arXiv:2601.05922v1 [math.AG] 9 Jan 2026

Hesse 形式中的阿贝尔曲面与显式同源公式

THOMAS DECRU, SABRINA KUNZWEILER

Abstract. 我们提出一种新方法，用于计算主极化阿贝尔曲面之间的 (3，3)-同源。其思路是使用由对称的 3 级 theta 结构诱导的 $\mathbb{P}^8$ 中的模型。在这一设定下，三扭点的作用是线性的，而同源公式可以简洁地描述为一系列易于计算的映射的复合。在对这些公式的描述中，与 Burkhardt 四次三维簇的关系发挥着重要作用。此外，我们还讨论了将这一思路推广到高维以及不同同源次数的情形。

1. 引言

对于椭圆曲线的显式计算，人们通常使用平面射影模型。具体而言，给定一条椭圆曲线 E 及其指定点 $\mathcal{O}$，通过选择 $L(3\mathcal{O})$ 的一组基，即可定义一个到射影平面的嵌入。典型的选择是 $\{1, x, y\}$，其中 x 在 $\mathcal{O}$ 处有二阶极点，而 y 有三阶极点。在这一设定下，E 在该嵌入下的像

$$E \hookrightarrow \mathbb{P}^2, \quad P \mapsto (x(P) : y(P) : 1),\ P \neq \mathcal{O},$$
$$\mathcal{O} \mapsto (0 : 1 : 0),$$

由一个 Weierstrass 方程定义。下文中，我们关注 $L(3\mathcal{O})$ 的另一种坐标选取。

从现在起，假设我们在特征为 $p \neq 3$ 的域上进行研究。我们知道，E 的 3-扭点通过线性变换作用于点的坐标。记 $E[3] = \langle P, Q\rangle$，我们选取一组基，使得相应的嵌入 $\iota\colon E \to \mathbb{P}^2$ 满足

$$\iota(R) + \iota(P) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdot \iota(R), \quad \iota(R) + \iota(Q) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \cdot \iota(R),$$

对任意点 $R \in E$ 都成立。这里，$\omega = e_3(Q, P)$ 表示 P 与 Q 的 Weil 配对；特别地，ω 是一个本原三次单位根。E 在 $\mathbb{P}^2$ 中的像具有 *Hesse* 形式。也就是说，存在一个射影参数 $d = (d_0 : d_1)$，使得 $d_0(d_0^3 - d_1^3) \neq 0$，从而 $\iota(E) = \mathcal{H}_d$，其中

$$\mathcal{H}_d : d_1(X^3 + Y^3 + Z^3) = 3d_0XYZ. \tag{1}$$

更形式化地说，这个嵌入由一个 3 级对称 theta 结构诱导；特别是，坐标函数 X, Y, Z 对应于 3 级 theta 函数，见 [28, 第 5 节，情形 (b)]。注意，如果 E 具有全有理 3-扭点，那么这个模型定义在基域上。文献中通常将单位元选为 $0_{\mathcal{H}_d} = (0 : -1 : 1)$。在这种情况下，上述 3-扭点基的生成元具有如下形式

$$P = (-1 : 1 : 0), \quad Q = (0 : -\omega^2 : 1) \quad \in \quad \mathcal{H}_d. \tag{2}$$

本文着重研究主极化阿贝尔曲面。全文中，我们均在一个特征为 $p \neq 2$，3 且含有本原三次单位根 ω 的域 k 上进行讨论。

上述构造可推广到高维。特别地，对于具有全有理 3-扭点的主极化阿贝尔曲面，我们可以考虑如下嵌入：

$$\iota : A \hookrightarrow \mathbb{P}^8$$

由 3 级对称 theta 结构诱导。与椭圆曲线的情形一样，此模型中 3-扭点的作用是规范化的。像 $\mathcal{A}_{d,\ h} := \iota(A)$ 在 $\mathbb{P}^8$ 中的显式方程已知。更确切地说，$\mathcal{A}_{d,\ h}$ 被描述为 8 个二次曲面和 4 个三次方程的零点集，[19]。在我们的记号中，$d = (d_0 : \cdots : d_4) \in \mathbb{P}^4$ 是定义三次方程的系数向量，而 $h = (h_0 : \cdots : h_4) \in \mathbb{P}^4$ 定义二次曲面（精确定义见定理 3.1）。类比椭圆曲线的情形，我们称 $\mathcal{A}_{d,\ h}$ 为 Hesse 形式的主极化阿贝尔曲面。

1.1. 贡献。本文的主要结果是提出一种新方法，用于计算 Hesse 形式的主极化阿贝尔曲面之间的 (3，3)-同源。这里，前缀 (3，3) 表示该同源的核是一个极大 3-各向同性群。同源计算将分解为四个简单操作（更正式的定义见记号 6.1）：

– S_K：依赖输入核 K 的辛变换，– $\odot^3$：逐坐标立方，– $M_{3,\ 3}$：离散傅里叶变换（它同样是辛变换），– C_λ：按向量 $\lambda \in \mathbb{P}^4$ 进行逐坐标（对称）缩放。

使用这些记号，我们的结果可概括如下。

主定理 （非正式表述）。 设 $\mathcal{A}_{d,\ h}$ 是 *Hesse* 形式的阿贝尔曲面。给定一个极大各向同性群 $K = \langle Q_1, Q_2 \rangle \subset \mathcal{A}_{d,\ h}[3]$ 和 9 阶挠点 R_1, R_2，满足 $3 \cdot R_1 = Q_1, 3 \cdot R_2 = Q_2$，我们可以确定一个辛变换 S_K 和一个向量 $\lambda \in \mathbb{P}^4$，使得

$$\phi = (C_\lambda \circ M_{3,3} \circ \odot^3 \circ S_K) : \mathcal{A}_{d,h} \to \mathcal{A}_{d',h'},$$

描述一个核为 K 的 (3,3)-同源，它连接两个 *Hesse* 形式的主极化阿贝尔曲面。

忽略加法和乘以三次单位根 ω 的标量乘法的开销后，映射 S_K 和 $M_{3,\ 3}$ 基本上是免费的。因此，同源计算的开销是在定义域上进行 9 次立方运算（应用 $\odot^3$）和 9 次乘法（应用 C_λ）。

我们指出，该方法允许我们将 $\mathcal{A}_{d,\ h}$ 上乘以 3 的运算，计算为一个 (3，3)-同源与其对偶的复合（前提是我们像定理中那样给定两个辅助 9-挠点）。此外，我们强调，该方法原则上适用于 Hesse 形式下的一般主极化阿贝尔曲面。特别是，所谓的粘合、分裂和对角同源都包括在内。不过，在处理某些边界情形时，系数向量 λ 的具体计算必须作相应调整。

从技术层面来说，我们的方法基于 theta 结构以及 3 级阿贝尔曲面模空间的经典结果。一个重要的组成部分是 Gunji [19] 对 $\mathcal{A}_{d,\ h}$ 的显式描述，该描述以 Coble [7]，对 3 级 theta 函数二次关系的描述以及 Birkenhake 和 Lange [25] 对三次关系的描述为基础。此外，模型 $\mathcal{A}_{d,\ h}$ 与 Burkhardt 四次曲面及其对偶之间的显式关系也发挥着重要作用。对此，我们依据 Freitag 和 Manni [15], [16]，对模空间的分析、Hunt [21]，关于 Burkhardt 四次曲面几何的论述，以及 Bruin 和 Nasserden [5] 关于 Burkhardt 四次曲面算术的进一步结果。

本文附带一个 SageMath [35] 软件包，实现了文中介绍的方法，并提供了有关 Hesse 形式阿贝尔曲面算术的各种功能：

https://github.com/sabrinakunzweiler/level-3-arithmetic

1.2. **与文献中的同源公式比较**。 我们的方法受到使用 2 级 theta 结构的 Kummer 曲面上的 (2,2)-同源公式的启发， [17, 32, 11]。在该设定中，加上 2-扭点会通过线性变换作用于点的坐标。这带来了极其简洁的同源公式。与我们的结果类似，一个 (2,2)-同源被分解为四个简单操作：辛变换、逐坐标平方、哈达玛变换和逐坐标缩放。注意，哈达玛变换是一种离散傅里叶变换（相对于一个本原单位平方根）；显然，立方运算是平方运算的自然类比。从这个意义上说，我们计算 (3,3)-同源的方法可视为其自然类比。

我们注意到，Cosset、Lubicz 和 Robert 在一系列工作中开发了用于在 2 级（或 4 级） theta 模型中计算 (ℓ, ℓ)-同源的通用算法 [26, 9, 27], 另见[37] ，其中针对不同的 ℓ 给出了具体优化。尽管这些算法同样基于 theta 函数理论，但其性质有所不同。尤其是在偶数级下，3-扭点的平移并非由线性变换给出，因此无法利用这一对称性推导同源公式。

先前用于计算 (3,3)-同源的专用算法基于不同的思路。Bruin、Flynn 和 Testa 最早给出了 2 属曲线雅可比簇之间 (3,3)-同源的显式公式 [4] ，其背景是 (3,3)-下降。后来， [13] 对这些公式作了一些代数化简，使其适用于密码分析场景。Bruin、Flynn 和 Testa 的方法有一个优点：只要求 (3,3)- 同源的核是有理的，而我们的方法要求全有理 3- 挠点。不过，与我们的新框架相比，这些公式的求值代价要高得多。目前已知最高效的 (3,3)-同源计算方法，是 Corte-Real Santos、Costello 和 Smith 提出的算法 [8]；该算法基于所谓的快速 Kummer 曲面，并要求全有理 2-扭点。在他们优化后的公式中，一次同源计算需要 4 次平方运算和 26 次乘法运算；而在我们的方法中，计算一个 (3,3)-同源需要 9 次平方运算和 18 次乘法运算。因此，我们的新方法（略微）更快。不过值得一提的是，反过来说，Kummer 曲面上的三倍公式效率更高。

上述用于计算 (3，3)-同源的方法都作用于 Kummer 曲面的不同模型上。与此相反，在我们的方法中，我们直接作用于阿贝尔曲面本身。此外，我们的方法并不局限于处理不可约主极化阿贝尔曲面。但是，Hesse 形式下的主极化阿贝尔曲面描述 $\mathcal{A}_{d,\ h}$ 自然包含椭圆曲线的乘积。

1.3. **应用与展望**。 显式同源计算对于算法数论十分重要。例如，(3，3)-同源已被用于下降 [4] ，或用于构造具有大阶点的 2 属曲线的雅可比簇 [20]。此外，(3，3)-同源最近已在后量子密码学中得到应用 [6]。对于某些大整数 n，我们的方法特别适合计算 $(3^n,\ 3^n)$-同源。将计算分解为一系列 (3，3)-同源后，每一步都能自然获得辅助的 9-挠点。例如，我们的方法可以应用于基于同源的密码学，更确切地说，可用于签名方案 SQIsign 的二维变体 [14, 2, 30], ，其中一种方案正处于由美国国家标准与技术研究院进行标准化的过程中 [34]。该方案中的一项瓶颈计算是对 $(2^n,\ 2^n)$-同源进行求值，而在经过一些参数调整后，这项计算可以由 $(3^n,\ 3^n)$-同源所取代。

除了这些具体应用之外，我们的结果更广泛地表明，主极化阿贝尔曲面的 $\mathbb{P}^8$-模型非常适合进行显式计算。尽管它与椭圆曲线的 $\mathbb{P}^2$-模型有相似之处，但据我们所知，文献中尚无多少关于前者的计算应用。

一个有趣的问题是，我们的方法能否推广到任意维数。我们在论文最后一节简要探讨了这个问题，但将对特定维数进行具体分析留作未来工作。[1] 在准备本文期间，我们验证了 Hesse 形式的椭圆曲线之间的 3-同源计算完全类似。更确切地说，核为 K 的 3-同源 $\phi : \mathcal{H}_d \to \mathcal{H}_{d'}$ 可以计算为

$$\phi = (C_\lambda \circ M \circ \odot^3 \circ S_K)(P),$$

其中，与之前类似， $C_\lambda : \mathbb{P}^3 \to \mathbb{P}^3$ 表示逐坐标（对称）缩放， M 表示离散傅里叶变换， $\odot^3$ 表示逐坐标立方， S_K 表示辛变换。一篇介绍这些公式、且将范围限定于椭圆曲线的短文目前正在投稿，拟收入某密码学会议的论文集；我们曾在该会议上展示这一现象 [12]。鉴于 Hesse 形式下椭圆曲线之间的 3-同源公式众所周知，这种情况下的证明很简单，且独立于本文所发展的理论。不过，椭圆曲线情形下的公式可以直接由我们的主要结果推出，只需将其应用于 Hesse 形式下椭圆曲线的乘积。

未来的另一个研究方向是将我们的公式推广到$\mathcal{A}_{d,\ h}$的 Kummer 曲面。一方面，在投影$\mathcal{A}_{d,\ h} \to \mathcal{A}_{d,\ h}/\langle \pm 1 \rangle$ 下，关于 3-扭点作用的部分对称性会丢失。另一方面，可用的坐标更少。值得研究的是，由此得到的用于计算 (3，3)-同源，尤其是三倍运算的公式，是否会更加高效。

1.4. **概述**。 第2节回顾 Burkhardt 四次曲面、其对偶曲面及其 Hessian 的性质。第3节专门介绍 Hesse 形式的主极化阿贝尔曲面。特别地，我们分析其与 Burkhardt 四次曲面、辛变换以及乘积曲面这一特殊情形之间的关系。第4节描述 $\mathcal{A}_{d,h}$ 的 3-扭点及其作用，第5节则简要介绍 $\mathcal{A}_{d,h}$的扭曲。第6节专门讨论 (3,3)-同源。我们证明主要结果（定理 6.4），并解释如何进行调整以获得一种完全通用的方法。第7节通过一个详细示例进一步说明这一点。最后，在第8节中，我们讨论将该方法推广到高维和不同同源次数的情形。

1.5. **致谢**。 我们感谢 Damien Robert 在整个项目期间提供了非常有帮助且富有洞见的反馈。Thomas Decru 获得科学研究基金会（FWO）资助，参考编号为 1245025N；获得欧洲研究委员会（ERC）在欧盟 Horizon 2020 研究与创新计划下的资助（资助协议 ISOCRYPT – 编号 101020788）；获得鲁汶大学研究委员会资助，编号为 C14/24/099；并获得网络安全研究佛兰德斯资助，参考编号为 VOEWICS02。Sabrina Kunzweiler 获得法国国家研究署（ANR）在 ANR CIAO 项目下提供的资助，参考编号为 ANR-19-CE48-0008；并获得法国2030计划资助，编号为 ANR-22-PETQ-0008（PQ-TLS）。

