arXiv:2601.03126v1 [cs.IT] 6 Jan 2026

# 有限阿贝尔群的对偶性及其在编码理论中的应用

JAY A. WOOD

谨以此文悼念故友：*Russell R. Kieckhafer，1954–2025；Randy L. Koehler，1954–2021*

Abstract. 在有限阿贝尔群 $A$ 与其特征群之间选取一个同构，即一种对偶，便可定义 $A$上的加性码的对偶码。本文研究对偶性和对偶码的性质，延续了 Delsarte 于 1973 年开展的工作，以及 Dougherty 及其合作者近年来的研究。

## 1. Introduction

人们对加性码的兴趣日益浓厚，随之而来的是，人们也越来越希望将一些适用于线性码的工具用于加性码，例如对偶码和麦克威廉斯恒等式。本文试图综合阐述如何实现这一点，借鉴了许多作者的研究成果，尤以 Delsarte [3] 以及 Dougherty 及其合作者的工作为主，也包括我本人的一些研究。本文还对文献中出现的若干误解作了纠正。本文力求做到相当完备自足。

^有限阿贝尔群 $A$ 与其特征群 $A$之间的对偶是一个同构 $\phi : A \to \hat{A}$。选择一种对偶等价于存在一个非退化复值内积$\Phi : A \times A \to \mathbb{C}^\times$。Delsarte 的论文 [3] 考虑对称的内积，即 $\Phi(a,b) = \Phi(b,a)$ 对 $a, b \in A$成立；并利用内积定义了复数域 $A$上的加性码的对偶码，同时确立了对偶码的大小条件、双重对偶性以及关于汉明重量的麦克威廉斯恒等式。

本文允许使用非对称内积。与对偶 $\phi : A \to \hat{A}$ 自然关联的是另一个对偶 $\phi^* : \hat{A} \to A$，它是线性变换转置的特征论类比。

2010 数学主题分类。主要分类：20K01, 94B05。关键词与短语。对偶、对偶码、麦克威廉斯恒等式。

相关内积满足 $\Phi^*(a,b) = \Phi(b,a)$ 当 $a, b \in A$时，因此当且仅当 $\Phi$ 为对称内积时，$\phi^* = \phi$ 成立。内积 $\Phi$提供了两种正交性的概念；当 $\Phi$ 为对称内积时，这两种概念相同。如果 $H$ 是 $A$的子群，则可定义左正交补与右正交补如下：

$$\mathfrak{L}(H) = \{a \in A : \Phi(a,h) = 1, \text{ for all } h \in H\},$$
$$\mathfrak{R}(H) = \{a \in A : \Phi(h,a) = 1, \text{ for all } h \in H\}.$$

同样，大小条件成立，即 $|H| \cdot |\mathfrak{L}(H)| = |H| \cdot |\mathfrak{R}(H)| = |A|$，双对偶也成立：$\mathfrak{L}(\mathfrak{R}(H)) = H = \mathfrak{R}(\mathfrak{L}(H))$。完全计数多项式和汉明重量枚举多项式均满足麦克威廉斯恒等式。

通过选择不同的对偶来定义加性码的不同对偶码，这一想法似乎始于 [7]。本文考察 $A$的所有对偶，它们与 $A$的自同构群一一对应。子群的对偶码如何依赖于对偶的选择，这个问题与自同构群 $\mathrm{Aut}(A)$ 对 $A$ 的子群的作用密切相关。例如，当且仅当一个子群是特征子群时，它对每一种对偶都有相同的对偶码。

对偶的合同有一个自然的定义，它将对称双线性形式的合同推广了。若存在 $A$ 的一个自同构 $\tau$，使得相应的内积满足 $\Phi_2(a, b) = \Phi_1(a\tau, b\tau)$，其中 $a, b \in A$，则称 $A$ 的两个对偶合同。粗略地说，合同的对偶除了基变换之外并无区别。

以下简要介绍本文的结构。第 2 节介绍后续各节所需的特征群性质，尤其是形成特征群构成一个正合反变函子，且其平方为恒等函子这一事实。第3节定义对偶性及其相关内积。第 4节讨论加性码及其对偶码，包括大小条件和双重对偶性。第 5节探讨对偶码对对偶性选择的依赖性；第 6节讨论合同；第 7节给出完全枚举式和汉明枚举式的麦克威廉斯恒等式。本文最后在第 8节简述有限环上的对偶性，并提出若干未来研究课题。

致谢。 感谢 Steven T. Dougherty 与我讨论他及其合作者工作的各个方面，鼓励我撰写本文，并为本文早期版本提出意见。

谨以本文纪念 Russ Kieckhafer 和 Randy Koehler；他们是我相交五十余年的朋友。

## 2. Character groups

设 $A$ 是一个有限阿贝尔群。 $A$ 的特征 $\pi$ 是一个群同态 $\pi: A \to \mathbb{C}^\times$，其中 $\mathbb{C}^\times$ 是所有非零复数构成的乘法群。将 $A$的群运算记作加法，则特征 $\pi$ 满足 $\pi(a_1 + a_2) = \pi(a_1)\pi(a_2)$，对所有$a_1, a_2 \in A$均成立。

记$A = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$为$A$的所有特征的集合。因此$(\pi_1\pi_2)(a) = \pi_1(a)\pi_2(a)$ 下构成一个乘法阿贝尔群，其中$\pi_1, \pi_2 \in A$且 $a \in A$。 $A$ 的单位元是平凡特征，其所有取值均为 1。我们称 $A$ 为 $A$ 的特征群。我们采用如下约定：将特征 $\pi \in A$ 在元素 $a \in A$ 处的取值记作 $\langle \pi \,|\, a \rangle = \pi(a) \in \mathbb{C}^\times$。如果需要明确指出群，我们记作 $\langle \pi \,|\, a \rangle_A$。因此，特征的同态性质以及 $A$ 中群运算的定义可表示为：

$$\langle \pi \,|\, a_1 + a_2 \rangle = \langle \pi \,|\, a_1 \rangle \langle \pi \,|\, a_2 \rangle, \quad \pi \in \widehat{A}, \quad a_1, a_2 \in A; \tag{2.1}$$

$$\langle \pi_1\pi_2 \,|\, a \rangle = \langle \pi_1 \,|\, a \rangle \langle \pi_2 \,|\, a \rangle, \quad \pi_1, \pi_2 \in \widehat{A}, \quad a \in A. \tag{2.2}$$

注记 2.3. 也可以将特征定义为群同态 $\varpi: A \to \mathbb{Q}/\mathbb{Z}$, 因此，特征群是 $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$,参见 [18, §2.2]。由于 $A$ 是有限的，$\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})$ 与 Hom 同构$_{\mathbb{Z}}(A, \mathbb{C}^\times)$ 通过 $\varpi \mapsto \pi$，其中

$$\pi(a) = \exp(2\boldsymbol{\pi} i \varpi(a)), \quad a \in A,$$

其中 exp 是复指数函数，而 $\boldsymbol{\pi}$ 是众所周知的常数。请注意：在如下所示的公式（2.19）中，必须使用 $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$。

接下来的几个结果概述了特征群的一些基本性质，其编排旨在迅速切入主题。这些结果取自诸如 [15, 16, 17, 18]等资料。

**引理 2.4**。 若 $A$ 是有限循环群，则 $A \cong A$。若 $a \neq 0$，则存在一个特征 $\pi \in A$，使得 $\pi(a) \neq 1$。

证明。 设 $m = |A|$，并令 $\gamma$ 为 $A$ 的一个生成元。固定 $\mathbb{C}^\times$ 中的一个本原 $m$ 次单位根 $\zeta_m$。任意特征 $\pi \in A$ 都完全由 $\pi(\gamma)$ 的取值决定，而该取值是一个 $m$ 次单位根。定义函数 $f: \mathbb{Z}/m\mathbb{Z} \to \widehat{A},\ j \mapsto f_j,$，其中 $f_j(\gamma) = \zeta_m^j$。容易验证， $f$ 是一个群同构。由于 $A \cong \mathbb{Z}/m\mathbb{Z},$，我们有 $A \cong A$。

对于任意与 $m$ 互素的 $k$，$\zeta_m^k$ 都是一个本原 $m$ 次单位根。因此，特征 $f_k : A \to \mathbb{C}^\times$ 是单射，所以对于任意 $a \neq 0$，都有 $f_k(a) \neq 1$。□

注记 2.5. 引理 2.4 中的同构通常并不唯一：它取决于生成元的选择 $\gamma$ 属于 $A$ 以及本原 $m$次单位根 $\zeta_m$。这预示了命题 3.1。

**引理 2.6。** 设 $A_1, A_2$ 是有限阿贝尔群。那么

$$\widehat{A_1 \times A_2} \cong \widehat{A}_1 \times \widehat{A}_2.$$

证明。给定一个特征 $\pi \in A_1 \times A_2$，定义 $\pi_1 \in A_1$ 和 $\pi_2 \in A_2$ 如下

$$\pi_1(a_1) = \pi(a_1, 0), \quad \pi_2(a_2) = \pi(0, a_2), \quad a_1 \in A_1, a_2 \in A_2.$$

反过来，给定 $\pi_1 \in A_1$ 和 $\pi_2 \in A_2$，定义 $\pi \in A_1 \times A_2$ 如下

$$\pi(a_1, a_2) = \pi_1(a_1)\pi_2(a_2), \quad (a_1, a_2) \in A_1 \times A_2.$$

容易验证，这些定义给出了互为逆映射的同态。□

**引理 2.7。** 设 $H \subseteq A$ 是有限阿贝尔群 $A$的子群。若 $\theta \in \widehat{H}$，则存在一个特征 $\pi \in \widehat{A}$ 延拓了 $\theta$，即$\pi(h) = \theta(h)$ 对所有 $h \in H$均成立。

证明。若 $H = A$，则无需证明。若 $H \neq A$，任取满足 $g \notin H$的 $g \in A$，并令 $P$ 为由 $H$ 和 $g$生成的 $A$ 的子群；$|P| > |H|$因为 $g \notin H$。我们将把 $\theta$延拓为 $P$上的一个特征 $\pi$。

令 $m$ 为 $g$的阶，并用 $\langle g \rangle$表示由 $g$生成的循环子群。若 $H \cap \langle g \rangle = \{0\}$，在 $\mathbb{C}^\times$中任取一个 $m$次单位根 $\zeta$。定义

$$\pi(a) = \begin{cases} \theta(a), & a \in H, \\ \zeta, & a = g, \end{cases} \tag{2.8}$$

并将其延拓为一个同态，我们得到 $P$ 上的特征 $\pi$，它延拓了 $\theta$。

若 $H \cap \langle g \rangle \neq \{0\}$，令 $k$ 为满足以下条件的最小正整数：$H \cap \langle g \rangle = \langle kg \rangle$。任取 $k$次根 $\zeta$，满足 $\theta(kg) \in \mathbb{C}^\times$。同样使用（2.8），并将其延拓为同态，从而得到良定义的特征 $\pi$，定义在$P$ 上，并延拓了 $\theta$。

如果 $P$ 是子群，则我们已经完成。否则，只需有限次重复此过程。□

命题 *2.9*。 *</style>*设 $A$ 为有限阿贝尔群。则 $A \cong \widehat{\widehat{A}}$。特别是，在 $\widehat{\widehat{A}}$ 中， $|A| = |\widehat{A}|$。如果 $a \neq 0$，则存在一个特征 $\pi \in \widehat{A}$ ，使得$\pi(a) \neq 1$。

证明。 群 $A$ 根据有限阿贝尔群基本定理，是素数幂阶循环群的直积 [12, 第一章，§10]。然后应用引理 2.4 和 2.6。

若 $a \neq 0$，令 $H$ 为由 $a$生成的子群，并由引理 2.4，$\widehat{H}$ 令 $\theta \in \widehat{H}$ 为满足 $\theta(a) \neq 1$的特征。然后由引理将 $\theta$ 延拓到 $\pi \in \widehat{A}$2.7。 □

如注记 2.5所示，同构 $A \cong \widehat{A}$ 通常并不唯一。

给定两个有限阿贝尔群 $A_1$， $A_2$ 以及一个同态 $\alpha : A_1 \to A_2$，存在一个诱导同态 $\alpha^* : \widehat{A}_2 \to \widehat{A}_1$ ，定义为

$$\langle \alpha^*(\pi_2) \,|\, a_1 \rangle_{A_1} = \langle \pi_2 \,|\, \alpha(a_1) \rangle_{A_2}, \quad a_1 \in A_1, \quad \pi_2 \in \widehat{A}_2. \tag{2.10}$$

若 $\alpha$ 可逆，则可验证 $(\alpha^*)^{-1} = (\alpha^{-1})^*$。

对于任意有限阿贝尔群 $A$，定义一个从 $A$到其双重特征群 $\mathrm{Hom}_{\mathbb{Z}}(\widehat{A}, \mathbb{C}^\times)$ 的同态 eval，定义为

$$\langle \mathrm{eval}(a) \,|\, \pi \rangle_{\widehat{A}} = \langle \pi \,|\, a \rangle_A, \quad a \in A, \quad \pi \in \widehat{A}. \tag{2.11}$$

也就是说，$\mathrm{eval}(a)$ 是“在 $a$ 处取值”的特征 $\widehat{A}$。

**命题 2.12**。 对于任意有限阿贝尔群 $A$，同态eval: $A \to \mathrm{Hom}_{\mathbb{Z}}(\widehat{A}, \mathbb{C}^\times)$ 是一个同构。

证明。 考虑 eval 的核。如果 $a \in \ker \mathrm{eval}$，则 $\langle \pi \,|\, a \rangle = 1$对所有 $\pi \in \widehat{A}$ 均成立。由命题 2.9 可知，如果 $a \neq 0$，则存在一个特征 $\pi$ 满足 $\pi(a) \neq 1$。因此 $\ker \mathrm{eval} = 0$，且 eval 是单射。命题 2.9应用两次可推出 $|A| = |\mathrm{Hom}_{\mathbb{Z}}(\widehat{A}, \mathbb{C}^\times)|$因此 eval 也是满射。 □

令**FinAb** 为这样一个范畴：其对象是所有有限阿贝尔群，态射是群同态。定义 $\mathcal{F} : \widehat{\mathbf{FinAb}} \to \mathbf{FinAb}$如下 $\mathcal{F}(A) = \widehat{A}$并且 $\mathcal{F}(\alpha) = \alpha^*$，其中 $\alpha : A_1 \to A_2$是一个态射。下一个结果表明， $\mathcal{F}$ 是一个 Morita 对偶函子；参见 [17, 定理 3。2]。

