gottesman。 稳定子码与量子纠错。加州理工学院，1997。[5] E. Hostens、J. Dehaene 和 B. De Moor。任意维数系统与模算术中的稳定子态和克利福德操作。《物理评论*A*：原子、分子与光学物理》，71(4):042315，2005。[6] A. Y. Kitaev。利用任意子实现容错量子计算。《物理年鉴》，303 30，2003 1 2( ): – 。[7]R. Maksimau。什么是自旋？量子比特简介。2025。网址：`https://hal.science/ hal-05557990v1/document`。

R. M.：分析、几何与建模实验室，CY 塞尔吉-蓬图瓦兹大学，95302 塞尔吉-蓬图瓦兹（法国），ruslmax@gmail.com，ruslan.maksimau@cyu.fr