arXiv:2601.16553v1 [math.LO] 23 Jan 2026

群 $\mathbb{Z}_8$ 的扩张（第一部分）

Miroslav Ploščica, Radka Schwartzová, Ivana Varga

（收稿日期：2026年1月26日）

Abstract. 我们研究 $\mathbb{Z}_8$ 的群多项式与环多项式之间的区间中的克隆。这是该问题最简单的开放情形，因为对于 $\mathbb{Z}_{p^2}$（其中 p 为素数），答案已知；而一般而言，$\mathbb{Z}_n$ 可归结为 n 为素数幂的情形。事实证明，所研究的结构非常复杂，因此我们只给出部分描述。我们将研究范围限制在非线性单项式的系数均为偶数的多项式。

Keywords：克隆，同余，环，多项式

MSC 2020：08A40,03B50

1. Introduction

集合 A 上一个有限元运算族，若包含所有投影且对复合封闭，则称为一个克隆。克隆在现代泛代数中占有重要地位。这是因为代数结构的许多重要性质由其项运算或多项式运算的克隆所决定。

给定集合 A 上的所有克隆构成一个完备格。对于二元集合 A，这个格是可数的，且已由 E. Post [14] 描述。若所考察的集合至少有三个元素，克隆格便不可数，也不可能对其进行完整描述，参见 [9]。因此，研究通常旨在描述这个格中一些有趣的部分。所研究的克隆常常与基集上的某种特殊代数结构有关。例如，许多论文研究包含群运算的克隆（[4, 5, 19, 18]）。论文 [8, 7, 15, 16,17, 3, 1, 12] 着重研究 $\mathbb{Z}_n$ 的环多项式所生成的克隆。

本研究得到 VEGA资助项目1/0152/22 以及欧盟通过“斯洛伐克复苏与韧性计划”提供的下一代欧盟资金支持，项目编号为 09I03-03-V05-00008。

本文研究克隆格中的区间 $\mathcal{J}_n = \langle P(\mathbb{Z}_n,\ +)\ P(\mathbb{Z}_n,\ +,\ \cdot)\rangle$。这里，$P(\mathbb{Z}_n,\ +)$ 是群 $(\mathbb{Z}_n,\ +)$ 的所有多项式运算所生成的克隆，而 $P(\mathbb{Z}_n,\ +,\ \cdot)$ 表示环 $(\mathbb{Z}_n,\ +,\ \cdot)$ 的所有多项式运算所生成的克隆。因此，$P(\mathbb{Z}_n,\ +)$ 的元素具有以下形式

$$p(x_1, \ldots, x_k) = a_0 + a_1x_1 + a_2x_2 + \cdots + a_nx_k,$$

其中 $a_0 \in \mathbb{Z}_n$、a_1、.....、$a_n \in \mathbb{Z}$。$P(\mathbb{Z}_n$、+、·) 中的运算可以表示为如下形式的多项式

$$f(\mathbf{x}) = \sum_{\alpha} a_\alpha \mathbf{x}^\alpha, \tag{1.1}$$

其中 $\mathbf{x} = (x_1$、.....、$x_n)$，求和遍历有限多个由自然数组成的 n 元组 $\alpha = (\alpha_1$、.....、$\alpha_n)$，系数 a_α 属于 $\mathbb{Z}_n$，而$\mathbf{x}^\alpha$ 是 $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$的缩写。

引理 1.1。设 n、m 为自然数。如果 $(m$、$n) = 1$，那么

$$\mathcal{J}_{mn} \cong \mathcal{J}_m \times \mathcal{J}_n.$$

引理 1.1 的证明隐含在 [13]中。为完整起见，我们在下一节给出证明。该引理意味着，为了描述区间 $\mathcal{J}_n$，只需研究 $n = p^k$ 的情形，其中 p 是素数。

$k = 1$ 的情形是众所周知的。由于 $\mathbb{Z}_p$ 是一个域，每个运算都是环多项式。根据 I. Rosenberg ([17])，克隆 $P(\mathbb{Z}_p$、+) 是极大的，这意味着区间 $\mathcal{J}_p$ 仅由两个克隆组成：$P(\mathbb{Z}_p$、+) 和 $P(\mathbb{Z}_p$、+、·)。