**命题 2.13.** 如上所定义， $\mathcal{F} : \mathbf{FinAb} \to \mathbf{FinAb}$是一个正合反变函子，使得 $\mathcal{F}^2$ 与恒等函子自然等价。

证明。根据 $\alpha^*$ 的定义，函子 $\mathcal{F}$ 是逆变的。当然， $\mathcal{F}^2(A) = \mathrm{Hom}_{\mathbb{Z}}(\widehat{A}, \mathbb{C}^\times)$。可以验证，对于有限阿贝尔群

$A_1$、 $A_2$ 和态射 $\alpha:\ A_1 \to A_2$，下图交换：

$$\begin{array}{ccc} A_1 & \xrightarrow{\text{eval}} & \mathrm{Hom}_{\mathbb{Z}}(\widehat{A}_1, \mathbb{C}^\times) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^{**}} \\ A_2 & \xrightarrow{\text{eval}} & \mathrm{Hom}_{\mathbb{Z}}(\widehat{A}_2, \mathbb{C}^\times). \end{array}$$

确实，对于 $a_1 \in A_1$， $\pi_2 \in A_2$，并利用（2.10）和（2.11），我们有

$$\langle \mathrm{eval}(\alpha(a_1)) \,|\, \pi_2 \rangle_{\widehat{A}_2} = \langle \pi_2 \,|\, \alpha(a_1) \rangle_{A_2} = \langle \alpha^*(\pi_2) \,|\, a_1 \rangle_{A_1},$$
$$\langle \alpha^{**}(\mathrm{eval}(a_1)) \,|\, \pi_2 \rangle_{\widehat{A}_2} = \langle \mathrm{eval}(a_1) \,|\, \alpha^*(\pi_2) \rangle_{\widehat{A}_1} = \langle \alpha^*(\pi_2) \,|\, a_1 \rangle_{A_1}.$$

为验证正合性，任取有限阿贝尔群的一个短正合列

$$0 \longrightarrow H \xrightarrow{\alpha} A \xrightarrow{\beta} Q \longrightarrow 0\ .$$

我们需要证明相应的序列

$$1 \longleftarrow \widehat{H} \xleftarrow{\alpha^*} \widehat{A} \xleftarrow{\beta^*} \widehat{Q} \longleftarrow 1 \tag{2.14}$$

也是一个短正合列。

设 $\pi \in \ker\, \beta^*$。这意味着对所有 $a \in A$，都有 $\langle \beta^*(\pi) \,|\, a \rangle_A = 1$。于是，$1 = \langle \pi \,|\, \beta(a) \rangle_Q$ 对所有 $a \in A$均成立。因此， $\pi \in Q$ 是平凡的，因为 $\beta$ 是满射。

由于 $\mathrm{im}\, \alpha \subseteq \ker\, \beta$，我们有 $\mathrm{im}\ \beta^* \subseteq \ker\ \alpha^*$。反过来，假设$\pi \in \ker\ \alpha^*$。这意味着，对于任意 $h \in H$， $1 = \langle \alpha^*(\pi) \,|\, h \rangle_H = \langle \pi \,|\, \alpha(h) \rangle_A$。因此， $\pi$在 $\mathrm{im}\, \alpha = \ker\ \beta$上为零。这说明 $\pi$可下降为 $Q$ 上良定义的特征 $\tilde{\pi}$：
$\langle \pi \,|\, a \rangle_A = \langle \tilde{\pi} \,|\, \beta(a) \rangle_Q = \langle \beta^*(\tilde{\pi}) \,|\, a \rangle_A$。因此， $\pi = \beta^*(\tilde{\pi}) \in \mathrm{im}\, \beta^*$，且 $\ker\ \alpha^* = \mathrm{im}\ \beta^*$。

最后， $\alpha^*$ 由引理 2.7可知是满射。 □

从这里开始，我们将通过求值映射把 $A$ 与 $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$ 视为相同。利用这一识别，我们有

$$\alpha^{**} = \alpha, \tag{2.15}$$

对于任意同态 $\alpha : A_1 \to A_2$。

如果 $H \subseteq A$ 是有限阿贝尔群 $A$ 的子群，其 湮灭子 是由 $\widehat{\ }$ 和 $A$ 定义的子群

$$(\widehat{A} : H) = \{\pi \in \widehat{A} : \langle \pi \,|\, h \rangle = 1 \text{ for all } h \in H\}. \tag{2.16}$$

**推论 2.17**。 对于有限阿贝尔群 $A$ 及子群 $H \subseteq A$，

$\widehat{\ \ }$ $\widehat{\ }$ $\sim A/H \cong (A:\ \ H)$。特别地， $|(A : H)| = |A|/|H|$。通过 eval，将 $A$ 和 $\widehat{\ }\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$ 视为同一对象，我们有

$$(A : (\widehat{A} : H)) = H.$$

证明。在（2.14）的记号下，$A/H = Q \cong$ 像 $\beta^* =$ 核 $\alpha^*$，但核 $\alpha^* = (A : H)$。现在由命题 2.9 即可得到大小关系。

至于双重湮灭子，$H \subseteq (A : (A : H))$ 可直接由 $(A$ 的定义得到：$H)$。然后将大小关系应用两次即可得到相等性。□

命题 *2.18*。*</style}*对于有限阿贝尔群 $A$、子群 $H \subseteq A$ 以及 $\pi \in A$，

$$\sum_{h\in H}\langle \pi \,|\, h\rangle = \begin{cases} |H|, & \pi \in (\widehat{A} : H), \\ 0, & \pi \notin (\widehat{A} : H). \end{cases} \tag{2.19}$$

对偶地，对于子群 $E \subseteq A$ 和 $a \in A$，

$$\sum_{\pi\in E}\langle \pi \,|\, a\rangle = \begin{cases} |E|, & a \in (A : E), \\ 0, & a \notin (A : E). \end{cases}$$

证明。</style}若 $\pi \in (A : H)$，则对所有 $h \in H$ 都有 $\langle \pi \,|\, h\rangle = 1$；该和等于 $|H|$。若 $\pi \notin (A : H)$，则存在 $h_0 \in H$ 使得 $\langle \pi \,|\, h_0\rangle \neq 1$。通过利用 $h = h_0 + h'$ 对该和重新编号，我们得到

$$\sum_{h\in H}\langle \pi \,|\, h\rangle = \sum_{h'\in H}\langle \pi \,|\, h_0 + h'\rangle = \sum_{h'\in H}\langle \pi \,|\, h_0\rangle\langle \pi \,|\, h'\rangle = \pi(h_0)\sum_{h'\in H}\langle \pi \,|\, h'\rangle.$$

由于 $\langle \pi \,|\, h_0\rangle \neq 1$，该和必为零。 □

通过选择 $H = A$ 和 $E = A$ 在命题2.18中，并使用命题2.9，我们得到以下推论。

**推论 2.20**。设 $A$ 为有限阿贝尔群。对于 $\pi \in A$ 和 $a \in A$，

$$\sum_{a\in A}\langle \pi \,|\, a\rangle = \begin{cases} |A|, & \pi = 1, \\ 0, & \pi \neq 1; \end{cases} \qquad \sum_{\pi\in \widehat{A}}\langle \pi \,|\, a\rangle = \begin{cases} |A|, & a = 0, \\ 0, & a \neq 0. \end{cases}$$

有限阿贝尔群基本定理表明，任意有限阿贝尔群都可以写成若干个素数幂阶循环子群的直积。循环子群的数量和阶是唯一确定的，但这些子群本身通常并不唯一。例如，在维数至少为 2 的有限域 $\mathbb{F}_p$ 上的有限维向量空间中，基的选择有很多种。

有限阿贝尔群存在一种较粗分解，按素数逐个进行，其优点是分量子群是唯一的。

设 $A$ 是一个有限阿贝尔群。我们知道，任意元素 $a \in A$ 的阶 $o(a)$ 必须整除 $|A|$。对于每个整除 $|A|$ 的素数 p $p$，

定义 $A_p = \{a \in A\colon\ o(a) = p^k$，其中 $k\}$ 是某个整数。可以证明， $A_p$ 是 $A$ 的子群。令 $\mathrm{Aut}(A)$ 为 $A$ 的自同构群。

**命题 2.21.** 设 $A$是一个有限阿贝尔群， $s(A)$是整除 $|A|$的素数集合。那么，

- 对于 $p \in s(A)$， $A_p$ 是一个 $p$-群；
- $A = \oplus_{p\in s(A)} A_p$；• 自同构群
- $(A) = \oplus_{p\in s(A)}$自同构群$(A_p)$。

证明. 前两项是 [12, 第一章，§10]中的定理 5。自同构群 $\mathrm{Aut}(A)$ 的分解可由以下观察得出：对于互不相同的素数 $p \neq \ell$，任意同态 $\alpha$ : $A_p \to A_\ell$ 必为零同态，因为 $|\mathrm{im}\,\alpha|$ 必须同时整除 $|A_p|$ 和 $|A_\ell|$。 □

命题 2.21 使我们能够一次考察一个素数，从而研究有限阿贝尔群。

## 3. Dualities and inner products

为了定义有限阿贝尔群上的加法码$A$ 及其对偶码，我们遵循 [3, 7] 并定义 $A$ 及其相关内积的对偶。

设 $A$是一个有限阿贝尔群。其对偶是 $A$ 群同构态$\widehat{\ }$ $\widehat{\ }$射 $\phi$ : $A \to A$。令 $\mathrm{Isom}(A, A)$ 为$\backsim A$的所有对偶组成的集合。根据命题2.9，对偶存在，因此 $\mathrm{Isom}(A, A)$ 非空。正如备注2.5中所述，$A$通常不止有一个对偶。下面的命题3.1 将对此作出明确说明。

设$A$是一个对偶。定义映射 $f$ : $\mathrm{Aut}(A) \to \mathrm{Isom}(A, \widehat{A})$，将 $\tau \in \mathrm{Aut}(A)$映射为复合 $A \overset{\tau}{\to} A \overset{\phi_0}{\to} \widehat{A}$。

$\widehat{\ }$**命题 3.1**。 映射 $f$ : 自同构群$(A) \to$ 同构集$(A, A)$ 是一个双射。$\widehat{\ }$特别地， $|$同构集$(A, A)| = |$自同构群$(A)|$。

$\widehat{\ }$ $\widehat{\ }$证明。 定义映射 $g$: 同构集$(A, A) \to$自同构群$(A)$，将 $\phi \in$同构集$(A, A)$映到复合映射 $A \overset{\phi}{\to} \widehat{A} \overset{\phi_0^{-1}}{\to} A$, ，这是一个自同构 $\tau \in$自同构群$(A)$，其中 $\phi_0 \circ \tau = \phi$。可验证 $f$ 和 $g$ 互为逆映射，因此它们是双射。□

$\widehat{\ }$ $\widehat{\ }$假设 $\phi$ : $A \to A$ 是 $A$的一个对偶。由于 $A$ 和 $A$ 都是有限阿贝尔群，且 $\phi$是它们之间的一个同态，故（2.10）所诱导的同态，即

$$\phi^* : \mathrm{Hom}_{\mathbb{Z}}(\widehat{A}, \mathbb{C}^\times) = A \to \widehat{A}$$

^也是一个对偶。若对偶 $\phi\colon A \to A$ 是对称的，则称其$\phi^* = \phi$。根据（2.15），对于任意对偶 $\phi^{**} = \phi$，总有 $\phi$。

^**引理 3.2.** 设 $A$ 是一个有限阿贝尔群，且 $\phi\colon A \to A$ 是 $A$的一个对偶。那么，

$$\langle \phi^*(a) \,|\, b\rangle = \langle \phi(b) \,|\, a\rangle, \quad a, b \in A.$$

因此，$\phi$是对称的，当且仅当对所有 $a$、$b \in A$，$\langle \phi(b) \,|\, a\rangle = \langle \phi(a) \,|\, b\rangle$。

^证明。 关键在于揭示 $A$ 和 $\mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{C}^\times)$通过 eval 建立的对应关系。利用（2.10）和（2.11），对所有 $a$，$b \in A$，

$$\begin{aligned}\langle \phi^*(a) \,|\, b\rangle_A &= \langle \phi^*(\mathrm{eval}(a)) \,|\, b\rangle_A \\ &= \langle \mathrm{eval}(a) \,|\, \phi(b)\rangle_{\widehat{A}} = \langle \phi(b) \,|\, a\rangle_A.\end{aligned}$$

□

**引理 3.3** ([4, 推论 4.2])。 设 $A$ 是一个有限循环群。那么，$A$ 的每个对偶都是对称的。

证明。 令 $m = |A|$。设 $\gamma$ 是 $A$的一个生成元，且 $\zeta_m$ 是 $\backsim m$在 $\mathbb{C}$中的一个本原 次单位根。对每个 $j \in \mathbb{Z}/m\mathbb{Z},$，定义特征 $\pi_j \in A$ 为$\pi_j(\gamma^i) = \zeta_m^{ij}$，其中 $i \in \mathbb{Z}/m\mathbb{Z}$。我们在引理 2.4 的证明中看到，$A$ 的每个特征都具有这种形式。

定义 $\phi_0\colon A \to \widehat{A}$ 由 $\phi_0(\gamma^i) = \pi_i$给出。容易验证，$\phi_0$ 是一个对偶。由于对于所有 $i$都有 $\langle \pi_i \,|\, \gamma^j\rangle = \zeta_m^{ij} = \langle \pi_j \,|\, \gamma^i\rangle$，引理 3.2 蕴含 $\phi_0$ 是对称的。众所周知，$A$ 的自同构由将 $\gamma$ 映射为 $\gamma^k$所诱导，其中 $k$ 与 $m$互素。因此$\phi(\gamma^i) = \phi_0(\gamma^{ki})$，$i \in \mathbb{Z}/m\mathbb{Z},$ 定义了 $A$的另一个对偶；根据命题 3.1，$A$ 的每个对偶都具有这种形式。于是 $\langle \phi(\gamma^i) \,|\, \gamma^j\rangle = \langle \phi_0(\gamma^{ki}) \,|\, \gamma^j\rangle = \zeta_m^{kij} = \langle \phi_0(\gamma^{kj}) \,|\, \gamma^i\rangle = \langle \phi(\gamma^j) \,|\, \gamma^i\rangle$，并且根据引理 3.2，$\phi$是对称的。□

**引理 3.4**。 设 $A_1$、$A_2$ 为有限阿贝尔群。若 $\phi_1$、$\phi_2$ 分别是 $A_1$、$A_2$ 的对称对偶，则 $\phi_1 \times \phi_2$ 是 $A_1 \times A_2$的对称对偶。

