arXiv:2601.22337v1 [math.CO] 29 Jan 2026

# 四元数完美序列与哈达玛矩阵

Aidan Bennett* Curtis Bright† Paul Colinot‡
Ashwin Nayak§

2026年1月29日

**摘要**

如果一个有限数值序列在非平凡循环移位后具有零周期自相关，则称其为完美序列。在这项工作中，我们研究四元数完美序列，它们与 Williamson 构造四元数型 Hadamard 矩阵时产生的二进制序列一一对应。利用这种对应关系，我们设计了一种枚举算法，其速度显著快于以往使用的算法，且不要求序列对称。我们实现了该算法，并用它枚举了阶数不超过 21 的所有循环且可能非对称的 Williamson型矩阵；此前，穷举枚举的最大阶数为 13。我们

2020 数学主题分类。主要分类号：05B20；次要分类号：94A55、15B33关键词与短语。
完美序列、哈达玛矩阵、四元数。

*温莎大学计算机科学学院。加拿大温莎市日落大道401号。电子邮箱：bennet43@uwindsor.ca。研究经费由加拿大自然科学与工程研究委员会本科生研究助理项目提供。

†滑铁卢大学计算机科学学院。加拿大滑铁卢市 University Ave. W. 200 号。电子邮件：cbright@uwaterloo.ca，个人网页：www.curtisbright.com。研究部分由加拿大自然科学与工程研究委员会发现基金资助。通讯作者。

‡格勒诺布尔-阿尔卑斯大学，G-SCOP，法国国家科学研究中心。法国圣马丹代埃尔市 Rue de la Passerelle 681 号。电子邮件：paul.colinot@grenoble-inp.org。研究工作在 Mitacs Globalink研究实习项目框架下开展。§滑铁卢大学组合学与优化系及量子计算研究所。加拿大滑铁卢市 University Ave. W. 200 号。电子邮件：academic@ashwinnayak.info。研究部分由加拿大自然科学与工程研究委员会发现基金资助。

证明了当四元数型 Hadamard 矩阵的块为循环矩阵时，这些块必然两两相容。这大幅增强了我们算法的筛选能力：在 20 阶时，需要考虑的块配对数量减少了 25,000 多倍。我们利用这些结果构造了在量子通信中具有应用价值的四元数 Hadamard 矩阵，并证明它们与通过其他方法构造的矩阵不等价。我们还从解析角度研究了四元数 Hadamard 矩阵的性质，并展示了刻画具有固定元素模式的四元数 Hadamard 矩阵的可行性。这些结果表明，此类矩阵具有更丰富的性质，也说明在阶数足够大时，四元数 Hadamard 矩阵可能为数众多。

# 1 引言

如果一个有限序列在经过非平凡循环移位后与自身没有相关性，则称其为完美序列。矩阵 $H \in \{\pm 1\}^{n\times n}$ 是（实）*Hadamard* 矩阵，当且仅当它满足 $HH^\top = n\mathbf{I}_n$；如果矩阵的每一行都是上一行向右循环移位一位得到的，则称其为循环矩阵。当其元素取自 $\pm 1$字母表时，完美序列等价于循环 Hadamard 矩阵 [35]。例如，

$$\begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix}$$

是一个循环 Hadamard 矩阵，等价于定义其首行的完美序列 $[1,-1,-1,-1]$。

长期以来，人们一直在研究完美序列的实际应用及其优雅的数学性质。然而，在所有非平凡循环移位下与自身没有相关性这一条件，对于大多数字母表而言在实践中很难实现。事实上，对于二进制 $\{\pm 1\}$ 字母表，目前已知的最长完美序列是上文给出的长度为 4 的序列，并且有人猜想，除平凡情况外，这就是唯一一个在同构意义下的完美二进制序列 [33]。

通过增大字母表的大小，可以找到任意长的完美序列。最早的完美序列构造之一由 R. C. Heimiller 于 1961 年提出 [22]。他给出了一种构造完美序列的方法，其长度为 $p^2$

且其字母表由 $p$次单位根组成，其中 $p$ 为素数。事实上，R. L. Frank 在20世纪50年代于斯佩里陀螺仪公司担任飞机工程师期间，就发现了相同的构造方法，而且不要求长度为素数 [17]。例如，Frank 的构造可在四元（复数）字母表 $\{\pm 1, \pm \mathbf{i}\}$上生成长度为 $4^2 = 16$ 的完美序列。

在 $\{\pm 1, \pm \mathbf{i}\}$ 上的完美序列等价于循环复阿达玛矩阵；若矩阵 $H \in \mathbb{C}^{n\times n}$ 的所有元素的模均为 1，且 $HH^* = n\mathbf{I}_n$，其中 $H^*$ 表示 $H$ 的共轭转置，则称其为复*Hadamard*矩阵 。例如，Frank 的构造在长度为 4 时生成一个循环 $16 \times 16$ 复 Hadamard 矩阵，并且有人猜想这就是最大的循环复阿达玛矩阵 [38]。

尽管任意大的循环 Hadamard 矩阵可能并不存在，但任意大的非循环 Hadamard 矩阵确实存在。例如，1867年，西尔维斯特 [36] 构造了阶为 $2^k$的 Hadamard 矩阵，适用于所有 $k \geq 0$。1893年，阿达玛 [20] 证明，如果存在一个阶为 $n > 2$ 的 Hadamard 矩阵，那么 $n$ 必须能被 4 整除。阿达玛猜想认为，这一必要条件也是充分条件。计算证据支持这样的猜想：所有为 4 的倍数的阶都存在 Hadamard 矩阵。尽管这一猜想尚未得到证明，人们已经发现了许多 Hadamard 矩阵的无限类。

## 1.1 四元数型哈达玛矩阵

Williamson [43] 于1944年提出了一种构造哈达玛矩阵的重要方法。他考虑了如下形式的哈达玛矩阵

$$\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}.$$

这种形式的哈达玛矩阵被称为四元数型 [7], ，因为其结构基于基本四元数单位 1、i、j和k [39]的矩阵表示。在 Williamson 的原始论文中，块矩阵 $A$、$B$、 $C$ 和 $D$ 是两两可交换的对称 $\{\pm 1\}$ 阶矩阵，满足 $A^2 + B^2 + C^2 + D^2 = 4n\mathbf{I}_n$。Baumert 和 Hall [7] 指出，Williamson 的两两可交换条件可以替换为更

一般的条件

$$UV - VU + XY - YX = 0$$

对于 $(U, V, X, Y) \in \{(A, B, C, D), (A, C, B, D), (A, D, B, C)\}$。此外，四元数型 Hadamard 矩阵的块矩阵不必一定是对称的，但如果块矩阵不对称，则定义四元数型 Hadamard 矩阵的方程由下式给出

$$AA^\top + BB^\top + CC^\top + DD^\top = 4n\mathrm{I}_n, \tag{1.1}$$

and

$$\begin{aligned} BA^\top - AB^\top + DC^\top - CD^\top &= 0, \\ CA^\top - AC^\top + BD^\top - DB^\top &= 0, \\ DA^\top - AD^\top + CB^\top - BC^\top &= 0. \end{aligned} \tag{1.2}$$

满足 (1.1) 和 (1.2) 的哈达玛矩阵的块有时被称为 Williamson 型矩阵，不过我们遵循更为常见的惯例，将名称*Williamson*型 保留给一类更为特定的矩阵，即满足 (1.1)、但将 (1.2) 替换为更强的成对友好性 条件 $XY^\top = YX^\top$ （对所有 $X$,$Y \in \{A, B, C, D\}$ [42]）。

在本文中，如同在 Williamson 的原始论文中一样，我们还要求块矩阵 $A, B, C, D$ 是循环的，此时我们可以用它们的首行来描述这些矩阵。在块矩阵为循环的情形下，我们证明看似更强的成对友好性条件实际上等价于条件 (1.2)（见定理 9）。也就是说，将循环 Williamson 型矩阵的首行视为*Williamson* 型序列 ，并将四元数型矩阵的循环块的首行视为 *QT* 序列，我们证明 QT 序列与 Williamson 型序列这两个概念完全对应。我们在第 2 节中提供理解本文结果所需的背景，并借助相关性正式定义 QT 序列和 Williamson 型序列，而 QT 序列与 Williamson 型序列的等价性则在第 2.4 节中加以证明。

关于循环 Williamson 型矩阵的先前研究还包括寻找解析构造或证明其不存在。Fitzpatrick 和 O'Keeffe [16] 采用解析方法证明，不存在长度为 35、47、53 和 59 的 Williamson 型序列，尽管他们的结果依赖于计算机辅助

证明：不存在阶为 35 的循环对称 Williamson 型矩阵（最早由 Đoković [13] 证明），也不存在阶为 47、53 和 59 的循环对称 Williamson 型矩阵（由 Holzmann、Kharaghani 和 Tayfeh-Rezaie [25]证明）。Fitzpatrick 和 O'Keeffe 在证明中利用了 Williamson 型矩阵的相容性，因此，阶为 35、47、53 和 59 且具有循环块的四元数型阿达玛矩阵理论上仍有可能存在。我们在定理 9 中证明的等价关系表明，事实上这类矩阵并不存在。

## 1.2 四元数完美序列

本文研究的是具有循环块的四元数型阿达玛矩阵，但可以证明，这类对象等价于取值于四元数字母表的完美序列。四元数由威廉·罗恩·哈密顿爵士 [21]首次提出，是对复平面的扩展，增加了另外两个数$\mathbf{j}$ 和$\mathbf{k}$ ，其中$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ ，且$\mathbf{ij} = \mathbf{k}$。哈密顿在尝试寻找一种类似于复数（二维空间中的点）相乘的方式来乘以三维空间中的点时，发现了这些数。请注意，四元数一般不满足交换律，因为$\mathbf{ji} = -\mathbf{k}$。

Kuznetsov [26] 最早研究了四元数完美序列。他证明了若干结果，其中包括四元数空间的对称变换会保持序列的完美性，并列举了能够保持完美性的序列运算。他构造出了一个长度为5,354,228,880的完美四元数序列，并将复数序列的许多结果推广到了四元数。在一项重要进展中，Barrera Acevedo 和 Hall [5] 构造了取值于字母表 $\{\pm 1, \pm \mathbf{i}, \mathbf{j}\}$ 的完美序列，其长度满足 $n = p^k + 1 \equiv 2 \pmod 4$，其中 $p$ 为素数，且 $k \in \mathbb{N}$。这首次表明，尽管预期字母表 $\{\pm 1, \pm \mathbf{i}\}$上只有有限多个完美序列，但仍能找到长度无界、取值于基本四元数字母表 $\mathcal{Q}_8 := \{\pm 1, \pm \mathbf{i}\ \pm \mathbf{j}\ \pm \mathbf{k}\}$ 的完美序列。Blake [8] 对取值于字母表 $\mathcal{Q}_8$的完美序列进行了广泛搜索；Bright、Kotsireas 和 Ganesh [10] 则证明，对于所有 $k \in \mathbb{N}$，长度为 $2^k$ 且取值于$\mathcal{Q}_8$ 的完美序列均存在。Barrera Acevedo 和 Dietrich [2] 研究了取值于 $\mathcal{Q}_+$ 的完美四元数序列，其中 $q := (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$，并建立了取值于 $\mathcal{Q}_+$ 的完美序列与四元组 QT 序列之间的一一对应关系。

本文介绍了对 QT 序

列（等价地， $\mathcal{Q}_+$ 上的完美序列）进行穷举搜索的结果。此前，Barrera Acevedo、Catháin 和 Dietrich [6], 穷举搜索的最长长度为 $n = 13$，据估计耗费的计算时间最长可达一周 [1]。我们的算法可在不到 5 秒内穷举完成长度为 $n \leq 13$ 的搜索。Barrera Acevedo、Catháin 和 Dietrich 有意搜索各种类型的素数长度序列，以生成余循环哈达玛矩阵（包括作为特殊情形的 QT 序列），但他们的搜索算法无法处理长度为 17 和 19 的序列。我们能够在不到 8 小时内穷举枚举长度为 $n \leq 20$ 的 QT 序列，并在不到 40 小时内完成长度为 $n = 21$ 的枚举（结果见第 3 节）。第 1.1 节提到的 QT 序列与 Williamson 型序列之间的等价关系，在搜索中发挥了关键作用，大幅提升了第 3 节所述枚举算法的筛选能力。在枚举长度为 $n = 20$的 QT 序列时，利用这种等价关系可使我们的算法的筛选量提升约 25,000 倍。因此，这种等价关系不仅具有理论意义，也有实际用途。

非必然对称的 Williamson 型矩阵已有五十多年的研究历史 [40, 41], ，但与对称情形形成鲜明对比的是，我们惊讶地发现，没有专门针对不假设对称性的循环 Williamson 型矩阵进行过枚举。这可能是因为对称性假设大幅缩小了搜索空间并简化了搜索，从而能够利用更多限制性性质，并开展更全面的枚举（包括所有阶 $n$ 不超过 $60$ [9, 25]的情形）。例如，当块 $A$、$B$、 $C$、 $D$ 既对称又循环时，条件（1.2）便自动成立。Barrera Acevedo、Catháin 和 Dietrich [6]对素数 $p \leq 13$ 阶 $4p$ 余循环哈达玛矩阵所作的枚举，是我们所知最全面的穷举枚举，且不依赖对称性假设。由于循环 Williamson 型矩阵可以生成余循环哈达玛矩阵，作为他们结果的一个特例，他们生成了素数 $p$对应的所有长度为 $p \leq 13$ 的 Williamson 型序列。第 3 节中计算搜索所采用的优化方法，使我们能够枚举 $n \leq 21$的所有长度为 $n$ 的 Williamson 型序列。

## 1.3 四元数哈达玛矩阵

一个阶为 $n$ 的四元数 *Hadamard* 矩阵 (QHM) 是一个 $n \times n$ 矩阵 $G$，其元素为单位四元数，且满足 $GG^* = n\mathbf{I}$，其中 $G^*$ 是其共轭

$G$ 的转置。Farkas、Kaniewski 和 Nayak [15] 近期揭示了四元数 Hadamard 矩阵与量子信息之间的联系，再度激发了人们对构造 QHM 的兴趣。具体而言，他们利用四元数与复数 $2\times2$矩阵集合的一个子代数之间的代数同构，使用 QHM 构造了酉算子的 Hadamard 矩阵。后者对应于互 unbiased 测量 (MUMs)，而互 unbiased 测量是互 unbiased 基 ( MUBs) 的扩展。因此，每个阶为 $n$ 的四元数 Hadamard 矩阵都对应一个“$n$结果”MUM。感兴趣的读者可参阅 [15] ，了解这些概念的定义及其在量子信息与通信中的意义。

一些互 unbiased 测量可通过直和构造从互 unbiased 基导出。Farkas、Kaniewski 和 Nayak [15] 给出了对由互 unbiased 基的直和构成的互 unbiased 测量进行刻画的完整证明。Tavakoli、Farkas、Rosset、Bancal 和 Kaniewski [37]此前已部分证明了这一刻画。该刻画表明，当且仅当归一化四元数 Hadamard 矩阵的所有元素均可交换时，与该矩阵对应的互 unbiased 测量才是互 unbiased 基的直和。

Farkas、Kaniewski 和 Nayak 证明，不是互 unbiased 基直和的互 unbiased 测量不 会产生用于超密编码的新型量子通信协议。这一联系促使他们构造了此类新型互 unbiased 测量。他们给出了若干阶下这类互 unbiased 测量的显式形式，并展示了如何利用它们推导出无穷多个阶下的此类互 unbiased 测量。这些互 unbiased 测量要么是此前通过临时计算搜索 [37], 发现的，要么是针对少数几种阶，通过更系统的方法从四元数 Hadamard 矩阵 [15]推导而来。这促使人们进一步深入研究任意阶的四元数 Hadamard 矩阵。

Chterental 和 Đoković [12] 指出，阶数不超过三的四元数 Hadamard 矩阵都等价于复 Hadamard 矩阵。他们通过证明这类矩阵恰有两个族，且每个族的基数均不可数无限，从而刻画了所有四阶四元数 Hadamard 矩阵。他们还用少数几个参数给出了这些矩阵的显式表达式。Higginbotham 和 Worley [24]沿着类似的思路继续研究，考察了特定类型的五阶四元数 Hadamard 矩阵以及更一般的四元数 Hadamard 矩阵构造。

Barrera Acevedo、Dietrich 和 Lionis [4] 通过推广实 Hadamard 矩阵与复 Hadamard 矩阵的方法，给出了若干四元数 Hadamard 矩阵的构造。这些构造对无穷多个阶给出了具有非交换元素的新的标准化四元数 Hadamard 矩阵。这些构造还包括固定阶上此类互不等价矩阵的无穷族。

与实数情形不同，所有阶的四元数 Hadamard 矩阵都存在。复傅里叶矩阵是众所周知的例子。上述工作表明，所有大于三的阶的四元数 Hadamard 矩阵都存在多个等价类，甚至固定阶上具有非交换元素的标准化四元数 Hadamard 矩阵（以及相应的互 unbiased 测量）也存在多个无穷等价类。受此推动，我们继续对四元数 Hadamard 矩阵进行计算与分析研究。

循环四元数 Hadamard 矩阵等价于完美四元数序列。因此，对 QT 序列的计算枚举可得出新的完美四元数序列，进而得到新的四元数 Hadamard 矩阵。归一化矩阵通常包含非交换元素，因此可导出在量子信息领域颇受关注的新型互 unbiased 测量。我们在第 4.1 节列举了这类四元数 Hadamard 矩阵的若干实例。这与早期针对非平凡互 unbiased 测量的计算搜索形成对比：早期搜索只在少数几个较小的阶上得到互 unbiased 测量（即 [37] 中报告的结果）[14]。

我们证明，与实数或复 Hadamard 矩阵的情形不同，只要四元数 Hadamard 矩阵的规范化形式中至少含有一个非实元素，它们就存在包含不可数多个规范化矩阵的等价类（命题 17）。我们还提出了一种刻画低阶四元数 Hadamard 矩阵的方法，并以五阶矩阵为例加以说明（第4.3节）。最后，我们证明，由完美 $\mathcal{Q}_+$序列生成的五阶四元数 Hadamard 矩阵，与 Higginbotham 和 Worley [23], 所研究的矩阵并不等价；同样，在七阶情形下，也存在由完美 $\mathcal{Q}_+$序列生成的四元数 Hadamard 矩阵，它们与 Kuznetsov [27] 以及 Barrera Acevedo、Dietrich 和 Lionis [4] 列出的完美序列所生成的四元数 Hadamard 矩阵并不等价（见第 4.4 节）。因此，五阶和七阶至少各有三个互不等价的四元数 Hadamard 矩阵族；结合此前的研究，我们猜想所有阶数 $\geq 4$都存在多个互不等价的四元数 Hadamard 矩阵。不过，如果只考虑 $\mathcal{Q}_+$ 上的循环四元数 Hadamard 矩阵，我们的结果表明此猜想并不成立。定理 9 中给出的等价关系与 Fitzpatrick 和 O'Keeffe [16], 的结果共同表明，35、47、53 和 59 阶的循环四元数 Hadamard 矩阵若其元素属于 $\mathcal{Q}_+$ ，则不存在。