2. The Burkhardt quartic

Burkhardt 四次曲面是在 $\mathbb{P}^4$ 中由四次方程定义的超曲面 n

$$\mathcal{B} : F(x_0, x_1, x_2, x_3, x_4) = x_0(x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3) + 3x_1x_2x_3x_4 = 0 \subset \mathbb{P}^4. \tag{3}$$

Burkhardt 四次曲面与定义在 $\mathbb{Z}[1/3, \omega]$, [36] 上、具有完整 3 级结构的主极化阿贝尔曲面模空间双有理等价。特别地，对于任意非奇异点 $h = (h_0 : \cdots : h_4) \in \mathcal{B}$，都可以关联一个带标记的 3 级结构的不可约主极化阿贝尔曲面。文献 [5] 给出了一个显式构造。

[1]已知，类似的 (2,2)-同源公式在任意维数 [32] 中成立。实际上，这些公式已在维数 1,2,3 和 4 [33, 11, 24, 10] 中用于不同目的。

2.1. **自同构群**。Burkhardt 四次曲面的自同构群同构于射影辛群 $\mathrm{PSp}_4(\mathbb{F}_3)$。我们使用表示 $\mathrm{Aut}(\mathcal{B}) = \langle M,\ S_0,\ S_1,\ S_2\rangle$，其中

$$M = \begin{pmatrix} 1 & 2 & 2 & 2 & 2 \\ 1 & -1 & 2 & -1 & -1 \\ 1 & 2 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 2 \\ 1 & -1 & -1 & 2 & -1 \end{pmatrix}, \qquad \begin{aligned} S_0 &= diag(1,\omega,1,\omega,\omega) \\ S_1 &= diag(1,1,1,\omega^2,\omega) \\ S_2 &= diag(1,1,\omega,\omega,\omega). \end{aligned} \tag{4}$$

来自 [15, 命题 1]。这里，$diag(\alpha_0, \ldots\ldots, \alpha_4)$表示以 $\alpha_0, \ldots\ldots, \alpha_4$为对角线元素的对角矩阵。四次曲面上各点的作用由坐标向量上的右作用给出；我们将 $h \cdot g$ 简记为 $h \in \mathcal{B}$ 和 $g \in \langle M,\ S_0,\ S_1,\ S_2\rangle$。

注 2.1。由 $S_0,\ S_1,\ S_2$ 定义的自同构以相容的方式，通过三次单位根缩放 Burkhardt 四次曲面上点的坐标。注意，

$$\langle S_0, S_1, S_2\rangle = \{diag(1,\omega^a,\omega^b,\omega^c,\omega^{2(a+b+c)}) \mid a,b,c \in \{0,1,2\}\}.$$

此外，我们稍后将看到，由 M 定义的自同构与离散傅里叶变换（定义 3.11）有关。

在我们的应用中，我们也会关注可约阿贝尔曲面。为此，我们先回顾一个关于 $\mathcal{B}$的奇点的结果。

引理 2.2. *Burkhardt 四次曲面的奇异轨迹 $\mathcal{B}^{sing}$由45个奇点组成。具体而言，奇点 $h = (h_0 :\ h_1 :\ h_2 :\ h_3 :\ h_4) \in \mathcal{B}$ 如下给出*

$$(a) \quad h = \sigma(0:0:0:-\omega^i:1), \quad with\ i \in \{0,1,2\}$$

以及 $\sigma \in \mathcal{S}_4 \subset \mathcal{S}_5$ 一个固定 $h_0 = 0$的置换，

$$(b) \quad h = (1:-\omega^i:-\omega^j:-\omega^k:-\omega^{-i-j-k}) \quad with\ i,j,k \in \{0,1,2\}.$$

此外，$Aut(\mathcal{B})$ 在 $\mathcal{B}^{sing}$上传递地作用。

证明。对 $h_0 = 0$ 和 $h_0 \neq 0$ 进行分类讨论，可得 $\mathcal{B}$的奇点的显式描述。其中有 18 个奇点属于类型 (a)，27 个属于类型 (b)。

可以显式验证该作用的传递性。具体而言，对于任意奇点 $h \in \mathcal{B}$，我们计算得到一个元素 $g \in \mathrm{Aut}(\mathcal{B})$，使得 $h \cdot g = (0:0:0:-1:1)$；见 [23]。□

2.2. **伯克哈特对偶**。Burkhardt 四次曲面仅与带 3 级结构的主极化阿贝尔曲面的模空间双有理等价。该模空间的佐藤紧化由*Burkhardt 四次曲面的对偶*的正规化给出，即 [15]。后者将使我们能够描述可约阿贝尔曲面。

定义 2.3。伯克哈特对偶 $\mathcal{B}$ 是 Burkhardt 四次曲面的对偶 $\mathcal{B}$，也就是说，它是 $\mathbb{P}^4$ 中的一个超曲面，由 $\tilde{F}$定义，其中 $\tilde{F}$ 是定义 $\mathcal{B}$的多项式 F 的对偶。

多项式 F 是 18 次齐次多项式。其显式描述见 [15, 命题 3]。我们进一步回顾，根据对偶的定义，F 是满足以下条件的最小多项式

$$\tilde{F}(\nabla F) \cong 0 \pmod{F},$$

其中 ∇ 表示梯度算子。特别地，∇ 定义了一个嵌入 $\nabla\colon \mathcal{B}\setminus\mathcal{B}^{\mathrm{sing}}\to\tilde{\mathcal{B}}$。具体而言，

$$\nabla : (x_0 : \cdots : x_4) \mapsto \begin{pmatrix} 4x_0^3 + x_1^3 + x_2^3 + x_3^3 + x_4^3 \\ 3(x_0x_1^2 + x_2x_3x_4) \\ 3(x_0x_2^2 + x_1x_3x_4) \\ 3(x_0x_3^2 + x_1x_2x_4) \\ 3(x_0x_4^2 + x_1x_2x_3) \end{pmatrix}. \tag{5}$$

$\mathcal{B}$ 的自同构群作用可扩展为对偶上的作用，其中 $g\in\mathrm{Aut}(\mathcal{B})$ 中的元素通过从左侧乘以 g^{-1} 进行作用；对于 $d\in\tilde{\mathcal{B}}$，我们将 $g^{-1}\cdot d$ 记作。注意，除相差一个标量因子外，对于上文定义的矩阵 M，$M\equiv M^{-1}$。

2.3. **Burkhardt 四次曲面的 Hessian**。研究具有 3 级结构的阿贝尔曲面的模空间时，还会遇到另一个簇，即 Burkhardt 四次曲面的 Hessian。

定义 2.4。*Burkhardt 四次曲面的 Hessian* $H(\mathcal{B})$ 是 $\mathbb{P}^4$ 中由下式定义的射影超曲面

$$H(\mathcal{B}) : H(F) := \frac{1}{486}\det\left(\frac{\partial F}{\partial x_i\partial x_j}\right) = 0,$$

其中 F 是定义 $\mathcal{B}$ 的多项式。

注意，缩放确保 $H(F)$ 是整系数且内容为 1（例如参见 [5, 第 3] 节）。可以验证，$H(F)$ 是 10 次齐次多项式。

3. Principally polarized abelian surfaces in Hesse form

设 A 是一个主极化阿贝尔曲面。考虑一个诱导主极化的线丛 L。那么 $L^{\otimes 3}$ 非常丰，并定义一个嵌入 $\iota\colon A\hookrightarrow\mathbb{P}^8$。对于任意 3-挠点 $T\in A[3]$，平移映射 $P\mapsto P+T$ 在 $\iota(A)$ 的坐标上作用为线性变换。在这里，我们将考虑由 3 级对称 theta 结构诱导的特定嵌入 $\Theta : A\to\mathbb{P}^8$。在此设定下，3-挠点的作用经过归一化。

我们首先回顾模型 $\Theta(A)\subset\mathbb{P}^8$ 的显式描述。然后在第 3.2 小节解释该模型与 Burkhardt 四次曲面上的点及其对偶之间的关系，在第 3.3 小节讨论辛变换，并在第 3.4 小节更详细地分析可约情形。三扭点的作用将在第4节讨论。

定理 3.1 ([19]中的定理 8.3)。设 A 是一个带有 *level*-3结构的主极化阿贝尔曲面。那么存在系数向量 $d=(d_0\colon\cdots\colon d_4)$ $h=(h_0\colon\cdots\colon h_4)\in\mathbb{P}^4$，以及一个嵌入 $\iota\colon A\to\mathbb{P}^8$，使得

$$\iota(A) = V(F_1, F_2, F_3, F_4, G_0, \ldots, G_8),$$

其中 F_i 是三次多项式

$$\begin{aligned} F_1 &= d_1\sum_{j=0}^{8} X_j^3 - 3d_0(X_0X_1X_2 + X_3X_4X_5 + X_6X_7X_8), \\ F_2 &= d_2\sum_{j=0}^{8} X_j^3 - 3d_0(X_0X_3X_6 + X_1X_4X_7 + X_2X_5X_8), \\ F_3 &= d_3\sum_{j=0}^{8} X_j^3 - 3d_0(X_0X_4X_8 + X_1X_5X_6 + X_2X_3X_7), \end{aligned}$$

$$F_4 \;=\; d_4\sum_{j=0}^{8}X_j^3 - 3d_0(X_0X_5X_7 + X_1X_3X_8 + X_2X_4X_6),$$

而 G_i 是二次多项式

$$\begin{aligned}
G_0 &= h_0x_0^2 + h_1x_1x_2 + h_2x_3x_6 + h_4x_5x_7 + h_3x_4x_8,\\
G_1 &= h_0x_1^2 + h_1x_0x_2 + h_2x_4x_7 + h_3x_5x_6 + h_4x_3x_8,\\
G_2 &= h_0x_2^2 + h_1x_0x_1 + h_2x_5x_8 + h_3x_3x_7 + h_4x_4x_6,\\
G_3 &= h_0x_3^2 + h_1x_4x_5 + h_2x_0x_6 + h_3x_2x_7 + h_4x_1x_8,\\
G_4 &= h_0x_4^2 + h_1x_3x_5 + h_2x_1x_7 + h_3x_0x_8 + h_4x_2x_6,\\
G_5 &= h_0x_5^2 + h_1x_3x_4 + h_2x_2x_8 + h_3x_1x_6 + h_4x_0x_7,\\
G_6 &= h_0x_6^2 + h_1x_7x_8 + h_2x_0x_3 + h_3x_1x_5 + h_4x_2x_4,\\
G_7 &= h_0x_7^2 + h_1x_6x_8 + h_2x_1x_4 + h_3x_2x_3 + h_4x_0x_5,\\
G_8 &= h_0x_8^2 + h_1x_6x_7 + h_2x_2x_5 + h_3x_0x_4 + h_4x_1x_3.
\end{aligned}$$

我们注意到， [19, 定理 8.3] 中的描述并未包含多项式 F_4，因为它包含在由其余多项式生成的理想中。不过，在我们的设定中，将该多项式纳入描述会更加自然。此外，我们指出，所引用的定理更为精确，因为它明确描述了系数。不过，就我们的目的而言，上述陈述已经足够。

注 3.2。 在 [19], 中，作者使用了关于 $\mathbb{C}$上的 theta 函数的经典解析理论。利用 Mumford 的 theta 函数代数理论，可以将这些结果推广到特征为 $p > 3$ 的任意域。对特征的限制源于这样一个事实：定义方程的系数由 18 级 theta 函数描述，因此这些方程在 $\mathbb{Z}[1/18]$上有定义。

另一方面，坐标函数 x_0，……， x_8 只有 3 级。若能将这些结果也推广到 $p = 2$，将会很有意思。关于 n 级 theta 结构的提升论证，更多详情请参见 [31, 第 2.3 节。6]

定义 3.3。 我们称主极化阿贝尔曲面 A 处于*Hesse* 形式，如果 $A = V(F_1,\ F_2,\ F_3,\ F_4,\ G_0,\ \ldots\ldots,\ G_8)$，其中 $F_i,\ G_i$ 如定理 3.1 所述。在此情况下，我们记 $A = \mathcal{A}_{d,\ h}$ 其中$d = (d_0 :\ d_1 :\ d_2 : d_3 : d_4)$，且 $h = (h_0 :\ h_1 :\ h_2 : h_3 :\ h_4)$中的记号沿用定理 3.1。

我们使用*Hesse* 形式这一术语，因为这种形式可以看作椭圆曲线的 Hesse 形式的类比。

注 3.4。 如果 $\mathcal{A}_{d,\ h}$ 是不可约的，那么该簇已经由二次曲面定义，即$V(F_1,\ F_2,\ F_3,\ F_4,\ G_0,\ \ldots\ldots,\ G_8) = V(G_0,\ \ldots\ldots,\ G_8)$。Coble [7] 已经提出了这一结论，并由 Barth [1]证明。三次关系对于纳入退化情形是必要的。我们在此使用的 Gunji [19] 给出的显式描述，建立在 Birkenhake 和 Lange 关于三次 theta 关系 [25]的工作之上。

3.1. 的 2-挠点。 乘以 $[-1]$ 在 $\mathcal{A}_{d,h}$中点的坐标上作用为线性变换。更确切地说，它对点的坐标施加置换 (0)(1 2)(36)(4 8)(3 7)，即

$$\begin{array}{c} P = (x_0 : x_1 : x_2 : x_3 : x_4 : x_5 : x_6 : x_7 : x_8) \\ \downarrow \\ -P = (x_0 : x_2 : x_1 : x_6 : x_8 : x_7 : x_3 : x_5 : x_4). \end{array}$$

注 3.5. 我们回顾一下，坐标 $x_0, \ldots, x_8$ 对应于 3 级 theta 函数。使用指标的三元表示，即

$$x_0 = x_{00},\ x_1 = x_{01},\ \ldots\ ,\ x_8 = x_{22},$$

按 $[-1]$ 进行乘法由 $(x_i)_{i\in(\mathbb{Z}/3\mathbb{Z})^2} \mapsto (x_{-i})_{i\in(\mathbb{Z}/3\mathbb{Z})^2}$ 给出，这是惯常的写法。我们注意到，这种记号更接近 [19]，中使用的记号；特别参见 [19，第 3] 节，了解其与 theta 函数的关系。