证明。 利用引理 2.6，可以验证引理 3.2中的条件。 □

**命题 3.5**。 设 $A$ 是一个有限阿贝尔群。那么，$A$至少存在一个对称对偶。

证明。 将 $A$ 根据有限阿贝尔群基本定理写成有限循环群的直积。然后使用引理 3.3 和 3.4。 □

注记 3.6。 注意！命题 3.5的证明并未说明有限阿贝尔群的每个对偶都是对称的。原因在于，引理 3.4 仅适用于具有以下形式的直积的对偶：

其“对角”形式 $\phi_1 \times \phi_2$。尤其重要的是 $A_1 = A_2$ 这一情形，此时 $A_1 \times A_2$ 的自同构不止对角自同构。例 3.7对此有进一步讨论。

**例 3.7.** 设 $p$ 是素数，并假设 $A$ 是阶为 $p^n$的初等阿贝尔 $p$-群。那么 $A$ 同构于某个有限域 $\mathbb{F}_p$上维数为 $n$ 的向量空间的底层阿贝尔群。将 $A$的元素视为行向量 $a = [a_1, a_2, \ldots\ldots, a_n]$，其中每个 $a_i \in \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$。$A$ 的自同构由 $\mathbb{F}_p$ 上的可逆 $n \times n$矩阵给出，这些矩阵通过矩阵乘法从右侧作用于 $A$；即 $\mathrm{Aut}(A) = \mathrm{GL}(n, \mathbb{F}_p)$。

在 $\mathbb{C}$中取一个本原 $p$次单位根 $\zeta_p$。对于 $a \in A$，定义 $\pi_a \in \widehat{A}$ by

$$\langle \pi_a \,|\, b \rangle = \zeta_p^{ab^\top} \in \mathbb{C}^\times, \quad b \in A.$$

那么 $\phi_0 : A \to A$，$\phi_0(a) = \pi_a$，是一个对称对偶。根据命题 3.1，其他任一对偶 $\phi : A \to A$ 都具有如下形式 $\phi(a) = \phi_0(aP)$，其中 $P \in \mathrm{GL}(n, \mathbb{F}_p)$。因此 $\langle \phi(a) \,|\, b \rangle = \langle \pi_{aP} \,|\, b \rangle = \zeta_p^{aPb^\top}$。那么 $\phi^* : A \to A$ 由下式给出

$$\langle \phi^*(a) \,|\, b \rangle = \langle \phi(b) \,|\, a \rangle = \zeta_p^{bPa^\top} = \zeta_p^{aP^\top b^\top},$$

这里用到了以下事实：$bPa^\top$ 是一个 $1 \times 1$ 矩阵，因此等于其自身的转置。于是 $\phi^*(a) = \pi_{aP^\top}$，并且 $\phi$ 是对称的，当且仅当 $P$是对称的。关于对称对偶性的这一刻画与 [4, 定理 2。5] 和 [9, 引理 4]中的刻画相矛盾；后者的修正见 [6]。

对称性是常见还是罕见？下一个结果表明，至少在向量空间上，对称对偶性渐近地说是罕见的。此结果也由他人独立得到，见 [6]。

**命题 3.8。** 设 $A = \mathbb{F}_p^n$。对于固定的素数 $p$ $p$，$A$ 的一个对偶是对称的概率趋于$0$，当 $n \to \infty$ 时。同样，对于固定的 $n$，$A$ 的一个对偶是对称的概率趋于$0$，当素数 $p \to \infty$ 时。

证明。对偶 $\phi$: $A \to A$ 是对称的概率为

$$\frac{|\{P \in \mathrm{GL}(n, \mathbb{F}_p) : P = P^\top\}|}{|\mathrm{GL}(n, \mathbb{F}_p)|}.$$

MacWilliams [13, 素数 p。 156] 给出了任意有限域 $\mathbb{F}_q$上对称可逆矩阵 $n \times n$ 的数量 $N(n)$：

$$N(2t) = \prod_{i=1}^{t} (q^{2t+1} - q^{2i}), \quad N(2t+1) = \prod_{i=0}^{t} (q^{2t+1} - q^{2i}). \tag{3.9}$$

可逆矩阵的数量为

$$|\mathrm{GL}(n,\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i).$$

对于 $n$ 偶数或奇数，也就是说，分别对于 $n=2t$ 或 $n=2t+1$，我们有

$$\frac{N(2t)}{|\mathrm{GL}(2t,\mathbb{F}_q)|} = \frac{q^t}{\prod_{j=0}^{t-1}(q^{2t}-q^{2j})} < \frac{q^t}{q^{2t}-1},$$
$$\frac{N(2t+1)}{|\mathrm{GL}(2t+1,\mathbb{F}_q)|} = \frac{1}{\prod_{j=1}^{t}(q^{2t+1}-q^{2j-1})} < \frac{1}{q^{2t+1}-1}.$$

两种情况下，当固定 $q\geqslant 2$ 且令 $t\to\infty$ （或固定 $t\geqslant 1$ 且令 $q\to\infty$）时，该比值都趋于 0。当然，将 $q$ 限制为素数 $p$时，结论也同样成立。□

我们以描述有限阿贝尔群 $A$上的内积作为本节的结尾，并证明 $A$ 上的对偶性等价于 $A$上的内积。这部分内容几乎全部可见于 Delsarte[3, §6。1]。

设 $A$ 是一个有限阿贝尔群。若函数 $\Psi\colon A\times A\to\mathbb{C}^\times$ 满足以下性质，则称其为 $A$上的内积：

- $\Psi(a_1+a_2,\ b)=\Psi(a_1,\ b)\Psi(a_2,\ b)$，对所有 $a_1,\ a_2,\ b\in A$；
- $\Psi(a,\ b_1+b_2)=\Psi(a,\ b_1)\Psi(a,\ b_2)$，对所有 $a,\ b_1,\ b_2\in A$；
- 若 $\Psi(a,\ b)=1$ 对所有 $b\in A$均成立，则 $a=0$；• 若 $\Psi(a,\ b)=1$ 对所有 $a\in A$均成立，则 $b=0$。

此外，若对于所有 $a,b\in A$，都有 $\Psi(a,b)=\Psi(b,a)$，则称 $\Psi$ 为对称的。注意，Delsarte 将对称性纳入内积的定义中；我们则不这样做。取值于 $\mathbb{Q}/\mathbb{Z}$ 而非 $\mathbb{C}^\times$ 的内积，在 [14, 18] 中也占有重要地位。

**备注 3.10。** 当 $n\in\mathbb{Z}$ 时，注意 $\Psi(na,b)=(\Psi(a,b))^n$。

给定有限阿贝尔群 $A$ 的一个对偶 $\phi$，定义 $\Phi\colon A\times A\to\mathbb{C}^\times$:

$$\Phi(a,b)=\langle\phi(a)\,|\,b\rangle,\quad a,b\in A. \tag{3.11}$$

反过来，给定一个内积 $\Psi\colon A\times A\to\mathbb{C}^\times$，定义 $\psi\colon A\to A$:

$$\langle\psi(a)\,|\,b\rangle=\Psi(a,b),\quad a,b\in A. \tag{3.12}$$

**命题 *3.13.*** 若 $\phi: A\to A$ 是 $A$的对偶，则 ***(3.11)*** 中的 $\Phi$ 是 $A$上的内积。反之，若 $\Psi: A\times A\to\mathbb{C}^\times$ 是 $A$上的内积，则 ***(3.12)*** 中的 $\psi$ 是 $A$的对偶。此外，对于 $A$的任意对偶 $\phi$: $A\to A$，与对偶 $\phi^*$: $A\to A$ 相关联的内积 $\Phi^*$ 满足：对于所有 $a,b\in A$，均有 $\Phi^*(a,b)=\Phi(b,a)$。特别地，

对偶 $\phi$ 是对称的，当且仅当其相关联的内积 $\Phi$是对称的。

证明。要使 $\Phi$ 成为内积，前两个性质由（2.1）、（2.2）以及 $\phi$ 是同态可得。第三个性质成立，是因为 $\phi$ 是单射；第四个性质则根据命题 2.9成立，因为 $\phi$是满射。基本相同的论证可得$\psi$ 是一个对偶。关于 $\Phi^*$ 与 $\Phi$之间的关系，以及关于对称性的陈述，均由引理 3.2得出。□

**例 3.14**。令 $A = \mathbb{F}_2^2$为克莱因四元群。将$A$中的元素写成对 $ab$，其中 $a, b \in \mathbb{F}_2$。于是 $\mathrm{Aut}(A) = \mathrm{GL}(2, \mathbb{F}_2)$，它同构于阶为 6 的二面体群 $D_3$（也同构于 3 次对称群）。这些自同构置换 $\mathbb{F}_2^2$中的三个非零向量。

将 $A$ 的对称对偶 $\phi_0$ 定义为

$$\Phi_0(ab, cd) = \langle \phi_0(ab) \,|\, cd \rangle = (-1)^{ac+bd} = (-1)^{ab[cd]^\top}.$$

特征标 $\pi_i = \phi_0(ab)$ 的取值如下：

| $\pi$ | $ab$ | $\langle \pi \,\|\, 00 \rangle$ | $\langle \pi \,\|\, 01 \rangle$ | $\langle \pi \,\|\, 10 \rangle$ | $\langle \pi \,\|\, 11 \rangle$ |
|---|---|---|---|---|---|
| $\pi_0$ | 00 | 1 | 1 | 1 | 1 |
| $\pi_1$ | 01 | 1 | −1 | 1 | −1 |
| $\pi_2$ | 10 | 1 | 1 | −1 | −1 |
| $\pi_3$ | 11 | 1 | −1 | −1 | 1 |

对于 $P \in \mathrm{Aut}(A)$ 中的六个元素，下面列出了相关对偶性 $\phi_P(ab) = \phi_0(abP)$，以及 $\phi_P^*$ 和 $P$ 的群阶 $o(P)$。

| $\phi_i$ | $P$ | $\phi_P(00)$ | $\phi_P(01)$ | $\phi_P(10)$ | $\phi_P(11)$ | $\phi_P^*$ | $o(P)$ |
|---|---|---|---|---|---|---|---|
| $\phi_0$ | $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$ | $\pi_0$ | $\pi_1$ | $\pi_2$ | $\pi_3$ | $\phi_0$ | 1 |
| $\phi_1$ | $\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]$ | $\pi_0$ | $\pi_2$ | $\pi_3$ | $\pi_1$ | $\phi_1$ | 3 |
| $\phi_2$ | $\left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right]$ | $\pi_0$ | $\pi_3$ | $\pi_1$ | $\pi_2$ | $\phi_2$ | 3 |
| $\phi_3$ | $\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$ | $\pi_0$ | $\pi_2$ | $\pi_1$ | $\pi_3$ | $\phi_3$ | 2 |
| $\phi_4$ | $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ | $\pi_0$ | $\pi_1$ | $\pi_3$ | $\pi_2$ | $\phi_5$ | 2 |
| $\phi_5$ | $\left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right]$ | $\pi_0$ | $\pi_3$ | $\pi_2$ | $\pi_1$ | $\phi_4$ | 2 |

六个对偶中有四个是对称的：$\phi_i$，$i = 0, 1, 2, 3$。其余两个对偶 $\phi_4$，$\phi_5$构成一对非对称对偶：$\phi_4^* = \phi_5$ 和$\phi_5^* = \phi_4$。相同的对偶也列在 [9, 例 2], 中，但其中的对称性（ [4, 定理 2。5]中也是如此）与群阶相关，这与上表相矛盾。该表表明，自同构的阶无法决定其对应的对偶是否对称。

**例 3.15**。设 $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$。将 $A$ 的元素写成一对 $ab$，其中 $a \in \mathbb{Z}/2\mathbb{Z}$ 且 $b \in \mathbb{Z}/4\mathbb{Z}$。元素 **01**，**03**，**11**，**13** 中的

$A$ 的阶为 4，而元素 02，10，12 的阶为 2。群 $A$ 的一组生成元是 $\{10,\ 01\}$。$A$ 的任意特征都由其在生成元上的取值决定。

定义一个对称对偶 $\phi_0$ of $A$ 如下：

$$\Phi_0(ab, cd) = \langle \phi_0(ab) \,|\, cd \rangle = (-1)^{ac} i^{bd}.$$

$\pi_i = \phi_0(ab)$ of $A$ 的特征标如下列出，$ab$ 垂直方向，$cd$ 水平方向，表项等于 $\Phi_0(ab, cd) = \langle \phi_0(ab) \,|\, cd \rangle$。

| | | 00 | 01 | 02 | 03 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|
| $\pi_0$ | 00 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $\pi_1$ | 01 | 1 | $i$ | $-1$ | $-i$ | 1 | $i$ | $-1$ | $-i$ |
| $\pi_2$ | 02 | 1 | $-1$ | 1 | $-1$ | 1 | $-1$ | 1 | $-1$ |
| $\pi_3$ | 03 | 1 | $-i$ | $-1$ | $i$ | 1 | $-i$ | $-1$ | $i$ |
| $\pi_4$ | 10 | 1 | 1 | 1 | 1 | $-1$ | $-1$ | $-1$ | $-1$ |
| $\pi_5$ | 11 | 1 | $i$ | $-1$ | $-i$ | $-1$ | $-i$ | 1 | $i$ |
| $\pi_6$ | 12 | 1 | $-1$ | 1 | $-1$ | $-1$ | 1 | $-1$ | 1 |
| $\pi_7$ | 13 | 1 | $-i$ | $-1$ | $i$ | $-1$ | $i$ | 1 | $-i$ |

与特征标一样，$A$ 的一个自同构完全由其在生成元上的取值确定。一个自同构必须将 01 映到阶为 4 的元素之一，并将 10 映到 10 或 12（不能映到 02，因为 02 是每个阶为 4 的元素的两倍）。将每个自同构写成一个 $2 \times 2$ 矩阵，第一行等于 10 的像，第二行等于 01 的像。令

$$\sigma = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix},$$

由此可看出，Aut$(A)$ 是阶为 8 的二面体群 $D_4$，其中有$\sigma^2 = I$、$\tau^4 = I$和 $\tau\sigma = \sigma\tau^3$。