# 2 背景

本节介绍本文使用的符号和必要背景。首先，我们在第 2.1 节引入四元数代数，并说明用于表示重要四元数集合的符号。接着，我们在第 2.2 节正式定义 Hadamard 矩阵和四元数 Hadamard 矩阵，以及 Hadamard 矩阵之间的等价关系。然后，我们在第 2.3 节正式定义序列的相关性，以及完美序列、QT 序列和 Williamson 型序列，并介绍 Barrera Acevedo 和 Dietrich [2]证明的某些四元数完美序列与 QT 序列之间的一一对应关系。随后，我们在第 2.4 节证明 QT 序列与 Williamson 型序列之间的一一对应关系。最后，我们在第 2.5 节定义 QT 序列的等价关系，后文将借助这些定义对 QT 序列的枚举结果进行分类。

## 2.1 四元数

四元数可视为复数的一种非交换扩张。形式上，四元数实代数表示为

$$\mathbb{H} \coloneqq \{\, \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} : \alpha, \beta, \gamma, \delta \in \mathbb{R} \,\},$$

其中**i**、**j**和**k** 是基本单位四元数，满足以下关系：

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{ij} = \mathbf{k}, \quad \text{and} \quad \mathbf{ji} = -\mathbf{k}.$$

数值 $\alpha$ 是四元数 $\alpha+\beta\mathbf{i}+\gamma\mathbf{j}+\delta\mathbf{k}$的实部，而 $\beta\mathbf{i}+\gamma\mathbf{j}+\delta\mathbf{k}$是它的纯虚部。

该代数配备了共轭运算 $x \mapsto x^*$，满足：对于实数 $\alpha$，有 $\alpha^* = \alpha$；此外，$\mathbf{i}^* = -\mathbf{i}$、$\mathbf{j}^* = -\mathbf{j}$和$\mathbf{k}^* = -\mathbf{k}$。因此，四元数 $w$ 的实部 $\mathrm{Re}(w)$可表示为 $\mathrm{Re}(w) = (w + w^*)/2$。

共轭对加法满足分配律，并且满足 $(x_1x_2)^* = x_2^*x_1^*$。四元数 $x$ 的范数 $\|x\|$ 定义为

$$\|x\| \coloneqq \sqrt{xx^*} = \sqrt{x^*x},$$

当 $x \neq 0$ 时，其乘法逆元 $x^{-1}$ 由 $x^{-1} \coloneqq x^*/\|x\|$ 给出。范数为 1 的四元数称为单位四元数，我们用以下符号表示单位四元数的集合：

$$\mathsf{S}^3 \coloneqq \{\, w \in \mathbb{H} : \|w\| = 1 \,\}.$$

单位四元数在乘法运算下构成一个非阿贝尔群。我们用 $\mathsf{S}^2$ 表示 $-1$ 的四元数平方根集合。也就是说，

$$\mathsf{S}^2 := \{\, w \in \mathbb{H} : w^2 = -1 \,\},$$

并且可以证明

$$\mathsf{S}^2 = \{\, w \in \mathsf{S}^3 : \mathrm{Re}(w) = 0 \,\}.$$

因此，$\mathsf{S}^2$ 的元素都是纯虚四元数。

我们定义 $q := (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$。这是一个单位四元数，也是 $-1$的立方根。本文中三个重要的单位四元数集合为

$$\mathcal{Q}_8 := \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}, \quad \mathcal{Q}_+ := \mathcal{Q}_8 \cup q\mathcal{Q}_8\,, \quad \text{and} \quad \mathcal{Q}_{24} := \mathcal{Q}_+ \cup q^2\mathcal{Q}_8\,.$$

集合 $\mathcal{Q}_8$ 和 $\mathcal{Q}_{24}$ 在乘法下构成群，但 $\mathcal{Q}_+$ 不是，因为$q^2 = -q^* \notin \mathcal{Q}_+$。

欧拉公式 $e^{\mathbf{i}t} = \cos t + \mathbf{i}\sin t$ 通过指数函数的幂级数展开 [11]推广到四元数。对于 $t \in \mathbb{R}$ 和 $w \in \mathsf{S}^2$，我们有

$$\mathrm{e}^{wt} = \cos t + w \sin t.$$

## 2.2 哈达玛矩阵

如果方阵 $H$ 的阶为 $n$，且 $H$ 的元素满足 $\pm 1$ 并且 $HH^\top = n\mathbf{I}_n$，则称其为（实）*Hadamard* 矩阵。换言之，矩阵的所有元素均为单位模，且矩阵的各行两两正交。这意味着矩阵的各列也两两正交。

对于一个阶数为 $n$ 的四元数矩阵 $G$，矩阵 $G^*$ 表示 $G$ 的共轭转置，即对于所有指标 $i, j \in \{0, 1, \ldots, n-1\}$，都有 $(G^*)_{ij} := (G_{ji})^*$。如果矩阵 $G$ 的元素属于 $\mathsf{S}^3$，且满足 $GG^* = n\mathbf{I}_n$，则称其为四元数 *Hadamard* 矩阵（QHM）。后一条件要求矩阵的各行相对于 $\mathbb{H}$-模 $\mathbb{H}^n$ 上的一种半双线性型彼此正交，该型对第二个变量共轭线性。我们可以证明，该条件蕴含 $G^*G = n\mathbf{I}_n$，也就是说，$G$ 的各列相对于另一种对第一个变量共轭线性的半双线性型彼此正交。由于 $\mathbb{H}$ 中乘法的非交换性，使用这两种不同的半双线性型十分重要；相对于其中一种正交，并不一定意味着相对于另一种也正交。

我们可以将实数集合视为纯虚部为 0 的四元数子集，并将复数集合视为由 $\{1,\mathbf{i}\}$ 生成的四元数子集。因此，复Hadamard矩阵可以视为元素为复数的 QHM。

在本文其余部分中，我们考虑模等价意义下的哈达玛矩阵。如果一个实 Hadamard 矩阵可以通过将另一个矩阵的若干行或列取负、交换若干行或交换若干列得到，那么这两个实 Hadamard 矩阵就称为等价的 [30]。我们将这一等价关系推广到 QT 序列：如果两个 QT 序列生成的四元数型阿达玛矩阵等价，则称这两个 QT 序列为 ***Hadamard*等价** 。类似地，如果一个四元数 Hadamard 矩阵可以通过将若干行**左乘** 单位四元数、将若干列**右乘** 单位四元数、交换若干行或交换若干列得到，则称这两个四元数 Hadamard 矩阵等价。由于四元数乘法不满足交换律，这些运算中的乘法顺序至关重要。两个四元数 Hadamard 矩阵的等价性可如下刻画。

**引理 1.** 两个四元数 *Hadamard* 矩阵 $G, G'$ 等价，当且仅当存在置换矩阵 $P_1$, $P_2$ 以及由单位四元数组成的对角矩阵 $D_1, D_2$，使得 $G' = D_1 P_1 G P_2 D_2$。

实 Hadamard 矩阵或复 Hadamard 矩阵也有类似的引理。在实数情形下， $D_1$ 和 $D_2$ 的对角线为 $\pm 1$；在复数情形下，它们由单位复数组成。

如果实、复或四元数 Hadamard 矩阵的第一行和第一列中的元素全为「1」，我们就称其为规范化的。注意，每个 Hadamard 矩阵都等价于一个规范化Hadamard矩阵；我们可以将每一行左乘其首个元素的共轭，再将每一列右乘其首个元素的共轭，从而实现这一点。我们将这些操作称为「去相位」。

给定一个四元数 Hadamard 矩阵 $G$ 和四元数的一个代数自同构 $f$，我们可以验证，按 $(f(G))_{ij} := f(G_{ij})$ 对所有指标 $0 \le i,\ j < n$ 定义的矩阵 $f(G)$ 也是一个四元数 Hadamard 矩阵。事实上，四元数的每个自同构都对应于一个内自同构。

**命题 2 (**命题 2.4.7，第 19, [32])。 $\mathbb{H}$的每个自同构都是内自同构，也就是说，若 $f\colon \mathbb{H} \to \mathbb{H}$ 是一个自同构，则存在 $a \in \mathsf{S}^2$ 使得 $f(x) = a^* x a$，对所有 $x \in \mathbb{H}$ 均成立。

对矩阵的每个元素应用内自同构，可以通过等价操作实现；我们可以将每一行左乘 $a^*$，并将每一列右乘 $a$。因此，应用自同构会得到等价的四元数 Hadamard 矩阵。

**推论 3.** 对四元数 *Hadamard* 矩阵的每个元素应用 $\mathbb{H}$ 的一个自同构，会得到一个等价的四元数 *Hadamard* 矩阵。

## 2.3 完美序列、QT 序列和 Williamson 型序列

设 $A$ 和 $B$ 是长度为 $n$ 的序列，其中 $A = [a_0, \ldots, a_{n-1}]$ 和 $B = [b_0, \ldots, b_{n-1}]$。对于移位 $0 \le t < n$，$A$ 和 $B$ 的周期互相关 $R_{A,B}(t)$ 定义为

$$R_{A,B}(t) \coloneqq \sum_{r=0}^{n-1} a_r b^*_{r+t \bmod n}.$$

我们进一步将 $A$ 的右周期自相关 $R^R_A(t)$ 以及 $A$ 的左周期自相关 $R^L_A(t)$定义为

$$R^R_A(t) \coloneqq \sum_{r=0}^{n-1} a_r a^*_{r+t \bmod n}, \quad \text{and} \quad R^L_A(t) \coloneqq \sum_{r=0}^{n-1} a^*_r a_{r+t \bmod n},$$

分别。若一个序列 $S$ 的右周期 $t$-自相关对所有非零移位 $t$ 均为零，即对于所有满足 $1 \le t < n$ 的 $t$，都有 $R^L_S(t) = 0$，则称该序列为右完美。序列的左完美性定义类似。Kuznetsov [26] 证明了一个四元数序列是右完美的，当且仅当它是左完美的。因此，不失一般性，我们将 $A$ 的周期自相关 $R_A(t)$ 定义为

$$R_A(t) \coloneqq R^R_A(t) = R_{A,A}(t) = \sum_{r=0}^{n-1} a_r a^*_{r+t \bmod n},$$

并称该序列为完美序列，如果其对所有非零 $t$ 的周期自相关值均为零。$\mathbb{H}$ 上的完美序列称为完美四元数序列。

我们将具有 $\{\pm 1\}$ 个项的序列称为二进制序列。设 $A$、$B$、$C$和 $D$ 均为长度为 $n$的二进制序列。记克罗内克 delta

用$\delta_{0,\,t}$表示（注意：当 $t=0$ 时，$\delta_{0,\,t}$ 为1，否则为0）。若对所有 $0 \le t < n$ 均有，则称（$A$，$B$，$C$，$D$）为*QT* 序列四元组

$$R_A(t) + R_B(t) + R_C(t) + R_D(t) = \delta_{0,t} 4n, \tag{2.1}$$

$$R_{A,B}(t) - R_{B,A}(t) + R_{C,D}(t) - R_{D,C}(t) = 0, \tag{2.2}$$

$$R_{A,C}(t) - R_{C,A}(t) + R_{D,B}(t) - R_{B,D}(t) = 0, \tag{2.3}$$

$$R_{A,D}(t) - R_{D,A}(t) + R_{B,C}(t) - R_{C,B}(t) = 0. \tag{2.4}$$

我们将 (2.1) 称为 自相关条件，并将 (2.2)–(2.4) 称为 互相关条件。若将互相关条件替换为条件$R_{X,Y}(t) - R_{Y,X}(t) = 0$ 对所有 $X, Y \in \{A, B, C, D\}$ 成立，则该四元组中的序列称为 *Williamson*型。QT 序列等价于具有循环块的四元数型阿达玛矩阵（如引言中所定义），类似地，Williamson 型序列等价于循环 Williamson 型矩阵的第一行。若一组 Williamson 型序列四元组生成 对称 循环块矩阵，则称它们为 威廉姆森序列 [9]。注意，序列 $[a_0, \ldots, a_{n-1}]$ 在 $a_i = a_{n-i}$ 对所有 $1 \le i < n$成立时生成循环对称矩阵。

Barrera Acevedo 和 Dietrich [2] 证明，$\mathcal{Q}_+$ 上长度为 $n$ 的完美四元数序列等价于 $C_n \times \mathcal{Q}_8$中的某类相对差集，其中 $C_n$ 表示阶为 $n$的循环群。Schmidt [34] 的一个结果表明，$C_n \times \mathcal{Q}_8$ 中的这类相对差集等价于其块为循环（但不一定两两相容或对称）的四元数型阿达玛矩阵。确切地说，我们有如下定理。

**定理 4** （参见 [3, 定理 2。4]）。长度为 $n$ 的 *QT* 序列四元组与 $\mathcal{Q}_+$ 上长度为 $n$ 的完美序列之间存在一一对应关系。

这种对应关系可以用完美四元数序列 $S$ 的第 $r$ 个元素 $s_r$ 与 QT 序列 $(A, B, C, D)$ 的第 $r$ 个元素组成的四元组 $(a_r,\ b_r,\ c_r,\ d_r)$ 之间的映射来描述。下表给出了该映射的一半，其中 $+1$ 和 $-1$ 分别简写为“+”和“–”。

| $s_r$ | $1$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{k}$ | $q$ | $q\mathbf{i}$ | $q\mathbf{j}$ | $q\mathbf{k}$ |
|---|---|---|---|---|---|---|---|---|
| $a_r$ | $-$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ | $+$ |
| $b_r$ | $-$ | $-$ | $+$ | $-$ | $-$ | $+$ | $+$ | $-$ |
| $c_r$ | $-$ | $-$ | $-$ | $+$ | $-$ | $-$ | $+$ | $+$ |
| $d_r$ | $-$ | $+$ | $-$ | $-$ | $-$ | $+$ | $-$ | $+$ |

映射的另一半由以下规则给出：如果 $(a_r,\ b_r,\ c_r,\ d_r)$ 映射到 $s_r$，那么 $(-a_r,\ -b_r,\ -c_r,\ -d_r)$ 就映射到 $-s_r$。由于这种对应关系，在字母表 $\mathcal{Q}_+$ 上寻找完美四元数序列，等价于寻找 QT 序列。

我们强调，定理 4 所确立的等价关系并非 Williamson型序列与完美 $\mathcal{Q}_+$-序列之间的等价关系，而是 QT 序列（它们可能并非两两相容）与完美 $\mathcal{Q}_+$-序列之间的等价关系。Schmidt 明确指出，他并不 要求用于证明定理 4 的结果中的块矩阵满足两两相容条件：

> 我们指出，这一定义与通常的定义略有不同，通常的定义要求 $XY^t = YX^t$ 对$\{A, B, C, D\}$的所有二元子集 $\{X, Y\}$ 都成立。 [34]

因此，要通过这一等价关系完成对完美 $\mathcal{Q}_+$-序列的枚举，可惜不能 使用更强的两两相容条件，而必须改用 (1.2) 所给出的较弱的四元数型条件。幸运的是，我们将在下一节证明，条件 (1.2) 实际上蕴含两两相容，因此上述区别无关紧要，并由此得到以下结论。

**定理 5.** 长度为 $n$ 的 *Williamson* 型序列四元组与在 $\mathcal{Q}_+$ 上长度为 $n$ 的完美序列之间存在一一对应关系。

## 2.4 QT 序列与 Williamson 型序列的等价性

为证明 QT 序列与 Williamson 型序列的等价性，我们使用离散傅里叶变换（DFT）$_A$。我们用 DFT $\sum_{s=0}^{n-1} a_i$ $2\pi\ st/n$ $A$ $n$ $_A$ $=$ (*t*) 表示序列 $A$（长度为 ）的离散傅里叶变换的第 $t$ 个值，即 DFT (*t*) exp(i)；用 DFT( ) 表示离散傅里叶变换值构成的向量，即 DFT($A$) $=$ [DFT$_A$(0) … ,DFT$_A$($n-1$)]。我们还将 $A$ 的功率谱密度定义为 PSD$_A$(*t*) ≔ DFT$_A$(*t*) DFT$_{A^*}$(*t*) $=$ |DFT$_A$(*t*)|$^2$ ，并用 PSD$_A$ 表示 $t=0$ 到 $n-1$ 的 PSD$_A$(*t*) 值所构成的向量。这里， $A^*$ 表示作用于序列的共轭转置运算； $A^*$的第 $k$ 个元素为 $(A_{-k \bmod n})^*$，其中模运算符给出 $[0, n)$ 中与其参数模 $n$同余的整数。下面的等价性众所周知，但为求完整，我们仍给出证明。

**命题 6** （功率谱密度）。（$A, B, C, D$）是长度为 $n$ 的四元组 *QT* 序列，当且仅当

$$\mathrm{PSD}_A(t) + \mathrm{PSD}_B(t) + \mathrm{PSD}_C(t) + \mathrm{PSD}_D(t) = 4n \quad for\ all\ t \in \mathbb{Z}.$$

*Pr*哎呀。 自相关条件等价于卷积方程

$$A * A^* + B * B^* + C * C^* + D * D^* = [4n, 0, \ldots, 0] \tag{2.5}$$

其中， $X*Y$表示序列卷积，即序列$[x_0, \ldots, x_{n-1}]$和 $[y_0, \ldots, y_{n-1}]$的卷积，其第 $k$项为$\sum_{i=0}^{n-1} x_i y_{k-i \bmod n}$。 根据离散傅里叶变换卷积定理，我们有 $\mathrm{DFT}_{X*X^*}(t) = \mathrm{DFT}_X(t)\ \mathrm{DFT}_{X^*}(t) = \mathrm{PSD}_X(t)$。对(2.5)两边应用离散傅里叶变换，利用离散傅里叶变换的线性性质以及 $[4n, 0, \ldots, 0]$ 的离散傅里叶变换为 $[4n, \ldots, 4n]$这一事实，可得(2.5)意味着

$$\mathrm{PSD}_A + \mathrm{PSD}_B + \mathrm{PSD}_C + \mathrm{PSD}_D = [4n, \ldots, 4n].$$