$k = 2$ 的情形要复杂得多。A. Bulatov 在 [3]中给出了 $\mathcal{J}_{p^2}$ 的详细描述。下面给出了该格的图示。

（我们想指出的是，Krokhin 等人在 [11]中描述了 $\mathcal{J}_{p^2}$ 的 $p = 2$，随后 A. Bulatov 和 P. Idziak 在 [6]中对其进行了推广。）

$k = 3$ 的情形仍未解决。在我们的论文中，我们研究了 $p = 2$的情形。即使是这个特殊情形也非常复杂，以至于我们只能描述区间$\mathcal{J}_8$的一部分，即区间 $\langle P(\mathbb{Z}_8,\ +)\ M_1\rangle$，其中克隆 M_1 由满足以下性质的所有环多项式组成：所有非线性单项式的系数都是偶系数。

2. 化归为素幂

在本节中，我们证明引理 1.1。事实上，我们证明一个稍强的结论。我们将$\mathbb{Z}_n$ 视为元素为 $0, .., n-1$的集合。回顾一下，群 $\mathbb{Z}_n$ 和环 $\mathbb{Z}_n$具有相同的同余关系，即对每个整除 n 的 m，其模运算为 m，定义如下

$$x \equiv y \pmod m \quad \text{iff} \quad m|(x-y).$$

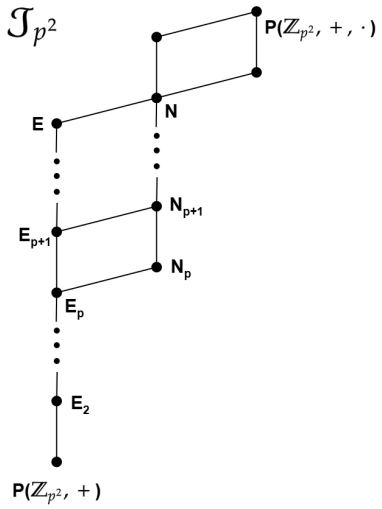

FIGURE 1. $\mathcal{J}_{p^2}$的多项式克隆格

我们还将"mod"用作运算符号，因此 x 模 m是 $\mathbb{Z}_m$ 中与 x 模 m同余的唯一元素。设 m 和 n 为互素自然数。设 $\mathcal{O}$ 为集合 $\mathbb{Z}_{mn}$ 上所有保持模 m 和模 n 同余关系的有限元运算所成的集合。此外，设 $\mathcal{O}_m$ 和 $\mathcal{O}_n$ 分别为$\mathbb{Z}_m$ 和 $\mathbb{Z}_n$上的所有有限元运算所成的集合。

对于任意 k 元 $f \in \mathcal{O}$，我们定义 $f_m \in \mathcal{O}_m$ 和 $f_n \in \mathcal{O}_n$ 如下:

$$f_m(x_1, \ldots, x_k) = f(x_1, \ldots, x_k) \mod m,$$

$$f_n(x_1, \ldots, x_k) = f(x_1, \ldots, x_k) \mod n.$$

此外，对于 k 元 $(g, h) \in \mathcal{O}_m \times \mathcal{O}_n$ 和 $x_1, \ldots, x_k \in \mathbb{Z}_{mn}$，我们将 $(g \times h)(x_1, \ldots, x_k)$ 定义为满足以下条件的 $\mathbb{Z}_{mn}$ 中唯一元素:

$$(g \times h)(x_1, \ldots, x_k) \equiv g(x_1 \bmod m, \ldots, x_k \bmod m) \pmod m,$$

$$(g \times h)(x_1, \ldots, x_k) \equiv h(x_1 \bmod n, \ldots, x_k \bmod n) \pmod n,$$

根据中国剩余定理，这样的元素存在。显然，此运算保持模 m 和模 n 的同余关系，因此属于 $\mathcal{O}$。

引理 2.1. 对于任意 k元的 $f \in \mathcal{O}$, $g \in \mathcal{O}_m$, $h \in \mathcal{O}_n$，等式 $(g \times h)_m = g$，$(g \times h)_n = h$ 和 $f_m \times f_n = f$ 均成立。

证明。 前两个等式显然。为了证明第三个等式，我们需要证明对于任意 $x_1, \ldots,$ $x_k \in \mathbb{Z}_{mn}$,

$$f(x_1, \ldots, x_k) \equiv f_m(x_1 \bmod m, \ldots, x_k \bmod m) \pmod m,$$

$$f(x_1, \ldots, x_k) \equiv f_n(x_1 \bmod n, \ldots, x_k \bmod n) \pmod n.$$

根据 f_m的定义,

$$f_m(x_1 \bmod m, \ldots, x_k \bmod m) \equiv f(x_1 \bmod m, \ldots, x_k \bmod m) \pmod m.$$