对于 $P \in$Aut$(A)$ 中的八个元素，相关对偶性如下$\phi_P(ab) = \phi_0(abP)$。

| | $\sigma^\epsilon \tau^j$ | $P$ | $\phi_P(01)$ | $\phi_P(10)$ | $\phi_P^*$ |
|---|---|---|---|---|---|
| $\phi_0$ | $I$ | $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ | $\pi_1$ | $\pi_4$ | $\phi_0$ |
| $\phi_1$ | $\tau$ | $\left[\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right]$ | $\pi_5$ | $\pi_6$ | $\phi_1$ |
| $\phi_2$ | $\tau^2$ | $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right]$ | $\pi_3$ | $\pi_4$ | $\phi_2$ |
| $\phi_3$ | $\tau^3$ | $\left[\begin{smallmatrix} 1 & 2 \\ 1 & 3 \end{smallmatrix}\right]$ | $\pi_7$ | $\pi_6$ | $\phi_3$ |
| $\phi_4$ | $\sigma$ | $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right]$ | $\pi_5$ | $\pi_4$ | $\phi_7$ |
| $\phi_5$ | $\sigma\tau$ | $\left[\begin{smallmatrix} 1 & 2 \\ 0 & 3 \end{smallmatrix}\right]$ | $\pi_3$ | $\pi_6$ | $\phi_6$ |
| $\phi_6$ | $\sigma\tau^2$ | $\left[\begin{smallmatrix} 1 & 0 \\ 1 & 3 \end{smallmatrix}\right]$ | $\pi_7$ | $\pi_4$ | $\phi_5$ |
| $\phi_7$ | $\sigma\tau^3$ | $\left[\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right]$ | $\pi_1$ | $\pi_6$ | $\phi_4$ |

其中四种对偶性是对称的：$\phi_i$，$i = 0$，1，2，3。其余对偶性分为两对：$\phi_4^* = \phi_7$ 和 $\phi_5^* = \phi_6$，这与 [4, 例 4]相反。

## 4. Additive codes and dual codes

本节中，我们定义加性码，并选择一种对偶来定义对偶码。

设 $A$ 为一个有限阿贝尔群，并选取一个对偶 $\phi\colon A \to \widehat{A}$。利用引理 3.4，$\phi$ 可通过如下设定诱导出一个对偶 $A^n \to \widehat{A^n}$：

$$\langle \phi(a_1, a_2, \dots, a_n) \,|\, (b_1, b_2, \dots, b_n) \rangle_{A^n} = \prod_{i=1}^{n} \langle \phi(a_i) \,|\, b_i \rangle_A, \tag{4.1}$$

对于 $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in A^n$。若 $\phi\colon A \to A$ 是对称的，那么其扩张 $\phi\colon A^n \to A^n$ 也是对称的。将 $A$ 上的内积 $\Phi$ 扩展为 $A^n$ 上的内积（仍称为 $\Phi$，此处沿用记号），定义如下：

$$\Phi((a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n)) = \prod_{i=1}^{n} \Phi(a_i, b_i),$$

对于 $(a_1, a_2, \dots, a_n), (b_1, \dots, b_n) \in A^n$。

注记 4.2。并非每一种复数域 $A^n$ 上的对偶都具有（4.1）的形式。在例 3.14中，$\phi_3$ 复数域 $\mathbb{F}_2^2$ 上的对偶不等于 $\phi_1$。即使按照恰当的等价概念，这一点仍然成立，相关内容将在第 6 节中讨论。

长度为 $n$ 、定义在 $A$ 上的加性码是一个子群 $C \subseteq A^n$。加性码有一个湮灭子 $(A^n : C)$，如（2.16）所示。湮灭子 $(A^n : C)$ 具有作为对偶码所期望的大部分性质，包括大小条件 $|C| \cdot |(A^n : C)| = |A^n|$ 以及双重湮灭子性质 $(A^n : (A^n : C)) = C$，见推论 2.17；另见 [18, §11.2]。唯一的缺点是，湮灭子 $(A^n : C)$ 包含于 $A^n$，而非 $A^n$。讨论对偶性的全部目的，就是能够将湮灭子 $(A^n : C)$ 拉回到 $A^n$ 中。

对于加性码 $C \subseteq A^n$ 以及一种对偶 $\phi\colon A \to A$，定义左、右对偶码 如下：

$$\mathfrak{L}_\phi(C) = \{x \in A^n : \Phi(x, c) = 1 \text{ for all } c \in C\},$$
$$\mathfrak{R}_\phi(C) = \{x \in A^n : \Phi(c, x) = 1 \text{ for all } c \in C\}.$$

当 $\phi$ 没有歧义时，我们可以写作 $\mathfrak{L}(C)$ 或 $\mathfrak{R}(C)$。

**引理 4.3.** 给定有限阿贝尔群 $A$ 和对偶 $\phi\colon A \to A$，对于所有加性码 $C$、$C_1$、$C_2 \subseteq A^n$，以下结论成立：

- $\phi(\mathfrak{L}_\phi(C)) = (\widehat{A^n} : C)$ *and* $\phi^*(\mathfrak{R}_\phi(C)) = (\widehat{A^n} : C)$.
- *If* $C_1 \subseteq C_2 \subseteq A^n$, *then* $\mathfrak{L}_\phi(C_2) \subseteq \mathfrak{L}_\phi(C_1)$ *and* $\mathfrak{R}_\phi(C_2) \subseteq \mathfrak{R}_\phi(C_1)$.
- $\mathfrak{L}_{\phi^*}(C) = \mathfrak{R}_\phi(C)$ *and* $\mathfrak{R}_{\phi^*}(C) = \mathfrak{L}_\phi(C)$.

- 如果对偶 $\phi$ 是对称的，那么 $\mathfrak{L}_\phi(C) = \mathfrak{R}_\phi(C)$。

证明。 这些练习使用引理 3.2。 □

左对偶码 $\mathfrak{L}_\phi(C)$ 对应于 $C^M$ 的正交补 [4,定义 2。2], 并且 $\mathfrak{R}_\phi(C)$ 对应于 $C^{M^\top}$。

**命题 4.4**。 给定一个有限阿贝尔群 $A$和一个对偶 $\phi : {\sim}A \to A$，任意加性码 $C \subseteq A^n$ 的对偶码具有以下性质：

- $\mathfrak{L}_\phi(C)$ 和 $\mathfrak{R}_\phi(C)$是 $A^n$中的加性码。
- $|\mathfrak{L}_\phi(C)| \cdot |C| = |A|^n$ 和 $|\mathfrak{R}_\phi(C)| \cdot |C| = |A|^n$。
- $\mathfrak{L}_\phi(\mathfrak{R}_\phi(C)) = C$ 和 $\mathfrak{R}_\phi(\mathfrak{L}_\phi(C)) = C$。

证明。利用引理 4.3 和推论 2.17可验证前两项。对于最后一项，先证明 $C$ 包含于双对偶中，然后利用大小条件证明二者相等。 □

下一个命题是命题 2.18的一个版本。

**命题 4.5**。 设 $\phi$: $A \to A$ 是 $A$ 的一个对偶，将其扩展至 $A^n$，并具有相应的内积 $\Phi$。对于任意加性码 $C \subseteq A^n$,

$$\sum_{y\in C} \Phi(x,y) = \begin{cases} |C|, & x \in \mathfrak{L}_\phi(C), \\ 0, & x \notin \mathfrak{L}_\phi(C); \end{cases} \quad \sum_{x\in C} \Phi(x,y) = \begin{cases} |C|, & y \in \mathfrak{R}_\phi(C), \\ 0, & y \notin \mathfrak{R}_\phi(C). \end{cases}$$

证明。 在第一种情形下，$\sum_{y\in C} \Phi(x, y) = \sum_{y\in C} \langle \phi(x) \,|\, y \rangle$ 对于 $x \in A^n$。利用 $x \in \mathfrak{L}_\phi(C)$ 当且仅当 $\phi(x) \in (A^n : C)$，由命题 2.18即可得出结论。第二种情形可将第一种情形应用于对偶 $\phi$*得到。 □

利用这些对偶码，可以得到麦克威廉斯恒等式的相应版本。这将是第 7 节的主题。

由于 $\mathfrak{L}_\phi(C)$, $\mathfrak{R}_\phi(C) \subseteq A^n$，因此可以定义自正交码和自对偶码（带有左、右修饰语）：

- 左自正交: $C \subseteq \mathfrak{L}_\phi(C)$;
- 右自正交: $C \subseteq \mathfrak{R}_\phi(C)$;
- 左自对偶: $C = \mathfrak{L}_\phi(C)$;
- 右自对偶: $C = \mathfrak{R}_\phi(C)$。

事实上，正如下一个结果所示，左右区别并非必要。

**引理 4.6**。 加性码 $C \subseteq A^n$ 是左自正交的，当且仅当 $C$ 是右自正交的。类似地， $C$ 是左自对偶的，当且仅当 $C$ 是右自对偶的。

证明。 假设 $C \subseteq \mathfrak{L}(C)$。对等式两边取右对偶，并使用引理 4.3和命题 4.4。于是 $C = \mathfrak{R}(\mathfrak{L}(C)) \subseteq \mathfrak{R}(C)$。其余证明类似。 □

**例 4.7**。 设 $A$ 为克莱因四元群，将其视为行向量$a = [a_1, a_2]$ 定义在二元域 $\mathbb{F}_2$上。 $A$ 的六种对偶性出现在例3.14中，每一种都具有以下形式:

$$\Phi_P(a, b) = \langle \phi_P(a) \,|\, b \rangle = (-1)^{aPb^\top} \in \mathbb{C}^\times, \quad a, b \in A,$$

对于 $P \in \mathbf{GL}(2, \mathbb{F}_2)$。

$A$ 有三个阶为二的子群。（我们将不加括号地书写元素。）这些子群为:

$$C_0 = \{00, 10\}, \quad C_1 = \{00, 11\}, \quad C_\infty = \{00, 01\}.$$

这三个子群的对偶码的阶也都为二。对于每个矩阵 $P \in \mathbf{GL}(2, \mathbb{F}_2)$，下面给出其左对偶码和右对偶码。

| $P$ | $\mathfrak{L}(C_0)$ | $\mathfrak{R}(C_0)$ | $\mathfrak{L}(C_1)$ | $\mathfrak{R}(C_1)$ | $\mathfrak{L}(C_\infty)$ | $\mathfrak{R}(C_\infty)$ |
|---|---|---|---|---|---|---|
| $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$ | $C_\infty$ | $C_\infty$ | $C_1$ | $C_1$ | $C_0$ | $C_0$ |
| $\left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right]$ | $C_0$ | $C_0$ | $C_\infty$ | $C_\infty$ | $C_1$ | $C_1$ |
| $\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]$ | $C_1$ | $C_1$ | $C_0$ | $C_0$ | $C_\infty$ | $C_\infty$ |
| $\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$ | $C_0$ | $C_0$ | $C_1$ | $C_1$ | $C_\infty$ | $C_\infty$ |
| $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ | $C_\infty$ | $C_1$ | $C_0$ | $C_\infty$ | $C_1$ | $C_0$ |
| $\left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right]$ | $C_1$ | $C_\infty$ | $C_\infty$ | $C_0$ | $C_0$ | $C_1$ |

对于前三个矩阵中的每一个 $P$，恰好有一个自对偶码（对于每个 $P$，对应的自对偶码都不同）。对于 $P = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$，三个码都是自对偶码。对于两个 $P$ 不对称的矩阵，不存在自对偶码，且左、右对偶码不同。我们将在例 6.6中回到自对偶码。

**例 4.8.** 设 $A = \mathbb{F}_2^3$。共有 $|\mathrm{GL}(3, \mathbb{F}_2)| = 168$ 个对偶性，其中 28 个（总数的六分之一）是对称的（3.9）。

选取一个非对称的 $P \in \mathbf{GL}(3, \mathbb{F}_2)$ 例如

$$P = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

设 $C = \{000, 100\}$。则 $\mathfrak{L}(C) = \{000, \mathbf{100}, \mathbf{011}, 111\}$，而 $\mathfrak{R}(C) = \{000, \mathbf{100}, \mathbf{010}, 110\}$。我们有 $C = \mathfrak{L}(C) \cap \mathfrak{R}(C)$，但 $\mathfrak{L}(C) \neq \mathfrak{R}(C)$。码 $C$ 既是左自正交也是右自正交的，但左对偶码与右对偶码不同。

根据命题 4.4 可知，对于子群 $H$， $K \subseteq A$，若 $K = \mathfrak{L}_\phi(H)$ 对于 $A$ 的某个对偶 $\phi$ 成立 $A$，则 $|H| \cdot |K| = |A|$。其逆命题曾

对于初等阿贝尔 2-群，该问题已在 [9, 定理 15], 中讨论；对于任意有限阿贝尔群，则已在 [8, 定理 5]中讨论。事实证明，后一结果的表述过于乐观，接下来的几个结果将对此作出说明。

**命题 4.9**。 设 $A$ 是一个有限阿贝尔群，其子群为 $H$、$K \subseteq A$，满足 $A = H \oplus K$。则存在一个对称对偶 $\phi$： $A \to A$，使得 $K = \mathfrak{L}(H) = \mathfrak{R}(H)$ 且 $H = \mathfrak{L}(K) = \mathfrak{R}(K)$。

证明。 直和假设意味着 $|A| = |H| \cdot |K|$。将 $A = H \oplus K$ 的元素写成有序对 $(h, k)$ 其中 $h \in H$ 且 $k \in K$。

令$\phi_H$ 是 $H$ 的对称对偶，$\phi_K$ 是 $K$ 的对称对偶。定义 $\widehat{\phi}$： $A \to A$ 为 $\phi_H \times \phi_K$，引理 3.4。也就是说，

$$\langle \phi(h,k) \,|\, (h',k') \rangle_A = \langle \phi_H(h) \,|\, h' \rangle_H \langle \phi_K(k) \,|\, k' \rangle_K \in \mathbb{C}^\times.$$

直接计算可得

$$\langle \phi(0,k) \,|\, (h',0) \rangle_A = \langle \phi_H(0) \,|\, h' \rangle_H \langle \phi_K(k) \,|\, 0 \rangle_K = 1,$$
$$\langle \phi(h,0) \,|\, (0,k') \rangle_A = \langle \phi_H(h) \,|\, 0 \rangle_H \langle \phi_K(0) \,|\, k' \rangle_K = 1,$$

从而 $K \subseteq \mathfrak{L}(H)$ 且 $K \subseteq \mathfrak{R}(H)$以及 $H \subseteq \mathfrak{L}(K)$ 和 $H \subseteq \mathfrak{R}(K)$。根据大小条件，等号成立，命题 4.4。 □

有两种情形可以将命题 4.9 推广到任意两个满足大小条件的子群：循环 $p$-群和初等阿贝尔 $p$-群。

**命题 4.10**。 设 $A = \mathbb{Z}/p^k\mathbb{Z},$，其中 $p$是某个素数。假设 $H, K \subseteq A$ 是 $A$ 的子群，且满足 $|H| \cdot |K| = |A|$。那么对于 $A$的任意对偶 $\phi$，都有 $\mathfrak{L}(H) = \mathfrak{R}(H) = K$ 和 $\mathfrak{L}(K) = \mathfrak{R}(K) = H$。