对该功率谱密度方程应用逆离散傅里叶变换，可知它等价于(2.5)。

□

同样，下面的命题表明，我们也可以对互相关方程应用离散傅里叶变换，从而在频域中推导出这些方程的等价形式。定义互功率谱密度为 $\mathrm{CPSD}_{X,\ Y}(t) =$ 离散傅里叶变换$_X(t)$ 离散傅里叶变换$_Y(t)^*$，并令 $\mathrm{CPSD}_{X,\ Y}$ 表示从 $t = 0$ 到 $n - 1$ 的互功率谱密度值向量。

**命题 7** (互功率谱密度)。 对所有整数 $t$ 成立的互相关方程 (2.2) 等价于以下条件

$$\mathrm{CPSD}_{A,B}(t) - \mathrm{CPSD}_{B,A}(t) + \mathrm{CPSD}_{C,D}(t) - \mathrm{CPSD}_{D,C}(t) = 0 \quad for\ all\ t \in \mathbb{Z}.$$

证明。 $X$ 和 $Y$ 的互相关向量等于卷积向量 $X * Y^*$，因此互相关条件 (2.2) 等价于

$$A * B^* - B * A^* + C * D^* - D * C^* = [0, \ldots, 0]. \tag{2.6}$$

通过应用离散傅里叶变换并利用离散傅里叶变换卷积定理，我们有离散傅里叶变换$_{X*Y^*}(t) =$ 离散傅里叶变换$_X(t)$ 离散傅里叶变换$_{Y^*}(t) = \mathrm{CPSD}_{X,Y}(t)$，因此对(2.2)应用离散傅里叶变换，并注意到 $[0, \ldots, 0]$ 的离散傅里叶变换为 $[0, \ldots, 0]$，我们得到(2.6)等价于

$$\mathrm{CPSD}_{A,B} - \mathrm{CPSD}_{B,A} + \mathrm{CPSD}_{C,D} - \mathrm{CPSD}_{D,C} = [0, \ldots, 0]. \qquad \square$$

**注释8.** 与命题 7 类似的证明表明，(2.3) 对所有 $t$等价于$\mathrm{CPSD}_{A,C} - \mathrm{CPSD}_{C,A} = \mathrm{CPSD}_{B,D} - \mathrm{CPSD}_{D,B}$，并且(2.4) 对所有 $t$ 等价于$\mathrm{CPSD}_{A,D} - \mathrm{CPSD}_{D,A} = \mathrm{CPSD}_{C,B} - \mathrm{CPSD}_{B,C}$。

尽管 QT 序列和 Williamson 型序列的定义不同，我们现在证明这两个概念实际上是等价的。

**定理 9.** *$(A, B, C, D)$ 是一个四元组 QT 序列，当且仅当$(A, B, C, D)$ 是一个 Williamson 型序列四元组。*

证明. 如果 $(A, B, C, D)$ 是一组 Williamson 型序列，那么对于所有整数 $t$ 和 $X, Y \in \{A, B, C, D\}$，$R_{X,Y}(t) - R_{Y,X}(t) = 0$。将 $(X, Y) = (A, B)$ 和 $(X, Y) = (C, D)$ 的条件相加，可推出 (2.2)。条件 (2.3) 和 (2.4) 的推导类似。

反过来，假设 $(A, B, C, D)$ 是一组 QT 序列。取 $t$ 为一个固定整数，并令 $a :=$ 离散傅里叶变换$_A(t)$，$b :=$ 离散傅里叶变换$_B(t)$，$c :=$ 离散傅里叶变换$_C(t)$，以及$d :=$ 离散傅里叶变换$_D(t)$。根据命题 7，我们有

$$ab^* - ba^* + cd^* - dc^* = 0. \tag{2.7}$$

对于 $x \in \mathbb{C}$，记作 $x = r_x + i_x\mathbf{i}$，其中 $r_x, i_x \in \mathbb{R}$。等价地，将 $x$ 视为 $\mathbb{R}^2$ 中的行向量，我们将矩阵 $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] = \left[\begin{smallmatrix} r_x & i_x \\ r_y & i_y \end{smallmatrix}\right]$ 的行列式写作$\left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right| = r_x i_y - r_y i_x$，并注意到 $yx^* - xy^* = 2\mathbf{i}\left|\begin{smallmatrix} x \\ y \end{smallmatrix}\right|$。因此，(2.7) 等价于$\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right| + \left|\begin{smallmatrix} c \\ d \end{smallmatrix}\right| = 0$ 或 $\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right| = \left|\begin{smallmatrix} d \\ c \end{smallmatrix}\right|$。由频域中的互相关方程（参见注释8），我们得到

$$\begin{vmatrix} a \\ b \end{vmatrix} = \begin{vmatrix} d \\ c \end{vmatrix}, \quad \begin{vmatrix} a \\ c \end{vmatrix} = \begin{vmatrix} b \\ d \end{vmatrix}, \quad \text{and} \quad \begin{vmatrix} a \\ d \end{vmatrix} = \begin{vmatrix} c \\ b \end{vmatrix}. \tag{2.8}$$

现在我们证明，这意味着所有这些行列式都为 0。反设不然，且不失一般性地，$\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right| \neq 0$。于是 $\{a, b\}$ 构成了 $\mathbb{R}^2$的一组基，因此将$c = \alpha a + \beta b$和 $d = \gamma a + \delta b$ 写作 $\alpha$、$\beta$、$\gamma$、$\delta \in \mathbb{R}$。现在 $\left|\begin{smallmatrix} d \\ c \end{smallmatrix}\right| = \left|\begin{smallmatrix} \gamma a + \delta b \\ \alpha a + \beta b \end{smallmatrix}\right| = \left|\begin{smallmatrix} \gamma a \\ \alpha a + \beta b \end{smallmatrix}\right| + \left|\begin{smallmatrix} \delta b \\ \alpha a + \beta b \end{smallmatrix}\right| = \left|\begin{smallmatrix} \gamma a \\ \beta b \end{smallmatrix}\right| + \left|\begin{smallmatrix} \delta b \\ \alpha a \end{smallmatrix}\right| = (\gamma\beta - \alpha\delta)\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right|$、$\left|\begin{smallmatrix} a \\ c \end{smallmatrix}\right| = \beta\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right|$、$\left|\begin{smallmatrix} b \\ d \end{smallmatrix}\right| = \left|\begin{smallmatrix} b \\ \gamma a + \delta b \end{smallmatrix}\right| = \left|\begin{smallmatrix} b \\ \gamma a \end{smallmatrix}\right| = -\gamma\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right|$、$\left|\begin{smallmatrix} a \\ d \end{smallmatrix}\right| = \delta\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right|$，并且 $\left|\begin{smallmatrix} c \\ b \end{smallmatrix}\right| = \alpha\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right|$。将这些表达式代入 (2.8)，得到

$$\gamma\beta - \alpha\delta = 1, \quad \beta = -\gamma, \quad \text{and} \quad \delta = \alpha.$$

这意味着 $\alpha^2 + \beta^2 = -1$，矛盾。因此必有 $\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right| = \left|\begin{smallmatrix} a \\ c \end{smallmatrix}\right| = \left|\begin{smallmatrix} a \\ d \end{smallmatrix}\right| = \left|\begin{smallmatrix} b \\ c \end{smallmatrix}\right| = \left|\begin{smallmatrix} b \\ d \end{smallmatrix}\right| = \left|\begin{smallmatrix} c \\ d \end{smallmatrix}\right| = 0$。由 $\left|\begin{smallmatrix} a \\ b \end{smallmatrix}\right| = 0$ 可得 $ab^* =$

$ba^*$。由于 $a =$ 离散傅里叶变换$_A(t)$，且 $b =$离散傅里叶变换$_B(t)$，并且 $t$ 是任意的，因此 CPSD$_{A,\ B}$ = CPSD$_{B,\ A}$。应用逆离散傅里叶变换，得到 $R_{A,\ B}(t) = R_{B,\ A}(t)$，对所有 $t$ 均成立。类似地，对所有 $t$，有 $R_{X,\ Y}(t) = R_{Y,\ X}(t)$，因此 ($A$，$B$，$C$，$D$) 是 Williamson型。 □

尽管 Williamson 型序列与 QT 序列之间存在一一对应关系，我们仍认为有必要分别使用不同的术语来称呼它们。在下一节中，我们将介绍两种不同的 QT 序列四元组等价概念（一种基于 QT 序列的定义，另一种基于 Williamson 型序列的定义），并说明同时采用这两种等价概念的好处。

## 2.5 序列等价操作

QT 序列有若干等价操作，可用来定义等价类；这些等价类通常不同于第 2.2 节所述 Hadamard 等价所形成的等价类。由于我们关注的是对 QT 序列进行穷举搜索，并将结果按等价关系归类，因此采用这些等价操作，便可在不失一般性的前提下有效缩小搜索空间。每种操作都作用于一个 QT 序列四元组（$A$，$B$，$C$，$D$），并生成另一个 QT 序列四元组。

### QT 等价操作

- NS：（取反并交换）将 $A$、$B$、$C$、$D$ 中的一个序列取反，并交换 $A$、$B$、$C$、$D$ 中的一对序列。
- AN：（交替取反）当长度 $n$ 为偶数时，同时将 $A$、$B$、$C$和 $D$ 中每隔一个元素乘以 $-1$ 。
- DE：（抽取）同时对序列 $A$、$B$、$C$和 $D$ 的下标应用循环群 $C_n$ 的一个自同构。
- CS：（循环移位）同时对 $A$、$B$、$C$和 $D$中的所有元素进行任意量的循环移位。
- DH：（双半移位）当长度 $n$ 为偶数时，将 $A$、$B$、$C$ 和 $D$ 中任意两个的各项移位 $n/2$ 。

如果两个 QT 序列四元组在这些操作下等价，我们就称它们为*QT* 等价。为方便起见，我们还定义了以下两种额外的等价操作。它们都可以通过两次 NS 操作推导得出。

- 双重取反：对 $A$、 $B$、 $C$ 或 $D$ 中的两个序列取反。
- 双重交换：交换 $A$、 $B$、 $C$、 $D$ 中的两对。

NS 等价操作保持自相关条件，因为对于所有 $t$，$R_X(t) = R_{-X}(t)$；它也保持互相关条件，因为执行单次取反与执行单次交换的作用，都是在以如下形式书写时，将三个互相关条件中的每一个条件的一侧取反（交换还会使其中两个条件彼此置换）：

$$\begin{aligned} R_{A,B}(t) - R_{B,A}(t) &= R_{D,C}(t) - R_{C,D}(t), \\ R_{A,C}(t) - R_{C,A}(t) &= R_{B,D}(t) - R_{D,B}(t), \\ R_{A,D}(t) - R_{D,A}(t) &= R_{C,B}(t) - R_{B,C}(t). \end{aligned}$$

因此，NS 操作保持互相关条件。DE、AN 以及两种移位操作都众所周知会保持自相关值之和 [29]，也会保持互相关值之和。例如，若 $(-1) * X$ 表示对 $X$ 交替取反，则对于偶数长度序列，$R_{(-1)*A,\ (-1)*B}(t) = (-1)^t R_{A,\ B}(t)$；若 $s(X)$表示将 $X$ 循环移位 1 位，则 $R_{s(A),\ s(B)}(t) = R_{A,\ B}(t)$，并且

$$R_{s^{n/2}(A),B}(t) = R_{A,s^{n/2}(B)}(t) = R_{A,B}(t \pm n/2)$$

当 $n$为偶数时。序列反转也可以视为一种等价操作，但在这种情况下，可以先使用自同构 $x \mapsto -x$ 执行 DE，再向左循环移位来实现。

请注意，上述等价操作没有 利用定理 9 提供的 QT 序列与 Williamson 型序列之间的一一对应关系。结合定理 9，我们可以用单取反操作和单交换操作取代取反并交换操作，并用单半移位取代双半移位：

- 单重取反：（单重取反）对 $A$、 $B$、 $C$ 或 $D$ 中的一个序列取反。

- SS：（单次交换）交换 $A$、 $B$、 $C$、 $D$ 中的一对。
- SH：（单半移位）当 $n$ 为偶数时，将• 、 $A$、 $B$、 $C$之一的各项移位 $n/2$。

这是因为 SN、SS 和 SH 操作保持 Williamson 型序列满足的两两互补条件 $R_{X,\ Y}(t) = R_{Y,\ X}(t)$。因此，如果两个四元组在将 NS 操作替换为 SN 和 SS 、将 DH 操作替换为 SH 后，依据 QT 等价操作彼此等价，我们就称它们为*Williamson* 型等价。

我们以不同于 Williamson 型等价的方式定义 QT 等价，主要是因为 QT 等价与阿达玛等价的关联更紧密——定理 10 表明，QT 等价蕴含阿达玛等价，因此，要在阿达玛等价意义下枚举所有 QT 序列，可以先在 QT 等价意义下枚举所有序列，再按阿达玛等价进行筛选。另一方面，Williamson 型等价通常不蕴含阿达玛等价。因此，在 Williamson 型等价意义下枚举 QT 序列，并不能保证得到在阿达玛等价意义下的 QT 序列枚举。为简单起见，我们提出的算法将按 Williamson 型等价枚举 QT 序列；不过，我们会在第 3.4 节介绍如何同时确保在 QT 等价和阿达玛等价意义下进行完整枚举。

**定理 10.** 彼此 *QT* 等价的 *QT* 序列也彼此 *Hadamard* 等价。

证明. 我们需要证明，每种等价操作 NS、AN、DE、CS 和 DH 都保持 Hadamard 等价。Barrera Acevedo 、 Catháin 和 Dietrich 已证明，若两个 QT 序列在 NS 等价下等价，则它们在 Hadamard 等价下也等价 [6, 命题 4.4(a,b)], ，因此还需考察其余四种操作。对于每种操作，我们都证明，将该操作应用于一个四元组 QT 序列后得到的新四元组与原四元组 Hadamard 等价。为此，我们证明每种等价操作（将其视为作用于四元数型阿达玛矩阵的操作）都可以由对行或列取负以及置换行或列这些操作构成。

对于 AN 操作，假设 $n$ 为偶数。考虑对一个具有循环块的四元数型 Hadamard 矩阵的每隔一行和每隔一列取负

的操作。由于 $n$ 为偶数，所得的 Hadamard 矩阵仍具有循环块，并且每个循环块的定义序列都经过了 AN 操作。因此，对一个 QT 序列四元组应用 AN 操作会得到一个 Hadamard 等价四元组。

DE 操作将同一个置换 $\phi$ 作用于 $\{0,\ldots,n-1\}$，对四元组中所有项的指标进行置换。考虑这样一种操作：用 $\phi$ 对四元数型 Hadamard 矩阵的循环块中指标为 $[0,n)$、$[n,2n)$、$[2n,3n)$ 和 $[3n,4n)$ 的列与行同时进行置换。（此处必须将 $\phi$ 扩展为作用于 $\{0,\ldots,4n-1\}$，例如通过 $\phi(i) = \phi(i-n) + n$ 来实现$n \le i < 4n$。）由于每个循环块的行和列都应用了相同的置换，所得 Hadamard 矩阵仍然具有循环块（但其定义序列已被 $\phi$ 置换，因此也对其应用了 DE 操作）。因此，将 DE 操作应用于 QT 序列四元组会得到一个 Hadamard 等价四元组。

移位量为 $c$ 的 CS 操作会对四元组中所有元素的索引应用 $s^c(i) = (i+c) \bmod n$。考虑使用 $s^c$ 对一个具有循环块的四元数型 Hadamard 矩阵中索引为 $[0,n)$、$[n,2n)$、$[2n,3n)$ 和 $[3n,4n)$ 的列进行循环移位。由于对循环矩阵的列进行循环移位会得到另一个循环矩阵，因此所得 Hadamard 矩阵仍具有循环块，且这些块的定义序列经过了 CS 操作。因此，对 QT 序列四元组应用 CS 操作会得到一个 Hadamard 等价四元组。

DH 操作对一组 QT 序列四元组中的两个序列施加 $s^{n/2}$ 的半移位（不失一般性，假设 DH 操作施加于四元组中的前两个序列）。若 $X$ 是一个循环矩阵，则用$X'$ 表示将 $X$ 的列循环移位 $n/2$的偏移量后所得的矩阵。若 $A$、$B$、$C$ 和$D$ 表示一个四元数型 Hadamard 矩阵的循环块，在对索引为 $[0,n)$ 和 $[n,2n)$ 的列应用 $s^{n/2}$ 后，所得的 Hadamard 矩阵形式如下

$$\begin{bmatrix} A' & B' & C & D \\ -B' & A' & -D & C \\ -C' & D' & A & -B \\ -D' & -C' & B & A \end{bmatrix}.$$

现在，对索引为 $[2n, 3n)$ 和 $[3n, 4n)$ 的行应用 $s^{n/2}$，我们得到

$$\begin{bmatrix} A' & B' & C & D \\ -B' & A' & -D & C \\ -C & D & A' & -B' \\ -D & -C & B' & A' \end{bmatrix}$$

这是通过对对应于（$A$、$B$、$C$、$D$）的 QT 四元组应用 DH 而生成的 Hadamard 矩阵。 □

# 3 QT序列的穷举搜索

本节首先介绍此前针对完美四元数序列、QT序列及相关问题所开展的穷举搜索工作（见第 3.1 节）。随后，我们将在第 3.2 节介绍用于将 QT序列搜索扩展到更长长度的算法，并在第 3.3 节说明该算法的实现与优化。枚举完成后，我们会对结果进行后处理，删除在 QT、Williamson型以及 Hadamard 等价意义下等价的 QT 序列（见第 3.4 节）。最后，我们将在第3.5节总结枚举所得结果。

## 3.1 先前工作

2010 年，Kuznetsov [27]研究了 $\mathcal{Q}_{24}$ 上的完美序列，并搜索了与形如以下形式的序列等价的完美 $\mathcal{Q}_{24}$-序列

$$[z, 1, \mathbf{j}, x_0, x_1 \ldots, x_t, x_t, \ldots, x_1, x_0, \mathbf{j}, 1]$$