由于 f 保持模 m同余，我们有

$$f(x_1 \bmod m, \ldots, x_k \bmod m) \equiv f(x_1, \ldots, x_k) \pmod m,$$

因此我们得到了关于 m的结论。关于 n 的论证相同。 □

引理 2.2。等式

$$f(g^1, \ldots, g^k)_m = f_m(g_m^1, \ldots, g_m^k)$$

对 $\mathcal{O}$中的任意 k元 f 和 l元 g^i 均成立。

证明。 设 k元 f和 l元 $g^1, \ldots, g^k$属于 $\mathcal{O}$。令 $\mathbf{x} = (x_1, \ldots, x_l) \in (\mathbb{Z}_m)^l$。对于每个 i，我们有

$$g_m^i(\mathbf{x}) \equiv g^i(\mathbf{x}) \pmod m.$$

由于 f 保持模 m 同余，我们有

$$f(g^1(\mathbf{x}), \ldots, g^k(\mathbf{x})) \equiv f(g_m^1(\mathbf{x}), \ldots, g_m^k(\mathbf{x})) \pmod m.$$

此外,

$$f_m(g_m^1(\mathbf{x}), \ldots, g_m^k(\mathbf{x})) \equiv f(g_m^1(\mathbf{x}), \ldots, g_m^k(\mathbf{x})) \pmod m,$$

这意味着 $f(g^1, \ldots, g^k)_m = f_m(g_m^1, \ldots, g_m^k)$。 □

引理 2.1 中描述的对应关系可扩展到子克隆，如下所示。设C 是 $\mathcal{O}$ 的一个子克隆。我们定义

$$C_m = \{f_m \mid f \in \mathcal{O}\};$$

$$C_n = \{f_n \mid f \in \mathcal{O}\}.$$

显然，如果 f 是投影，那么 f_m 和 f_n 都是作用于同一变量的投影。由此可得引理 2.2 的以下推论。

引理 2.3。对于每个克隆 $C \subseteq \mathcal{O}$， C_m 和 C_n 分别是 $\mathcal{O}_m$ 和 $\mathcal{O}_n$ 的子克隆。此外，如果 C 由其子集 F 生成，那么 C_m 和 C_n 分别由 $\{f_m \mid f \in F\}$ 和 $\{f_n \mid f \in F\}$ 生成。

进一步，设 D 和 E 分别是 $\mathcal{O}_m$ 和 $\mathcal{O}_n$的子克隆。我们定义

$$D \times E = \{g \times h \mid g \in \mathcal{O}_m,\ h \in \mathcal{O}_n,\ \text{of the same arity}\}.$$

引理 2.4. 对于任意的 D 和 E， $D \times E$ 是一个克隆。

证明。如果 g 和 h 是同一变量上的投影，那么 $g \times h$ 也是一个投影。因此，只需证明

$$(f_1 \times f_2)(g_1 \times h_1, \ldots, g_k \times h_k) = f_1(g_1, \ldots, g_k) \times f_2(h_1, \ldots, h_k)$$

对于所有适当元数的 $f_1, g_1, \ldots, g_k \in \mathcal{O}_m$ 和 $f_2, h_1, \ldots, h_k \in \mathcal{O}_n$。我们有

$$(f_1 \times f_2)(g_1 \times h_1, \ldots, g_k \times h_k)_m = (f_1 \times f_2)_m((g_1 \times h_1)_m, \ldots, (g_k \times h_k)_m) =$$

$$= f_1(g_1, \ldots, g_k).$$

同理，

$$(f_1 \times f_2)(g_1 \times h_1, \ldots, g_k \times h_k)_n = f_2(h_1, \ldots, h_k).$$

令 $f = (f_1 \times f_2)(g_1 \times h_1, \ldots, g_k \times h_k)$，所需等式由引理 2.1 得出。□

令Sub($\mathcal{O}$)、Sub($\mathcal{O}_m$)和Sub($\mathcal{O}_n$)分别表示 $\mathcal{O}$、 $\mathcal{O}_m$和 $\mathcal{O}_n$的所有子克隆所构成的格。