证明。 群 $A$ 非常特殊：对于任意 $j = 0, 1, \ldots, k$，都存在唯一一个 $A_j$ 阶为 $p^j$的子群。满足 $|H| \cdot |K| = |A|$的子群具有如下形式 $H = A_j$和 $K = A_{k-j}$，其中 $j = 0, 1, \ldots, k$。对偶码的大小条件（命题 4.4）迫使 $A_j$ 和 $A_{k-j}$ 在任意对偶下都是对偶码。 □

**定理 4.11**。 设 $A$ 是初等阿贝尔 $p$ 群。假设 $H$、$K \subseteq A$ 是 $A$ 的子群，且 $|H| \cdot |K| = |A|$。则存在 $A$ 的对称对偶 $\phi$，使得 $\mathfrak{L}(H) = \mathfrak{R}(H) = K$ 且 $\mathfrak{L}(K) = \mathfrak{R}(K) = H$。

证明。 将 $A$ 视为 $\mathbb{F}_p^n$，并将 $H$，$K$ 视为线性子空间。记 $h = \dim H$ 和 $k = \dim K$。基数假设表明 $h + k = n$。

若 $i =$维数$(H \cap K) > 0$，则选取 $H \cap K$的一组基 $e_1$，$e_2$，……，$e_i$。（若 $i = 0$，则 $H \cap K$的基为空。）选取元素 $e_{i+1}$，……，$e_h$

使得 $e_1$，……，$e_h$ 是 $H$的一组基。选取 $e_{h+1}$，……，$e_{h+k-i}$，使得$e_1$，……，$e_i$，$e_{h+1}$，……，$e_{h+k-i}$ 是 $K$的一组基。于是 $e_1$，……，$e_{h+k-i}$ 是 $H+K$的一组基。选取 $e_{h+k-i+1}$，……，$e_n$，使得 $e_1$，……，$e_n$ 是 $A$的一组基。

构造对偶基 $\pi_1$，……，$\pi_n$，其属于 $\widehat{A}$，满足

$$\langle \pi_j \,|\, e_\ell \rangle = \begin{cases} \zeta_p, & j = \ell, \\ 1, & j \neq \ell, \end{cases}$$

对于所有 $j$，$\ell = 1$，2，……，$n$，其中 $\zeta_p$ 是复数域 $\mathbb{C}^\times$ 中的一个本原 $p$ 次单位根。

我们定义通过指定 $A \xrightarrow{\phi} \widehat{A}$ 在 $A$ 的基 $e_1$，……，$e_n$ 上的取值来定义。为方便起见，令 $c = h + k - i$。注意，$c + i = h + k = n$。定义

$$\phi(e_j) = \begin{cases} \pi_{c+j}, & j = 1, 2, \ldots, i, \\ \pi_j, & j = i+1, i+2, \ldots, c, \\ \pi_{j-c}, & j = c+1, c+2, \ldots, c+i. \end{cases}$$

这 $\phi$ 将 $A$ 的一个基映射为 $\widehat{A}$的一个基，因此 $\phi$ 定义了 $A$的一个对偶。通过逐一考察各种情况，可以验证 $\phi$ 是对称的；并利用命题4.4的大小条件可知，$H$ 和 $K$ 互为对偶码。□

下一个例子表明，定理4.11 无法进一步推广，这与 [8, 定理 5]相反。

**例 4.12**。设 $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$,，于是 $|A| = 8$。例3.15展示了 $A$的对偶性。这里，我们确定 $A$ 的子群相对于这些对偶性的对偶码。

$A$ 有三个阶为 2 的子群：$\ell_0 = \{00,\ 10\}$, $\ell_1 = \{00,\ 12\}$，以及 $\ell_\infty = \{00,\ 02\}$。此外还有三个阶为 4 的子群：$C_1 = \{00,\ \mathbf{01},\ \mathbf{02},\ 03\}$, $C_2 = \{00,\ \mathbf{11},\ \mathbf{02},\ 13\}$，以及 $S = \{00,\ \mathbf{10},\ \mathbf{02},\ 12\}$；$C_1$，$C_2$ 是循环群，而 $S$（$A$的根基）是初等阿贝尔群。

下表展示了关于各种对偶性的阶为 2 的子群的左对偶码和右对偶码。

| $\phi$ | $\mathfrak{L}(\ell_0)$ | $\mathfrak{R}(\ell_0)$ | $\mathfrak{L}(\ell_1)$ | $\mathfrak{R}(\ell_1)$ | $\mathfrak{L}(\ell_\infty)$ | $\mathfrak{R}(\ell_\infty)$ |
|---|---|---|---|---|---|---|
| $\phi_0$ | $C_1$ | $C_1$ | $C_2$ | $C_2$ | $S$ | $S$ |
| $\phi_1$ | $C_2$ | $C_2$ | $C_1$ | $C_1$ | $S$ | $S$ |
| $\phi_2$ | $C_1$ | $C_1$ | $C_2$ | $C_2$ | $S$ | $S$ |
| $\phi_3$ | $C_2$ | $C_2$ | $C_1$ | $C_1$ | $S$ | $S$ |
| $\phi_4$ | $C_2$ | $C_1$ | $C_1$ | $C_2$ | $S$ | $S$ |
| $\phi_5$ | $C_1$ | $C_2$ | $C_2$ | $C_1$ | $S$ | $S$ |
| $\phi_6$ | $C_2$ | $C_1$ | $C_1$ | $C_2$ | $S$ | $S$ |
| $\phi_7$ | $C_1$ | $C_2$ | $C_2$ | $C_1$ | $S$ | $S$ |

利用双对偶和命题 4.4，可以确定 $C_1$、$C_2$、$S$ 的对偶码。

注意，$|\ell_\infty| \cdot |C_1| = |A|$，但不存在具有 $\mathfrak{L}(\ell_\infty) = C_1$ 的对偶性，这与 [8, 定理 5]相反。

这个例子将在定理5.9中推广；参见注 5.10。

## 5. Structural questions

本节中，我们研究一个问题：子群 $H \subseteq A$ 的对偶码如何取决于对偶性的选择。一个极端情形是初等阿贝尔 $p$-群，此时定理4.11指出，任意两个满足大小条件的子群，在 某种对偶性下都是对偶码。另一个极端情形是例 4.12，其中给出了 $A = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ 的子群，它们在 所有对偶性下都是对偶码。我们将发现，对偶码对对偶性的依赖，与自同构群对该群子群的作用密切相关。

设 $A$是一个有限阿贝尔群。自同构群 $\mathsf{Aut}(A)$作用于 $A$。我们将此作用记作右作用，其中输入写在左侧。设 $\mathscr{S}_d$ 为 $A$ 中所有阶为 $d$的子群的集合。于是 $\mathsf{Aut}(A)$ 也在 $\mathscr{S}_d$ 上右作用。对于满足 $|H| = d$的子群$H \subseteq A$，即 $H \in \mathscr{S}_d$，令 $\mathsf{Stab}(H)$ 为其稳定子群：

$$\mathrm{Stab}(H) = \{\tau \in \mathrm{Aut}(A) : H\tau = H\}.$$

**引理 5.1.** 设 $A$ 是一个有限阿贝尔群。取任意子群 $H \subseteq A$、任意自同构 $\tau \in$ 自同构群$(A)$，以及 $A$的任意对偶 $\phi$ 。那么，$\mathfrak{R}_\phi(H\tau) = \mathfrak{R}_\phi(H)$ 当且仅当 $\tau \in$稳定子群$(H)$。同样，$\mathfrak{L}_\phi(H\tau) =\mathfrak{L}_\phi(H)$ 当且仅当 $\tau \in$稳定子群$(H)$。

证明。 根据双重对偶性质，$\mathfrak{R}_\phi(H\tau) = \mathfrak{R}_\phi(H)$ 当且仅当$H\tau = H$。对左对偶码也可作同样的推理。□

**引理 5.2.** 设 $A$ 为有限阿贝尔群，其子群为 $H \subseteq A$。假设 $A$ 的对偶性 $\phi_1$、$\phi_2$ 满足 $\phi_2 = \phi_1 \circ \tau$，其中 $\tau \in$ 自同构群$(A)$。则 $\mathfrak{R}_{\phi_2}(H) = \mathfrak{R}_{\phi_1}(H\tau)$ 且 $\mathfrak{L}_{\phi_2}(H)\tau = \mathfrak{L}_{\phi_1}(H)$。

证明。 计算：

$$\begin{aligned}
\mathfrak{R}_{\phi_2}(H) &= \{y \in A : \langle \phi_2(h) \,|\, y\rangle = 0 \text{ for all } h \in H\} \\
&= \{y \in A : \langle \phi_1(h\tau) \,|\, y\rangle = 0 \text{ for all } h \in H\} = \mathfrak{R}_{\phi_1}(H\tau); \\
\mathfrak{L}_{\phi_2}(H) &= \{x \in A : \langle \phi_2(x) \,|\, h\rangle = 0 \text{ for all } h \in H\} \\
&= \{x \in A : \langle \phi_1(x\tau) \,|\, h\rangle = 0 \text{ for all } h \in H\} = \mathfrak{L}_{\phi_1}(H)\tau^{-1}. \quad \square
\end{aligned}$$

**命题 5.3**。 设 $H$ 是有限阿贝尔群 $A$ 的一个子群。假设 $\phi_1$、$\phi_2$ 是 $A$ 的两个对偶性。那么 $\mathfrak{R}_{\phi_1}(H) = \mathfrak{R}_{\phi_2}(H)$ 当且仅当存在某个 $\tau \in$ 稳定子群$(H)$ 使得 $\phi_2 = \phi_1 \circ \tau$。同样， $\mathfrak{L}_{\phi_1}(H) = \mathfrak{L}_{\phi_2}(H)$ 当且仅当存在某个 $\tau \in$ 稳定子群$(H)$ 使得 $\phi_2^* = \phi_1^* \circ \tau$。

证明。 根据命题 3.1， $\phi_2 = \phi_1 \circ \tau$ 对于某个 $\tau \in$ 自同构群$(A)$。于是，$\mathfrak{R}_{\phi_2}(H) = \mathfrak{R}_{\phi_1}(H\tau)$根据引理 5.2。因此，根据引理 5.1， $\mathfrak{R}_{\phi_1}(H) =\mathfrak{R}_{\phi_2}(H)$ 当且仅当 $\tau \in$稳定子群$(H)$。对于左对偶，应用右对偶情形于 $\phi_1^*$ 和 $\phi_2^*$，利用引理 4.3。 □

回顾一下， $H \subseteq A$ a 特征子群 是指：若 $H$ 在 $A$的每个自同构下均保持不变，即 $H\tau = H$ 对于每个 $\tau \in$ 自同构群$(A)$，或者等价地，Stab$(H)$ =自同构群$(A)$。

**定理 5.4**。 设 $H$ 和 $K$ 是有限阿贝尔群 $A$的子群。假设 $K = \mathfrak{R}_{\phi_0}(H)$ 对于某个对偶 $\phi_0$， $A$成立。那么，对于 $A$ 的每个对偶 $\phi$， $K = \mathfrak{R}_{\phi}(H)$ 当且仅当 $H$ 是特征子群。左对偶码同样如此。此外， $K = \mathfrak{R}_{\phi}(H)$ 对于 $A$ 的每个对偶$\phi$ 当且仅当 $K = \mathfrak{L}_{\phi}(H)$ 对于 $A$的每个对偶 $\phi$。

证明。 应用命题 5.3。 □

**推论 5.5**。 设 $H, K$ 是有限阿贝尔群 $A$ 的子群，且对于某个对偶 $\phi_0$，有 $K = \mathfrak{R}_{\phi_0}(H)$ $A$。那么， $H$ 是特征子群，当且仅当 $K$ 是特征子群。

证明。 若 $H$ 是特征子群，则根据定理 5.4， $K =\mathfrak{R}_{\phi}(H)$ 对任意 $\phi$ 的对偶 $A$，都有 $\mathfrak{R}_{\phi}(H) = \mathfrak{L}_{\phi^*}(H)$。由于 $\mathfrak{R}_{\phi}(H) = \mathfrak{L}_{\phi^*}(H)$，根据引理 4.3，对于任意 $\phi$ 的对偶 $A$，也有 $K = \mathfrak{L}_{\phi}(H)$。

取任意自同构 $\tau \in$自同构群$(A)$。令 $\phi = \phi_0 \circ \tau$。根据引理 5.2，我们知道 $\mathfrak{L}_{\phi}(H)\tau = \mathfrak{L}_{\phi_0}(H)$。但这意味着 $K\tau = K$，并且 $K$ 是特征子群。

当 $K$ 是特征子群时，基本相同的论证也适用，其中 $H = \mathfrak{L}_{\phi_0}(K)$。□

命题 2.21 使我们能够逐个素数地研究有限阿贝尔群。因此，在本节余下部分，我们假设 $A$ 是一个有限阿贝尔$p$-群，其中某个固定素数为 $p$。我们将介绍 $A$的两种相关滤过。

定义 $f\colon A \to A$ 由 $f(a) = pa, a \in A$给出； $f$ 是一个群同态。用指数记号表示 $f$与自身的复合，因此 $f^2 = f \circ f$。于是 $f^k(a) = p^k a$, $a \in A$, $k$ 正整数。我们约定 $f^0 = \mathrm{id}_A$。由于 $A$ 是一个有限阿贝尔 $p$-群，存在最小正整数 $N$ 使得 $f^N = 0$。（根据有限阿贝尔群基本定理， $A$ 是若干循环群的直和

它们的阶是 $p$ 的幂。如果 $p^N$ 是其中出现的最大幂，则 $f^N = 0$。）

我们有如下滤过：

$$0 = \ker f^0 \subseteq \ker f \subseteq \ker f^2 \subseteq \cdots \subseteq \ker f^{N-1} \subseteq \ker f^N = A, \tag{5.6}$$
$$A = \operatorname{im} f^0 \supseteq \operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \cdots \supseteq \operatorname{im} f^{N-1} \supseteq \operatorname{im} f^N = 0.$$

备注 5.7。（5.6）中的滤过是底层级数（对于 $\ker f^j$）以及根基或洛伊级数（对于 $\operatorname{im} f^j$）的例子，将 $A$ 视为一个 $\mathbb{Z}$-模，[1, 定义 1.2。1]。