其中 $z \in \mathcal{Q}_{24}$和 $x_0$，…， $x_t \in \mathcal{Q}_8$。请注意，这类序列是对称的，这一假设使 Kuznetsov 能够使用台式计算机进行搜索，在未明确说明的时间内找到长度为 23 的序列。他发现了长度为 5、7、9、11、13、17、19 和 23 的序列，并利用这些序列构造了一个长度超过 50 亿的完美 $\mathcal{Q}_{24}$-序列。2012 年，Barrera Acevedo 和 Hall [5] 构造了字母表为 $\{\pm 1, \pm \mathbf{i}, \mathbf{j}\}$ 的完美序列，其长度均为 $q+1$ 的形式，其中 $q \equiv 1$ （模 4），且 $q$ 为素数幂。2017 年，Blake [8]对字母表为 $\mathcal{Q}_8$的完美序列进行了广泛搜索。

2019年，Barrera Acevedo、Catháin 和 Dietrich [6]进行了一项穷举搜索，以寻找素数阶 $p \leq 13$的余循环哈达玛矩阵。其中一部分

结果直接包含 QT 序列，不过他们的搜索还包括其他类型的四元组，这些四元组与 QT 序列不同。他们的算法枚举四个序列中其中三个序列的所有可能性，然后利用前面三个序列生成第四个序列的所有可能性。

同样在2019年，Bright、Kotsireas 和 Ganesh 对威廉姆森序列进行了搜索。他们的算法将四个序列分成两对，枚举这两对的所有可能情况，然后将两对的枚举结果组合起来，生成所有威廉姆森序列四元组。我们对该算法进行了调整，使其适用于 QT 序列，并证明这种方法比先枚举四个序列中任意三个序列的所有可能情况更高效。

## 3.2 QT 序列的枚举算法

我们希望搜索一组满足 QT 序列自相关和互相关条件的四个二进制序列。我们所提出的算法（下文的算法 1）的第一步是考察这些序列的“行和”。对于一个二进制序列 $A = [a_0, \ldots, a_{n-1}]$，我们将 $r_A := \sum_{i=0}^{n-1} a_i$ 定义为 $A$的行和。下面的引理是经典结果（参见 [43, 式 15]）。

**引理11** (行和分解)。若 $A$、$B$、$C$、$D$ 是长度为 $n$ 的四元组 *QT* 序列，则

$$r_A^2 + r_B^2 + r_C^2 + r_D^2 = 4n\,.$$

这个引理意味着，对于给定的长度 $n$，我们可以将搜索范围限定为行和满足 $4n$ 的特定行和分解的序列。我们计算 $4n$ 作为四个整数平方之和的所有可能分解，并针对每种可能的分解枚举 QT 序列。

算法的下一步是选取一种分解方式，并将四个序列分成两对。每一对都可用于检验它们整体上是否满足所需条件中的相应部分。例如，对于所有移位 $t \neq 0$，第一对序列的自相关之和必须与第二对序列的自相关之和互为相反数（因为两者相加必须为零）。我们也可以将这种思路应用于互相关条件：一旦已知第一对（例如 $(A,\ B)$），定理 9 就意味着，对于所有 $t$，$R_{A,\,B}(t) = R_{B,\,A}(t)$。因此，如果对于某个 $t$，$R_{A,\,B}(t) \neq R_{B,\,A}(t)$，那么配对 $(A,\ B)$ 就不可能是 QT 序列的一部分，可以将其忽略。

因此，我们枚举行和为 $(r_A,\ r_B)$ 的序列配对，并单独枚举行和为 $(r_C,\ r_D)$ 的序列配对，计算它们的自相关与互相关，然后检查第一轮和第二轮枚举中是否存在这样的序列配对：其自相关恰好相互抵消，且互相关在交换后保持不变。如果存在这样的配对，我们就找到了满足 (2.1) 和 (2.2) 的二进制序列四元组，因此也得到一个可能的 QT 序列四元组。为确保这四个序列确实构成一个 QT 序列四元组，我们还需要检查它们是否满足另外两个互相关条件 (2.3) 和 (2.4)。

该算法的伪代码见算法 1。直观而言，该算法之所以比枚举 QT 序列三元组更快，是因为枚举行和为 $(r_A,\ r_B)$ 和 $(r_C,\ r_D)$ 的配对，比枚举行和为 $(r_A,\ r_B,\ r_C)$ 的三元组更快。此外，按照第 3.3 节所述的方法进行高效实现时，在相关值中查找匹配项的步骤（第 8 步）在实践中很快。为缩小搜索空间并提高效率，算法 1 仅通过采用 $4n$ 的某些四平方和分解来枚举 Williamson 型等价下的 QT 序列；这些分解可在不失一般性的前提下假定成立（其理由见命题 13）。尽管算法 1 保证能枚举给定阶数下 Williamson 型等价意义下的所有 QT 序列，但通常会在同一等价类中生成多个四元组。因此，运行算法 1 后，我们会执行一个后处理步骤（见第 3.4 节），以去除等价意义下的重复序列。

## 3.3 实现与优化

加快 QT 序列搜索速度的一项最重要优化，是快速排除不符合要求的序列。一种广为人知、能够筛除许多序列的“过滤”技术，基于第 2.4 节定义的离散傅里叶变换（DFT）。命题 6 指出，如果 $(A, B, C, D)$ 是长度为 $n$ 的 QT 序列四元组，那么

$$\mathrm{PSD}_A(t) + \mathrm{PSD}_B(t) + \mathrm{PSD}_C(t) + \mathrm{PSD}_D(t) = 4n \quad \text{for all } t \in \mathbb{Z}.$$

Williamson [43, eq. 14]，已经使用过这一性质，只是将其写成 $\mathrm{DFT}_A(t)^2 + \mathrm{DFT}_B(t)^2 + \mathrm{DFT}_C(t)^2 + \mathrm{DFT}_D(t)^2 = 4n$，因为

**算法 1** 枚举给定阶数 $n$ 的 QT 序列的算法
在 Williamson 型等价意义下。

$\mathcal{L} := \emptyset$ // 用于存放找到的 QT 序列的集合
// 将 $4n$ 分解为四个非负整数平方之和
$\mathcal{D} := \{(w,\ x,\ y,\ z) \in \mathbb{N}^4 :\ w^2 + x^2 + y^2 + z^2 = 4n$ 和 $w \geq x \geq y \geq z\}$
**对于** $(w,\ x,\ y,\ z) \in \mathcal{D}$ **执行**
    构造 $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$，即行和为
    分别等于 $w, x, y, z$ 的二进制序列集合
    $\mathcal{L}_1 := \mathcal{W} \times \mathcal{Z}$ 和 $\mathcal{L}_2 := \mathcal{X} \times \mathcal{Y}$
    // 计算 $\mathcal{L}_1$ 中每个候选对的自相关
    计算所有满足条件的 $(W,\ Z)$ 的 $[R_W(t) + R_Z(t) :\ 1 \leq t \leq n/2]$
    $R_{W,\ Z}(t) = R_{Z,\ W}(t)$，针对所有 $1 \leq t \leq n/2$ 并存储到列表 $C_1$
    // 计算 $\mathcal{L}_2$ 中每个候选对的取负自相关
    对所有满足 $\in \mathcal{L}_2$ 的 $(X, Y)$，计算 $[-R_X(t) - R_Y(t) :\ 1 \leq t \leq n/2]$
    $R_{X,Y}(t) = R_{Y,X}(t)$，对所有 $1 \leq t \leq n/2$ 进行计算，并存入列表 $C_2$
    // $C_1$ 和 $C_2$ 中的匹配向量给出了 (2.1) 和 (2.4) 的解
    **对于** $C_1$ 和 $C_2$ 中都出现的每个值列表 $v$，**执行**
        获取集合 $\mathcal{S}$，其中包含在两者中生成 $v$ 的所有序列四元组
        列表 $C_1$ 和 $C_2$
        **对于**每个四元组 $(W, X, Y, Z)$，在 $\mathcal{S}$ **中执行**
            **如果**$(W, X, Y, Z)$ 是一个四元组 QT 序列，**则**
                将 $(W, X, Y, Z)$ 添加到 $\mathcal{L}$
            **结束 if**
        **结束 for**
    **结束循环**
**结束循环**
**返回** $\mathcal{L}$

Williamson 假设序列具有对称性（并且如果 $X$ 是共轭对称的，则 $\mathrm{PSD}_X(t)$ ＝离散傅里叶变换$_X(t)^2$）。

**推论 12.** 如果 $(A, B, C, D)$ 是长度为 $n$ 的四元组 *QT* 序列，那么

$$\mathrm{PSD}_A(t) + \mathrm{PSD}_B(t) \leq 4n \ \textit{and} \ \mathrm{PSD}_C(t) + \mathrm{PSD}_D(t) \leq 4n.$$

证明。 由命题 6 可得，因为功率谱密度值非负。 □

推论 12 被用作算法 1 第 5 步中的筛选条件；如果任意一对的功率谱密度值之和大于 $4n$ ，则不会将其纳入 $\mathcal{L}_1$ 或 $\mathcal{L}_2$。同样，在第 4 步中，任何功率谱密度值大于 $4n$ 的序列都不会纳入 $\mathcal{W}$、 $\mathcal{X}$、 $\mathcal{Y}$ 或 $\mathcal{Z}$。在我们的实现中，功率谱密度值是使用 FFTW [18] 计算的。

对于第 2 步，可以通过蛮力法找出将 $4n$ 分解为四个整数平方之和的所有分解，但并非所有分解都是必要的。一种直接的优化是只考虑分解 $(w, x, y, z)$，其中 $w$、 $x$、 $y$ 和 $z$ 的奇偶性与 $n$ 的奇偶性相同，因为如果 $X \in \{\pm 1\}^n$ ，那么 $r_X \equiv n$ (模 2)。下面的命题说明了为何只考虑按顺序排列的非负分解就足够了。

**命题 13**。每个四元组 *QT* 序列都 *Williamson* 型等价于一个行和具有如下形式的四元组 $(w, x, y, z)$ 其中$w \geq x \geq y \geq z \geq 0$。

证明。 通过应用 SN 操作，每个 QT 序列都可以变为与一个所有行和均为非负数的序列等价。随后应用 SS 操作，可以按降序排列这些行和，同时保持其非负性。因此，每个 QT 序列都等价于一个行和非负且按降序排列的序列。 □

下面的命题给出了命题 13 的一个变体，但采用的是 QT 等价，而非 Williamson 型等价。

**命题 14**。 每个四元组 *QT* 序列都 *QT* 等价于一个行和形如 $(\pm w, x, y, z)$ 的四元组，其中 $w \geq x \geq y \geq z \geq 0$。此外，如果 $w = x$、 $x = y$、 $y = z$ 或 $z = 0$，则还可以将第一个行和的符号取为正。

证明。 通过应用适当的双重取反和双重交换操作，每个 QT 序列都可以变换为一个序列，使其后三个行和均为非负数，并按递减顺序排列，且第一个行和的绝对值为最大或次大。通过应用 NS 操作，还可以按绝对值对前两个行和进行排序（如有必要，只需交换前两个序列，然后将其取反），因此任何 QT 序列都等价于一个具有如下行和分解的序列：$(\pm w, x, y, z)$，其中$w \geq x \geq y \geq z \geq 0$。此外，在 $z = 0$ 的情况下，可以应用双重取反操作，使第一个行和为正，同时保持行和的排序顺序（将第一个和最后一个序列取反）。类似地，如果 $\{w, x, y, z\}$ 中至少有两个值相等，则可以应用 NS 操作，使第一个行和为正，同时保持行和的排序顺序（先将第一个序列取反，然后交换行和相等的序列）。因此，如果 $z = 0$ 或 $w = x$ 或 $x = y$ 或 $y = z$，则可以避免分解 $(-w, x, y, z)$。

□

如果想修改算法 1，使其枚举模 QT 等价的 QT 序列（而非模 Williamson 型等价的序列），一种高效的方法是修改步骤 12：将 $(W, X, Y, Z)$ 添加到 $\mathcal{L}$ 后，再将 $(-W, X, Y, Z)$ 添加到 $\mathcal{L}$；不过，仅当 $z \neq 0$, $z \neq y$, $y \neq x$ 和 $x \neq w$ 时才需要这样做。命题 14 保证，在 $w = x$ 或 $x = y$ 或 $y = z$ 或 $z = 0$ 的情况下，算法 1 会生成模 QT 等价的所有 QT 序列。

对于步骤 5，我们选择生成配对，使最大和最小的行和 $w$ 和 $z$ 属于同一配对。我们尝试了所有可能的配对组合，发现这种方法效率最高。

根据定理 9，所有 QT 序列都满足 $R_{X,Y}(t) = R_{Y,X}(t)$ 和 $R_{W,Z}(t) = R_{Z,W}(t)$，因此在步骤 6 和 7 中不会考虑任何不满足这些相容条件的配对。此筛选大幅减少了添加到列表 $C_1$ 和 $C_2$中的配对数量。例如，对于长度 20，不使用此筛选会生成超过 160 亿个配对，而使用后仅生成 625,896 个——配对数量减少了约 26,000 倍。

对于步骤 6 和 7，无需考虑 $t = 0$ 处的相关值，原因是 $t = 0$ 处的自相关等于该序列的行和（构造时已固定），而对于实数序列，互相关差 $R_{X,\,Y}(0) - R_{Y,\,X}(0)$ 始终为零$X$ 和 $Y$。同样，无需考虑 $n/2 < t < n$ 处相关值的原因在于对称性 $R_X(t) = R_X(n - t)$ 以及

$R_{X,\ Y}(t) = R_{Y,\ X}(n-t)$ 对于实数序列 $X$ 和 $Y$。

对于步骤 6 和 7，我们将一对序列生成的自相关值列表存储为文件中的一行，并在行末存储用于生成这些值的序列索引。这样，即使文件中的各行经过重新排列，我们也能快速确定每行相关值是由哪一对序列生成的。

为了高效实现步骤 8，我们按字典序对包含相关值的文件中的各行进行排序。这样，我们就能通过线性扫描同时遍历这些文件，高效地找出包含列表 $C_1$ 的文件和包含列表 $C_2$ 的文件中所有匹配的相关值。我们检查所有匹配项，并保留满足三个互相关条件的项。

使用直接方法计算步骤 6 和 7 中的相关向量，需要进行 $O(n^2)$ 次算术运算。一种优化方法是匹配功率谱密度值，而不是匹配相关值。也就是说，不再寻找满足以下条件的匹配项

$$[R_W(t) + R_Z(t) : 1 \le t \le n/2] = [-R_X(t) - R_Y(t) : 1 \le t \le n/2],$$

根据命题 6，只需找出满足以下条件的匹配

$$[\mathrm{PSD}_W(t) + \mathrm{PSD}_Z(t) : 1 \le t \le n/2] = [4n - \mathrm{PSD}_X(t) - \mathrm{PSD}_Y(t) : 1 \le t \le n/2].$$

功率谱密度值已在第 4 步所使用的滤波过程中计算完成，因此可以将这些值缓存起来，无需重新计算。一般来说，功率谱密度值为实数而非整数，因此，为了将 $\mathrm{PSD}_W(t) + \mathrm{PSD}_Z(t)$ 和 $4n - \mathrm{PSD}_X(t) - \mathrm{PSD}_Y(t)$ 的值写入文件，我们会将其四舍五入到最近的整数。这可能会引入虚假匹配，这是其缺点。不过，在实践中这并不是问题；一旦找到匹配，就可以轻松检查式 (2.1) 是否成立。

类似地，在第 6 步和第 7 步中，无需验证条件 $R_{W,Z}(t) = R_{Z,W}(t)$ 以及 $R_{X,Y}(t) = R_{Y,X}(t)$，只需在频域中操作并改为验证

$$\mathrm{CPSD}_{W,Z}(t) = \mathrm{CPSD}_{Z,W}(t) \quad \text{and} \quad \mathrm{CPSD}_{X,Y}(t) = \mathrm{CPSD}_{Y,X}(t).$$

这很有益，因为通过缓存 $1 \le t \le n/2$ 的 $\mathrm{DFT}_W(t)$、$\mathrm{DFT}_X(t)$、$\mathrm{DFT}_Y(t)$、$\mathrm{DFT}_Z(t)$，可以优化互功率谱密度值的计算

在第 4 步中。为了考虑浮点舍入误差，我们筛选出满足存在某个 $t$ 使得以下条件成立的配对 ($W$、 $Z$)

$$|\mathrm{CPSD}_{W,Z}(t) - \mathrm{CPSD}_{Z,W}(t)| > 10^{-4},$$

因为 FFTW 计算互功率谱密度值的精度将比 $10^{-4}$ 高出许多个数量级。$\mathrm{CPSD}_{W,Z}(t) - \mathrm{CPSD}_{Z,W}(t)$ 值没有实部，因为它们的形式为 $ab^* - ba^*$，其中复数 $a, b$；正如第 2.4 节所述，这类数没有实部。

## 3.4 等价过滤

使用算法 1 枚举长度为 $n$ 的所有 QT 序列后，我们按照阿达玛等价（如第 2.2 节所述），以及 QT 等价和 Williamson 型等价（如第 2.5 节所述）对这些序列进行分类。算法 1 将生成行和具有命题 13 所给形式的长度为 $n$ 的所有 QT 序列。由于命题 13 仅利用 SS 和 SN 操作证明，算法 1 将从每个 Williamson 型等价类中至少生成一个四元组 QT 序列。不过，如果我们还想按阿达玛等价枚举 QT 序列，就需要改为按 QT 等价进行枚举，因为这样定理 10 能保证列表在阿达玛等价意义下是完备的。第 3.3 节将介绍如何修改算法 1，以按 QT 等价枚举序列（参见命题 14 后的说明）。现在，我们来说明如何过滤掉按 QT 等价视为重复的序列。

作为等价过滤过程的第一步，我们对算法 1 的输出进行筛选，确保每个 NS 等价类恰好保留一个“规范”代表元。一个等价类的规范代表元，是将四元组 QT 序列中的序列连接起来后，按字典序排列得到的最小四元组。为了找到字典序最小值，我们首先使用 NS 操作，使四元组中每个序列的首项都为 $-1$。接着，使用 DS 操作，使字典序最小的序列位于四元组的首位，字典序第二小的序列位于第二位。如果此时所有序列已按字典序升序排列，那么该四元组 QT 序列就是规范的。否则，最后两个序列的顺序颠倒。如果四元组中有两个相同的序列，那么我们使用 DS 操作交换这两个相同的序列，并交换第三和第四个

序列，从而使四元组中的序列按升序排列，并使四元组成为规范形式。如果四元组中没有两个相同的序列，我们就使用 NS 操作交换第三和第四个序列，最后将第四个序列取反，使四元组成为规范形式。