$\mathcal{A}_{d,h}$ 上的 2-扭点是在按 $[-1]$ 进行乘法时保持不变的点。这些点分为两类：$\mathcal{A}_{d,h}[2] = U_1 \cup U_2$ 其中

$$\begin{aligned} U_1 &= \mathcal{A}_{d,h} \cap \{x_1 = x_2, x_3 = x_6, x_4 = x_8, x_5 = x_7\}, \\ U_2 &= \mathcal{A}_{d,h} \cap \{x_0 = 0, x_1 = -x_2, x_3 = -x_6, x_4 = -x_8, x_5 = -x_7\}. \end{aligned}$$

U_1 中的元素对应于特征值 $+1$ （即按 $[-1]$ 映射进行乘法的特征值），称为 偶 2-扭点； U_2 中的元素对应于特征值 -1 ，称为 奇2-扭点。总共有 10 个偶 2-扭点和 6 个奇 2-扭点 [21, 第 5.3 节。1]。

单位元可以是偶的，也可以是奇的，这取决于底层 theta 结构是偶的还是奇的。在全文中，我们假设底层 theta 结构是偶的，因此单位元属于集合 U_1。记

$$0_{\mathcal{A}_{d,h}} = (t_0 : t_1 : t_1 : t_2 : t_3 : t_4 : t_2 : t_4 : t_3), \tag{6}$$

对于某个 t_0，...， t_4。

对于我们的应用而言，这一选择是自然的，因为我们通常构造 $\mathcal{A}_{d,\ h}$ ，它与椭圆曲线的乘积 $E_1 \times E_2$ 同源。后者带有乘积 theta 结构——当 E_1 和 E_2 都带有相同类型的 theta 结构时（即二者均为偶的，或均为奇的），该结构是偶的。[2]

最后，我们注意到，单位元的坐标与 Burkhardt 四次曲面的几何有关。成立

$$(t_0 : 2t_1 : 2t_2 : 2t_3 : 2t_4) \in H(\mathcal{B}), \tag{7}$$

其中 $H(\mathcal{B})$ 是 Burkhardt 四次曲面的 Hessian（定义 2.4）。事实上，对于所有偶 2-扭点，该结论都成立。通过研究 Kummer 曲面 $\mathcal{A}_{d,\ h}/\langle\pm 1\rangle \subset \mathbb{P}^4$ 的坐标 $(x_0\colon\ x_1+x_2\colon\ x_3+x_6\colon\ x_4+x_8\colon\ x_5+x_7)$，并注意到十个偶 2-扭点对应于该 Kummer 曲面的节点，可以得到这一关系，参见 [21,第 5 节3]。

3.2. **与 Burkhardt 四次曲面的关系**。我们已经看到，$\mathcal{A}_{d,h}$ 单位元的坐标与 Burkhardt 四次曲面的 Hessian 上的一个点相关 $\mathcal{B}$。此外，众所周知，定义 $\mathcal{A}_{d,h}$ 的二次曲面的系数向量 h 位于 Burkhardt 四次曲面本身上：

$$h = (h_0 : \cdots : h_4) \in \mathcal{B}, \tag{8}$$

例如参 见 [21, 第 5.3 节1]。此外，系数向量 d也存在一种关系 ：

$$h_0d_0 + h_1d_1 + h_2d_2 + h_3d_3 + h_4d_4 = 0,$$

[19, 公式 83] ，这意味着 d 位于 Burkhardt 四次曲面的对偶上：

$$d = (d_0 : \cdots : d_4) \in \tilde{\mathcal{B}}. \tag{9}$$

这很自然，因为n t关于 [15], 模空间的描述，另见小节2.2。

[2]在文献中，我们只遇到过以奇数阶 2-挠点为单位元的例子，例如参见 [18]中的定理 3.14(b)。感谢 Damien Robert 为我们阐明此事。

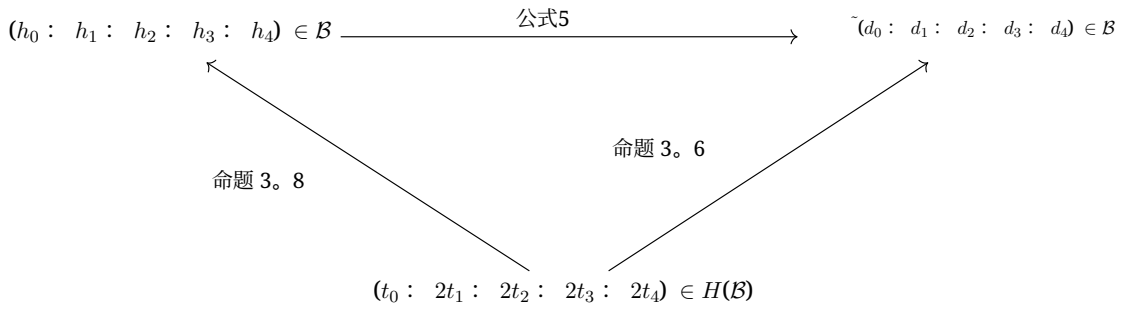


FIGURE 1. Burkhardt 四次曲面的所用元素、其对偶及其 Hessian 之间的关系。

下文将给出显式公式，用于计算系数向量 d 和 h；已知 Hesse 形式 $\mathcal{A}_{d,h}$下阿贝尔曲面的单位元 $0_{\mathcal{A}_{d,h}}$ 。这些公式定义了 Burkhardt 四次曲面的 Hessian、其对偶与 Burkhardt 四次曲面本身之间的映射。我们在图 1 中总结这些关系。

我们对这些关系的证明是显式的，只需了解定义方程即可。然而，我们注意到，这些关系源于 [25] 中所描述的 theta 函数的三次关系；这些关系最初曾被用于求出 $\mathcal{A}_{d,\ h}$ [19] 的显式方程。

命题 3.6。 令 $0_{\mathcal{A}_{d,\ h}}$ 为单位元，其坐标由 t_0、.....、t_4 按照公式*6*定义。若 $t_0^3 + 2($ $t_1^3 + t_2^3 + t_3^3 + t_4^3) \neq 0$，则 $d = (d_0 : \ \cdots : \ d_4)$ 满足

$$d_0 = t_0^3 + 2(t_1^3 + t_2^3 + t_3^3 + t_4^3), \quad d_i = 3t_0 t_i^2 + 6 \prod_{j \neq 0,i} t_j.$$

证明。 d_i 的值可通过在单位元处求定理 3.1 中三次方程 F_1、.....、F_4 的值获得。当和 $t_0^3 + 2($ $t_1^3 + t_2^3 + t_3^3 + t_4^3)$ 不为零时，这给出唯一解。□

推论 3.7。 设 $\mathcal{A}_{d,\ h}$ 是一个采用 *Hesse* 形式的阿贝尔曲面，且 $0_{\mathcal{A}_{d,\ h}} =$ （$t_0 : \ t_1 : \ t_1 : \ t_2 : \ t_3 :$ $t_4 : t_2 : \ t_4 : \ t_3$）是单位元。则至少存在两个指标 $i \neq j$ 满足 t_i 、 $t_j \neq 0$。
证明。假设只有一个指标 i 满足 $t_i \neq 0$。根据命题 3.6，我们有$d =$ (1 : 0 : 0 : 0 : 0)。然而，这一点定义了一个奇异曲面。我们不进行显式计算，而是注意到这可以从模解释中推导出来：点~ $d =$ (1 : 0 : 0 : 0 : 0) $\in B$ 属于尖点 [15, 第 5] 节。□

该推论中的界是紧的，即存在 $\mathcal{A}_{d,\ h}$ 恰好有两个 t_i，$t_j \neq 0$对于 $i \neq j$ （见第6.3小节）。

~此外，我们回顾一下，$(t_0 : 2t_1 : \cdots : 2t_4)$ 是 $H(B)$ 上的一个点（参见公式7），因此在适当缩放坐标后，命题 3.6 中的对应关系定义了一个映射

$$H(\mathcal{B}) \cap \{4t_0^3 + t_1^3 + t_2^3 + t_3^3 + t_4^3 \neq 0\} \to \tilde{\mathcal{B}}, \quad (t_0 : \cdots : t_4) \mapsto (d_0 : \cdots : d_4).$$

~有趣的是，这个映射的描述与公式5中的梯度算子 $\nabla : \ \mathcal{B} \to \mathcal{B}$ 相吻合。

命题 3.8。 令 $0_{\mathcal{A}_{d,h}}$ 为单位元，其坐标由公式*6*中的 $t_0, \ldots, t_4$ 定义。则 $h = (h_0 : \cdots : h_4)$ 是矩阵的核中的一个元素

$$Hess(F)(t_0, 2t_1, 2t_2, 2t_3, 2t_4) = \left(\frac{\partial F}{\partial x_i \partial x_j} \right) (t_0, 2t_1, 2t_2, 2t_3, 2t_4),$$

其中 $Hess(F)$ 表示定义 *2.4* 中方程 F 的海森矩阵。一般而言，存在唯一的非平凡解。此外，若对所有 $i \in \{1,2,3,4\}$均有 $t_0 t_i^2 - \prod_{j\neq 0,i} t_j \neq 0$，则该解为 $h = (1 : h_1 : h_2 : h_3 : h_4)$，其中

$$h_i = -\frac{t_0^3 + 2t_i^3 - \sum_{j\neq 0,i} t_j^3}{3(t_0 t_i^2 - \prod_{j\neq 0,i} t_j)}.$$

证明。该命题的第一部分是经典结果。Burkhardt 四次曲面是自施泰纳曲面的事实，其证明正是以此为基础的 [21, 第 5.3 节1]。我们在此重述这一论证，因为它有助于证明第二部分。将定理 3.1 中的九个二次方程 $G_0, \ldots, G_8$代入单位元 $0_{\mathcal{A}_{d,h}}$，可得五个不同的线性条件 $c_0, \ldots, c_4$，这些条件必须满足：

$$\begin{aligned}
(c_0)\text{:} \qquad & 0 = t_0^2 h_0 + t_1^2 h_1 + t_2^2 h_2 + t_3^2 h_3 + t_4^2 h_4,\\
(c_1)\text{:} \qquad & 0 = t_1^2 h_0 + t_0 t_1 h_1 + t_3 t_4 h_2 + t_2 t_4 h_3 + t_2 t_3 h_4,\\
(c_2)\text{:} \qquad & 0 = t_2^2 h_0 + t_3 t_4 h_1 + t_0 t_2 h_2 + t_1 t_4 h_3 + t_1 t_3 h_4,\\
(c_3)\text{:} \qquad & 0 = t_3^2 h_0 + t_2 t_4 h_1 + t_1 t_4 h_2 + t_0 t_3 h_3 + t_1 t_2 h_4,\\
(c_4)\text{:} \qquad & 0 = t_4^2 h_0 + t_2 t_3 h_1 + t_1 t_3 h_2 + t_1 t_2 h_3 + t_0 t_4 h_4.
\end{aligned}$$

这些条件意味着 h 是某个 5×5 矩阵的核中的一个元素。可以看出，这个矩阵恰好是 Hessian 在点 $(t_0 : 2t_1 : 2t_2 : 2t_3 : 2t_4)$处的取值。因此，核中存在一个非零元素，并且一般而言，该元素是唯一的（作为射影点）。

陈述中的显式公式可通过考虑三次方程，从条件 c_0、.....、 c_4 推导得出

$$\begin{aligned}
(c_0 t_0 + 2c_1 t_1 - c_2 t_2 - c_3 t_3 - c_4 t_4)\text{:} \qquad & 0 = h_0(t_0^3 + 2t_1^3) + 3h_1(t_0 t_1^2 - t_2 t_3 t_4),\\
(c_0 t_0 + 2c_2 t_2 - c_1 t_1 - c_3 t_3 - c_4 t_4)\text{:} \qquad & 0 = h_0(t_0^3 + 2t_2^3) + 3h_2(t_0 t_2^2 - t_1 t_3 t_4),\\
(c_0 t_0 + 2c_3 t_3 - c_1 t_1 - c_2 t_2 - c_4 t_4)\text{:} \qquad & 0 = h_0(t_0^3 + 2t_3^3) + 3h_3(t_0 t_3^2 - t_1 t_2 t_4),\\
(c_0 t_0 + 2c_4 t_4 - c_1 t_1 - c_2 t_2 - c_3 t_3)\text{:} \qquad & 0 = h_0(t_0^3 + 2t_4^3) + 3h_4(t_0 t_4^2 - t_1 t_2 t_3).
\end{aligned}$$

我们注意到，这些对应于定理 4.1] 中类型为 (d) 的三次关系（另见 [19,第 8] 节）。□

命题 3.8 定义了一个映射 $H(\mathcal{B}) \to \mathcal{B}$。我们指出，该映射等同于所谓的施泰纳映射，它从 $H(\mathcal{B})$映射到 $\mathcal{B}$ 的施泰纳曲面；而后者（颇为令人惊讶地）等同于 $\mathcal{B}$ [21, 第 B.1.1 节3]。

3.3. **辛变换**。 Hesse 形式的主极化阿贝尔曲面的系数向量 $(d、 h)\mathcal{A}_{d、 h}$ 不是同构不变量。定义同构的主极化阿贝尔曲面的系数向量之间，由其底层 theta 结构上的辛变换联系起来。这些变换对应于 Burkhardt 四次曲面的自同构。这里，我们说明 Burkhardt 四次曲面的自同构如何作用于 $\mathcal{A}_{d、 h}$。

记号 3.9。 对于 $\lambda = (\lambda_0 : \cdots : \lambda_4) \in \mathbb{P}^4$，我们将 $\star$记作逐坐标缩放

$$\lambda \star x = (\lambda_0 x_0 : \cdots : \lambda_4 x_4) \quad \text{for } x \in \mathbb{P}^4,$$

并且当所有 $\lambda_i \neq 0$ 时，我们记为

$$\lambda^{-1} = (\lambda_0^{-1} : \cdots : \lambda_4^{-1})$$

对于逐坐标取逆。

我们进一步将缩放映射扩展到 $x \in \mathcal{A}_{d,\ h} \subset \mathbb{P}^8$:

$$C_\lambda(x) = (\lambda_0 x_0 : \lambda_1 x_1 : \lambda_1 x_2 : \lambda_2 x_3 : \lambda_3 x_4 : \lambda_4 x_5 : \lambda_2 x_6 : \lambda_4 x_7 : \lambda_3 x_8).$$