**命题 5.8。** 滤过（5.6）中的每个子群都是 $A$ 的特征子群。

证明。同态 $f$ 与任意自同构 $\tau$：$(f(a))\tau = (pa)\tau = p(a\tau) = f(a\tau)$ 对任意 $a \in A$ 均可交换。这意味着任意 $f^j$ 都与任意自同构可交换。如果 $a \in \ker f^j$，则 $f^j(a\tau) = (f^j(a))\tau = 0\tau = 0$，因此 $a\tau \in \ker f^j$。对于 $\operatorname{im} f^j$，论证类似。□

**定理 5.9。** 设 $A$ 是一个有限阿贝尔 $p$-群，带有滤过（5.6）。那么，对于每个 $j = 0、1、\ldots\ldots、N$ 以及每个对偶 $\phi$：$A \to A$，

$$\operatorname{im} f^j = \mathfrak{L}_\phi(\ker f^j) = \mathfrak{R}_\phi(\ker f^j),$$
$$\ker f^j = \mathfrak{L}_\phi(\operatorname{im} f^j) = \mathfrak{R}_\phi(\operatorname{im} f^j).$$

证明。根据有限阿贝尔群基本定理，$A$ 可写成若干循环 $p$-群的和：

$$A = \bigoplus_{i=1}^{\ell} \mathbb{Z}/p^{n_i}\mathbb{Z},$$

其中 $1 \leqslant n_1 \leqslant \cdots \leqslant n_\ell$ 为整数。将 $a \in A$ 写成相应的形式 $a = (a_1, a_2, \ldots\ldots, a_\ell)$。取 $\zeta$ 为 $\mathbb{C}^\times$ 中的一个本原 $p^{n_\ell}$ 次单位根，并定义 $A$ 的一个对称对偶 $\phi_0$：

$$\Phi_0(a, b) = \prod_{i=1}^{\ell} \zeta^{p^{n_\ell - n_i} a_i b_i}.$$

我们证明 $\ker f^j$ 和 $\operatorname{im} f^j$ 是对偶码。设 $a \in \ker f^j$ 且 $b \in \operatorname{im} f^j$，其中 $b = f^j(x) = p^j x$。那么，对于 $i = 1, 2, \ldots, \ell$，有 $a_i b_i = a_i p^j x_i = 0$，因为 $a \in \ker f^j$。因此 $\Phi_0(a, b) = 1$，从而 $\ker f^j \subseteq \mathfrak{L}_{\phi_0}(\operatorname{im} f^j)$ 且 $\operatorname{im} f^j \subseteq \mathfrak{R}_{\phi_0}(\ker f^j)$。两种情形下等号均成立，因为 $|\ker f^j| \cdot |\operatorname{im} f^j| = |A|$，并且满足对偶码的大小条件。由于 $\phi_0$ 是对称的，我们也有 $\ker f^j = \mathfrak{R}_{\phi_0}(\operatorname{im} f^j)$ 且 $\operatorname{im} f^j = \mathfrak{L}_{\phi_0}(\ker f^j)$。其他对偶性可使用定理 5.4 和命题 5.8。□

注 5.10。 当 $A$ 是初等阿贝尔 $p$-群时，滤过 (5.6) 退化为 $N = 1$: $A = \ker f$ 且 $0 = \operatorname{im} f$。相反，当$A = \mathbb{Z}/p^\ell\mathbb{Z}, \operatorname{im} f^j = p^j\mathbb{Z}/p^\ell\mathbb{Z},$且 $\ker f^j = p^{\ell-j}\mathbb{Z}/p^\ell\mathbb{Z}$。

设 $A = \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$。例 $\ell_\infty$ 和 $S$ 4.12 中的子群恰好是 $\ell_\infty = \operatorname{im} f$和 $S = \ker f$。

## 6. Congruence

对偶性之间存在一种等价关系，它推广了有限素数域上矩阵和对称双线性形式的合同关系。

**定义6.1**。 两个对偶性 $\phi_1, \phi_2 : A \to A$ 称为合同，记作$\phi_1 \simeq \phi_2$, 如果存在一个自同构 $\tau \in \mathrm{Aut}(A)$ ，使得 $\phi_2$等于以下复合映射

$$A \xrightarrow{\tau} A \xrightarrow{\phi_1} \widehat{A} \xrightarrow{\tau^*} \widehat{A}\,.$$

合同的条件意味着，对所有 $a, a' \in A$，都有

$$\Phi_2(a, a') = \langle \phi_2(a) \,|\, a' \rangle = \langle \phi_1(a\tau) \,|\, a'\tau \rangle = \Phi_1(a\tau, a'\tau). \tag{6.2}$$

当且仅当 $\phi_2$ 对称时， $\phi_1 \simeq \phi_2$, $\phi_1$ 对称。

**例6.3**。 设 $p$为素数，令 $A$ 为秩为 $p$的初等阿贝尔 $n$-群，记作 $A = \mathbb{F}_p^n$。在例 3.7中，定义 $\phi_0$ 的一个对偶 $A$ 为 $\langle \phi_0(a) \,|\, b \rangle = \zeta_p^{ab^\top} \in \mathbb{C}^\times$，其中 $a$， $b \in A$ （视为行向量）。其他任何对偶都具有以下形式: $\phi = \phi_0 \circ \tau$ 其中某个自同构$\tau \in$ 自同构群$(A) = \mathrm{GL}(n, \mathbb{F}_p)$。将 $\tau$ 视为可逆矩阵，则有 $\langle \phi(a) \,|\, b \rangle = \langle \phi_0(a\tau) \,|\, b \rangle = \zeta_p^{a\tau b^\top}$。

若 $\phi' = \phi_0 \circ \tau'$, $\tau' \in$ 自同构群$(A)$是另一个对偶，则当存在自同构 $\sigma \in$ 自同构群$(A)$ 使得 $\phi' = \sigma^* \circ \phi \circ \sigma$时， $\phi'$与$\phi$ 合同。这意味着，对于任意 $a$， $b \in A$,

$$\begin{aligned} \zeta_p^{a\tau' b^\top} &= \langle \phi'(a) \,|\, b \rangle = \langle \sigma^*(\phi(a\sigma)) \,|\, b \rangle \\ &= \langle \phi(a\sigma) \,|\, b\sigma \rangle = \zeta_p^{a\sigma\tau(b\sigma)^\top} = \zeta_p^{a\sigma\tau\sigma^\top b^\top}. \end{aligned}$$

当且仅当 $\tau' = \sigma\tau\sigma^\top$ 时，这些方程对所有 $a, b \in A$ 都成立。也就是说，$\tau$ 和 $\tau'$ 是合同矩阵。上述方程中显而易见地隐藏着

$$\langle \phi'(a) \,|\, b \rangle = \langle \phi(a\sigma) \,|\, b\sigma \rangle, \quad a, b \in A.$$

由于将 $r \in \mathbb{F}_p$ 发送到 $\zeta_p^r \in \mathbb{C}^\times$ 的同态 $\mathbb{F}_p \to \mathbb{C}^\times$ 是单射，$A = \mathbb{F}_p^n$ 上的内积与取值于 $\mathbb{F}_p$ 的 $A$ 上的非退化双线性型相同。

当 $p=2$ 时，已有众所周知的结果对非退化对称双线性型进行了分类。型 $I$ 由 $1\times 1$ 矩阵 $[1]$ 表示，而型 $H$ 由下式表示

$$H=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

$\mathbb{F}_2$ 上的每个非退化对称双线性形式都合同于若干个 $I$ 和 $H$ 的直和，且满足关系 $I+H\simeq 3I$。

对于奇素数 $p$，非退化对称双线性形式有两种类型，且都可对角化：1，1，……，1，1 和 1，1，……，1，$\lambda$，其中 $\lambda$ 用 Robert Wilson 的话来说，是 $\mathbb{F}_p$ 中的“你最喜欢的非平方元”。（当$p\equiv 1$模 4 时，$-1$ 是 $\mathbb{F}_p$中的一个平方。）

当两个对偶性合同的时候，子群及其对偶码的比较结构相互对应。

**定理 6.4**。设 $A$ 是一个有限阿贝尔群。假设 $\phi_1\simeq\phi_2$ 是 $A$ 的合同对偶性，其中 $\phi_2=\tau^*\circ\phi_1\circ\tau$ 对某个 $\tau\in$ 自同构群$(A)$ 成立。对于子群 $H$、$K\subseteq A$、$K=\mathfrak{L}_{\phi_2}(H)$，当且仅当 $K\tau=\mathfrak{L}_{\phi_1}(H\tau)$。同样，$K=\mathfrak{R}_{\phi_2}(H)$ 当且仅当 $K\tau=\mathfrak{R}_{\phi_1}(H\tau)$。

证明。所有结论均由（6.2）和大小条件得出。 □

**推论 6.5**。设 $A$ 是一个有限阿贝尔群。假设 $\phi_1\simeq\phi_2$ 是 $A$的合同对偶，其中 $\phi_2=\tau^*\circ\phi_1\circ\tau$，且 $\tau\in$ 自同构群$(A)$。对于一个子群 $H\subseteq A$，$H$ 在 $\phi_2$ 下自对偶，当且仅当 $H\tau$ 在 $\phi_1$下自对偶。在 $\phi_1$ 下的自对偶码数量等于在 $\phi_2$下的自对偶码数量

**例 6.6**。设 $A=\mathbb{F}_2^2$。例 $A$ 3.14 中列出了六种对偶。三种对称对偶性合同：$\phi_0\simeq\phi_1\simeq\phi_2$。对称对偶性 $\phi_3$ 只与其自身合同。两种非对称对偶性合同：$\phi_4\simeq\phi_5$。例 $A$ 列出了阶为 2 的子群及其对偶码，见例4.7。合同对偶性的自对偶码数量相同。

**例 6.7.** 令 $A=\mathbb{F}_3^2$；则 $\mathrm{Aut}(A)=\mathrm{GL}(2,\ \mathbb{F}_3)$。由于 $|\mathrm{GL}(2,\ \mathbb{F}_3)|=(3^2-1)(3^2-3)=48$，共有 48 个对偶性。计算（我使用了 SageMath）表明，其中 18 个对偶性是对称的，30 个不是对称的。下面列出了各合同类的代表元以及每个合同类中的对偶性数量。

| 代表元 | $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$ | $\left[\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right]$ | $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ | $\left[\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right]$ | $\left[\begin{smallmatrix}2&1\\0&1\end{smallmatrix}\right]$ | $\left[\begin{smallmatrix}2&2\\0&2\end{smallmatrix}\right]$ |
|---|---|---|---|---|---|---|
| 数量 | 6 | 12 | 8 | 2 | 12 | 8 |

阿贝尔群 $A$ 有四个（必为循环）3 阶子群。它们及其选定的生成元如下：$\ell_0=\langle 10\rangle$、$\ell_1=\langle 11\rangle$、

$\ell_2 = \langle 12 \rangle$和 $\ell_\infty = \langle 01 \rangle$。对于任意对偶，$\ell_j$的对偶码将是 $\ell_j$ 的某种排列。下面给出了上述同余类代表的各种对偶码。请注意，当对偶为对称时，左对偶码和右对偶码将相同。

| $\phi$ | $\tau$ | $\mathfrak{L}(\ell_0)$ | $\mathfrak{R}(\ell_0)$ | $\mathfrak{L}(\ell_1)$ | $\mathfrak{R}(\ell_1)$ | $\mathfrak{L}(\ell_2)$ | $\mathfrak{R}(\ell_2)$ | $\mathfrak{L}(\ell_\infty)$ | $\mathfrak{R}(\ell_\infty)$ |
|---|---|---|---|---|---|---|---|---|---|
| $\phi_0$ | $\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$ | $\ell_\infty$ | $\ell_\infty$ | $\ell_2$ | $\ell_2$ | $\ell_1$ | $\ell_1$ | $\ell_0$ | $\ell_0$ |
| $\phi_1$ | $\left[\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right]$ | $\ell_\infty$ | $\ell_\infty$ | $\ell_1$ | $\ell_1$ | $\ell_2$ | $\ell_2$ | $\ell_0$ | $\ell_0$ |
| $\phi_2$ | $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$ | $\ell_\infty$ | $\ell_2$ | $\ell_1$ | $\ell_1$ | $\ell_0$ | $\ell_\infty$ | $\ell_2$ | $\ell_0$ |
| $\phi_3$ | $\left[\begin{smallmatrix}0&2\\1&0\end{smallmatrix}\right]$ | $\ell_0$ | $\ell_0$ | $\ell_1$ | $\ell_1$ | $\ell_2$ | $\ell_2$ | $\ell_\infty$ | $\ell_\infty$ |
| $\phi_4$ | $\left[\begin{smallmatrix}2&1\\0&1\end{smallmatrix}\right]$ | $\ell_\infty$ | $\ell_1$ | $\ell_0$ | $\ell_2$ | $\ell_1$ | $\ell_\infty$ | $\ell_2$ | $\ell_0$ |
| $\phi_5$ | $\left[\begin{smallmatrix}2&2\\0&2\end{smallmatrix}\right]$ | $\ell_\infty$ | $\ell_2$ | $\ell_1$ | $\ell_1$ | $\ell_0$ | $\ell_\infty$ | $\ell_2$ | $\ell_0$ |

计算还表明，对于所有的对偶 $\phi$ $A$，$\phi^* \simeq \bar{\phi}$。对于 $A$ 的对偶 $\phi$，对所有 $a \in A$ 定义 $\phi(a) = \phi(-a)$。四个$^-$合同类满足 $\phi_i \simeq \phi_i$，即 $i = 0$，1，3，4，而 $\phi_2 \simeq \phi_5$。后者解释了为什么 $\phi_2$ 和 $\phi_5$ 对每个子群都给出相同的对偶码。

我们进一步探讨例 6.7 中的观察：某些对偶对每个子群都给出相同的对偶码。

设 $A$ 是一个有限阿贝尔 $p$-群。令 $m$ 为一个与 $p$ 互素的整数。给定 $A$ 的一个对偶 $\phi$，定义 $\phi^m$ 为

$$\langle \phi^m(a) \,|\, b \rangle = \langle \phi(a) \,|\, b \rangle^m, \quad a, b \in A.$$

也就是说，对于 $a \in A$，$\phi^m(a) = (\phi(a))^m$，其中右侧表示群 $A$ 中的乘$\hat{}$法。可以验证，$\phi^m$ 是 $A$ 的一个对偶；事实上，$\phi^m = \phi \circ (m\,\mathrm{id}_A)$，其中 $m\mathrm{id}_A$ 是 $A$ 的自同构，它将$a \in A$ 映射到 $ma \in A$。