通过上述过程，我们计算算法 1 找到的每个四元组 QT 序列的规范代表元，并丢弃规范形式之前已经出现过的四元组，从而得到按 NS 等价分类的 QT 序列完整列表。现在，我们希望根据第 2.5 节中的 QT 等价进一步筛选此列表。为此，我们改编了 Lumsden、Kotsireas 和 Bright [29, 算法 7]所描述的筛选算法。首先，考虑由 AN、DE、CS 和 DH 操作生成的对称群 $S$ （令 $\varphi$ 表示欧拉函数，当 $n$为偶数且不能被 4 整除时，该群的大小为$2^6 n\varphi(n)$；当 $n$ 能被 4 整除时，大小为 $2^4 n\varphi(n)$；当 $n$ 为奇数时，大小为 $n\varphi(n)$）。为了找到四元组 QT 序列 $(W, X, Y, Z)$ 的字典序最小代表元，我们将 $S$中的所有操作应用于 $(W, X, Y, Z)$，从而形成 $|S|$ 个 QT 序列，并使用上述排序过程，通过 NS 操作将每个 QT 序列按字典序最小化。这些$|S|$ 个序列的全局字典序最小值，便成为由 NS,AN、 DE、 CS、 DH}操作生成的等价类的最小代表元。

我们还会对列表进行筛选，使其在 Hadamard 等价意义下去重。根据定理 10，我们知道，上述筛选得到的列表至少包含每个 Hadamard 等价类中的一个代表元。不过，可能还需要进一步筛选，以去除 Hadamard 等价意义下的重复项。从按 QT 等价去重后的四元组完整列表出发，我们将每个四元组 QT 序列转换为一个 Hadamard 矩阵，并按照 McKay [30]所述，将该矩阵化为其图表示。然后，我们使用程序 nauty [31] 将每个图转换为规范形式。两个图具有相同的规范形式，当且仅当它们同构，因此我们会筛除所有会生成图表示且其规范形式此前已出现过的 QT 序列。

上述按 QT 等价进行筛选的过程也可用于按 Williamson型等价进行筛选，只需将单重交换（SS）和单重取反（SN）操作用于替代取反并交换（NS）操作，并类似地使用单半移位（SH）替代双半移位（DS）。在这种情况下，通过{SS、SN} 操作得到的规范代表元，其每个序列始终按字典序降序排列，且每个序列的首项均为 $-1$。

在实践中，为了将 QT 序列枚举到每一种 Williamson型

等价、QT 等价和 Hadamard 等价，我们按如下方式进行。

1. 使用算法 1 枚举 Williamson 型等价下的序列，并将其放入列表中。
2. 根据 Williamson 型等价筛选列表，移除在等价意义下重复的四元组。
3. 对于列表中的每个 $(W, X, Y, Z)$，将 $(-W, X, Y, Z)$ 加入列表。随后，如果 $n$ 为偶数，则对列表中的每个 $(W, X, Y, Z)$，将 $(s^{n/2}(W)\ X, Y, Z)$ 加入列表。4. 按 QT 等价筛选列表。该列表在 QT 等价意义下是完备的，因为每个 NS 等价类在 {SS、SN} 等价下至多分裂为两个等价类；若确实分裂，则 $(W, X, Y, Z)$ 和 $(-W, X, Y, Z)$ 将属于不同的等价类。同理，每个 DH 等价类在 SH 等价下至多分裂为两个等价类；若确实分裂，则 $(W, X, Y, Z)$ 和 $(s^{n/2}(W)\ X, Y, Z)$ 将属于不同的等价类。

5. 将列表筛选至 Hadamard 等价类。

## 3.5 结果

我们使用 Rust 1.91.0 和 Bash shell 脚本实现了该算法。该算法在一台配备 AMD EPYC 处理器、运行频率为 2.7 GHz 且配置为使用不超过 4 GiB RAM 的机器上运行。排序使用 GNU sort 实用程序完成。该算法的代码和结果可在 https://github.com/colinotp/quaternion-sequences 找到。算法得到的结果摘要见表 1。

在附录中，我们给出了通过我们的实现找到的长度为 $n \leq 21$的全部 124 组 QT 序列（按 Williamson 型等价计）的完整枚举。结合 Holzmann、Kharaghani 和 Tayfeh-Rezaie [25] 以及 Bright、Kotsireas 和 Ganesh [10] 的枚举，对于长度为$n \leq 60$的所有 Williamson 序列（即 对称 QT 序列）集合，其结果已为人所知。此前已确定，按 Williamson 型等价计，长度为 $n \leq 21$ 的 Williamson 序列恰有 94 组，我们的搜索证实了这一数量。此外，搜索还确定，对于长度为 $n \leq 21$ ，另有 30 组 QT 序列不与 Williamson 等价

表 1：算法 1 按长度 $n$ 得出的结果。 $W_{\mathrm{equ}}$、 $Q_{\mathrm{equ}}$ 和 $H_{\mathrm{equ}}$分别表示按 Williamson型、QT 和 Hadamard 等价分类后找到的 QT 序列总数。“时间”是枚举运行时间总秒数，“配对”是在步骤 5 中生成的配对总数（生成配对是该算法的瓶颈），而“空间”是所用磁盘空间，以兆二进制字节为单位。

| $n$ | $W_{\mathrm{equ}}$ | $Q_{\mathrm{equ}}$ | $H_{\mathrm{equ}}$ | 时间（秒） | 配对 | 空间 |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0.16 | 2 | 0.0 |
| 2 | 1 | 1 | 1 | 0.08 | 4 | 0.0 |
| 3 | 1 | 1 | 1 | 0.08 | 6 | 0.0 |
| 4 | 2 | 3 | 2 | 0.19 | 46 | 0.0 |
| 5 | 1 | 1 | 1 | 0.08 | 20 | 0.0 |
| 6 | 1 | 1 | 1 | 0.16 | 48 | 0.0 |
| 7 | 2 | 3 | 3 | 0.15 | 182 | 0.0 |
| 8 | 3 | 4 | 3 | 0.08 | 384 | 0.0 |
| 9 | 4 | 7 | 7 | 0.31 | 999 | 0.0 |
| 10 | 2 | 4 | 2 | 0.23 | 770 | 0.0 |
| 11 | 1 | 2 | 2 | 0.15 | 715 | 0.0 |
| 12 | 5 | 10 | 6 | 0.80 | 6288 | 0.2 |
| 13 | 4 | 6 | 6 | 3.14 | 8216 | 0.4 |
| 14 | 5 | 12 | 10 | 3.15 | 5334 | 0.3 |
| 15 | 4 | 7 | 7 | 23.46 | 15732 | 1.0 |
| 16 | 18 | 44 | 19 | 121.20 | 206480 | 7.9 |
| 17 | 4 | 5 | 5 | 361.36 | 39372 | 3.6 |
| 18 | 28 | 88 | 82 | 2001.79 | 275184 | 17.5 |
| 19 | 6 | 11 | 11 | 7753.85 | 200526 | 22.0 |
| 20 | 24 | 84 | 54 | 17632.48 | 625896 | 46.1 |
| 21 | 7 | 13 | 13 | 141267.63 | 561519 | 86.1 |

序列，因为它们仅与非对称序列集等价。

有趣的是，Fitzpatrick 和 O'Keeffe [16] 证明，对于某些奇数长度 $n$（当 $n$ 为素数，或具有如下形式时： $n = pq$ ，其中$p$ 和 $q$ 是互异的奇素数，且各自都是另一个的生成元），长度为 $n$ 的所有 Williamson 型序列集都必定与某个对称序列集 Williamson 型等价。对于 $n \leq 21$，他们的定理未涵盖的奇数长度只有 $n = 9$ 和 $n = 21 = 3 \cdot 7$ （因为 7 不是模 3 的生成元）。我们的搜索表明，他们的定理对 $n = 21$也成立，因为我们没有找到长度为 21 的非对称 QT 序列。对于 $n = 9$，存在一个非对称 QT 序列集；Fitzpatrick 和 O'Keeffe 早已知道一个例子，而我们的枚举显示，在 Williamson 型等价意义下，这是长度为 9 的非对称 QT 序列集中唯一的一个。目前，这是已知的唯一一个奇数长度 Williamson 型序列集，它不与某个对称序列集等价；不过，我们找到了 29 个偶数长度 Williamson 型序列集的例子，它们不与任何对称序列集等价。

Fitzpatrick 和 O'Keeffe 的结果，结合 Baumert 和 Hall [7] 对长度为 $n = 23$ 的威廉姆森序列进行穷举搜索的结果，表明在威廉姆森型等价意义下，长度为 23 的 QT 序列恰好存在一组。我们发现，这组序列生成了两组在 QT 等价和阿达玛等价意义下互不等价的 QT 序列。

# 4 四元数阿达玛矩阵的构造

完美序列与哈达玛矩阵之间存在直接对应关系。正如第 1.3 节所述，这类矩阵在通信和信息论中备受关注。这进一步促使我们深入研究四元数 Hadamard 矩阵（QHMs）。第 3 节通过计算搜索发现的新序列，产生了新的四元数 Hadamard 矩阵。第 4.1 节给出了这类在量子通信中具有应用价值的矩阵示例。与实数和复数情形不同，这些矩阵可用于生成不可数多个（等价的）四元数 Hadamard 矩阵；参见第4.2节。第4.3节中，我们提出了一种刻画四元数 Hadamard 矩阵的方法，并以五阶矩阵为例加以说明。第 4.4 节中，我们正式证明

通过计算搜索完美序列得到的矩阵彼此非等价。

## 4.1 由完美序列构造阿达玛矩阵

完美四元数序列可以直接用于构造四元数 Hadamard 矩阵。给定一个长度为 $n$ 的此类序列 $S$，我们可以通过将矩阵的第一行设为序列 $S$，并将其余各行设为第一行依次循环移位后的结果，来构造一个 $n \times n$ 循环四元数哈达玛矩阵 $M$。形式上，我们定义 $M_{ij} \coloneqq S_{j-i}$，其中 $0 \le i,\ j < n$，并将指标按模 $n$ 计算。

如第3.5节所述，我们的计算搜索得到了许多在量子信息与通信领域具有研究价值的完美四元数序列。考虑由这些序列按上述方法构造的四元数 Hadamard 矩阵，以及与它们等价的归一化矩阵。（回顾一下，归一化是指通过等价操作将矩阵的第一行和第一列变换为全 1 的过程。）对于第3.5节所述搜索中的所有长度 $n$（其中 $3 < n \le 21$），我们都得到了含有非交换元素的标准化四元数Hadamard矩阵。

下面列出我们找到的几个矩阵示例。矩阵元素使用映射所给出的符号来表示

$$\left[\begin{array}{cccccccccccc} \texttt{+} & \texttt{-} & \texttt{i} & \texttt{j} & \texttt{k} & \texttt{q} & \texttt{x} & \texttt{y} & \texttt{z} & \texttt{s} & \texttt{u} & \texttt{v} & \texttt{w} \\ 1 & -1 & \mathbf{i} & \mathbf{j} & \mathbf{k} & q & q\mathbf{i} & q\mathbf{j} & q\mathbf{k} & q^* & q^*\mathbf{i} & q^*\mathbf{j} & q^*\mathbf{k} \end{array}\right], \tag{4.1}$$

大写字母表示与其对应的小写字母所代表的四元数互为相反数。例如，X 表示 $-q\mathbf{i}$。规范化

6、8、10 和 12 阶的四元数 Hadamard 矩阵由下式给出

$$\begin{bmatrix} + & + & + & + & + & + \\ + & s & Q & k & S & x \\ + & z & S & + & Q & U \\ + & - & + & - & + & - \\ + & S & Q & K & S & X \\ + & Z & S & - & Q & u \end{bmatrix}, \quad \begin{bmatrix} + & + & + & + & + & + & + & + \\ Y & I & q & - & y & i & Q & \\ + & I & - & i & + & I & - & i \\ + & q & i & Y & - & Q & I & y \\ + & - & + & - & + & - & + & - \\ + & y & I & Q & - & Y & i & q \\ + & i & - & I & + & i & - & I \\ + & Q & i & y & - & q & I & Y \end{bmatrix},$$

$$\begin{bmatrix} + & + & + & + & + & + & + & + & + & + \\ + & J & + & Y & U & - & j & - & y & u \\ + & Q & q & W & y & + & Q & q & W & y \\ + & w & J & Z & + & - & W & j & z & - \\ + & j & U & z & J & + & j & U & z & J \\ + & - & - & j & - & - & + & + & J & + \\ + & J & - & y & v & + & J & - & y & v \\ + & Y & y & V & q & - & y & Y & v & Q \\ + & S & J & Z & - & + & S & J & Z & - \\ + & j & v & z & J & - & J & V & Z & j \end{bmatrix},$$

$$\begin{bmatrix} + & + & + & + & + & + & + & + & + & + & + & + \\ W & Y & - & W & y & - & w & y & + & w & Y & \\ + & Y & W & - & y & w & + & Y & W & - & y & w \\ + & - & - & + & + & - & - & + & + & - & - & + \\ + & W & y & + & W & y & + & W & y & + & W & y \\ + & y & w & - & y & W & - & Y & W & + & Y & w \\ + & - & + & - & + & - & + & - & + & - & + & - \\ + & w & Y & + & W & Y & - & W & y & - & w & y \\ + & y & W & + & y & W & + & y & W & + & y & W \\ + & + & - & - & + & + & - & - & + & + & - & - \\ + & w & y & - & W & Y & + & w & y & - & W & Y \\ + & Y & w & + & & & y & w & - & y & & W & - & Y & W \end{bmatrix}.$$

这些矩阵可通过四元数的代数自同构生成无穷多个哈达玛矩阵族，详见第4.2节。它们也可用于刻画具有第4.3节所述相同元素排列模式的矩阵。然而，这样生成的矩阵未必涵盖给定阶数的所有四元数 Hadamard 矩阵。我们将在本节后文探讨这种可能性。

## 4.2 固定阶数的无限族

对于固定的实Hadamard 矩阵或复Hadamard矩阵 $M$，与 $M$ 等价的不同规范化矩阵只有有限个。

**引理15**。 设 $M$ 是一个实（或复）阿达玛矩阵。与 $M$ 等价的规范化实（分别为复）阿达玛矩阵的数量有限。

证明。 根据引理 1 及其后的注释，任何与 $M$等价的矩阵 $M'$ 都可写成 $D_1P_1MP_2D_2$，其中 $P_1$ 和 $P_2$ 是置换矩阵， $D_1$ 和 $D_2$ 是由实数或复数单位构成的对角矩阵。对于实矩阵，该引理显然成立，因为上述矩阵 $D_1$、$D_2$、 $P_1$和 $P_2$ 的数量有限。下面证明复矩阵的情形。

设 $M''\coloneqq P_1MP_2$。通过对 $M$ 的行和列进行置换，可以得到有限个这样的矩阵 $M''$。假设 $M''=(x_{ij}\colon 0\leq i,j<n)$。则对 $M''$进行归一化得到矩阵 $N''\coloneqq(x^*_{i0}x_{ij}x^*_{0j}\colon 0\leq i,j<n)$。

假设 $D_1=\mathrm{diag}(a)$ 且 $D_2=\mathrm{diag}(b)$。则 $M'=(a_ix_{ij}b_j\colon 0\leq i,j<n)$，而对 $M'$进行归一化得到矩阵 $N'\coloneqq(b^*_0x^*_{i0}x_{ij}x^*_{0j}a^*_0\colon 0\leq i,j<n)$。由于 $N'$的第一行全为 1，我们有 $b^*_0x^*_{00}a^*_0=1$，即 $b^*_0=a_0x_{00}$。因此 $N'=(a_0x_{00}x^*_{i0}x_{ij}x^*_{0j}a^*_0\colon 0\leq i,j<n)$。由于复数乘法是可交换的， $N'$的元素可化简为： $N'=(x_{00}x^*_{i0}x_{ij}x^*_{0j}\colon 0\leq i,j<n)=x_{00}N''$。由于互异矩阵 $M''$（因而 $N''$）的个数有限，且 $x_{00}$是 $M''$的一个元素，矩阵 $N'$的个数也是有限的。 □

我们现在证明，只要存在一个含有非实元素的 $n$ 阶归一化四元数 Hadamard 矩阵，就存在无穷不可数多个 $n$ 阶归一化四元数 Hadamard 矩阵。我们先刻画四元数自同构。任何此类自同构都对应于由基本单位四元数 {i、j、k} 张成的实向量空间上的一个正交变换（更具体地说，是一个旋转）。

**定理 16** （定理 2.4.4，第 17, [32]页）。四元数自同构群与三维特殊正交群 $\mathrm{SO}(3)$ 同构（即二维球面的旋转群）。

这意味着，对于任意一对范数相同的纯虚四元数 $a$， $b$ ，都存在一个自同构将 $a$ 映射到 $b$。这一性质有助于证明以下结论。

**命题 17**。 设 $G$ 是一个含有至少一个非实元素的 $n$ 阶归一化四元数 *Hadamard* 矩阵。存在无穷不可数多个与 $G$ 等价的 $n$ 阶归一化四元数 *Hadamard* 矩阵。

证明。 设 $\alpha+w$ 是 $G$ 的一个元素，其实部为 $\alpha$ ，且纯虚部非零，为 $w$。

令 $S$ 为所有与 $G$ 等价的标准化四元数Hadamard矩阵构成的集合。为反证，假设 $S$ 是可数的。令 $Q$ 为满足以下条件的四元数集合： $x$ ，其中 $x$ 是某个矩阵的一个元素

属于 $S$。集合 $Q$ 也是可数的。与 $w$ 范数相同的纯虚四元数构成一个半径为 $\|w\|$、位于张成空间 {**i**, **j**、**k**} 中的球面。因此，存在一个纯虚四元数 $y$，其 $\|y\| = \|w\|$ 不同于 $Q$ 中任意四元数的虚部。根据定理 16，存在一个自同构 $f$，将 $\mathbb{H}$ 映射到 $y$。根据命题 2，存在一个纯虚单位四元数 $a$，使得对每个 $x$，都有 $f(x) = a^* x a$。因此， $f(G)$ 是一个与 $G$ 等价的四元数 Hadamard 矩阵。根据构造，矩阵 $f(G)$ 有一个元素不属于 $Q$，所以 $f(G) \notin S$。这与假设矛盾，因此 $S$ 是不可数无限集。 □