这种缩放具有对称性，即它与乘以 $[-1]$相交换。

注意，像 $C_\lambda(\mathcal{A}_{d,\ h})$ 不一定采用 Hesse 形式。在下一个命题中，我们给出使其采用该形式的 $\lambda \in \mathbb{P}^4$ 值。

命题 3.10。 设 $\mathcal{A}_{d,\ h} \subset \mathbb{P}^8$ 是一个采用 *Hesse* 形式的主极化阿贝尔曲面，并考虑缩放向量

$$a_0 = (1 : \omega : 1 : \omega : \omega), \quad a_1 = (1 : 1 : 1 : \omega^2 : \omega), \quad a_2 = (1 : 1 : \omega : \omega : \omega).$$

于是对于任意 $\lambda \in \{t_0, t_1, t_2\}$，像 C_λ（$\mathcal{A}_{d,\ h}$）仍采用 *Hesse* 形式，更准确地说，

$$C_\lambda(\mathcal{A}_{d,h}) = \mathcal{A}_{\lambda^{-1} \star d, \lambda \star h}.$$

证明。 利用定理 3.1 中给出的$\mathcal{A}_{d,\ h}$ 描述，通过显式计算即可验证这一点。□

我们注意到，命题 3.10 中描述的变换是 Burkhardt 四次曲面的（必然）自同构。 C_{λ_i} 在 h 上的作用对应于式 4 中的元素 S_i ；如小节2.2所述，这可扩展为对偶上的作用，即对 d的作用。

由矩阵 M 描述的自同构（参见公式 4）可解释为对 $\mathcal{A}_{d,h}$ 的离散傅里叶变换。

定义 3.11。令

$$M_{3,3} = \begin{pmatrix} M_3 & M_3 & M_3 \\ M_3 & \omega M_3 & \omega^2 M_3 \\ M_3 & \omega^2 M_3 & \omega M_3 \end{pmatrix}, \quad \text{with } M_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}.$$

离散傅里叶变换定义为 $M_{3,3}$ 对点 $P = (x_0 : \cdots : x_8) \in \mathcal{A}_{d,h}$ 的坐标向量的左作用。记作

$$M_{3,3} : (x_0 : \cdots : x_8) \mapsto M_{3,3} \cdot (x_0 : \cdots : x_8).$$

命题3.12。 设 $\mathcal{A}_{d,h}$ 是 *Hesse* 形式的主极化阿贝尔曲面。则离散傅里叶变换定义了一个同构 $\mathcal{A}_{d,\ h} \to \mathcal{A}_{\tilde{d},\tilde{h}}$，满足

$$\tilde{d} = M \cdot d, \quad \tilde{h} = h \cdot M, \quad \tilde{t} = M \cdot t.$$

证明。 利用定理 3.1 中对 $\mathcal{A}_{d,h}$ 的描述，通过显式计算即可验证这一点。□

与命题 3.10 类似，离散傅里叶变换在 h （分别在 d）上的作用，对应于公式 4 中的 M 在 Burkhardt 四次曲面（分别在其对偶）上的作用。

3.4. **乘积曲面**。 定理 3.1 中对 Hesse 形式的阿贝尔曲面的描述包括乘积曲面。这里，我们将更详细地研究这一特殊情形。回顾一下，Hesse 形式的椭圆曲线由一个三次方程定义

$$\mathcal{H}_d : d_1(X^3 + Y^3 + Z^3) = 3 d_0 XYZ.$$

对于某个 $d = (d_0 : d_1) \in \mathbb{P}^1 \setminus \{1, \omega, \omega^2, \infty\}$ (见公式 1)，并将单位元设为 $0_{\mathcal{H}_d} = (0 : -1 : 1)$。

引理 3.13. 设 $\mathcal{H}_{(d_0:d_1)}$、$\mathcal{H}_{(d_0':d_1')}$ 是两条 *Hesse* 形式的椭圆曲线。此外，设 $A = \mathcal{H}_{(d_0:d_1)} \times \mathcal{H}_{(d_0':d_1')}$ 并考虑 *Segre* 嵌入

$$\iota_S : A \to \mathbb{P}^8,$$
$$\big((x:y:z),(x':y':z')\big) \mapsto (xx' : xy' : xz' : yx' : yy' : yz' : zx' : zy' : zz').$$

于是 $\iota_S(A) = \mathcal{A}_{d,h}$，其中

$$d = (d_0d_0' : d_0d_1' : d_1d_0' : d_1d_1' : d_1d_1'), \quad h = (0:0:0:-1:1).$$

单位元为

$$0_{\mathcal{A}_d} = (0:0:0:0:1:-1:0:-1:1).$$

证明。 我们记

$$(x_0 : \cdots : x_8) = (xx' : xy' : xz' : yx' : yy' : yz' : zx' : zy' : zz')$$

为 $\iota_S(A)$ 上的一般点。只需证明该点满足定理 3.1 中的方程。

二次关系由 Segre 嵌入导出。更确切地说，$\iota_S(\mathbb{P}^2 \times \mathbb{P}^2) \subset \mathbb{P}^8$ 的像由以下零点集定义：

$$x_{3i+j}x_{3k+\ell} - x_{3i_\ell}x_{3k+j} \quad \text{for } i,j,k,\ell \in \{0,1,2\}.$$

这些关系给出定理 3.1 中的 8 个二次曲面，其系数向量为 $h = (0:0:0:-1:1)$。三次关系由 $\mathcal{H}_{(d_0:d_1)}$ 和 $\mathcal{H}_{(d_0':d_1')}$的方程导出。为说明这一点，我们注意到

$$\begin{aligned}
x_0^3 + \ldots + x_8^3 &= (x^3+y^3+z^3)\cdot(x'^3+y'^3+z'^3),\\
x_0x_1x_2 + x_3x_4x_5 + x_6x_7x_8 &= (x^3+y^3+z^3)\cdot(x'y'z'),\\
x_0x_3x_6 + x_1x_4x_7 + x_2x_5x_8 &= (x'^3+y'^3+z'^3)\cdot(xyz),\\
x_0x_4x_8 + x_1x_5x_6 + x_2x_3x_7 &= 3\cdot(xyz)\cdot(x'y'z'),\\
x_0x_5x_7 + x_1x_3x_8 + x_2x_4x_6 &= 3\cdot(xyz)\cdot(x'y'z').
\end{aligned}$$

将这些恒等式代入定理 3.1 中系数向量为

$$d = (d_0d_0' : d_0d_1' : d_1d_0' : d_1d_1' : d_1d_1')$$

的三次关系后，可化为椭圆曲线的定义方程。

最后，单位元计算为 $\iota_S((0:-1:1),(0:-1:1))$ □

注意，单位元如公式6所示，其中 $t_0 = t_1 = t_2 = 0$ 和 $t_3 = -t_4 = 1$。特别地，它是一个偶 2-挠点。

如果一个可约阿贝尔曲面来自两个 Hesse 形式椭圆曲线的 Segre 嵌入，那么我们称其为乘积形式。更准确地说：

定义 3.14。 当且仅当 $h = (0:0:0:-1:1)$ 时，我们称 Hesse 形式的可约主极化阿贝尔曲面 $\mathcal{A}_{d,\,h}$配备了乘积极化。

请注意，一般而言，对于可约阿贝尔曲面，定理 6.4 中的二次方程由某个系数向量 h 确定，而该向量是 Burkhardt 四次曲面上的一个奇点。奇点总共有 45 个。正如引理 2.2 中所述，Burkhardt 四次曲面的自同构群在这些奇点上具有传递作用。结合我们在第 3.3 小节对辛变换作用的分析，可得以下事实。

推论 3.15. 设 $\mathcal{A}_{d,h}$ 是 *Hesse* 形式下的一个可约主极化阿贝尔曲面。那么存在一个辛变换 T，使得 $T(\mathcal{A}_{d,h}) = \mathcal{A}_{d',h'}$ 带有乘积极化。

请注意，推论 3.15 是有效的。在我们的实现中，我们针对 Burkhardt 四次曲面的每个奇点，给出了一个具体的辛变换，将其变为乘积形式。

4. The 3-torsion group

设 $\mathcal{A}_{d,h}$ 是一个具有 Hesse 形式的主极化阿贝尔曲面。回顾一下，平移 3-扭点会在点的坐标上诱导线性变换。这意味着群 $G = (\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^2$ 作用于 $\mathcal{A}_{d,h} \subset \mathbb{P}^8$。此作用是规范化的，我们固定生成元

$$G \cong \langle \sigma_1, \sigma_2, \tau_1, \tau_2 \rangle,$$

其在点 $P = (x_0 : \cdots : x_8) \in \mathcal{A}_{d,h}$ 上的作用由下式给出

$$\begin{aligned}
\sigma_1(P) &= (x_1 : x_2 : x_0 : x_4 : x_5 : x_3 : x_7 : x_8 : x_6),\\
\sigma_2(P) &= (x_3 : x_4 : x_5 : x_6 : x_7 : x_8 : x_0 : x_1 : x_2),\\
\tau_1(P) &= (x_0 : \omega x_1 : \omega^2 x_2 : x_3 : \omega x_4 : \omega^2 x_5 : x_6 : \omega x_7 : \omega^2 x_8),\\
\tau_2(P) &= (x_0 : x_1 : x_2 : \omega x_3 : \omega x_4 : \omega x_5 : \omega^2 x_6 : \omega^2 x_7 : \omega^2 x_8),
\end{aligned} \tag{10}$$

That 其中 σ_1, σ_2 作为置换作用；而 τ_1, τ_2 通过乘以单位根的三次方根进行缩放 y.

命题 4.1。 设 $\mathcal{A}_{d,h}$ 是一个具有 *Hesse* 形式的主极化阿贝尔曲面，并设

$$0_{\mathcal{A}_{d,h}} = (t_0 : t_1 : t_1 : t_2 : t_3 : t_4 : t_2 : t_4 : t_3),$$

为单位元。则 (P_1, P_2, Q_1, Q_2) 满足

$$P_1 = \sigma_1(0_{\mathcal{A}_{d,h}}), \quad P_2 = \sigma_2(0_{\mathcal{A}_{d,h}}), \quad Q_1 = \tau_1(0_{\mathcal{A}_{d,h}}), \quad Q_2 = \tau_2(0_{\mathcal{A}_{d,h}})$$

是 $\mathcal{A}_{d,h}[3]$ 的辛基。

证明。 根据 $\sigma_1, \sigma_2, \tau_1, \tau_2$ 的定义，点 P_1, P_2, Q_1, Q_2 构成 $\mathcal{A}_{d,h}[3]$ 的一组基。为验证其为辛基，我们计算交换子配对。[3] 为此，我们将描述 $\sigma_1, \sigma_2, \tau_1, \tau_2$ 对坐标向量作用的 9×9 矩阵记为 S_1, S_2, T_1, T_2。我们计算

$$e_3(P_i, P_j) = \frac{S_i S_j}{S_j S_i} = 1, \quad e_3(Q_i, Q_j) = \frac{T_i T_j}{T_j T_i} = 1$$

and

$$e_3(P_i, Q_j) = \frac{S_i T_j}{T_j S_i} = \begin{cases} \omega & \text{if } i = j, \\ 1 & \text{if } i \neq j. \end{cases}$$

□

定义 4.2。 我们称基 (P_1, P_2, Q_1, Q_2) 为 $\mathcal{A}_{d,h}[3]$ 的典范基，并定义辛分解 $\mathcal{A}_{d,h}[3] = K_1 + K_2$，其中 $K_1 = \langle P_1, P_2 \rangle$ 且 $K_2 = \langle Q_1, Q_2 \rangle$。

注意， K_1 和 K_2 是$\mathcal{A}_{d,\ h}[3]$极大各向同性子群。

对于乘积曲面，典范辛基由 Hesse 形式下椭圆曲线的规范化基诱导而来。下面的陈述将对此作出精确说明。

[3]配对的形式化定义见 [29, 第227]页，且已证明其与 Weil 配对一致，另见[26, 第 6 节1]。

推论 4.3。Le t $\mathcal{H}_d$ 和 $\mathcal{H}'_d$ 是 *Hesse* 形式的椭圆曲线，并考虑 *Segre* 嵌入 ng

$$\iota_S : \mathcal{H}_d \times \mathcal{H}_{d'} \to \mathcal{A}_{d,h} \subset \mathbb{P}^8$$

如引理 *3.13* 所示。进一步地，令$(P$、 $Q)$ 和$(P'$、 $Q')$ 分别为 $\mathcal{H}_d[3]$ 和 $\mathcal{H}_{d'}[3]$的典范基，参见公式 *2*。也就是说

$$P = (-1:1:0), Q = (0:-\omega^2:1) \in \mathcal{H}_d, \quad P' = (-1:1:0), Q' = (0:-\omega^2:1) \in \mathcal{H}_{d'}.$$

于是，$\mathcal{A}_{d、\ h}[3]$ 的典范基由$(P_1$、 P_2、 Q_1、 $Q_2)$ 给出，其中

$$P_1 = \iota_S(0, P'), \quad P_2 = \iota_S(P, 0), \quad Q_1 = \iota_S(0, Q'), \quad Q_2 = \iota_S(Q, 0).$$

4.1. 辛变换对 3-挠的作用。 对于给定的 $\mathcal{A}_{d,h}$中的一个 (3,3)-子群 K，可以考虑同源 $\phi : \mathcal{A}_{d,\ h} \to \mathcal{A}_{d',h'}$ ，其核为 K。在第 6 节中，我们将给出计算此类同源的显式公式，但这要求输入是特定形式的 (3,3)-子群：来自典范辛分解（定义 4.2）的群 K_2 。为了将任意 (3,3)-群 K 变换为正确形式的群，有必要应用适当的辛变换。为此，我们研究 3.3 中所述的辛变换在 3-挠上的作用。

引理 4.4。 设 $\mathcal{A}_{d,h}$ 是一个具有 *Hesse* 形式的主极化阿贝尔曲面，并考虑离散傅里叶变换 $M_{3,3} : \mathcal{A}_{d,\ h} \to \mathcal{A}_{d',h'}$。此外，设 (P_1, P_2, Q_1, Q_2) 和 (P'_1, P'_2, Q'_1, Q'_2)分别是 $\mathcal{A}_{d,h}$ 和 $\mathcal{A}_{d',h'}$ 的典范基。那么

$$M_{3,3}(P_1) = -Q'_1, \quad M_{3,3}(P_2) = -Q'_2, \quad M_{3,3}(Q_1) = P'_1, \quad M_{3,3}(Q_2) = P'_2.$$