**引理 6.8.** 设 $A$ 是一个有限阿贝尔 $p$-群，且 $m$ 是一个与 $p$ 互素的整数。若 $\phi$ 是 $A$ 的一个对偶，则 $(\phi^m)^* = (\phi^*)^m$。特别地，若 $\phi_2 = \phi_1 \circ m$恒等映射$_A$，则 $\phi_2^* = \phi_1^* \circ m$恒等映射$_A$。

证明. 由引理 3.2，对任意 $a$，$b \in A$，

$$\begin{aligned}\langle (\phi^m)^*(a) \,|\, b \rangle &= \langle \phi^m(b) \,|\, a \rangle = \langle \phi(b) \,|\, a \rangle^m \\ &= \langle \phi^*(a) \,|\, b \rangle^m = \langle (\phi^*)^m(a) \,|\, b \rangle.\end{aligned}$$

□

**定理 6.9.** 设 $A$ 是一个有限阿贝尔 $p$-群，并设 $\phi_1$、$\phi_2$ 是 $A$ 的两个对偶。那么，

$$\mathfrak{L}_{\phi_2}(H) = \mathfrak{L}_{\phi_1}(H), \quad \mathfrak{R}_{\phi_2}(H) = \mathfrak{R}_{\phi_1}(H).$$

对所有子群 $H \subseteq A$均成立，当且仅当 $\phi_2 = \phi_1^m$对于某个与 $p$互素的整数$m$成立。

证明。若 $m$ 与 $p$互素，则 $m\mathrm{id}_A$ 是 $A$ 的自同构，并使 $A$ 的每个子群保持不变。根据引理 6.8 和命题 5.3，若 $\phi_2 = \phi_1^m$，则 $\phi_1$ 和 $\phi_2$ 对于每个子群都会产生相同的对偶码。

反过来，设 $\phi_2 = \phi_1 \circ \tau$ 对于某个 $\tau \in$ 自同构群$(A)$，并设$\phi_1$，$\phi_2$ 对每个子群都产生相同的对偶码。由命题 5.3，$\tau$ 必须保持 $A$ 的每个子群不变。我们需要证明$\tau = m\mathrm{id}_A$，其中某个整数 $m$ 与 $p$互素。

根据有限阿贝尔群基本定理，存在整数 $1 \leqslant e_1 \leqslant e_2 \leqslant \cdots \leqslant e_\ell$，使得 $A$ 同构于

$$\mathbb{Z}/p^{e_1}\mathbb{Z} \oplus \mathbb{Z}/p^{e_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{e_\ell}\mathbb{Z}.$$

$A$的子群中包括形如 $0\oplus\cdots\oplus H_i\oplus\cdots\oplus 0$ 的子群（除一个位置外，其余位置均为 0），以及 $H_i = \mathbb{Z}/p^{e_i}\mathbb{Z}$。由于 $\tau$保持所有这类子群不变，我们得出 $\tau = \tau_1\oplus\tau_2\oplus\cdots\oplus\tau_\ell$，其中每个$\tau_i$ 都是 $\mathbb{Z}/p^{e_i}\mathbb{Z}$的自同构。根据 $\mathbb{Z}/p^{e_i}\mathbb{Z}$, 的结构可知，每个 $\tau_i$ 都是乘以某个整数 $m_i$，且该整数与 $p$互素。考虑由形如(0, ……，0，1，1，0，……，0)的元素生成的循环子群（其中有两个相邻的非零项），不变性意味着 $m_{i+1} \equiv m_i$ 模 $p^{e_i}$。于是令 $m = m_\ell$。□

## 7. MacWilliams identities

有限阿贝尔群上的麦克威廉斯恒等式有多种形式 [2, 11, 18]。我们考察两种情况：汉明重量枚举式和完全枚举式。（群作用的对称化枚举器将留待另一篇论文讨论。）这两种情况都用到了傅里叶变换和泊松求和公式。

设$A$对于有限阿贝尔群，其特征群为$\widehat{A}$。对于元素 $a = (a_1, \ldots, a_n) \in A^n$，定义其汉明重量为 $\mathrm{H}(a) = |\{i : a_i \neq 0\}|$。当阿贝尔群采用乘法记法时，例如 $A$，汉明重量为 $\mathrm{H}(\pi) = |\{i : \pi_i \neq 1\}|$。对于加性码 $C \subseteq A^n$，其汉明重量枚举式是以下关于 $\mathbb{C}[X, Y]$的多项式：

$$\mathrm{hwe}_C(X, Y) = \sum_{c\in C} X^{n-\mathrm{H}(c)}Y^{\mathrm{H}(c)}.$$

为定义完全枚举式，令 $\mathbb{C}[Z_a : a \in A]$（简称为 $\mathbb{C}[Z_*]$）为一个以$a \in A$为索引、含有 $|A|$个不定元 $Z_a$ 的多项式环。对于加性码 $C \subseteq A^n$，其完全枚举式 为

$\mathbb{C}[Z_*]$中的下列多项式:

$$\mathrm{ce}_C(Z_*) = \sum_{c\in C}\prod_{i=1}^{n} Z_{c_i}.$$

继续设 $A$ 为有限阿贝尔群，其特征群为$\widehat{A}$。设 $V$ 为复数域 $\mathbb{C}$ 上的向量空间。定义$F(A,\ V) = \{f\colon\ A \to V\}$，即从 $A$到 $V$的所有函数的集合； $F(A,\ V)$在逐点加法和函数的数乘运算下也是 $\mathbb{C}$ 上的向量空间。傅里叶变换 是一个 $\mathbb{C}$-线性变换$\widehat{\ }$， $F(A,\ V) \to F(A,\ V)$ 定义为

$$\widehat{f}(\pi) = \sum_{a\in A}\langle \pi \,|\, a\rangle f(a), \quad f \in F(A,V), \quad \pi \in \widehat{A}. \tag{7.1}$$

**引理 7.2**。 傅里叶变换是可逆的。对于 $f \in F(A、\ V)$和 $a \in A$,

$$f(a) = \frac{1}{|A|}\sum_{\pi\in\widehat{A}}\langle \pi \,|\, -a\rangle \widehat{f}(\pi).$$

证明。 利用（7.1）、推论 2.20和命题 2.9进行计算:

$$\begin{aligned}\sum_{\pi\in\widehat{A}}\langle \pi \,|\, -a\rangle \widehat{f}(\pi) &= \sum_{\pi\in\widehat{A}}\langle \pi \,|\, -a\rangle \sum_{b\in A}\langle \pi \,|\, b\rangle f(b)\\ &= \sum_{b\in A}\left(\sum_{\pi\in\widehat{A}}\langle \pi \,|\, b-a\rangle\right) f(b) = |A| f(a).\end{aligned}$$

□

**定理 7.3** （泊松求和公式）。 设 $H \subseteq A$ 是有限阿贝尔群 $A$的一个子群。若 $f \in F(A、\ V)$, 则

$$\sum_{a\in H} f(a) = \frac{1}{|(A:H)|}\sum_{\pi\in(\widehat{A}:H)} \widehat{f}(\pi).$$

证明。 将引理 7.2 中的等式对 $a \in H$求和:

$$\begin{aligned}|A|\sum_{a\in H} f(a) &= \sum_{a\in H}\sum_{\pi\in\widehat{A}}\langle \pi \,|\, -a\rangle \widehat{f}(\pi)\\ &= \sum_{\pi\in\widehat{A}}\left(\sum_{a\in H}\langle \pi \,|\, -a\rangle\right)\widehat{f}(\pi) = |H| \sum_{\pi\in(\widehat{A}:H)} \widehat{f}(\pi),\end{aligned}$$

利用命题 2.18 和推论 2.17。 □

现在，我们将应用泊松求和公式，证明汉明重量计数多项式和完全枚举式的麦克威廉斯恒等式。在泊松求和公式中，阿贝尔群将为 $A^n$ ， 而

子群将为加性码 $C \subseteq A^n$。函数 $f\colon A^n \to V$将为 $f\colon A^n \to \mathbb{C}[X, Y]$, $f(x) = X^{n-\mathrm{H}(x)}Y^{\mathrm{H}(x)}$（对于汉明重量计数多项式的情况），而在完全枚举式的情况下，将为 $f\colon A^n \to \mathbb{C}[Z_*]$, $f(x) = \prod_{i=1}^n Z_{x_i}$。

两个函数 $f\colon A^n \to V$ 具有特殊形式。向量空间$V$ 实际上是一个交换复代数 $\mathscr{A}$，而该函数是从 $A$ 到 $\mathscr{A}$的函数的直积。具体而言，在汉明情形中，令 $g\colon A \to \mathbb{C}[X, Y]$ 为 $g(a) = X^{1-\mathrm{H}(a)}Y^{\mathrm{H}(a)}$。在完全情形中，令 $g\colon A \to \mathbb{C}[Z_*]$为 $g(a) = Z_a$。于是，在每种情形下，对于 $x = (x_1, x_2, \ldots\ldots, x_n) \in A^n$, $f(x) = \prod_{i=1}^n g(x_i)$。由于这种特殊形式，傅里叶变换很容易计算。

**引理 7.4**。设 $A$ 为有限阿贝尔群，$\mathscr{A}$ 为交换复代数。假设存在函数 $f_i\colon A \to \mathscr{A}, i = 1, 2, \ldots, n$，使得 $f\colon A^n \to \mathscr{A}$ 满足 $f(x) = \prod_{i=1}^n f_i(x_i)$, 其中 $x = (x_1, x_2, \ldots, x_n) \in A^n$。那么，对于 $\pi = (\pi_1, \pi_2, \ldots, \pi_n) \in \widehat{A}^n$,

$$\widehat{f}(\pi) = \prod_{i=1}^n \widehat{f}_i(\pi_i).$$

证明。这是一个计算，使用引理 2.6:

$$\begin{aligned}\widehat{f}(\pi) &= \sum_{x\in A^n} \langle \pi \,|\, x\rangle f(x) = \sum_{x\in A^n} \prod_{i=1}^n \left(\langle \pi_i \,|\, x_i\rangle f_i(x_i)\right) \\ &= \prod_{i=1}^n \left( \sum_{x_i \in A} \langle \pi_i \,|\, x_i\rangle f_i(x_i)\right) = \prod_{i=1}^n \widehat{f}_i(\pi_i).\end{aligned}$$

□

现在我们来计算各种情况下单变量函数的傅里叶变换。

**引理 7.5**。设 $A$ 是一个有限阿贝尔群。若 $g\colon A \to \mathbb{C}[X, Y]$ 由 $g(a) = X^{1-\mathrm{H}(a)}Y^{\mathrm{H}(a)}$给出，则对于 $\pi \in \widehat{A}$,

$$\widehat{g}(\pi) = \begin{cases} X + (|A| - 1)Y, & \pi = 1, \\ X - Y, & \pi \neq 1. \end{cases}$$

证明。利用 $\pi(0) = 1$ 和推论 2.20进行计算:

$$\begin{aligned}\widehat{g}(\pi) &= \sum_{a\in A} \langle \pi \,|\, a\rangle X^{1-\mathrm{H}(a)}Y^{\mathrm{H}(a)} = X + \sum_{a\neq 0} \langle \pi \,|\, a\rangle Y \\ &= \begin{cases} X + (|A| - 1)Y, & \pi = 1, \\ X - Y, & \pi \neq 1. \end{cases}\end{aligned}$$

□

**引理 7.6**。 设 $A$ 是一个有限阿贝尔群。如果给定 $g\colon A \to \mathbb{C}[Z_*]$ 为 $g(a) = Z_a$，那么，对于 $\pi \in A$，

$$\widehat{g}(\pi) = \sum_{a\in A} \langle \pi \,|\, a\rangle Z_a.$$

证明。 这是（7.1）。 □

现在我们将所有部分组合起来。

**定理 7.7** （麦克威廉斯恒等式）。 设 $A$ 是一个有限阿贝尔群。若 $C \subseteq A^n$ 是一个加性码，则

$$\operatorname{hwe}_C(X,Y) = \frac{1}{|(\widehat{A}^n : C)|} \operatorname{hwe}_{(\widehat{A}^n:C)}(X + (|A|-1)Y, X - Y),$$
$$\operatorname{ce}_C(Z_*) = \frac{1}{|(\widehat{A}^n : C)|} \operatorname{ce}_{(\widehat{A}^n:C)}(\mathcal{Z}_*)\Big|_{\mathcal{Z}_\pi \leftarrow \sum_{a\in A}\langle \pi \,|\, a\rangle Z_a}.$$

证明。如前所述，将泊松求和公式定理 7.3应用于 $C \subseteq A^n$，其中 $f(x) = X^{n-\mathrm{H}(x)}Y^{\mathrm{H}(x)}$ 用于汉明情形，而 $f(x) = \prod_{i=1}^n Z_{x_i}$用于完全情形。关键在于认识到，由引理 $\widehat{f}(\pi)$给出的因子分解形式 7.4 恰好取决于 $f(\pi)$。因此，泊松求和公式右侧具有计数多项式的形式。接着代入适当的$\widehat{g}(\pi_i)$。 □

汉明重量计数多项式可通过将 $X$ 代入 $Z_0$，并将 $Y$ 代入完全枚举式中的每个 $Z_a$来得到， $a \neq 0$。由此得到的项的化简过程与引理 7.5的证明类似。

备注 7.8。 由于双重对偶性，引理 2.17 中的$\widehat{\ }$ $\widehat{\ }$加性码 $C \subseteq A^n$ 及其湮灭子 $(A^n : C) \subseteq A^n$ 的角色可以互换。请注意完全情形下替换的细微差异，这是（2.11）的结果。

$$\operatorname{hwe}_{(\widehat{A}^n:C)}(X,Y) = \frac{1}{|C|} \operatorname{hwe}_C(X + (|A|-1)Y, X - Y),$$
$$\operatorname{ce}_{(\widehat{A}^n:C)}(\mathcal{Z}_*) = \frac{1}{|C|} \operatorname{ce}_C(Z_*)|_{Z_a \leftarrow \sum_{\pi\in\widehat{A}}\langle \pi \,|\, a\rangle \mathcal{Z}_\pi}.$$