因此，第 4.1 节所列的阿达玛矩阵导出了无穷多个（等价的）四元数 Hadamard 矩阵族。附录列出了与长度不超过 21 的非等价 QT 序列相对应的完美四元数序列。由我们通过计算搜索找到的完美序列导出的归一化四元数 Hadamard 矩阵通常含有非实元素，因此也会导出无穷多个四元数 Hadamard 矩阵等价类。正如第 4.1 节中的示例所示，归一化矩阵通常也含有非交换元素。这类四元数 Hadamard 矩阵可导出在量子通信理论中颇受关注的互 unbiased 测量 [15]。

## 4.3 五阶四元数 Hadamard 矩阵

Chterental 和 Đoković [12] 确定了所有四阶四元数 Hadamard 矩阵，并用两个参数化的四元数 Hadamard 矩阵族对其进行了刻画。他们将五阶四元数 Hadamard 矩阵的刻画作为一个开放问题提出。Higginbotham 和 Worley [24]通过研究一种特定类型的、具有循环核心的归一化五阶四元数 Hadamard 矩阵，在这一问题上取得了进展。归一化矩阵的核心 是通过删除其首行和首列得到的。

由于刻画所有 $5 \times 5$ 四元数 Hadamard 矩阵似乎颇具挑战，一个自然的做法是研究具有固定元素模式的矩阵。这种方法似乎可行，我们将通过一个例子加以说明。对该例子的分析最终将使我们能够证明（见第 4.4 节），由五阶 QT 序列的唯一一个（在 QT 等价意义下）四元组 QT 序列所产生的无限族四元数 Hadamard 矩阵并不等价于 Higginbotham 和 Worley [24]所研究的四元数 Hadamard 矩阵。

考虑四元数 Hadamard 矩阵 $5 \times 5$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & c\mathbf{j}+s\mathbf{i} & c\mathbf{j}-s\mathbf{i} & \mathbf{j} \\ 1 & c\mathbf{j}+s\mathbf{i} & -1 & \mathbf{j} & c\mathbf{j}-s\mathbf{i} \\ 1 & c\mathbf{j}-s\mathbf{i} & \mathbf{j} & -1 & c\mathbf{j}+s\mathbf{i} \\ 1 & \mathbf{j} & c\mathbf{j}-s\mathbf{i} & c\mathbf{j}+s\mathbf{i} & -1 \end{bmatrix} \tag{4.2}$$

其中 $c \coloneqq \cos\left(\frac{2\pi}{3}\right)$ 和 $s \coloneqq \sin\left(\frac{2\pi}{3}\right)$。这对应于 Tavakoli 等人 [37], 通过反同态映射的 $\mathbb{R}$-线性扩张所报告的由酉算子构成的 $5 \times 5$ Hadamard 矩阵

$$1 \leftrightarrow \mathrm{I}, \quad \mathbf{i} \leftrightarrow -\mathrm{i}\sigma_{\mathrm{x}}, \quad \mathbf{j} \leftrightarrow -\mathrm{i}\sigma_{\mathrm{y}}, \quad \mathbf{k} \leftrightarrow \mathrm{i}\sigma_{\mathrm{z}}, \tag{4.3}$$

其中 $\mathrm{I}$ $\sigma_{\mathrm{x}}$、 $\sigma_{\mathrm{y}}$、 $\sigma_{\mathrm{z}}$ 是泡利算子

$$\mathrm{I} \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \sigma_{\mathrm{x}} \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ \sigma_{\mathrm{y}} \coloneqq \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \text{ and } \sigma_{\mathrm{z}} \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

且 $\mathrm{i} \coloneqq \sqrt{-1}$ 是 $-1$ 的复平方根（详情参见 [15, 第 II.D 节] ）。Higginbotham 和 Worley 在 [24,例 3] 中给出了一个类似的四元数 Hadamard 矩阵，作为一个具有非循环核心的五阶四元数 Hadamard 矩阵的例子。事实上，由下文的定理 19 可知， [24, 例 3]中的四元数 Hadamard 矩阵等价于 (4.2)。

矩阵 (4.2) 的元素排列模式与矩阵中的相同

$$G(a,b,c) \coloneqq \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & a & b & c \\ 1 & a & -1 & c & b \\ 1 & b & c & -1 & a \\ 1 & c & b & a & -1 \end{bmatrix}, \tag{4.4}$$

其中 $a$、 $b$、 $c \in \mathsf{S}^3$ 是单位四元数。我们希望确定 $a$、$b$ 和 $c$，使得 $G(a, b, c)$ 是一个 Hadamard 矩阵。我们先介绍四元数的一个简单性质。

**引理 18.** 设 $a$、 $b \in \mathsf{S}^3$ 是单位四元数，且满足

$$1 + a + b = 0. \tag{4.5}$$

那么，存在 $-1$ 的一个四元数平方根 $w$，即 $w \in \mathsf{S}^2$,，使得 $a = \mathrm{e}^{\frac{2\pi}{3}w}$ 且 $b = \mathrm{e}^{\frac{-4\pi}{3}w}$。换言之，$a$ 和 $b$ 是 $1$ 和 $b = a^2$ 的非平凡四元数立方根。

证明。令 $a = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$ 和 $b = b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}$。式 (4.5) 等价于

$$\begin{aligned} a_1 + b_1 &= -1 \quad \text{and} \\ a_i &= -b_i \quad \text{for } i \in \{2,3,4\}. \end{aligned} \tag{4.6}$$

此外，由于 $a$ 和 $b$ 是单位四元数，我们有 $1 = \|a\| = \|b\|$，即 $1 = a_1^2 + a_2^2 + a_3^2 + a_4^2 = b_1^2 + b_2^2 + b_3^2 + b_4^2$。根据（4.6），对于 $i > 1$，有 $a_i^2 = b_i^2$，因此 $a_1^2 = b_1^2$。于是 $a_1 = b_1 = -\frac{1}{2}$ 和 $b = a^*$。定义 $w := \frac{2}{\sqrt{3}}(a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k})$。我们看到 $\|w\|^2 = \frac{4}{3}(a_2^2 + a_3^2 + a_4^2) = \frac{4}{3}(1 - a_1^2) = 1$。因此 $w \in \mathbb{S}^2$。此外，根据四元数的欧拉公式，$\mathrm{e}^{\frac{2\pi}{3}w} = \cos\left(\frac{2\pi}{3}\right) + w\sin\left(\frac{2\pi}{3}\right) = a$。类似地，$b = \mathrm{e}^{\frac{4\pi}{3}w}$。 □

我们可以验证，逆命题也成立。也就是说，对于任意非平凡的 1 的四元数立方根 $a$（$a^3 = 1$ 和 $a \neq 1$），都有 $1 + a + a^2 = 0$。利用这一性质，我们可以精确确定何时 $G(a,\ b,\ c)$ 是 Hadamard 矩阵。

**定理 19**。考虑式 (4.4) 中定义的矩阵 $G(a,b,c)$，其中 $a,b,c$ 是单位四元数。假设 $G(a,b,c)$ 是 *Hadamard* 矩阵。那么，在 $\mathbb{H}$ 的一个自同构作用下，它等于

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \mathbf{i} & \mathbf{i}\,\mathrm{e}^{\frac{2\pi}{3}\mathbf{j}} & \mathbf{i}\,\mathrm{e}^{\frac{4\pi}{3}\mathbf{j}} \\ 1 & \mathbf{i} & -1 & \mathbf{i}\,\mathrm{e}^{\frac{4\pi}{3}\mathbf{j}} & \mathbf{i}\,\mathrm{e}^{\frac{2\pi}{3}\mathbf{j}} \\ 1 & \mathbf{i}\,\mathrm{e}^{\frac{2\pi}{3}\mathbf{j}} & \mathbf{i}\,\mathrm{e}^{\frac{4\pi}{3}\mathbf{j}} & -1 & \mathbf{i} \\ 1 & \mathbf{i}\,\mathrm{e}^{\frac{4\pi}{3}\mathbf{j}} & \mathbf{i}\,\mathrm{e}^{\frac{2\pi}{3}\mathbf{j}} & \mathbf{i} & -1 \end{bmatrix}, \tag{4.7}$$

也就是说，$G(a,b,c)$ 等价于矩阵 (4.7)。

证明。为便于记号，我们将 $G(a,\ b,\ c)$ 简记为 $M$。假设 $M$ 是 Hadamard 矩阵。令 $M_i$ 表示 $M$ 的第 $i$ 行，其中 $0 \le i < 5$。条件 $MM^* = 5\mathbf{I}_5$ 等价于行正交条件 $M_iM_j^* = 5\delta_{ij}$，对所有 $0 \le i,\ j < 5$ 均成立。

由 $M_2M_1^* = 0$，我们得到 $a+b+c = 0$，即 $a(1+a^*b+a^*c) = 0$。根据引理 18，存在 $-1, w \in \mathbb{S}^2$，的一个四元数平方根，使得 $b = a\,\mathrm{e}^{\frac{2\pi}{3}w}$ 且 $c = a\,\mathrm{e}^{\frac{4\pi}{3}w}$。行 $M_2$ 和 $M_3$ 的正交性以及

$a$、 $b$与 $c$ 之间的关系给出

$$\begin{aligned}
& 1 - a^* - a + bc^* + cb^* && = 0 \\
\iff\ & 1 - 2\,\mathrm{Re}(a) + a\,\mathrm{e}^{\frac{-2\pi}{3}w}\,a^* + a\,\mathrm{e}^{\frac{2\pi}{3}w}\,a^* && = 0 \\
\iff\ & 1 - 2\,\mathrm{Re}(a) + a\big(2\cos\big(\tfrac{2\pi}{3}\big)\big)a^* && = 0 \\
\iff\ & 1 - 2\,\mathrm{Re}(a) - \|a\|^2 && = 0 \\
\iff\ & \mathrm{Re}(a) && = 0.
\end{aligned}$$

因此， $a \in \mathsf{S}^2$。

由 $M_2 M_4^* = 0$（这与 $M_3 M_5^* = 0$ 相同），可得

$$\begin{aligned}
& 1 - b^* - ac^* - b + ca^* && = 0 \\
\iff\ & 1 - 2\,\mathrm{Re}(b) + a\,\mathrm{e}^{\frac{-4\pi}{3}w}\,a^* + a\,\mathrm{e}^{\frac{4\pi}{3}w}\,a^* && = 0 \\
\iff\ & 1 - 2\,\mathrm{Re}(b) - aa^* && = 0 \\
\iff\ & \mathrm{Re}(a\,\mathrm{e}^{\frac{2\pi}{3}w}) && = 0 \\
\iff\ & \mathrm{Re}\big(a\big(-\tfrac{1}{2} + \tfrac{\sqrt{3}}{2}w\big)\big) && = 0 \\
\iff\ & \mathrm{Re}(aw) && = 0,
\end{aligned}$$

因为 $\mathrm{Re}(a) = 0$。

定义 $x := aw$。上述推导表明 $x \in \mathsf{S}^2$, ，因此 $x^* = -x = -aw$。由于 $a, w \in \mathsf{S}^2$, ，我们还有 $-aw = x^* = w^* a^* = (-w)(-a) = wa$。也就是说， $a$ 和 $w$ 是反交换的纯虚单位四元数。换言之， $a$、 $w$和 $x$ 满足与 **i**、**j** 和 **k**相同的关系，并且存在一个 $\mathbb{H}$ 的自同构 $f$，由映射给出

$$a \leftrightarrow \mathbf{i}, \quad w \leftrightarrow \mathbf{j}, \quad \text{and} \quad x \leftrightarrow \mathbf{k}.$$

在自同构 $f$ 下，矩阵 $M$ 等于 (4.7)。我们可以验证，矩阵 (4.7) 满足其余所有行正交条件，因此是一个 Hadamard 矩阵。

□

因此，所有形如 $G(a,\ b,\ c)$ 的四元数 Hadamard 矩阵，都是由矩阵 $G(\mathbf{i},\ \mathbf{i}\,\mathrm{e}^{\frac{2\pi}{3}\mathbf{j}},\ \mathbf{i}\,\mathrm{e}^{\frac{4\pi}{3}\mathbf{j}})$ 通过四元数自同构生成的。根据推论 3，四元数自同构保持 QHM 等价性，因此所有形如 $G(a,\ b,\ c)$ 的 QHM 都彼此等价。由于 $G(a,\ b,\ c)$ 与 [24, Example 3] 中的 QHM 等价（通过交换第二行与倒数第二行，以及中间行与最后一行），Higginbotham 和 Worley [24] 研究的具有非循环核心的五阶 QHM 族也与形如 $G(a,\ b,\ c)$ 的 QHM 等价。这类分析或许可以作为完整刻画五阶 QHM 的良好起点。

## 4.4 小阶非等价四元数 Hadamard 矩阵

由完美序列构造的 QHM 可能得到与其他构造所得矩阵不等价的矩阵。现在我们证明，由长度为五的完美序列 x+JJ+ 构造的 QHM，与形如 (4.4) 的矩阵或 Higginbotham 和 Worley [24] 研究的其他五阶 QHM 均不等价。

考虑附录中列出的长度为五的完美序列 x+JJ+ ，以及由该序列得到的四元数 Hadamard 矩阵。为便于比较，我们采用与其等价的循环矩阵

$$M := \begin{bmatrix} 1 & q\mathbf{i} & 1 & -\mathbf{j} & -\mathbf{j} \\ -\mathbf{j} & 1 & q\mathbf{i} & 1 & -\mathbf{j} \\ -\mathbf{j} & -\mathbf{j} & 1 & q\mathbf{i} & 1 \\ 1 & -\mathbf{j} & -\mathbf{j} & 1 & q\mathbf{i} \\ q\mathbf{i} & 1 & -\mathbf{j} & -\mathbf{j} & 1 \end{bmatrix}. \tag{4.8}$$

其首行为 +x+JJ。我们首先证明， $M$ 与第4.3节研究的形如 $G(a,\ b,\ c)$ 的五阶矩阵不等价。下文中，我们假设指标均按 $n$ 取模，其中 $n$ 是完美序列的长度或相应四元数 Hadamard 矩阵的阶数。

**~引理 20。** 设 $H$ 是一个阶数为 $n$、首行为 $h$ 的循环四元酉矩阵。令 $H$ 表示 ~，即通过对 $H$ 的第一列去相位得到的四元数 *Hadamard* 矩阵，即 $H :=\mathrm{diag}(c)^* H$，其中 $c$ 是 $H$ 的第一列。任何与 $H$~ 等价的归一化四元数 *Hadamard* 矩阵都可表示为 $\alpha h_k Q_1 H \mathrm{diag}(g(k))^* Q_2 \alpha^*$，其中 $\alpha$ 是某个单位四元数，$k \in [0, n)$，且 $Q_1$、$Q_2$ 是置换矩阵；其中 $g(k)$ 是将 $h$ 的各项向左循环置换 $k$ 位所得的向量。

证明。令 $h$ 表示 $H$ 的第一行，则 $g(k)_i = h_{i+k}$, $H =(h_{j-i} : 0 \leq i, j < n)$ 和 $H =(h^*_{-i} h_{j-i} :\ 0 \leq i, j < n)$。

设 $H'$ 是一个与 $H$ 等价的归一化四元数 Hadamard 矩阵。根据引理 1，我们有 $H' = D_1 P_1 H P_2 D_2$，其中 $D_1$、$D_2$ 是对角线上为单位四元数的对角矩阵，$P_1$、$P_2$ 是置换矩阵。我们可以写作 $H' = P_1 D_1' H D_2' P_2$，其中 $D_1' := P_1^* D_1 P_1$ 且 $D_2' := P_2 D_2 P_2^*$。注意，$D_1'$、$D_2'$ 也是对角线上为单位四元数的对角矩阵。

令 $K := D_1' H D_2'$。只需证明 $K$ 具有~引理中所述的形式，即对于某些置换矩阵 $Q_1'$、$Q_2'$ 以及引理中的 $\alpha$、$k$、$g(k)$，有 $K = \alpha h_k Q_1' H \mathrm{diag}(g(k))^* Q_2' \alpha^*$。

令 $D_1' = \mathrm{diag}(a)$，且令 $D_2' = \mathrm{diag}(b)$，使得 $K = (a_i h_{j-i} b_j : 0 \le i,\ j < n)$。假设 $P_1$ 将 $K$ 的第 $(r+1)$ 行映射到 $H'$ 的第一行，而 $P_2$ 将 $K$ 的第 $(s+1)$ 列映射到 $H'$ 的第一列。由于 $H'$ 已规范化，$H'$ 的第 $(r+1)$ 行及其第 $(s+1)$ 列的所有元素均为 1。因此，对于所有 $0 \le i,\ j < n$，都有 $a_r h_{j-r} b_j = 1 = a_i h_{s-i} b_s$。解这些方程可得 $b_j = h_{j-r}^* a_r^*$ 和 $a_i = b_s^* h_{s-i}^* = a_r h_{s-r} h_{s-i}^*$。因此

$$K = (a_r h_{s-r} h_{s-i}^* h_{j-i} h_{j-r}^* a_r^* : 0 \le i, j < n) = a_r h_{s-r} K' a_r^* \ ,$$

其中 $K' = (h_{s-i}^* h_{j-i} h_{j-r}^* : 0 \le i, j < n)$。注意，$K'^{\sim}$的第 $(i, j)$ 个元素是 $H\,\mathrm{diag}(g(k))^*$的第 $(i-s, j-s)$ 个元素，其中 $k := s - r$。引理得证。 □

该引理有助于我们证明，矩阵 $M$ 不等价于四元数 Hadamard 矩阵 $G(\mathbf{i}, \mathbf{i}e^{\frac{2\pi}{3}}\mathbf{j}, \mathbf{i}e^{\frac{4\pi}{3}}\mathbf{j})$，因此也不等价于任何形如 $G(a, b, c)$ 的四元数 Hadamard 矩阵。

**命题21。** 式 $(4.8)$ 中的四元数 *Hadamard* 矩阵 $M$ 不等价于第*4.3*节中定义的四元数 *Hadamard* 矩阵$G(\mathbf{i}, \mathbf{i}e^{\frac{2\pi}{3}}\mathbf{j}, \mathbf{i}e^{\frac{4\pi}{3}}\mathbf{j})$。

证明。观察可知，$G(\mathbf{i}, \mathbf{i}e^{\frac{2\pi}{3}}\mathbf{j}, \mathbf{i}e^{\frac{4\pi}{3}}\mathbf{j})$中除第一列外，每一列都恰好包含三个纯虚四元数。我们将证明，对于任何与 $M$等价的归一化四元数 Hadamard 矩阵，都存在某个非第一列不具备这一性质。