特别地，$M_{3,3}(K_1) = K'_2$ 和 $M_{3,3}(K_2) = K'_1$。

证明。 这可通过直接计算验证。 □

引理 4.5。 设 $\mathcal{A}_{d,h}$ 是一个具有 *Hesse* 形式的主极化阿贝尔曲面，并考虑辛变换

$$C_{a_i} : \mathcal{A}_{d,h} \to C_{a_i}(\mathcal{A}_{d,h}), \quad for\ i = 0, 1, 2,$$

来自命题 *3.10*。那么这些变换分别将 $\mathcal{A}_{d,h}$ 的典范基映射为 $C_{a_i}(\mathcal{A}_{d,h})$ 的典范基

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

证明。 这可通过直接计算验证；另见 [15, 命题 1]。

□

5. Abelian surfaces in twisted Hesse form

本节简要介绍 Hesse 形式下阿贝尔曲面的扭曲。这些内容将在第 6.4 节主定理的证明中出现。虽然我们不详细探讨这一构造，但我们指出，它可以视为 [3]中扭曲 *Hesse* 形式 下椭圆曲线的二维类比。

定义 5.1. 设 $\mathcal{A}_{d,h}$ 是一个 Hesse 形式下的主极化阿贝尔曲面，且 $\lambda = (\lambda_0 : \cdots : \lambda_4) \in \mathbb{P}^4$。我们称 $C_\lambda(\mathcal{A}_{d,h})$ 为 $\mathcal{A}_{d,h}$ 经 λ 的扭曲。

注意，对 Hesse 形式中的曲面进行扭曲，不会影响 3-挠子群K_2的作用。为便于后文参考，我们在下一个引理中陈述这一观察结果。

引理 5.2. 设 A 是某个 *Hesse* 形式下的主极化阿贝尔曲面 $\mathcal{A}_{d,h}$的扭曲，即存在 $\lambda \in \mathbb{P}^4_{\bar{k}}$ 使得 $A = C_\lambda(\mathcal{A}_{d,h})$。

若基域 k 包含本原单位根 ω，则存在有理3-挠点$Q_1, Q_2 \in A[3]$，它们对 A 中各点的作用由下式给出

$$P + Q_1 = \tau_1(P), \quad P + Q_2 = \tau_2(P), \quad \textit{for all } P \in A$$

其中 τ_1, τ_2 如公式 *10* 所示。此外，乘以 -1 由下式给出

$$\begin{aligned} P &= (x_0 : x_1 : x_2 : x_3 : x_4 : x_5 : x_6 : x_7 : x_8) \\ &\downarrow \\ -P &= (x_0 : x_2 : x_1 : x_6 : x_8 : x_7 : x_3 : x_5 : x_4) \end{aligned}$$

对所有 $P \in A$均成立。

证明。考虑 $\mathcal{A}_{d,h}[3]$ 的典范基 (P_1, P_2, Q_1, Q_2)。映射 C_λ 通过缩放一个点的坐标给出。3-挠点 Q_1 和 Q_2 的作用也同样如此（尽管在后一种情况下，这种缩放相对于乘以 $[-1]$而言必然不对称）。因此，这些3-挠点的作用与映射 C_λ的应用可交换。这说明 $A = C_\lambda(\mathcal{A}_{d,h})$ 中的点 $Q_1 = C_\lambda(Q_1)$ 和 $Q_2 = C_\lambda(Q_2)$ 具有引理中所述的性质。

通过 C_λ 映射对乘以 $[-1]$ 映射的翻译是直接的。 □

我们注意到，一般而言，引理 5.2 中的阿贝尔曲面并不具有全有理 3-扭点。只有当扭曲由一个 k-有理元素 $\lambda \in \mathbb{P}^4$ 定义时，情况才是如此。

6. $(3,3)$-ISOGENIES

设$\mathcal{A}_{d,\,h}$ 是 Hesse 形式下的主极化阿贝尔曲面。我们考虑辛分解 $\mathcal{A}_{d,\,h}[3] = K_1 + K_2$（参见定义 4.2），其中的极大 3-各向同性群为 K_1，K_2。

记号 6.1。我们回顾点 $x = (x_0 : \cdots : x_8) \in \mathcal{A}_{d,\,h}$ 上下列基本运算所采用的记号。

– $\odot^3$：逐坐标立方，即 $\odot^3(x) = (x_0^3 : \cdots : x_8^3)$ – $M_{3,\,3}$：离散傅里叶变换（参见定义 3.11）。– C_λ，其中 $\lambda = (\lambda_0 : \cdots : \lambda_4)$：逐坐标缩放（参见记号 3.9）。

我们的主要结果表明，Hesse 形式阿贝尔曲面的 3-同源可以表示为记号 6.1 中基本运算的复合，并给出缩放向量 $\lambda \in \mathbb{P}^4$ 的显式公式，该公式用位于核上方的某些 9-挠点表示。

引理 6.2. 设 $\mathcal{A}_{d,h}$ 是 *Hesse* 形式的主极化阿贝尔曲面，并将 (P_1, P_2, Q_1, Q_2) 记为规范的 3-挠基。那么存在一个缩放向量 $\lambda \in \mathbb{P}^4$，使得

$$\phi : \mathcal{A}_{d,h} \to \mathcal{A}_{d',h'}, \quad P \mapsto C_\lambda \circ M \circ \odot^3(P)$$

定义一个 (3,3)-同源，其核为 $K_2 = \langle Q_1, Q_2 \rangle$，且陪域仍为 *Hesse* 形式。

证明。在整个证明过程中，我们使用以下记号表示计算 ϕ 时出现的中间阿贝尔曲面和映射：$\mathcal{A}_{d,\,h} \to \mathcal{A}_{d',h'}$。

$$\mathcal{A}_{d,h} \xrightarrow{\odot^3} A_1 \xrightarrow{M_{3,3}} A_2 \xrightarrow{C_\lambda} \mathcal{A}_{d',h'}.$$
$$\phi_1 : \mathcal{A}_{d,h} \to A_1, \qquad \phi_2 : \mathcal{A}_{d,h} \to A_2$$

First，我们注意到映射 $\phi_1 : \mathcal{A}_{d,h} \to A_1$ 是一个同源，其核由 b y

$$\ker(\odot^3) = \{(x_0 : \cdots : x_8) \mid (x_0^3 : \cdots : x_8^3) = (t_0^3 : \cdots : t_3^3)\}$$

这正是 $K_2 = \langle Q_1,\ Q_2 \rangle$。还需证明存在 $\lambda \in \mathbb{P}^4$，使得应用线性变换 $M_{3,\ 3}$ 和 C_λ 后，可将陪域 A_1 变为某个 Hesse 形式的阿贝尔曲面 $A_{d',\ h'}$，其中 $d',\ h'$。

我们首先研究群 $K_1 = \langle P_1,\ P_2 \rangle$ 在 ϕ_2 下的像，以及它在 A_2各点上的作用。3-扭点 $P_1,\ P_2$ 在 $\mathcal{A}_{d,\ h}$ 中的点上的作用对应于 A_2。对一般点及其分别经 P_1 和 P_2平移后的点进行符号计算，我们得到

$$P + \phi_2(P_1) = \tau_1^2(P), \quad P + \phi_2(P_2) = \tau_2^2(P) \quad \text{for all } P \in A_2,$$

其中 $\tau_1,\ \tau_2$ 是第4节中描述的线性变换。另请注意，$[-1]$ 映射在 A_2 上的乘法描述与其在 $\mathcal{A}_{d,\ h}$ 上的描述一致。这些正是引理 5.2 中所描述的扭曲阿贝尔曲面的性质。不过，仍需证明A_2 确实是一个扭曲阿贝尔曲面。

我们知道存在一个线性变换 $F : A_2 \to \mathcal{A}_{d',h'}$，其中 d', h' 不一定定义在基域上。用 (P_1', P_2', Q_1', Q_2') 表示 $\mathcal{A}_{d',h'}[3]$ 的典范辛基。不失一般性，我们可以假设 $(F \circ \phi_2)(P_1) = [-1]Q_1'$ 且 $(F \circ \phi_2)(P_2) = [-1]Q_2'$。由于 $[-1]\phi_2(P_1)$ 和 $[-1]\phi_2(P_2)$ 的作用已经是典范形式，这进一步意味着，对于所有 $a, b \in \{0, 1, 2\}$，$F(a\phi_2(P_1) + b\phi_2(P_2)) = -aQ_1' - bQ_2'$。换言之，$F$ 的应用与 τ_1 和 τ_2 的作用可交换。这意味着 F 可由一个对角矩阵表示。此外，F 需要与乘以 $[-1]$ 相容，因此 $F = C_\lambda$，其中 $\lambda \in \mathbb{P}^4$。

□

在下一个定理中，我们给出 λ 的显式公式。我们证明，借助定义域上的一个 9阶扭子群，可以推导出正确的缩放。首先，我们给出一个仅依赖于该 9阶扭子群的两个生成元 $R_1,\ R_2$ 的坐标的公式（定理 6.4）。在某些例外情况下，还必须将 $R_1 + R_2$ 和 $R_1 - R_2$ 作为额外输入（命题 6.9）。

定义 6.3。设 $\mathcal{A}_{d,\ h}$ 是 Hesse 形式的主极化阿贝尔曲面，且 $0_{\mathcal{A}_{d,\ h}} = (t_0 : \cdots : t_3)$ 是单位元，并定义以下数值

$$\begin{aligned}
\tilde{t}_0 &= t_0^3 + 2t_1^3 + 2t_2^3 + 2t_3^3 + 2t_4^3, \\
\tilde{t}_1 &= t_0^3 - t_1^3 + 2t_2^3 - t_3^3 - t_4^3, \\
\tilde{t}_2 &= t_0^3 + 2t_1^3 - t_2^3 - t_3^3 - t_4^3, \\
\tilde{t}_3 &= t_0^3 - t_1^3 - t_2^3 - t_3^3 + 2t_4^3, \\
\tilde{t}_4 &= t_0^3 - t_1^3 - t_2^3 + 2t_3^3 - t_4^3.
\end{aligned}$$

如果存在一个指标 $i > 0$ 满足 $\tilde{t}_i = 0$，我们称 $\mathcal{A}_{d,\ h}$ 为例外 。

请注意，根据定义，当 $\tilde{t}_0 = 0$ 时，$\mathcal{A}_{d,\ h}$ 不一定是例外的。不过，我们仍将这个值纳入定义，因为它之后会出现。

定理 6.4。设 $\mathcal{A}_{d,\ h}$ 是 *Hesse* 形式下的主极化阿贝尔曲面，并假设 $\mathcal{A}_{d,\ h}$ 不是例外情形。记 (P_1, P_2, Q_1, Q_2) 为规范的 3-扭点基，并设 $\langle R_1,\ R_2 \rangle \subset \mathcal{A}_{d,\ h}[9]$为一个极大各向同性子群，其中 $3 \cdot R_1 = Q_1$ 且 $3 \cdot R_2 = Q_2$。我们记

$$(x_{i,0} : \cdots : x_{i,8}) = M \circ \odot^3(R_i) \quad \textit{for } i = 1, 2.$$

并令

$$(\lambda_0 : \lambda_1) = (x_{1,1} : x_{1,0}),$$
$$(\lambda_0 : \lambda_2) = (x_{2,3} : x_{2,0}),$$
$$(\lambda_2 : \lambda_3) = (x_{1,4} : x_{1,6}),$$
$$(\lambda_3 : \lambda_4) = (x_{1,5} : x_{1,8}).$$

Then

$$\phi : \mathcal{A}_{d,h} \to \mathcal{A}_{d',h'}, \quad P \mapsto C_\lambda \circ M \circ \odot^3(P)$$

定义了一个核为 $K_2 = \langle Q_1, Q_2 \rangle$ 的(3,3)-同源，其陪域仍为 *Hesse* 形式。此外，$\mathcal{A}_{d',h'}[3]$ 的典范辛基为(P'_1, P'_2, Q'_1, Q'_2)，其中$P'_1 = \phi(R_1)$ $P'_2 = \phi(R_2)$ 且 $Q'_1 = [-1]\phi(P_1)$ $Q'_2 = [-1]\phi(P_2)$。

证明。 设 C_λ 如引理 6.2 的证明中所述，并回忆记号

$$\mathcal{A}_{d,h} \xrightarrow{\odot^3} A_1 \xrightarrow{M_{3,3}} A_2 \xrightarrow{C_\lambda} \mathcal{A}_{d',h'}.$$
$$\phi_1 \qquad \phi_2$$

We s说明 λ 的坐标由 9-挠点 R_1 和 R确定 $_{2\cdot}$

由于 $\langle R_1, R_2 \rangle$ 是位于同源 ϕ的核之上的一个极大各向同性子群，因此我们有

$$(\phi(R_1), \phi(R_2), \phi(P_1), \phi(P_2))$$

是 $A_2[3]$的一个辛基。此外，根据 Weil 配对的性质以及我们对 9-挠点 R_1, R_2 的选择，可得

$$e_3(\phi(R_1), \phi(P_1)) = e_3(P_1, Q_1)^{-1}, \quad e_3(\phi(R_2), \phi(P_2)) = e_3(P_2, Q_2)^{-1}.$$

我们将 (P'_1, P'_2, Q'_1, Q'_2) 记为 $\mathcal{A}_{d',h'}$ 的典范辛基。根据 C_λ 的构造（如引理 6.2 的证明所示），我们有 $\phi(P_1) = [-1]Q'_1$ 和 $\phi(P_2) = [-1]Q'_2$。这意味着

$$\phi(R_1) = P'_1 + aQ'_1 + bQ'_2,$$
$$\phi(R_2) = P'_2 + bQ'_1 + cQ'_2$$

对于某些 $a, b, c \in \{0, 1, 2\}$。由引理 4.5 可知，基变换

$$(\phi(R_1), \phi(R_2), \phi(P_1), \phi(P_2)) \mapsto (P'_1, P'_2, [-1]Q'_1, [-1]Q'_2)$$

仅仅是缩放，因此可以将其吸收到映射 C_λ 中，我们可以假设 $\phi(R_1) = P'_1$ 和 $\phi(R_2) = P'_2$。

令 $0_{\mathcal{A}_{d',h'}} = (t'_0 : \cdots : t'_3)$ 为陪域上的单位元。注意，根据同源的定义，对所有 i 都有 $t'_i = \lambda_i \cdot \tilde{t}_i$，其中 $\tilde{t}_i$ 如定义 6.3 所述。特别地，对所有 $i = 1, \ldots, 4$，都有 $t_i \neq 0$。