有了定理 7.7，现在我们固定一个对偶 $\phi$，其所在的 $A$，将其扩展到$A^n$，并将结果拉回到 $A^n$。

**定理 7.9 (**麦克威廉斯恒等式**)**。 设 $A$ 为一个有限阿贝尔群， $\phi$ 为 $A$的对偶，并将其扩展到 $A^n$。若 $C \subseteq A^n$ 是一个加性

码，则

$$\begin{aligned}
\mathrm{hwe}_C(X,Y) &= \frac{1}{|\mathfrak{L}_\phi(C)|}\,\mathrm{hwe}_{\mathfrak{L}_\phi(C)}(X+(|A|-1)Y, X-Y),\\
\mathrm{hwe}_C(X,Y) &= \frac{1}{|\mathfrak{R}_\phi(C)|}\,\mathrm{hwe}_{\mathfrak{R}_\phi(C)}(X+(|A|-1)Y, X-Y),\\
\mathrm{ce}_C(Z_*) &= \frac{1}{|\mathfrak{L}_\phi(C)|}\,\mathrm{ce}_{\mathfrak{L}_\phi(C)}(\mathfrak{Z}_*)\big|_{\mathfrak{Z}_b\leftarrow\sum_{a\in A}\Phi(b,a)Z_a},\\
\mathrm{ce}_C(Z_*) &= \frac{1}{|\mathfrak{R}_\phi(C)|}\,\mathrm{ce}_{\mathfrak{R}_\phi(C)}(\mathfrak{Z}_*)\big|_{\mathfrak{Z}_b\leftarrow\sum_{a\in A}\Phi(a,b)Z_a}.
\end{aligned}$$

证明。假设 $C\subseteq A^n$ 是一个加性码。对偶 $\phi$，逐坐标扩展后$\widehat{}$到 $A^n$，是一个从 $A^n$ 到 $A^n$ 的同构，它将$\widetilde{}\mathfrak{L}_\phi(C)$ 映射为 $(A^n:\ C)$，由引理 4.3可知。由于 $\phi$ 是逐坐标扩展的，$\phi$ 保持汉明重量，因此对所有 $\mathrm{H}(x)=\mathrm{H}(\phi(x))$ 都有$x\in A^n$。这就推出了定理中的第一个等式。对 $\phi$*应用相同的论证即可得到第二个等式。

对于完全枚举式，我们使用不定元 $Z_*$ 表示 $C$，$\widehat{}\widetilde{}\mathcal{Z}_*$ 表示 $(A^n:C)$，并使用 $\mathfrak{Z}_*$ 表示对偶码。在 $\phi:A^n\to A^n$下，$\mathfrak{Z}_a\widehat{}$将对应于 $\mathcal{Z}_{\phi(a)}$；而在 $\phi^*:A^n\to A^n$下，$\mathfrak{Z}_a$ 将对应$\widehat{}$于 $\mathcal{Z}_{\phi^*(a)}$。因此，使用 $\phi$时，$\mathfrak{L}_\phi(C)$ 对应于 $(A^n:\ C)$，代换为 $\mathfrak{Z}_b\leftarrow\sum_{a\in A}\langle\phi(b)\,|\,a\rangle Z_a=\sum_{a\in A}\Phi(b,\ a)Z_a$。相反，使用$\widehat{}\,\phi$*时，$\mathfrak{R}_\phi(C)$ 对应于 $(A^n:C)$，代换为 $\mathfrak{Z}_b\leftarrow\sum_{a\in A}\langle\phi^*(b)\,|\,a\rangle Z_a=\sum_{a\in A}\Phi^*(b,\ a)Z_a=\sum_{a\in A}\Phi(a,b)Z_a$。□

现在我们交换加性码 $C\subseteq A^n$ 及其对偶码 $\mathfrak{L}_\phi(C)$的角色，$\mathfrak{R}_\phi(C)\subseteq A^n$使用命题4.4。

**推论 7.10**。设 $A$为有限阿贝尔群，且设 $\phi$ 为 $A$上的一个对偶，并将其扩展到 $A^n$。如果 $C\subseteq A^n$ 是一个加性码，则

$$\begin{aligned}
\mathrm{hwe}_{\mathfrak{L}_\phi(C)}(X,Y) &= \mathrm{hwe}_{\mathfrak{R}_\phi(C)}(X,Y)\\
&= \frac{1}{|C|}\,\mathrm{hwe}_C(X+(|A|-1)Y, X-Y),\\
\mathrm{ce}_{\mathfrak{L}_\phi(C)}(\mathfrak{Z}_*) &= \frac{1}{|C|}\,\mathrm{ce}_C(Z_*)|_{Z_b\leftarrow\sum_{a\in A}\Phi(a,b)\mathfrak{Z}_a},\\
\mathrm{ce}_{\mathfrak{R}_\phi(C)}(\mathfrak{Z}_*) &= \frac{1}{|C|}\,\mathrm{ce}_C(Z_*)|_{Z_b\leftarrow\sum_{a\in A}\Phi(b,a)\mathfrak{Z}_a}.
\end{aligned}$$

证明。与定理 7.9 的证明一样，$\phi$ 和 $\phi^*$ 在对偶码 $\mathfrak{L}_\phi(C)$之间保持汉明重量，$\mathfrak{R}_\phi(C)$ 以及湮灭子$\widehat{}$ $(A^n:\ C)$，因此它们的汉明重量枚举式相等。汉明情形由注记 7.8 得出。

对于完全枚举式， $\phi$ 与 $\mathfrak{Z}_a$ 对应， $\mathcal{Z}_{\phi(a)}$而 $\phi^*$与 $\mathfrak{Z}_a$ 对应 $\mathcal{Z}_{\phi^*(a)}$。注记 $Z_b \leftarrow \sum_{\pi\in\hat{A}}\langle\pi \mid b\rangle\mathcal{Z}_\pi$ 7.8 中的替换随后变为 $Z_b \leftarrow \sum_{a\in A}\langle\phi(a) \mid b\rangle\mathfrak{Z}_a = \sum_{a\in A}\Phi(a,\ b)\mathfrak{Z}_a$对于 $\phi$ （与 [7, 定理 3.3] 相反）以及 $Z_b \leftarrow \sum_{a\in A}\langle\phi^*(a) \mid b\rangle\mathfrak{Z}_a = \sum_{a\in A}\Phi(b,\ a)\mathfrak{Z}_a$ 对于 $\phi^*$。□

注记 7.11。 关于完整枚举子和汉明联合枚举子的麦克威廉斯恒等式的各种版本见 [5]。

## 8. 关于有限环的评论

设有限阿贝尔群 $A$ 还具有有限环 $R$ 的加法群所带有的代数结构（该环可以有或没有^乘法单位元）。那么，特征群 $R$ 具有^ $R$-双模的结构。对于 $r,\ s \in R$ 和 $\pi \in R$，标量乘法写成乘法形式：

$$\langle {}^r\pi \mid s\rangle = \langle \pi \mid sr\rangle, \quad \langle \pi^r \mid s\rangle = \langle \pi \mid rs\rangle.$$

^将 $R$ 的对偶 $\phi$ 定义为当 $\phi:\ R \to R$ 是左（或右） $R$-模的同态时的线性的 对偶。线性对偶并非总是存在。如果有限环有单位元，那么当且仅当 $R$ 是弗罗贝尼乌斯环时，线性对偶才存在 [17, 定理 3.10]。如果 $R$ 是弗罗贝尼乌斯环，且 $\phi$ 是 $R$的左线性对偶，那么其像 $\chi = \phi(1) \in R$ 是一个生成^特征，其意义是 $\phi(r) = {}^r\chi$ 是左 $R$-模的同构 $R \to R$。继而可证明 $\phi^*(r) = \chi^r$ 是右 $R$-模的同构$\frown R \to R$。弗罗贝尼乌斯环上的线性对偶已有成熟的理论；参见 [18, §12]。

当 $R$ 是有限 rng（即不一定具有乘法单位元的有限环：没有“i”）时，我们所知较少。不过，有一种情形已得到理解：当 $R$ 具有生成特征时。

**定理 8.1.** 设 $R$ 是一个不一定具有乘法单位元的有限环。假设存在一个特征 $\chi \in R$，使得$\frown R \to R$和 $r \mapsto \chi^r$（分别）是右、左$R$-模之间的同构。那么 $R$ 具有乘法单位元，且 $R$ 是弗罗贝尼乌斯环。

证明。 由满射性，存在元素 $e \in R$ 使得 $\chi^e = \chi$。我们声称 $e$ 是一个乘法单位元。对于任意 $r \in R$，右乘以 $r$： $\chi^{er} = \chi^r$。单射性蕴含 $er = r$。现在考虑 $\chi^{re} = (\chi^r)^e$。对于任意 $s \in R$， $\langle\chi^{re} \mid s\rangle = \langle(\chi^r)^e \mid s\rangle = \langle\chi^r \mid es\rangle = \langle\chi^r \mid s\rangle$。因此， $\chi^{re} = \chi^r$，且单射性蕴含 $re = r$。于是，根据 [17, 定理 3.10]， $R$ 是 Frobenius 的。左模的情形类似。□

存在有限 rng 的线性对偶，它们不是定理 8.1.中的形式。

**例 8.2.** 考虑 rng $I$，它定义为理想 $(x) \subset \mathbb{F}_2[x]/(x^3)$。这是 rng $I$ 中列出的 [10]版本。下面给出加法表和乘法表。

| $+$ | $0$ | $x$ | $x+x^2$ | $x^2$ |
|---|---|---|---|---|
| $0$ | $0$ | $x$ | $x+x^2$ | $x^2$ |
| $x$ | $x$ | $0$ | $x^2$ | $x+x^2$ |
| $x+x^2$ | $x+x^2$ | $x^2$ | $0$ | $x$ |
| $x^2$ | $x^2$ | $x+x^2$ | $x$ | $0$ |

| $\times$ | $0$ | $x$ | $x+x^2$ | $x^2$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $x$ | $0$ | $x^2$ | $x^2$ | $0$ |
| $x+x^2$ | $0$ | $x^2$ | $x^2$ | $0$ |
| $x^2$ | $0$ | $0$ | $0$ | $0$ |

加法群是克莱因四元群；乘法是交换的。

特征模有以下元素和标量乘法。

| $s$ | $\pi_0(s)$ | $\pi_1(s)$ | $\pi_2(s)$ | $\pi_3(s)$ | $\pi_0^s$ | $\pi_1^s$ | $\pi_2^s$ | $\pi_3^s$ |
|---|---|---|---|---|---|---|---|---|
| $0$ | $1$ | $1$ | $1$ | $1$ | $\pi_0$ | $\pi_0$ | $\pi_0$ | $\pi_0$ |
| $x$ | $1$ | $1$ | $-1$ | $-1$ | $\pi_0$ | $\pi_3$ | $\pi_3$ | $\pi_0$ |
| $x+x^2$ | $1$ | $-1$ | $1$ | $-1$ | $\pi_0$ | $\pi_3$ | $\pi_3$ | $\pi_0$ |
| $x^2$ | $1$ | $-1$ | $-1$ | $1$ | $\pi_0$ | $\pi_0$ | $\pi_0$ | $\pi_0$ |

那么 $f\colon I \to I$ 定义为

| $s$ | $0$ | $x$ | $x+x^2$ | $x^2$ |
|---|---|---|---|---|
| $f(s)$ | $\pi_0$ | $\pi_1$ | $\pi_2$ | $\pi_3$ |

可见这是一个 $I$-模的同构。（也可以交换 $x$ 与 $x+x^2$ （或 $\pi_1$ 与 $\pi_2$）的角色。）

在未来的一篇论文中，我计划讨论与 $A$上的群作用相关联的对称化枚举器的麦克威廉斯恒等式，并探讨有限环上模字母表背景下的对偶性，以及对偶性如何与码的等价性这一概念相互作用。

## References

[1] D. J. Benson，《表示与上同调 I》，第2版，《剑桥高等数学研究丛书》第30卷，剑桥大学出版社，剑桥，1998年。MR 1644252 (99f:20001a)[2] P. Delsarte，《通过线性规划求无约束码的界》，《Philips Res. Rep.》**27** (1972), 272–289。MR 0314545 (47 #3096)

[3]____ ，编码理论关联方案的代数方法，《Philips Res. Rep. Suppl.》(1973), no. 10, vi+97。MR 384310[4] S. T. Dougherty，《有限阿贝尔群上码的对偶性》，《Adv. Math. Commun.》18 (2024), no. 6, 1827–1841。[5] ，具有任意对偶的加性码的广义完全联合重量枚举子的MacWilliams关系，预印本，2025年。[6] S. T. Dougherty、C. Fernández-Córdoba 和 M. Villanueva，《有限阿贝尔群的对称对偶性》，预印本，2025年。[7] S. T. Dougherty、J.-L. Kim 和 N. Lee，《偶数阶域上的加性自对偶码》，《 Bull. Korean Math. Soc. 》 55 (2018), no. 2, 341–357。MR 3789447[8] S. T. Dougherty 和 S. Myers，《由群特征得到的正交性》，《Involve》14 (2021), no. 4, 555–570。MR 4332568[9] S. T. Dougherty 和 S. Şahinkaya，《阶为2的循环群交叉积上的对偶性》，《 Adv. Math. Commun.》18 (2024), no. 5, 1531–1546。MR 4770737[10] B. Fine，《有限环的分类》，《Math. Mag.》66 (1993), no. 4, 248–252。MR 1240670[11] H. Gluesing-Luerssen，《加性码的傅里叶自反划分与麦克威廉斯恒等式》，《Des. Codes Cryptogr.》75 (2015), no. 3, 543–563。MR 3336966[12] S. Lang，《代数》，Addison-Wesley，马萨诸塞州雷丁，1971年。[13] J. MacWilliams，《有限域上的正交矩阵》，《Amer. Math. Monthly》76 (1969), 152–164。MR 238870[14] G. Nebe、E. M. Rains 和 N. J. A. Sloane，《自对偶码与不变量理论》，《Algorithms and Computation in Mathematics》第17卷，Springer-Verlag，柏林，2006年。MR 2209183 (2007d:94066)[15] J.-P. Serre，《有限群的线性表示》，Springer-Verlag，纽约，1977年，由Leonard L. Scott根据法文第2版翻译，《Graduate Texts in Mathematics》第42卷。MR 0450380 (56 #8675)[16] A. Terras，《有限群上的傅里叶分析及其应用》，《伦敦数学学会学生教材》第43卷，剑桥大学出版社，剑桥，1999年。MR 1695775 (2000d:11003)[17] J. A. Wood，《有限环上的模的对偶性及其在编码理论中的应用》，《Amer. J. Math.》121 (1999), no. 3, 555–575。MR 1738408
[18] ，有限模上线性码的基础：扩张定理与麦克威廉斯恒等式，载于《环上的码》（安卡拉，2008年）（P. Sol´e 编），《编码理论与密码学丛书》第6卷，World Sci. Publ.，新泽西州哈肯萨克，2009年，第124–190页。MR 2850303

Western Michigan University电子
邮件地址：jay.wood@wmich.edu