根据引理 20，任何与 $M$ 等价的规范化矩阵都具有以下形式

$$\alpha h_k Q_1 \widetilde{H}\,\mathrm{diag}(g(k))^* Q_2 \alpha^*$$

$\widetilde{}$对于 $\alpha$、$h$、$k$、$Q_1$、$H$、$g$（$k$），以及引理中所述的 $Q_2$。每个内自同构 $x \mapsto \alpha x \alpha^*$ 都保持纯虚四元数不变，而矩阵的行置换保持每列中纯虚四元数的数量不变。置换 $Q_2$ 将矩阵 $\widetilde{\ }\ L := h_k H\mathrm{diag}(g(k))^*$ 的某一列移至第一列，并对其余列进行置换。因此，只需证明 $L$ 存在另一列，其中纯虚四元数的数量不恰为三个。

考虑 $L$ 的第三列。根据 $k$ 的值，这一列

如表所示

| $k$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $h_k h_0^* h_2 h_{2+k}^*$ | 1 | $q\mathbf{k}$ | $\mathbf{j}$ | $-\mathbf{j}$ | $-\mathbf{k}q^*$ |
| $h_k h_4^* h_1 h_{2+k}^*$ | $\mathbf{j}q\mathbf{i}$ | $(q\mathbf{k})^2$ | $\mathbf{j}q\mathbf{k}$ | $q\mathbf{i}$ | 1 |
| $h_k h_3^* h_0 h_{2+k}^*$ | $\mathbf{j}$ | $-q\mathbf{i}$ | $-1$ | 1 | $-\mathbf{i}q^*$ |
| $h_k h_2^* h_4 h_{2+k}^*$ | $-\mathbf{j}$ | $q\mathbf{i}$ | 1 | $-1$ | $\mathbf{i}q^*$ |
| $h_k h_1^* h_3 h_{2+k}^*$ | $\mathbf{i}q^*\mathbf{j}$ | 1 | $-\mathbf{i}q^*$ | $\mathbf{k}q^*\mathbf{j}$ | $(\mathbf{k}q^*)^2$ |

. (4.9)

由于所有可能的列都不全为 1，置换 $Q_2$ 不会将 $L$ 的第三列映射到第一列。我们可以验证，上述列向量均不恰好包含三个纯虚四元数。由此得证。

□

回忆一下，阶数为 $n$ 的复傅里叶矩阵 $F_n$ 定义为 $F_n(i,j) := \omega^{ij}$，$0 \le i,j < n$，其中 $\omega := \exp(2\pi\mathbf{i}/n)$。对于所有 $n \ge 1$，矩阵 $F_n$ 都是四元数 Hadamard 矩阵。复傅里叶矩阵 $F_5$ 具有循环核心，并属于 Higginbotham 和 Worley [24, 定理 6]所刻画的一类具有循环核心的五阶 QHM。现在我们证明，矩阵 $M$ 与这一类 QHM 不等价。

**命题 22.** 式 (4.8) 中的 *QHM* $M$ 与核心具有两个复数元素的循环核心 *QHM* 不等价。

证明. 根据 [24, 定理 6], ，任何具有循环核心且核心中有两个复数元素的五阶 QHM，要么与复傅里叶矩阵 $F_5$ 等价，要么在除第一列外的每一列中都含有两对非实共轭四元数 $(\beta, \beta^*)$、$(\gamma, \gamma^*)$。此外，在后一种情况下，$\beta$ 和 $\gamma$ 的纯虚部系数向量的内积为 $\pm 5/16$。

每个内自同构 $x \mapsto \alpha x \alpha^*$ 都会保留共轭关系。根据定理 16，它也会保留任意一对四元数的纯虚部系数向量之间的内积。类似地，两个四元数 $\theta$、$\omega$ 可交换，当且仅当 $\alpha\theta\alpha^*$ 和 $\alpha\omega\alpha^*$ 可交换。还要注意，两个四元数可交换，当且仅当它们的纯虚部是同一个四元数的实数倍。

考虑 $M$ 与复傅里叶矩阵 $F_5$的非等价性。注意，复傅里叶矩阵的所有元素彼此可交换。仿照命题21的证明中的论证，只需证明

四元数 Hadamard 矩阵 $L$ 的第三列中，纯虚部并非全都是同一个四元数的实数倍。考察公式（4.9）中该列的各种可能形式可知，确实如此。

考虑 $M$ 与上文所述另一个五阶四元数 Hadamard 矩阵类别的非等价性。检查公式（4.9）中 $L$ 第三列的各种可能性可知，只有含有 $k = 0$ 的情形具有两对非实共轭四元数。然而，非共轭四元数的纯虚部系数向量的内积为 $\pm 1/2$。由此即可得证。

□

接下来，我们证明至少存在三个非等价的七阶四元数 Hadamard 矩阵。考虑由序列 +JYJ+ 得到的七阶四元数 Hadamard 矩阵 $R$ ——该序列已在附录中报告（相差一次移位），

$$R \coloneqq \begin{bmatrix} 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 & -1 & -1 \\ -1 & 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 & -1 \\ -1 & -1 & 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 \\ 1 & -1 & -1 & 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} \\ -\mathbf{j} & 1 & -1 & -1 & 1 & -\mathbf{j} & -q\mathbf{j} \\ -q\mathbf{j} & -\mathbf{j} & 1 & -1 & -1 & 1 & -\mathbf{j} \\ -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 & -1 & -1 & 1 \end{bmatrix}. \tag{4.10}$$

我们将 $R$ 与先前研究中报道的对应于 $\mathcal{Q}_{24}$-序列的四元数 Hadamard 矩阵进行比较，即 +jIIj+W [27, 示例 7.3] 和 qJIKKIJ [28]（见 [4, 表 1]）。由于存在 W 项，前一个序列无法直接转换为一组 QT 序列，因为 $q^*\mathbf{k} \notin \mathcal{Q}_+$。应用共轭可将 +jIIj+W 转换为一个完美的 $\mathcal{Q}_+$-序列，其对应的 QT 序列集合与 qJIKKIJ 对应的 QT 序列集合 QT 等价。然而，共轭并非 $\mathbb{H}$ 的自同构（它是一个反-自同构，即 $(xy)^* = y^*x^*$），因此共轭通常不能保持为四元数 Hadamard 矩阵的性质，也不是四元数 Hadamard 矩阵的等价操作。因此，下面我们将证明 $R$ 与规范化后的形式均不等价

该四元数 Hadamard 矩阵由 +jIIj+W 得到,

$$S \coloneqq \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -\mathbf{k}q\mathbf{j} & -\mathbf{k}q\mathbf{k} & \mathbf{k}q & \mathbf{k}q\mathbf{k} & \mathbf{k}q\mathbf{j} & (\mathbf{k}q)^2 \\ 1 & -q^*\mathbf{i} & \mathbf{i} & -\mathbf{k} & \mathbf{k} & -\mathbf{i} & \mathbf{i}q \\ 1 & -1 & \mathbf{j}q^*\mathbf{j} & \mathbf{k} & -\mathbf{j} & -\mathbf{k} & q \\ 1 & \mathbf{i} & -1 & -\mathbf{i}q^*\mathbf{j} & -\mathbf{k} & \mathbf{k} & \mathbf{k}q \\ 1 & -\mathbf{j} & \mathbf{j} & -1 & -\mathbf{i}q^*\mathbf{i} & \mathbf{i} & -q \\ 1 & -\mathbf{i} & -\mathbf{j} & \mathbf{i} & -1 & \mathbf{j}q^*\mathbf{k} & -\mathbf{i}q \end{bmatrix}, \tag{4.11}$$

以及由 jQjikki（对 qJIKKIJ 进行移位和取负）得到的四元数 Hadamard 矩阵的规范化形式,

$$T \coloneqq \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \mathbf{i}q^* & \mathbf{k}q\mathbf{j} & -1 & -\mathbf{i} & \mathbf{k} & \mathbf{i} \\ 1 & -q^* & -\mathbf{i} & -\mathbf{i}q\mathbf{i} & -1 & -\mathbf{k} & \mathbf{k} \\ 1 & -\mathbf{j}q^* & -\mathbf{j} & \mathbf{j} & -\mathbf{i}q\mathbf{k} & -1 & -\mathbf{i} \\ 1 & q^* & \mathbf{j} & \mathbf{k} & -\mathbf{j} & \mathbf{k}q\mathbf{k} & -1 \\ 1 & -\mathbf{i}q^* & \mathbf{i} & -\mathbf{j} & \mathbf{j} & -\mathbf{i} & q\mathbf{i} \\ 1 & (\mathbf{j}q^*)^2 & \mathbf{j}q^*\mathbf{k} & \mathbf{j}q^*\mathbf{j} & -\mathbf{j}q^* & -\mathbf{j}q^*\mathbf{j} & -\mathbf{j}q^*\mathbf{k} \end{bmatrix}. \tag{4.12}$$

为了证明 $R$ 与 $S$ 和 $T$非等价，我们沿用五阶矩阵所采用的方法。

**命题 23.** 式 (4.10)中的四元数 *Hadamard* 矩阵 $R$ 既不等价于式 (4.11) 中定义的四元数 *Hadamard* 矩阵 $S$，也不等价于式 (4.12)中定义的四元数 *Hadamard* 矩阵 $T$。

证明. 根据引理 20，任何与 $R$ 等价的规范化矩阵都具有如下形式

$$\alpha h_k Q_1 \widetilde{H} \operatorname{diag}(g(k))^* Q_2 \alpha^*$$

$\widetilde{\phantom{x}}$ $\widetilde{\phantom{x}}$，其中 $\alpha$、$h$、$k$、$Q_1$、$H$、$g$（$k$）和 $Q_2$ 如引理中所述。令 $L \coloneqq h_k H\mathrm{diag}(g(k))^*$。只需证明，$L$ 中存在某一列，在对其应用上述表达式中的置换 $Q_1, Q_2$和自同构 $x \mapsto \alpha x \alpha^*$ 之后，该列仍不对应于 $S$ 或 $T$ 中的任何一列。

考虑 $L$ 的第二列。根据 $k$ 的值，该

列等于表中的某一列

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $h_k h_0^* h_1 h_{1+k}^*$ | $1$ | $-\mathbf{j}q^*$ | $-q\mathbf{j}$ | $-1$ | $\mathbf{j}$ | $-\mathbf{j}$ | $\mathbf{j}$ |
| $h_k h_6^* h_0 h_{1+k}^*$ | $-\mathbf{j}$ | $-q^*$ | $-q$ | $\mathbf{j}$ | $1$ | $-1$ | $1$ |
| $h_k h_5^* h_6 h_{1+k}^*$ | $\mathbf{j}$ | $q^*$ | $q$ | $-\mathbf{j}$ | $-1$ | $1$ | $-1$ |
| $h_k h_4^* h_5 h_{1+k}^*$ | $-\mathbf{j}$ | $-q^*$ | $-q$ | $\mathbf{j}$ | $1$ | $-1$ | $1$ |
| $h_k h_3^* h_4 h_{1+k}^*$ | $-1$ | $\mathbf{j}q^*$ | $q\mathbf{j}$ | $1$ | $-\mathbf{j}$ | $\mathbf{j}$ | $-\mathbf{j}$ |
| $h_k h_2^* h_3 h_{1+k}^*$ | $\mathbf{j}q^*$ | $(q^*)^2$ | $1$ | $-q^*\mathbf{j}$ | $\mathbf{j}q^*\mathbf{j}$ | $-\mathbf{j}q^*\mathbf{j}$ | $\mathbf{j}q^*\mathbf{j}$ |
| $h_k h_1^* h_2 h_{1+k}^*$ | $\mathbf{j}q$ | $1$ | $q^2$ | $-q\mathbf{j}$ | $\mathbf{j}q\mathbf{j}$ | $-\mathbf{j}q\mathbf{j}$ | $\mathbf{j}q\mathbf{j}$ |

, (4.13)

因为 $k \in [0,7$ 对应列的第 $i$ 个元素为 $h_k h_{-i}^* h_{1-i} h_{1+k}^*$）。该列不全为 1，并且根据 $k$ 的值，属于以下类型之一。

1. 它在 $\{\pm 1\}$ 中有两个元素，在 $\{\pm\beta\}$ 中有三个元素，其中 $\beta \in \mathcal{Q}_8$ 是某个纯虚四元数。2. 它在 $\{\pm 1\}$ 中有三个元素，在 $\{\pm\beta\}$ 中有两个元素，其中 $\beta \in \mathcal{Q}_8$ 是某个纯虚四元数。3. 它有两对不同的形如 $(\beta, -\beta)$ 的四元数，其中 $\beta \in \mathcal{Q}_{24} \setminus \mathcal{Q}_8$；另有一对四元数 $(\gamma, \gamma^2)$，其中 $\gamma \in \mathcal{Q}_{24} \setminus \mathcal{Q}_8$ 是 $-1$ 的立方根。

$R$、$S$、$T$ 的所有元素都属于 $\mathcal{Q}_{24}$，但证明的其余部分只用到 $\mathcal{Q}_{24} \setminus \mathcal{Q}_8$ 的元素具有非零实部和虚部这一性质。假设 $R$ 等价于 $S$ 或 $T$。那么，自同构 $f\colon x \mapsto \alpha x \alpha^*$（以及置换 $Q_1$、$Q_2$）保持了上述三类列的性质。然而，$S$ 或 $T$ 的列都不属于类型 1 或 2。只有 $S$ 的最后一列和 $T$ 的第二列属于类型 3。因此，$L$ 的第二列只能映射到这些列，并且满足 $k \in \{1,2\}$（参见公式 (4.13)）。接下来我们将论证这同样不可能。

我们给出 $S$ 和 $k=1$最后一列的论证。其他情形的证明思路相同。在 $S$ 的最后一列中，形如（$\beta$，$-\beta$）的配对只有（$q$，$-q$）和（$\mathbf{i}q$，$-\mathbf{i}q$）；而在 $L$ 中与 $k=1$ 对应的第二列里，这样的配对只有（$q^*$，$-q^*$）和（$\mathbf{j}q^*$，$-\mathbf{j}q^*$）。由于 $\mathrm{Re}(q) = \mathrm{Re}(-\mathbf{i}q) = \mathrm{Re}(q^*) = \mathrm{Re}(\mathbf{j}q^*) = 1/2$，等价操作只能将（$q^* \mapsto q$，$\mathbf{j}q^* \mapsto -\mathbf{i}q$）或（$q^* \mapsto -\mathbf{i}q$，$\mathbf{j}q^* \mapsto q$）映射过去。此外，我们有 $-q^* \mapsto \mathbf{k}q$ 或 $-q^* \mapsto (\mathbf{k}q)^2$。然而，这两组条件并不一致，因为它们将 $q^*$ 映射为不同的四元数，因此所需的等价操作不存在。 □

运用上述类似的论证，我们证明四元数 Hadamard 矩阵 $R$ 和 $S$ 不等价于复傅里叶矩阵 $F_7$。

**命题 24.** 式 (4.10) 中的四元数 *Hadamard* 矩阵 $R$ 和式 (4.11) 中定义的四元数 *Hadamard* 矩阵 $S$ 均不等价于七阶傅里叶矩阵 $F_7$。

证明。 与命题 23 的证明相同，要证明 $R$ 与 $F_7$ 不等价，只需证明 (4.13) 中的列经过行置换和自同构后，均不等于 $F_7$ 的任何一列。 $F_7$ 的所有元素均可交换。然而，(4.13) 中的每一列至少有两个元素，其纯虚部不是同一个四元数的实数倍；行置换和自同构不会改变这一性质。关于 $R$ 的结论由此得出。

我们可以重复这一论证，证明 $S$ 与 $F_7$ 的非等价性。设 $L' :=$ $\sim h_k H \,\mathrm{diag}(g(k))^*$，其中参数 $h, H, g(k)$ 现在对应于由完美序列 +jIIj+W 生成的四元数 Hadamard 矩阵，而 $k$ 则由一组假定的等价操作确定。考察 $L'$ 的第二列。根据 $k$ 的取值，此列等于表中的某一列

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $h_k h_0^* h_1 h_{1+k}^*$ | $1$ | $-\mathbf{i}$ | $-\mathbf{j}$ | $-\mathbf{i}$ | $-1$ | $-\mathbf{i}q$ | $-q^*\mathbf{i}$ |
| $h_k h_6^* h_0 h_{1+k}^*$ | $\mathbf{k}q\mathbf{j}$ | $-\mathbf{i}q\mathbf{i}$ | $-\mathbf{j}q\mathbf{i}$ | $\mathbf{j}q\mathbf{j}$ | $-\mathbf{i}q$ | $(\mathbf{k}q)^2$ | $1$ |
| $h_k h_5^* h_6 h_{1+k}^*$ | $q^*\mathbf{i}$ | $\mathbf{j}q^*\mathbf{j}$ | $-\mathbf{i}q^*\mathbf{j}$ | $-\mathbf{i}q^*\mathbf{i}$ | $\mathbf{j}q^*\mathbf{k}$ | $1$ | $(q^*\mathbf{k})^2$ |
| $h_k h_4^* h_5 h_{1+k}^*$ | $-1$ | $\mathbf{i}$ | $\mathbf{j}$ | $\mathbf{i}$ | $1$ | $\mathbf{i}q$ | $q^*\mathbf{i}$ |
| $h_k h_3^* h_4 h_{1+k}^*$ | $\mathbf{i}$ | $-1$ | $-\mathbf{k}$ | $1$ | $\mathbf{i}$ | $q$ | $-q^*$ |
| $h_k h_2^* h_3 h_{1+k}^*$ | $-\mathbf{j}$ | $-\mathbf{k}$ | $1$ | $\mathbf{k}$ | $\mathbf{j}$ | $-\mathbf{k}q$ | $q^*\mathbf{k}$ |
| $h_k h_1^* h_2 h_{1+k}^*$ | $-\mathbf{i}$ | $1$ | $\mathbf{k}$ | $-1$ | $-\mathbf{i}$ | $-q$ | $q^*$ |

(4.14)

同样，(4.14)中的每一列至少有两个元素，其纯虚部不是同一四元数的实数倍。关于 $S$ 的结论也同样成立。

□

本节的结果表明，四元数 Hadamard 矩阵的等价类重数也会延伸到更大的阶；我们猜想，对于所有阶 $\geq 4$，情况皆是如此。

# 5 结论

我们枚举了长度为 $n \leq 21$、定义在 $\mathcal{Q}_+$ 上的完美四元数序列。在此过程中，我们推导出循环块四元数型阿达玛矩阵的新性质，形式化定义了这类对象的三种不同等价关系，并提出了确保按照每一种等价关系进行完整枚举的方法。特别是，威廉姆森型序列四元组的自然等价关系并不保留阿达玛矩阵的自然等价关系，但引入第三种等价关系后，我们得以将所有带循环块的四元数型阿达玛矩阵按照阿达玛矩阵的等价关系分类。最终，我们按照所考虑的每一种等价关系，对阶为 $n \leq 21$ 的所有带循环块的四元数型阿达玛矩阵进行了分类（见表 1）。