元素 P'_1 和 P'_2 的坐标是单位元坐标的置换。为了恢复缩放向量 λ，我们记

$$\phi_2(R_i) = (x_{i,0} : \cdots : x_{i,8}) \quad \text{for } i = 1, 2,$$

并使用等式 $C_\lambda(\phi_2(R_1)) = P'_1$，即

$$(\lambda_0 x_{1,0} : \lambda_1 x_{1,1} : \cdots : \lambda_3 x_{1,8}) = (t'_1 : t'_1 : t'_0 : t'_3 : t'_4 : t'_2 : t'_4 : t'_3 : t'_2)$$

以及 $C_\lambda(\phi_2(R_2)) = P'_2$，即

$$(\lambda_0 x_{2,0} : \lambda_1 x_{2,1} : \cdots : \lambda_3 x_{2,8}) = (t'_2 : t'_3 : t'_4 : t'_2 : t'_4 : t'_3 : t'_0 : t'_1 : t'_1).$$

由第一个等式，我们推得 $(\lambda_0 : \lambda_1) = (x_{1,1} : x_{1,0})$、$(\lambda_2 : \lambda_3) = (x_{1,4} : x_{1,6})$ 以及 $(\lambda_3 : \lambda_4) = (x_{1,5} : x_{1,8})$。由第二个等式，我们推得 $(\lambda_0 : \lambda_2) = (x_{2,3} : x_{2,0})$。□

6.1. 乘以3。 乘以 3 可以通过将定理 6.4 中的 3-同源与其对偶复合来计算。该定理中同源的对偶具有核 $K_2' = \langle Q_1', Q_2' \rangle$，其中 $K_1' + K_2' = \mathcal{A}_{d',h'}[3]$ 是陪域上 3-挠的典范分解。这意味着，定理 6。4 中的公式同样可以用于计算对偶同源。唯一微妙之处在于缩放向量的计算。直接应用该定理需要另外固定位于 P_1，P_2 之上的 9-挠点 S_1，S_2。下面我们将说明这是不必要的。

引理 6.5。 设 $\phi : \mathcal{A}_{d,h} \to \mathcal{A}_{d',h'}$ 是定理 *6.4* 中的 (3,3)-同源。那么，对偶同源 $\hat{\phi}: \mathcal{A}_{d',h'} \to \mathcal{A}_{d,h}$ 由下式给出

$$\hat{\phi} : P \mapsto C_{\lambda'} \circ M_{3,3} \circ \odot^3(P)$$

其中 $\lambda' = (t_0/a_0 : t_1/a_1 : t_2/a_2 : t_3/a_3 : t_4/a_4)$，其中

$$(a_0 : a_1 : a_1 : a_2 : a_3 : a_4 : a_2 : a_4 : a_3) = M_{3,3} \circ \odot^3 \circ C_\lambda \circ M_{3,3} \circ \odot^3(0_{\mathcal{A}_{d,h}}).$$

$\hat{}$证明。 首先注意到 $\phi(P_1, P_2) = \langle Q_1', Q_2' \rangle$，因此这是对偶同源 ϕ 的核。由定理 6.4 可知，存在一个向量 $\lambda' \in \mathbb{P}^4$，使得 $\hat{}\,\phi$ 由 $\hat{}\,\phi: P \mapsto C_{\lambda'} \circ M_{3,3} \circ \odot^3(P)$ 给出。为了计算 λ'，只需在单位元 $0_{\mathcal{A}_{d,h}}$ 处求乘以 3 的映射的值。这给出了条件

$$0_{\mathcal{A}_{d,h}} = C_{\lambda'} \circ M_{3,3} \circ \odot^3 \circ C_\lambda \circ M_{3,3} \circ \odot^3(0_{\mathcal{A}_{d,h}})$$

由此我们可以推出 λ' 的坐标。 □

6.2. 具有任意核的同源。 在定理 6.4 中，我们给出了一个显式公式，用于计算核为 $K_2 = \langle Q_1, Q_2 \rangle$ 的 (3,3)-同源，其中 (P_1, P_2, Q_1, Q_2) 是典范 3-扭点基。通过将该公式与适当的辛变换复合（见第 3.3 小节），可以用它来计算具有任意核的同源。这里，我们针对在应用中自然出现的 $\langle P_1 + aQ_1 + bQ_2, P_2 + bQ_1 + cQ_2 \rangle$ 形式的核，将这一点具体化。

引理 6.6. 设 $\mathcal{A}_{d,h}$ 是 *Hesse* 形式的主极化阿贝尔曲面，且 (P_1, P_2, Q_1, Q_2) 是 $\mathcal{A}_{d,h}[3]$的典范基。考虑极大各向同性子群 $K = \langle P_1 + aQ_1 + bQ_2, P_2 + bQ_1 + cQ_2 \rangle \subset \mathcal{A}_{d,h}[3]$。则变换 $C_{\lambda(a,b,c)} : \mathcal{A}_{d,h} \to \mathcal{A}_{d',h'}$ 满足

$$\lambda = (1 : \omega^{2a} : \omega^{2c} : \omega^{2a+b+2c} : \omega^{2a+2b+2c})$$

是辛变换，并且有

$$C_\lambda(K) = K_1',$$

其中 $K_1' + K_2' = \mathcal{A}_{d',h'}[3]$ 是典范分解。

证明。 首先注意，$C_\lambda = C_{a_0}^{-a} \circ C_{a_1}^{-b} \circ C_{a_2}^{-c}$满足 a_0, a_1, a_2，如命题 3.10 所述，因此 C_λ定义了一个辛变换。此外，由同一命题可知，变换 C_λ 由矩阵表示

$$\begin{pmatrix} 1 & 0 & -a & -b \\ 0 & 1 & -b & -c \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

分别相对于 $\mathcal{A}_{d,h}$ 和 $\mathcal{A}_{d',h'}$的典范基。 □

请注意，该定理要求输入一个形式为 K_2 的核，而引理 6.6 中的变换构造的是一个形式为 K_1 的核。只需应用离散傅里叶变换并乘以 $[-1]$ 即可实现这一点（参见引理 4.4 ）。整体过程总结于下一个推论。

推论 *6.7.* 设 $\mathcal{A}_{d,h}$ 是 *Hesse* 形式的主极化阿贝尔曲面，且 (P_1, P_2, Q_1, Q_2) 是 $\mathcal{A}_{d,h}[3]$ 的典范基。给定极大各向同性子群 $K = \langle P_1 + aQ_1 + bQ_2, P_2 + bQ_1 + cQ_2 \rangle \subset \mathcal{A}_{d,h}[3]$，以及满足 $3 \cdot R_1 = P_1 + aQ_1 + bQ_2$ 和 $3 \cdot R_2 = P_2 + bQ_1 + cQ_2$ 的 *9*-挠点 R_1, R_2。进一步设 C_λ 如引理 *6.6* 所述。那么，核为 K 的 *(3, 3)*-同源可利用定理 *6.4* 中的公式计算，输入为 $S_K(\mathcal{A}_{d,h})$ 和 $S_K(R_1)$ $S_K(R_2)$，其中 $S_K = [-1] \circ M_{3,3} \circ C_\lambda$。

6.3. **非一般同源**。 定理 6.4 假设同源 $\mathcal{A}_{d,h}$ 的定义域不是例外的（参见定义 6.3）。这一性质对于推导映射 C_λ 的具体标量至关重要。

在此，我们提供一种推导映射 C_λ 的标量的替代方法；除非陪域具有额外的 3 阶自同构，否则该方法在例外情形下也适用。除了 9-挠点 R_1 和 R_2 外，这些公式还需要输入 $R_1 + R_2$ 和 $R_1 - R_2$ 的坐标。

引理 6.8。 设 $\mathcal{A}_{d,h}$ 是一个例外的主极化阿贝尔曲面。令 $\tilde{t} = (\tilde{t}_0 : \cdots : \tilde{t}_4)$ 如定义 *6.3* 中所示。那么至少存在两个指标 $i \in \{0, \ldots, 4\}$，满足 $\tilde{t}_i \neq 0$。

证明。 设 $\mathcal{A}_{d,h} \to \mathcal{A}_{d',h'}$ 是引理 6.2 中的同源，并用 $t' = (t_0 : \cdots : t'_4)$ 表示陪域中单位元的坐标。于是，对每个 $i \in \{0, \ldots, 4\}$，都有 $t'_i = \lambda_i \cdot \tilde{t}_i$，其中 $\lambda = (\lambda_0 : \cdots : \lambda_4)$ 是定义 C_λ 的缩放向量。根据推论 3.7，至少存在两个指标 $i \neq j \in \{0, \ldots, 4\}$，使得 t'_i, t'_j 非零，因此结论成立。 □

命题 6.9. 设 $\mathcal{A}_{d,h}$ 是一个 *Hesse* 形式的主极化阿贝尔曲面。用 (P_1, P_2, Q_1, Q_2) 表示其规范 *3*-扭点基，并设 $\langle R_1, R_2 \rangle \subset \mathcal{A}_{d,h}[9]$ 是一个极大各向同性子群，其中 $3 \cdot R_1 = Q_1$, $3 \cdot R_2 = Q_2$ 且 $R_3 = R_1 + R_2$, $R_4 = R_1 - R_2$。

此外，令 $\tilde{t} = (\tilde{t}_0 : \cdots : \tilde{t}_4)$ 如定义 *6.3* 所示。若有两个指标 $i \neq j > 0$ 满足 $\tilde{t}_i, \tilde{t}_j \neq 0$，则存在唯一的 $\lambda \in \mathbb{P}^4$ 使得

$$\phi : \mathcal{A}_{d,h} \to \mathcal{A}_{d',h'}, \quad P \mapsto C_\lambda \circ M \circ \odot^3(P)$$

定义一个核为 $K_2 = \langle Q_1, Q_2 \rangle$ 的(3,3)-同源，而 $\mathcal{A}_{d',h'}[3]$的典范辛基为 (P'_1, P'_2, Q'_1, Q'_2)，其中 $P'_1 = \phi(R_1)$ $P'_2 = \phi(R_2)$ 且 $Q'_1 = [-1]\phi(P_1)$ $Q'_2 = [-1]\phi(P_2)$。此外， λ 的坐标可由 *9*-挠点 R_1, R_2, R_3, R_4读出。

证明。 我们采用定理 6.4 的证明中相同的记号。也就是说，我们将同源 $A \xrightarrow{\phi_2} A_2 \xrightarrow{C_\lambda} A_{d',h'}$ 分解，其中某个 $\lambda \in \mathbb{P}^4$。令 (P'_1, P'_2, Q'_1, Q'_2) 为 $\mathcal{A}_{d',h'}$ 的典范辛基。根据定理证明中的相同论证，我们可以假设 $\phi(R_1) = P'_1$ 且 $\phi(R_2) = P'_2$，因此 $\phi(R_3) = P'_1 + P'_2 =: P'_3$ 且 $\phi(R_4) = P'_1 - P'_2 =: P'_4$。

我们记

$$\phi_2(R_i) = (x_{i,0} : \cdots : x_{i,8}) \quad \text{for } i = 1, 2, 3, 4.$$

条件 $C_\lambda(\phi_2(R_i)) = P'_i$ 对 $i = 1$，2，3，4 给出了四个等式 .

$$\begin{aligned}
(\lambda_0 x_{1,0} : \lambda_1 x_{1,1} : \cdots : \lambda_3 x_{1,8}) &= (t'_1 : t'_1 : t'_0 : t'_3 : t'_4 : t'_2 : t'_4 : t'_3 : t'_2), \\
(\lambda_0 x_{2,0} : \lambda_1 x_{2,1} : \cdots : \lambda_3 x_{2,8}) &= (t'_2 : t'_3 : t'_4 : t'_2 : t'_4 : t'_3 : t'_0 : t'_1 : t'_1), \\
(\lambda_0 x_{3,0} : \lambda_1 x_{3,1} : \cdots : \lambda_3 x_{3,8}) &= (t'_3 : t'_4 : t'_2 : t'_4 : t'_3 : t'_2 : t'_1 : t'_1 : t'_0), \\
(\lambda_0 x_{4,0} : \lambda_1 x_{4,1} : \cdots : \lambda_3 x_{4,8}) &= (t'_4 : t'_3 : t'_2 : t'_1 : t'_1 : t'_0 : t'_3 : t'_4 : t'_2).
\end{aligned}$$

对于每个 i，条件 $\tilde{t}_i \neq 0$ 等价于 $t'_i \neq 0$ （参见引理 6.8 的证明）。现在，若对于某个 $i > 0$ 有 $t'_i \neq 0$，那么我们就能从上述每个等式中推导出关于 λ 坐标的一个关系。

具体而言，若 $t'_1 \neq 0$，则

$$(\lambda_0 : \lambda_1) = (x_{1,1} : x_{1,0}),\ (\lambda_4 : \lambda_3) = (x_{2,8} : x_{2,7}),\ (\lambda_2 : \lambda_4) = (x_{3,7} : x_{3,6}),\ (\lambda_2 : \lambda_3) = (x_{4,4} : x_{4,3}).$$

若 $t'_2 \neq 0$，则

$$(\lambda_4 : \lambda_3) = (x_{1,8} : x_{1,5}),\quad (\lambda_0 : \lambda_2) = (x_{2,3} : x_{2,0}),\quad (\lambda_1 : \lambda_4) = (x_{3,5} : x_{3,2}),\quad (\lambda_1 : \lambda_3) = (x_{4,8} : x_{4,2}).$$

如果 $t'_3 \neq 0$，则

$$(\lambda_2 : \lambda_4) = (x_{1,7} : x_{1,3}),\ (\lambda_1 : \lambda_4) = (x_{2,5} : x_{2,1}),\ (\lambda_0 : \lambda_3) = (x_{3,4} : x_{3,0}),\ (\lambda_1 : \lambda_2) = (x_{4,6} : x_{4,1}).$$

如果 $t'_4 \neq 0$，则

$$(\lambda_3 : \lambda_2) = (x_{1,6} : x_{1,4}),\ (\lambda_1 : \lambda_3) = (x_{2,4} : x_{2,2}),\ (\lambda_1 : \lambda_2) = (x_{3,3} : x_{3,1}),\ (\lambda_0 : \lambda_4) = (x_{4,7} : x_{4,0}).$$

请注意，在上述所有情况下，推导出的关系中都存在冗余。特别是，仅使用针对某个 $t'_i \neq 0$ 所得到的一组关系，不足以恢复坐标向量 $\lambda \in \mathbb{P}^4$。然而，将针对某个 t'_i，$t'_j \neq 0$ 所得到的两组关系结合起来，并满足 $i \neq j > 0$，就足以恢复 λ。□

注记 6.10。命题 6.9 中遗漏的唯一情况是：当 t 恰好有两个非零指标，其中一个是 $i = 0$ 时。在这种情况下，命题的表述确实不成立。陪域具有一个 3 阶的特殊自同构，因此，缩放 C_λ 不能由 9-挠点的像唯一确定。

为说明这一点，令 ${}^0\mathcal{A}_{d',h'} = (t'_0 : \cdots : t'_3)$ 为陪域的单位元。为简单起见，假设 $t'_0, t'_1 \neq 0$ 和 $t'_2 = t'_3 = t'_4 = 0$。其余情形的额外自同构也类似。

注意到 $t'^3_0 \neq -2t'^3_1, t'^3_1$，否则可以验证 $\mathcal{A}_{d',h'}$ 在 ${}^0\mathcal{A}_{d',h'}$ 处有一个奇点。关于 t'_i 的条件进而意味着

$$d' = (t'^3_0 + 2t'^3_1 : 3t'_0 t'^2_1 : 0 : 0 : 0), \quad h' = (0 : 0 : h'_2 : h'_3 : h'_4)$$

对于某个 h'_2, h'_3, h'_4。现在考虑映射 C_λ，其中 $\lambda = (1 : 1 : \omega : \omega : \omega)$（参见命题 3.10）。这定义了 $\mathcal{A}_{d,h}$ 的一个 3 阶自同构。

7. Example

为说明主定理及其应用，我们给出一个详细示例。在此示例中，我们计算乘积椭圆曲线之间的一个 (9,9)-同源。同源计算分解为一个 (3,3)-粘合和一个 $(3,3)$-分裂。该示例展示了计算 (3,3)-同源时可能遇到的最重要的细微之处。该示例不包含一般的 (3,3)-同源计算，但我们可以向读者保证，这是最直接的情形。更多详情和其他示例可在我们的 GitHub 仓库 [23]中找到。

7.1. 设定。我们在有限域 $\mathbb{F}_{p^2}$ 上工作，其中 $p = 269$。该域包含一个本原三次单位根 $\omega \in \mathbb{F}_{p^2}$。设 $E_1 : y^2 = x^3 + 1$ 和 $E_2 : y^2 = x^3 + 66x + 134$ 定义在 $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ 上。这两条曲线由一个 5-同源 $\phi : E_1 \to E_2$ 连接，其核为 $\ker(\phi) = \langle (8, 128) \rangle$。特别地，它们构成如下交换图：

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow{\scriptstyle [2]} & & \downarrow{\scriptstyle [2]} \\ E_1 & \xrightarrow{\phi} & E_2 \end{array}$$

由 Kani 引理　该图诱导出一个 (9,9)-同源 $\Phi\colon E_1\times E_2\to E_1\times E_2$，其核　　l

$$\ker(\Phi)=\{([2]P,\phi(P))\mid P\in E_1[9]\}.$$

这就是我们希望计算的同源。回想一下，我们用于计算 (3，3)-同源的算法需要以某些 9-挠点作为辅助输入。因此，我们先固定一个基

$$E_1[27]=\langle P,Q\rangle\quad\text{with } P=(252,71),\ Q=(7\omega,13\omega+141),$$

并固定以下记号

$$P_1=[2]\cdot P,\ Q_1=[2]\cdot Q\in E_1[27],\quad P_2=\phi(Q),\ Q_2=\phi(P)\in E_2[27].$$

特别地，在此记号下，$\ker(\Phi)=[3]\cdot\langle(P_1,\ Q_2),\ (Q_1,\ P_2)\rangle$。

7.2. **变换为 Hesse 形式**。要应用我们的算法，必须将输入椭圆曲线变换为 Hesse 形式。此变换是线性的，由指定 3-扭元素的像来确定。具体而言，这些变换如下

$$f_1:E_1\xrightarrow{\begin{pmatrix}1&0&231\omega\\1&19\omega&19\omega\\1&250\omega&19\omega\end{pmatrix}}\mathcal{H}_{(-2:1)},\quad f_2:E_2\xrightarrow{\begin{pmatrix}1&0&179\\-9\omega^2&9-9\omega&49\omega^2\\-9\omega^2&-9-9\omega&49\omega^2\end{pmatrix}}\mathcal{H}_{(-18\omega^2:1)}.$$

选择这些变换是为了使

$$f_1([9]P_1)=(-1:1:0),\ f_1([9]Q_1)=(0:-\omega^2:1),$$
$$f_2([9]P_2)=(-1:1:0),\ f_2([9]Q_2)=(0:-\omega^2:1).$$

在我们使用 SageMath 的实现中，调用 `H1 = EllipticCurveHessianForm(E1, basis=[9*P1,9*Q1])` 即可构造 Hesse 形式的椭圆曲线，其中 `E1` 是 Weierstrass 形式的椭圆曲线，`P1`、`Q1` 是上文定义的点 P_1，Q_1。描述相应变换的矩阵可通过 `H1.trafo` 访问。类似地，第二条 Hesse 形式的椭圆曲线通过 `H2 = EllipticCurveHessianForm(E2, basis=[9*P2,9*Q2])` 构造。

如第3.4小节所述，两条 Hesse 形式椭圆曲线的 Segre 嵌入的像为我们提供了一个 Hesse 形式的阿贝尔曲面。应用引理 3.13，我们得到

$$\iota_S\left(\mathcal{H}_{(18\omega^2:1)}\times\mathcal{H}_{(-2:1)}\right)=\mathcal{A}_{d,h},\quad\text{with } d=(-36\omega^2:18\omega^2:-2:1:1),\ h=(0:0:0:-1:1).$$

在实现中，曲面 $\mathcal{A}_{d,\ h}$ 通过 `A0 = AbelianSurfaceHessianForm([H2,H1])` 构造。

7.3. **总体策略**。以以上信息为输入，现在可以使用函数 compute isogeny chain 计算同源 Φ。该函数执行的中间计算可概括如下：

$$\begin{array}{ccccccc}\mathcal{H}_{(18\omega^2:1)}\times\mathcal{H}_{(-2:1)}&\xrightarrow{\iota_S}&\mathcal{A}_{d,h}&&\mathcal{A}_{d',h'}&&\mathcal{A}_{d'',h''}\\&&\downarrow{\scriptstyle S_K}&\overset{\Phi_1}{\nearrow}&\downarrow{\scriptstyle S_{K'}}&\overset{\Phi_2}{\nearrow}&\downarrow{\scriptstyle S_{K''}}\\&&\mathcal{A}_{\tilde{d},\tilde{h}}&&\mathcal{A}_{\tilde{d}',\tilde{h}'}&&\mathcal{A}_{\tilde{d}'',\tilde{h}''}\xrightarrow{\iota_S^{-1}}\mathcal{H}_{(-2:1)}\times\mathcal{H}_{(18\omega^2:1)}.\end{array}$$

映射 S_K，S'_K，S''_K是辛变换，而 Φ_1，Φ_2是利用定理 6.4 中的公式计算得到的 (3，3)-同源。下面，我们将更详细地介绍计算过程。需要指出的是，在该框架中计算一般的同源链时，所有中间的辛变换都具有 $[-1]\circ M_{3,\ 3}$ 的形式（此处 $S_{K'}$ 便是如此）；而在第一步和最后一步中，辛变换则取决于具体设置（此处 S_K 和 $S_{K''}$便是如此）。

7.4. **粘合同源**。根据推论 4.3，$\mathcal{A}_{d,\ h}[3]$ 的典范基由 b 给出 y

$$\left(P_1^0, P_2^0, Q_1^0, Q_2^0\right) = \left([9]\iota_S(0,P_1),\ [9]\iota_S(P_2,0),\ [9]\iota_S(0,Q_1),\ [9]\iota_S(Q_2,0)\right),$$

且 $\ker(\Phi)[3] = \langle Q_1^0 + P_2^0,\ Q_2^0 + P_1^0\rangle$。为了应用定理 6.4，我们需要应用一个辛变换，将 $K := \ker(\Phi)[3]$变换为 K_2 形式的群。如推论 6.7 所述，这可以通过以下变换实现

$$S_K := [-1] \circ M_{3,3} \circ \mathcal{C}_\lambda, \quad \text{with } \lambda = (1:1:1:\omega:\omega^2).$$

请注意，λ 的值可由引理 6.6 推得。具体而言，定义 $S_K : \mathcal{A}_{d,\ h} \to \mathcal{A}_{\tilde{d},\ \tilde{h}}$ 的陪域曲面的系数为

$$\tilde{d} = (263:54\omega+51:3:57\omega+57:51\omega+54),\ \tilde{h} = (-\omega:\omega:\omega:\omega^2:1).$$

按照等式 6 的记号，单位元由向量 $t = (-2\omega:\ \omega:\ \omega:\ \omega^2:1)$定义，并且可以验证 $\mathcal{A}_{\tilde{d},\ \tilde{h}}$ 并非例外。现在我们可以应用主定理计算 (3，3)-同源

$$\Phi_1 : \mathcal{A}_{\tilde{d},\tilde{h}} \to \mathcal{A}_{d',h'}, \quad P \mapsto C_{\lambda'} \circ M \circ \odot^3(P)$$

with

$$\lambda' = (88:170:181\omega+5:88\omega+93:1),$$

and

$$d' = (107:144:169\omega+200:100\omega+31:1), \quad h' = (104:76:203\omega+167:66\omega+233:1).$$

可以验证，h' 是 Burkhardt 四次曲面上的一个非奇异点。这意味着 $\mathcal{A}_{d',\ h'}$ 是不可约的，并且 (3，3)-同源 Φ_1 确实是一个粘合。

7.5. **分裂同源**。根据定理 6.4，我们有 $K' := \Phi_1(S_K(\ker(\Phi))[3] = K_1'$，其中$\mathcal{A}_{d',\ h'} = K_1' + K_2'$是 3-挠的辛分解。通过应用离散傅里叶变换（引理 4.4），可将其转换为形式为 K_2 的核。此外，为了将生成元转换为正确的形式，还需要乘以 $[-1]$。记 $S_{K'} = [-1] \circ M_{3,\ 3}$和 $\mathcal{A}_{\tilde{d}',\ \tilde{h}'}$ 为 $S_{K'}$的陪域。然后，可以再次应用定理 6.4 来计算分裂同源:

$$\Phi_2 : \mathcal{A}_{\tilde{d}',\tilde{h}'} \to \mathcal{A}_{d'',h''}, \quad P \mapsto C_{\lambda'} \circ M \circ \odot^3(P),$$

其中

$$\lambda'' = (144\omega:250\omega:126\omega+260:143\omega+134:1)$$

and

$$d'' = (99\omega+99:85\omega+85:100\omega+184:169\omega+84:1), \quad h'' = (-\omega:\omega:\omega:\omega^2:1).$$

正如预期，h'' 是 Burkhardt 四次曲面的一个奇点，因此 Φ_2 确实是一个 (3，3)-分裂。为了恢复这两条椭圆曲线，需要再应用一次辛变换，以得到一个带有乘积极化（定义 3.14）的模型。在我们的实现中，这一变换通过乘积结构变换计算得出。由此得到

$$S_{K''} : \mathcal{A}_{d'',h''} \to \mathcal{A}_{\tilde{d}'',\tilde{h}''}, \quad P \mapsto C_{(1:1:1:\omega:\omega^2)} \circ M_{3,3} \circ C_{(1:1:1:\omega:\omega^2)}(P)$$

with

$$\tilde{d}'' = (-36\omega^2:-2:18\omega^2:1:1), \quad \tilde{h}'' = (0:0:0:-1:1).$$

特别地，

$$\mathcal{A}_{\tilde{d}'',\tilde{h}''} = \iota_S\left(\mathcal{H}_{(-2:1)} \times \mathcal{H}_{(18\omega^2:1)}\right).$$

请注意，根据本示例中的构造，同源 Φ 的陪域已经很明确。

8. Generalization of the approach

我们新的同源公式的主要依据是引理 6.2，该引理指出，对于某个适当的缩放向量 λ，映射

$$\phi : \mathcal{A}_{d,h} \to \mathcal{A}_{d',h'}, \quad P \mapsto C_\lambda \circ M \circ \odot^3(P)$$

定义一个核为 K_2 的 (3,3)-同源。自然会让人想问，这种方法能否推广到由 3 级对称 theta 结构定义的高维阿贝尔簇，以及能否进一步推广到其他级数。

8.1. 提升维数。 为回答第一个问题，设 A 是一个维数为 g 的主极化阿贝尔簇。考虑一个线丛 L，它确定了 A 的主极化。根据 Lefschetz 定理，$L^{\otimes 3}$ 非常丰；它定义了一个嵌入 $A \hookrightarrow \mathbb{P}^{3^g-1}$，并且可以选取一个嵌入，使三阶扭点群的作用得到标准化。类比我们在维数 2 时的定义，我们称 A 为 *Hesse* 形式。这样的嵌入由一个对称 theta 结构诱导，其坐标函数对应于 3 级 theta 函数。下文将说明引理 6.2 证明中的步骤如何推广到任意维数。

与定义 4.2 类似，可以为

$$(P_1, \dots, P_g, Q_1, \dots, Q_g)$$

$A[3]$ 定义一个典范辛基，使得点 P_i 的作用由 3 阶置换给出，而 Q_i 的作用则由三次单位根的缩放给出（参见 [28]）。由此可知，在这一更一般的设定下，逐坐标立方映射也定义了一个同源 $\odot^3 : A \to A_1$，其核为$K_2 = \langle Q_1, \dots, Q_g \rangle$。

离散傅 里叶变换可相对于三次单位根 ω 归纳定义 :

$$M_{3^g} = \begin{pmatrix} M_{3^{g-1}} & M_{3^{g-1}} & M_{3^{g-1}} \\ M_{3^{g-1}} & \omega M_{3^{g-1}} & \omega^2 M_{3^{g-1}} \\ M_{3^{g-1}} & \omega^2 M_{3^{g-1}} & \omega M_{3^{g-1}} \end{pmatrix} \quad \text{for } g > 1.$$