我们还证明并利用了循环 Williamson 型矩阵四元组与具有循环块的四元数型阿达玛矩阵之间的一一对应关系。这两类阿达玛矩阵长期以来都受到研究 [19, 40]。循环 Williamson 型矩阵可以直接构造出四元数型阿达玛矩阵，但令人意外的是，此前人们并不知道，具有循环块的四元数型阿达玛矩阵必然具有 Williamson 型块。我们在定理 9 中证明了这一点。这一性质使我们能够在搜索由 QT 序列定义的四元数型阿达玛矩阵时，及早筛除绝大多数序列配对。

我们对 QT 序列进行计算枚举，帮助构造出新的具有循环块的四元数型阿达玛矩阵，以及可证明彼此不等价的四元数 Hadamard 矩阵。我们还通过解析方法研究了四元数 Hadamard 矩阵的性质，并展示了刻画具有固定元素模式的四元数 Hadamard 矩阵的可行性。正如我们在第 4.4 节所示，完美序列能够生成可证明不等价于通过其他方式构造的四元数 Hadamard 矩阵。这些结果表明，四元数 Hadamard 矩阵的数量比以往研究所知的更多，其中包括为量子通信协议应用而研究的矩阵 [15]。

# 参考文献

[1] Santiago Barrera Acevedo。个人通信，2023年7月25日。

[2] Santiago Barrera Acevedo 和 Heiko Dietrich。四元数上的完美序列以及 ($4n$，2，$4n$，$2n$)-相对差集，其中 $C_n \times Q_8$。*Cryptography and Communications*，10(2)：357–368，2018。doi:10.1007/s12095-017-0224-y。

[3] Santiago Barrera Acevedo 和 Heiko Dietrich。威廉姆森哈达玛矩阵的新无限族。*Australasian Journal of Combinatorics*，73(1):207–219，2019年1月。网址：https://ajc.maths.uq.edu.au/pdf/73/ajc_v73_p207.pdf。

[4] Santiago Barrera Acevedo、HeikoDietrich 和 Corey Lionis。四元数 Hadamard 矩阵的新族。*Designs, Codes and Cryptography*，92(9):2511–2525，2024年6月。doi:10.1007/s10623-024-01401-1。

[5] Santiago Barrera Acevedo 和 Thomas E. Hall。基本四元数上的无界长度完美序列。载于 Tor Helleseth 和 Jonathan Jedwab 编，*Sequences and Their Applications - SETA 2012* - 第7届国际会议，*Waterloo*（加拿大安大略省），*2012*年*6*月*4*日至*8*日。论文集，第7280卷，计算机科学讲义，第159–167页。Springer，2012年。doi:10.1007/978-3-642-30615-0_15。

[6] Santiago BarreraAcevedo、Padraig Ó. Catháin 和 HeikoDietrich。构造阶为 $4p$的余循环哈达玛矩阵。*Journal of Combina-torial Designs*，27(11):627–642，2019年8月。doi:10.1002/jcd.21664。

[7] L. D. Baumert 和 Marshall Hall。Williamson 型哈达玛矩阵。*Mathematics of Computation*，19(91):442–447，1965年。doi:10.1090/s0025-5718-1965-0179093-2。

[8] Samuel Thomas Blake。完美自相关序列和多维数组的构造。博士论文，莫纳什大学，2017年。doi:10.4225/03/58FD558C6A8E5。

[9] Curtis Bright、Ilias Kotsireas 和 Vijay Ganesh。将计算机代数系统与 SAT 求解器应用于威廉姆森猜想。*Journalof Symbolic Computation*，100:187–209，2020年9月。doi:10.1016/j.jsc.2019.07.024。

[10] Curtis Bright、Ilias Kotsireas 和 Vijay Ganesh。完美四元数序列和威廉姆森序列的新无限族。*IEEE*

《信息论汇刊》，66(12):7739–7751，2020年12月。doi:10.1109/TIT.2020.3016510。[11] E. Cho。四元数的棣莫弗公式。《应用数学快报》，11(6):33–35，1998年。doi:10.1016/S0893-9659(98)00098-6。[12] Oleg Chterental 和 Dragomir Ž. Đoković。关于正交随机矩阵、单随机矩阵和夸随机矩阵。《线性代数及其应用》，428(4):1178–1201，2008年。doi:10.1016/j.laa.2007.09.022。[13] Dragomir Ž. Đoković。阶为 $4n$ 、适用于 $n = 33$、35、39 的威廉姆森矩阵。《离散数学》，115(1–3):267–271，1993年5月。doi:10.1016/ 0012-365x(93)90495-f。[14] Máté Farkas。个人通信，2021年1月。[15] Máté Farkas、Jędrzej Kaniewski 和 Ashwin Nayak。相互无偏测量、哈达玛矩阵与超密编码。《IEEE信息论汇刊》，69(6):3814–3824，2023年6月。doi:10.1109/TIT.2023.3269524。[16] Patrick Fitzpatrick 和 Henry O’ Keeffe。具有循环分量的威廉姆森型哈达玛矩阵。《离散数学》，346(12):113615，2023年12月。doi:10.1016/j.disc.2023.113615。[17] R. L. Frank、S. A. Zadoff 和 R. C. Heimiller。具有良好周期相关特性的移相脉冲编码（通信）《IRE信息论汇刊》，8(6):381–382，1962年。doi:10.1109/TIT.1962. 1057786。[18] M. Frigo 和 S. G. Johnson。FFTW3 的设计与实现。《IEEE会议录》，93(2):216–231，2005年2月。doi:10.1109/ jproc.2004.840301。[19] Solomon W. Golomb 和 Leonard D. Baumert。哈达玛矩阵的搜索。《美国数学月刊》，70(1):12–17，1963年1月。doi:10.1080/00029890.1963.11990035。[20] Jacques Hadamard。关于一个行列式问题的解答。《数学科学通报》，2:240–246，1893年。

[21] William Rowan Hamilton. 论四元数；或论代数中一种新的虚数体系. 伦敦、爱丁堡和都柏林哲学杂志与科学杂志 , 25(163):10–13, 1844 年 7 月 . doi:10. 1080/14786444408644923.[22] R. Heimiller. 具有良好周期相关特性的移相脉冲编码. IRE信息论汇刊, 7(4):254–257, 1961年10月. doi:10.1109/tit.1961.1057655.[23] Logan M. Higginbotham与Chase T. Worley. 关于若干小阶四元数 Hadamard 矩阵. 2021年. arXiv:2112.09613v2 [math.CO]. doi:10.48550/ARXIV.2112.09613.[24] Logan M. Higginbotham与Chase T. Worley. 关于若干小阶四元数 Hadamard 矩阵. 技术报告 arXiv:2112.09613v2[math.CO],arXiv, 2022年. doi:10.48550/ARXIV.2112.09613.[25] W. H. Holzmann 、 H. Kharaghani与B. Tayfeh-Rezaie. 阶数不超过59的威廉姆森矩阵. Designs, Codes and Cryptography, 46(3):343–352, 2008年1月. doi:10.1007/s10623-007-9163-5.[26] Oleg Kuznetsov. 实四元数上的完美序列. 载于2009年第四届信号设计及其在通信中的应用国际研讨会, 第8–11页. IEEE, 2009年10月. doi:10.1109/iwsda. 2009.5346443.[27] Oleg Kuznetsov. 实四元数上的完美序列. 博士论文, 莫纳什大学, 墨尔本, 澳大利亚, 2010年. doi:10.4225/ 03/5927d7a6284be.[28] Wolfgang Lang与Ekkehard Schneider. 阶数不超过99的Turyn型威廉姆森矩阵. Designs, Codes and Cryptography, 62(1):79–84, 2011年3月. doi:10.1007/s10623-011-9492-2.[29] Tyler Lumsden、Ilias Kotsireas与Curtis Bright. 关于周期Golay配对的新结果. Mathematics of Computation, 2025年4月. doi: 10.1090/mcom/4096.[30] Brendan D. McKay. 经由图同构的Hadamard 等价. 离散数学, 27(2):213–214, 1979年. doi:10.1016/0012-365x(79) 90113-4.

[31] Brendan D. McKay与Adolfo Piperno. 实用图同构, II. Journal of Symbolic Computation, 60:94–112, 2014年1月. doi: 10.1016/j.jsc.2013.09.003.[32] Leiba Rodman. 四元数线性代数专题. 普林斯顿应用数学丛书. 普林斯顿大学出版社, 普林斯顿, 新泽西州, 美国, 2014年8月24日. doi:10.2307/j.ctt6wpz0p.[33] Herbert John Ryser. 组合数学. 卡鲁斯数学专著丛书第 14 号 . 美国数学协会 , 1963 年 .[34]Bernhard Schmidt. 威廉姆森矩阵与Ito的一个猜想. Designs, Codes and Cryptography, 17(1–3):61–68, 1999年9月. doi:10.1023/a:1008398319853.[35] Kai-Uwe Schmidt. 小相关序列. Designs, Codes and Cryptography, 78(1):237–267, 2016年. doi:10.1007/s10623-015-0154-7.[36] J.J. 西尔维斯特. 关于逆正交矩阵、同时符号变换以及两种或多种颜色的镶嵌铺面的思考，及其在牛顿法则、装饰性瓷砖工艺和数论中的应用. 伦敦、爱丁堡和都柏林哲学杂志与科学杂志, 34(232):461–475, 1867 年 12 月 . doi:10.1080/ 14786446708639914.[37] Armin Tavakoli、Máté Farkas、Denis Rosset、Jean-Daniel Bancal与Jędrzej Kaniewski. 贝尔实验中的互 unbiased 基与对称信息完备测量. 《科学进展》, 7(7), 2021年. doi:10.1126/sciadv.abc3847.[38] Richard J. Turyn. 复 Hadamard 矩阵. 组合结构及其应用, 第435–437页, 1970年.
[39] B. L. van der Waerden. 哈密顿对四元数的发现. 《数学杂志》, 49(5):227–234, 1976年. doi:10.2307/2689449.[40] Jennifer Seberry Wallis. 若干威廉姆森型矩阵. Utilitas Mathematics, 4:147–154, 1973年.

[41] Jennifer Seberry Wallis。偶数阶威廉姆森矩阵，第 132–142 页。Springer Berlin Heidelberg，1974 年。doi:10.1007/bfb0057387。
[42] Jennifer Seberry Wallis。威廉姆森型矩阵的构造。*Linear and Multilinear Algebra*，3(3):197–207，1975 年 1 月。doi:10.1080/03081087508817111。[43] John Williamson。阿达玛行列式定理与四平方和。*Duke Mathematical Journal*，11(1)，1944 年 3 月。doi:10.1215/s0012-7094-44-01108-7。

# 附录：QT 序列列表

此处我们给出所有长度为 $n \leq 21$ 的 QT 序列中，按 Williamson 型等价分类的完整列表。这些序列分为对称序列（此类序列也称为威廉姆森序列）和非对称序列。每组 QT 序列都根据定理 4 中的对应关系编码为完美四元数序列，具体如第 2.3 节所述。符号 + 和 - 分别表示 1 和 $-1$；q、i、j、k 分别表示四元数 $q = {}^{1+}\mathrm{i+j+k}\ {}^{2}$、i、j、k；x、y、z 分别表示 $q$i、$q$j、$q$k；大写字母表示与相同小写字母所表示的四元数互为相反数。例如，X 表示 $-q$i。

**长度 1（共 1 个；1 个对称，0 个非对称）**

+

**长度 2（共 1 个；1 个对称，0 个非对称）**

+J

**长度 3（共 1 个；1 个对称，0 个非对称）**

Q++

**长度 4（共 2 个；1 个对称，1 个非对称）**

*1* 对称：++-+

*1* 非对称：+YIQ

**长度 5（共 1 个；1 个对称，0 个非对称）**

x+JJ+

**长度 6（共 1 个；1 个对称，0 个非对称）**KJ+j+J

**长度 7（共 2 个；2 个对称，0 个非对称）**

YJ+--+J，y+JKKJ+

**长度 8（共 3 个；1 个对称，2 个非对称）**

*1* 对称：J++-
J-++

*2* 非对称：+
YYIiqq-，+JYZikqx

**长度 9（共 4 个；3 个对称，1 个非对称）**

*3* 对称：yi+JKKJ+i, XKJ+jj+JK, Z+J+--
+J+

*1* 非对称：+
YQJYZikx

**长度 10（共 2 个；2 个对称，0 个非对称）**

KJ+ikIki+J, K+J+j-j+J+

**长度 11（共 1 个；1 个对称，0 个非对称）**

z-+JKIIKJ+-

**长度 12（共 5 个；3 个对称，2 个非对称）**

*3* 个对称：Y++y-+y+-y++, YQ++-QyQ-++Q, JII
Y+-j-+YII

*2* 个非对称：+++Yy++-+yy-,
+++YQ++-+yQ-

**长度 13（共 4 个；4 个对称，0 个非对称）**

x-+JK+II+KJ+-, XKJ+jK--Kj+JK, QJ++jJjjJj++J, X-k+JKIIKJ+k-

**长度 14（共 5 个；5 个对称，0 个非对称）**

KJ+J+j-J-j+J+J, QQ+J+jzYzj+J+Q, +QY+kzxJxzk+YQ, YKJ+j-iQi-j+JK, QJ++
iIkxkIi++J

**长度 15（共 4 个；4 个对称，0 个非对称）**

XIij+JKJJKJ+jiI，QjJKj+JJJJ+jKJj，XIKJ+kKjjKk+JKI，Q+J+
jj+--+jj+J+

**长度 16（共 18 个；6 个对称，12 个非对称）**

*6* 个对称：-J+++-+j-j+-+++J, QJ++q-+jQj+-q++J, KJ++k-+jKj+-
k++J, JJ++j-+jJj+-j++J, YJ++y-+jYj+-y++J, +J++--+j+j+--++J

*12* 个非对称：
+Y+JYZ+qIxJkqQjy，++JJ+J+j+-jJ+j-j, ++JY+J+y+-jY+j-y,++J++J+-+-j++j--,
++JK+J+k+-jK+j-k, +++J+J-++-+j+j--,++YJ+Jy++-Yj+jy-，++JK+Kj++-Jk+
kj-, ++JJ+Jj++-Jj+jj-,+Q++JQYqKXJjixxz，++YJIJQ++-YjIjQ-, ++YIIIQ++-
YiIiQ-

**长度 17（共 4 个；4 个对称，0 个非对称）**

ZK+J+i-kKKk-i+J+K, yjKJ-+J+KK+J+-JKj, xkKIk+JJKKJJ+kIKk, y-+
Kk+JJKKJJ+kK+-

### 长度 18（共 28 个；23 个对称，5 个非对称）

*23* 个对称：
ZXY+i-KZyYyZK-i+YX, Z+J+i-KIjYjIK-i+J+, YJ++xyKiIZIiKyx++J, YJY+
yxJZkXkZJxy+YJ, Q+++i-IiIXIiI-i+++, I+Y+yqIQiJiQIqy+Y+, K+J+jiKIkIkIKij+J+,
ZKJ++jKk-Y-kKj++JK, KIJY+jQi-J-iQj+YJI, YQJ++jJiyXyiJj++JQ, YJQ++
jJxkXkxJj++QJ, QKJ++jJIjzjIJj++JK,+QY+-JJZyjyZJJ-+YQ, KJ++yZijkJkjiZy++J,
KZJ++kKiyIyiKk++JZ, ZKJ++kKi-X-iKk++JK, QIYJ+iIXjxjXIi+JYI, QY++
yXKIzxzIKXy++Y, Z+J+xQKIkxkIKQx+J+, ZKJ++kKI-q-IKk++JK, XXY+-
KkzqZqzkK-+YX, ZKJ+j+j-iXi-j+j+JK, QJ++jikKiyiKkij++J

*5* 个非对称：
+YXXXQY+kKqQyyXqK-, +YJXXIY+zKqIyyJqKy, ++YYXXQ+
KkJqxYyyJ-,++YJXIQ+JjJqiYjyJ-, ++YQJY+jqiIzxkZikx

### 长度 19（共 6 个；6 个对称，0 个非对称）

Qj-J-++JKIIKJ++-J-j, YKk-Kj+J+JJ+J+jK-kK, Y+-kJj+JKKKKJ+jJk-+, ZIKJJ+-
kiIIik-+JJKI, ZIKJ+kJj-JJ-jJk+JKI, ZJJJ+j+-jJJj-+j+JJJ

### 长度 20（总计 24；17 个对称，7 个非对称）

*17* 个对称：
JQ+Y+k+x-XjX-x+k+Y+Q, JIY++xKkzJjJzkKx++YI, IJY++xKkzIiIzkKx++YJ, IIYJ+
xkiQKiKQikx+JYI, YJXY+yjQz+y+zQjy+YXJ, XJ+Y+y-ZkJxJkZ-y+Y+J, QJ+Y+
jkY-IqI-Ykj+Y+J, +KJ++kjKIi-iIKjk++JK, JQJ++xkKKzjzKKkx++JQ, JKJ++xKjkJjJkjKx++
JK, KKJ++zjJK-k-KJjz++JK, IJXY+q-ZX-i-XZ-q+YXJ, QKJ++y-+jKqKj+-y++JK, YJ++jxJ+-
JyJ-+Jxj++J, QJJ++x-+jJqJj+-x++JJ, QKJ++z-+jKqKj+-z++JK, YJ++jyJ+-JyJ-+Jyj++J

*7* 非对称：
+++JKQzJK++-+jKqzjK-, ++JQQ+Jj+j-+jQq+jj-j, ++JKJQ+Ky++-JkJq+ky-,++JJJQ+Jx
++-JjJq+jx-, ++JKJQ+Kx++-JkJq+kx-, +++JKQyJK++-+jKqyjK-,++YJ+Jj+Jy-+yJ-JJ+j
y

### 长度 21（共 7 个；7 个对称，0 个非对称）

ZiIIk-+JKK++KKJ+-kIIi, x+iJ--+JK+II+KJ+--Ji+, zK+ikj+
JKJIIJKJ+jki+K, zK+jki+JKIJJIKJ+ikj+K,

Z++J+-jjJ-++-Jjj-+J++, XK+J+kj+I-ii-I+jk+J+K, ZIKJ+
j-kKiKKiKk-j+JKI