对基的生成元重新排序（$P_1, \dots, P_g, Q_1, \dots, Q_g$）后，可以验证$M_{3^g} \cdot P_i = -Q_i$ 和 $M_{3^g} \cdot Q_i = P_i$（如引理 4.4 中所示）。特别地，我们看到，在映射的陪域 A_2 上

$$\phi_2 = (M_{3^g} \circ \odot^3) : A \to A_2,$$

点 $\phi_2(P_i)$ 的作用处于标准形式。用第 5 节的术语来说，可以称 A_2 处于扭曲 Hesse 形式。特别地，存在一个缩放 C_λ，使得 $\lambda \in \mathbb{P}^{(3^g-1)/2}$ 能够将 A_2 变换为 Hesse 形式。

我们预期，除某些边界情形外，也可以从同源核上方给定的极大 9-各向同性子群 $\langle R_1, \dots, R_g \rangle$ 中确定缩放向量 λ。不过，我们没有详细推导一般公式。

注 8.1. 在准备这篇稿件期间，我们进一步将这一想法具体应用于椭圆曲线。Hesse 形式椭圆曲线的同源公式早已广为人知，我们验证了新方法得出的结果与之相同。有趣的是，对 3-同源的这种诠释使我们发现了一些新的三倍公式，它们定义在扭曲 Hesse 形式椭圆曲线的 Kummer 直线上。我们在一次密码学会议上展示了这些结果，目前该文章正提交至这次会议的会议论文集 [12]。

8.2. 不同的层级 ℓ。 我们指出，我们的思路也可能导出适用于不同层级的新同源公式 ℓ。事实上，正如引言中所述，我们的工作灵感源自 2级 theta 设置，其中已知特别高效的 2-同源公式。在这种情形下，同源公式源自 theta 函数的经典倍增公式，并且适用于任意维数 g。

注 8.2。 为了将引理 6.2 推广到任意层级 $\ell > 2$，我们引入以下记号：

– $\odot^\ell$：指数为 ℓ 的逐坐标乘方，即 $\odot^\ell(x) = (x_0^\ell : \cdots : x_{3^g-1}^\ell)$。– M_{ℓ^g}：关于 ℓ 次本原单位根且维数为 g 的离散傅里叶变换。– C_λ with $\lambda \in \mathbb{P}^{(\ell^g-1)/2}$：逐坐标缩放，并且关于乘以 $[-1]$ 对称。

现在令 A 为一个主极化阿贝尔簇，令 $\ell > 2$ 为一个素数。进一步，令 $\Theta_\ell : A \to \mathbb{P}^{\ell^g-1}$ 为由一个 ℓ 级对称 theta 结构诱导的嵌入。我们断言，存在一个缩放向量 $\lambda \in \mathbb{P}^{(\ell^g-1)/2}$，使得映射

$$\phi = (C_\lambda \circ M_{\ell^g} \circ \odot^\ell) : \Theta_\ell(A) \to A'$$

定义了一个具有极大 ℓ-各向同性核的同源；并且陪域 A' 也由一个 Θ'_ℓ 的 ℓ 级对称 theta 结构诱导。我们简要说明其思路。

首先，固定 $A[\ell]$ 的一个典范辛基 $(P_1, \ldots, P_g, Q_1, \ldots, Q_g)$。与 Hesse 形式下阿贝尔簇的设定类似，点 P_i 的加法通过某些阶为 ℓ 的置换作用；而点 Q_i 的加法则通过 ℓ 次单位根进行缩放。特别地，映射 $\odot^\ell$ 定义了一个核为 $K_2 = \langle Q_1, \ldots, Q_g \rangle$ 的同源。并且如同引理 6.2 的证明，必然存在一个线性变换，使陪域处于正确的形式。为了显式描述这一变换，关键在于注意到，点 $P_1, \ldots, P_g$ 的像在 ϕ_2 的陪域的点上通过 ℓ 次单位根进行缩放，其中 $\phi_2 := M_{\ell^g} \circ \odot^\ell$。

注 8.3。 注意，表示阿贝尔簇上一个点所需的坐标数量会随层级 ℓ 增长。值得探究上述方法是否仍能导出效率更高的同源公式。即使在椭圆曲线的情形下，这也可能为同源带来新的见解。接下来最容易考虑的情形，是将椭圆曲线定义为$\mathbb{P}^3$中两个二次曲面的交。适当选择坐标后，这对应于一个 4 级 theta 结构（参见 [28, §5，情形 (c)]）。因此，这种模型应适用于 4-同源的计算。

References

[1] W. Barth. 三级阿贝尔曲面的二次方程。,,, 第 – 页。https://doi.org/ 。/ 9783110889437.1.[2] Andrea Basso、Pierrick Dartois、Luca De Feo、Antonin Leroux、Luciano Maino、Giacomo Pope、Damien Robert 和 Benjamin Wesolowski。SQIsign2D-West——更快、更小、更安全。载于 *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security Kolkata India December 9-13 2024 Proceedings Part III* 15486 *Lecture Notes in Computer Science* ,,,,,, 第 卷，页码 –。 339 370 2024 10 1007 978 981 96 0891 1_11 施普林格，。https://doi.org/ 。/ - - - -。[3] Daniel J. Bernstein、Chitchanok Chuengsatiansup、David Kohel 和 Tanja Lange。扭曲 Hessian 曲线。载于*Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America Guadalajara Mexico August 23-26 2015 Proceedings* 9230 *Lecture Notes in Computer Science* ,,,,,, 第 卷，页码 –。施普林格，。https://doi.org/ 。/ - - - -。 269 294 2015 10 1007 978 3 319 22174 8_15 [4] Nils Bruin、E. Victor Flynn 和 Damiano Testa。通过 (3,3)-同源对亏格 2 曲线的雅可比簇进行下降。, ( ): –。http://eudml.org/doc/ 。[5] Nils Bruin 和 Brett Nasserden。Burkhardt 四次三维簇的算术方面。*Acta Arithmetica* 165 3 201 223, 2014 279018 *Journal of the London Mathematical Society* 98 3 536 556, 2018 10 1112 12153 , ( ): –。 https://doi.org/ 。/jlms. 。[6] Wouter Castryck 和 Thomas Decru。针对 SIDH 的高效密钥恢复攻击。载于 *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques Lyon France April 23-27 2023 Proceedings Part V* 14008 *Lecture Notes in Computer Science* ,,,,,, 第 卷，页码 –。 423 447 2023 10 1007 978 3 031 30589 4_15 施普林格，。https://doi.org/ 。/ - - - -。[7] Arthur B. Coble。点集及相关 Cremona 群（第三部分）。*Transactions of the American Mathematical Society* 18 3 331 372, 1917 10 2307 1988959 , ( ): –。 https://doi.org/ 。/ 。

[8] Maria Corte-Real Santos、Craig Costello 和 Benjamin Smith。快速库默尔曲面上的高效 (3, 3)-同源。*Research in Number Theory*, 11(1):25, 2025年。https://doi.org/10.1007/s40993-024-00600-y。[9] Romain Cosset 和 Damien Robert。在亏格 2 曲线的雅可比簇上以多项式时间计算 (ℓ,ℓ)-同源。*Mathematics of Computation*, 84(294):1953–1975, 2015。https://doi.org/10.1090/S0025-5718-2014-02899-8。[10] Pierrick Dartois。维数为 的 2 4 *Journal of* -同源快速计算及 *Algebra* 683 449 514, 2025 10 1016 2025 06 033 密码学应用。, :–。https://doi.org/ 。/j.jalgebra. 。 。 。[11] Pierrick Dartois、Luciano Maino、Giacomo Pope 和 Damien Robert。theta 模型中的 (2, 2)-同源算法方法及其在基于同源的密码学中的应用。载于 *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security,Kolkata, India, December 9-13*, 2024年, *Proceedings, Part III*, 第 15486 卷 *Lecture Notes in Computer Science*, 第 304–338 页。施普林格, 2024年。https://doi.org/10.1007/978-981-96-0891-1_10。[12] Thomas Decru 和 Sabrina Kunzweiler。通过同源分解在 Hessian 曲线上进行三倍运算。已投稿至 CECC 2025 会议论文集。[13] Thomas Decru 和 Sabrina Kunzweiler。$(3^n, 3^n)$-同源的高效计算。载于 *Progress in Cryptology- AFRICACRYPT 2023 - 14th International Conference on Cryptology in Africa, Sousse, Tunisia, July 19-21*, 2023 14064 53 78 2023 , *Proceedings*, 第 *Lecture Notes in Computer Science* 卷, 第 – 页。施普林格, 。https: //doi.org/10.1007/978-3-031-37679-5_3。[14] Max Duparc 和 Tako Boris Fouotsa。SQIPrime：一种 SQISignHD 的二维变体，采用非光滑挑战同源。载于 *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13*, 2024年, *Proceedings, Part III*, 第 15486 卷 *Lecture Notes in Computer Science*, 第 396–429 页。施普林格，2024年。https://doi.org/10.1007/ 978-981-96-0891-1_13。[15] Eberhard Freitag 和 Riccardo Salvati Manni。Burkhardt 群与模形式。 *Transformation groups*, 9 1 25 10 1007 00031 004 7002 6 ( ): –45, 2004。https://doi.org/ 。/s - - -。[16] Eberhard Freitag 和 Riccardo Salvati Manni。Burkhardt 群与模形式 2 *Transformation* 。, ( ): –。 *groups* 9 3 237 256, 2004 10 1007 00031 004 7012 4 https://doi.org/ 。/s - - -。[17] Pierrick Gaudry。基于 theta 函数的快速亏格 2 算术。 *Journal of Mathematical Cryptology*, 1(3):243–265, 2007。https://doi.org/10.1515/JMC.2007.012。[18] Laurent Gruson 和 Steven V. Sam。九维空间上的交错三线性形式及 (3, 3)-极化阿贝尔曲面的退化。 *Proceedings of the London Mathematical Society*, 110(3):755–785, 2015。https: // doi.org/10.1112/plms/pdu050。[19] Keiichi Gunji。具有三级结构的通用阿贝尔曲面的定义方程。 *manuscripta mathematica* 119 61 96, 2006 10 1007 00229 005 0606 , : –。 https://doi.org/ 。/s - - -x。[20] Everett W. Howe。具有大阶挠点的亏格- 2 *Bulletin of the London Mathematical* 雅可比簇。, ( ): –。 *Society* 47 1 127 135, 2015 10 1112 107 https://doi.org/ 。/blms/bdu 。[21] Bruce Hunt。Burkhardt 四次曲面。 *The Geometry of some special Arithmetic Quotients*, 第 168–221 页, 1996。https://doi.org/10.1007/BFb0094405。[22] Ernst Kani。具有椭圆微分的亏格二曲线的数量。 *Journal für die reine und angewandte Mathematik* 485 93 122, 1997 183547 , : –。 http://eudml.org/doc/ 。[23] Sabrina Kunzweiler。以 theta 坐标计算 (3,3)-同源。https://github.com/sabrinakunzweiler/level-3-arithmetic。访问日期：2025-12-11。[24] Sabrina Kunzweiler、Luciano Maino、Tomoki Moriya、Christophe Petit、Giacomo Pope、Damien Robert、Miha Stopar 和 Yan Bo Ti。维数 和 中的根式 2 1, 2 3 *IACR* -同源与密码学哈 *International Conference on Public-Key Cryptography – PKC 2025* 15676 希函数。载于 , 第 *Lecture Notes in Computer Science* 265 299 2025 10 1007 978 3 031 91826 1_9 卷，页码 –。施普林格，。https://doi.org/ 。/ - - - -。[25] H. Lange 和 Ch. Birkenhake。三次 theta 关系。 *Journal für die reine und angewandte Mathematik*, 407:167–177, 1990。http://eudml.org/doc/153234。[26] David Lubicz 和 Damien Robert。阿贝尔簇之间同源的计算。 *Compositio Mathematica*, 148 5 1483 1515, 2012 10 1112 0010437 12000243 ( ): –。 https://doi.org/ 。/S X 。[27] David Lubicz 和 Damien Robert。快速层级变换及其在同源中的应用。 *Research in Number Theory*, 9 1 10 1007 40993 022 00407 9 ( ):7, 2023年。https://doi.org/ 。/s - - -。[28] David Bryant Mumford。关于定义阿贝尔簇的方程。I。 *Inventiones mathematicae*, 1966。https: //doi.org/10.1007/BF01389737。[29] David Bryant Mumford。 *Abelian Varieties*。牛津大学出版社，牛津，1970年。[30] Kohei Nakagawa、Hiroshi Onuki、Wouter Castryck、Mingjie Chen、Riccardo Invernizzi、Gioella Lorenzon 和 Frederik Vercauteren。SQIsign2D-East：一种采用二维同源的新型签名方案。载于 *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology*

and Information Security Kolkata India December 9-13 2024 Proceedings Part III 15486 *Lecture ,,,,,,* 第 卷, *Notes in Computer Science* 272 303 2024 10 1007 978 981 96 0891 1_9
页码 – 。施普林格，。https://doi.org/ 。/ - - - - 。[31] Damien Robert. 阿贝尔簇理论及其模空间。
https://www.math.u-bordeaux.fr/ ~damienrobert/pro/publications/books/avtheory.pdf，2021年。[32] Damien Robert. 关于在高维中优化 2^n-同源的札记。https://www.math.u-bordeaux.fr/ ~da
mienrobert/pro/publications/notes/2023-06-optimising_isogenies.pdf，2023年。[33] Damien Robert 和 Nicolas Sarkis。计算 Kummer 直线之间的
2 *IACR Communications in* -同源。， （），。
Cryptology 1 1 2024 10 62056 69 1
https://doi.org/ 。/abvua p 。[34] SQIsign团队。SQIsign：算法规范与配套文档，2.0.1版。https: //
sqisign.org/spec/sqisign-20250707.pdf。访问日期：2025年12月12日。[35] Sage开发者。 *SageMath,*
the Sage Mathematics Software System (Version 10.5)，2025年。https://www. sagemath.org。[36] Gerard Van Der Geer。关于三级阿贝尔概形的札记。 *Mathematische Annalen*，278(1):401–408，1987年。http://eudml.org/doc/164298。[37] Ryo Yoshizumi、Hiroshi Onuki、Ryo Ohashi、Momonari Kudo 和 Koji Nuida。用于计算任意奇数 上 Kummer 曲面 (
ℓ ℓ ℓ *International Conference on Post-* ,)-同源的高效基于
Quantum Cryptography 3 37 2025 10 1007 978 3 031 86602 9_1
theta函数的算法。载于 ，页码 – 。施普林格，。https://doi.org/ 。/ - - - - 。