定理 2.1. 设 $C \in \mathrm{Sub}(\mathcal{O})$、 $D \in \mathrm{Sub}(\mathcal{O}_m)$、 $E \in \mathrm{Sub}(\mathcal{O}_n)$。则 $(D \times E)_m = D$、$(D \times E)_n = E$，且 $C \subseteq C_m \times C_n$。若 C 包含模mn 的（二元）加法，则 $C_m \times C_n = C$。

证明。我们有 $(D \times E)_m = \{(g \times h)_m \mid g \in D,\ \ h \in E \text{具有相同的元数}\} = \{g \mid g \in D\} = D$。类似地，$(D \times E)_n = E$。若 $f \in C$，则 $f = f_m \times f_n \in C_m \times C_n$。

现在假设 C 包含模 mn 加法。 $C_m \times C_n$ 中的每个元素都可表示为某个 k 元 g, $h \in C$的 $g_m \times h_n$。由于 m 和 n 互素，存在 $a \in \mathbb{Z}_m$、 $b \in \mathbb{Z}_n$，使得 $an \equiv 1$（模 m）且 $bm \equiv 1$（模 n）。运算 $f = ang + bmh = g + \cdots + g + h + \cdots + h$（ g出现 an 次以及 h 出现 bm 次）属于 C，我们断言 $f = g_m \times h_n$。对于每个 x_1、.....、 $x_k \in \mathbb{Z}_{mn}$，我们有

$$f(x_1, \ldots, x_k) \equiv g(x_1, \ldots, x_k) \pmod{m}.$$

由于 g 保持模 m 同余，我们还有

$$g(x_1,\dots,x_k) \bmod m = g(x_1 \bmod m,\dots,x_k \bmod m) \bmod m =$$

$$= g_m(x_1 \bmod m,\dots,x_k \bmod m),$$

因此

$$f(x_1,\dots,x_k) \equiv g_m(x_1 \bmod m,\dots,x_k \bmod m) \pmod m,$$

类似地,

$$f(x_1,\dots,x_k) \equiv h_n(x_1 \bmod n,\dots,x_k \bmod n) \pmod n,$$

因此 $f = g_m \times h_n$。 □

定理 2.2。 设 $J \subseteq \mathrm{Sub}(\mathcal{O})$ 由所有包含模 mn 加法的克隆组成。类似地，设 $J_m \subseteq \mathrm{Sub}(\mathcal{O}_m)$ 和 $J_n \subseteq \mathrm{Sub}(\mathcal{O}_n)$ 分别由所有包含模 m 和模 n 加法的克隆组成。则格 J同构于直积 $J_m \times J_n$。

证明。 显然，若 f 是模 mn 加法，则 f_m 和 f_n 分别是模m 和模 n 加法。由定理 2.1，映射 $C \mapsto (C_m, C_n)$ 和 $(D, E) \mapsto D \times E$是 J与 $J_m \times J_n$之间的互逆映射。显然，它们保序，因此是格同构。□

同样容易看出，若 f 是模 mn乘法，则 f_m 和 f_n 分别是模 m和 n乘法。此外，若 f 是（一元）常值运算，则 f_m 和 f_n 也都是常值运算。由此可知，若 C 是群（环） $\mathbb{Z}_{mn}$的所有多项式运算组成的克隆，则 C_m 和 C_n 分别是群（环） $\mathbb{Z}_m$ 和 $\mathbb{Z}_n$ 的所有多项式运算组成的克隆。因此，定理 2.2 证明中的同构限制为 $\mathcal{J}_{mn}$与 $\mathcal{J}_m \times \mathcal{J}_n$， 之间的同构，从而证明了引理 1.1。

3. The clone M_1

从现在起，我们考虑 $\mathbb{Z}_8$的情形。我们研究 $\mathbb{Z}_8$ 中形如（1.1）的 n元（环）多项式运算。

不同的多项式可能表示相同的运算。特别容易看出,

$$0 = (x-1)x(x+1)(x+2) = x^4 + 2x^3 - x^2 - 2x$$

and

$$0 = (x^2 - x)(y^2 - y)(z^2 - z)$$

对于每个 x, y, $z \in \mathbb{Z}_8$, 因此我们可以假设在 (1.1) 中，每个 α 至多有两个大于 1 的分量，且没有分量大于 3。

形如 (1.1) 的多项式若能被 $x_1x_2\dots x_n$ 整除，就称为全可除多项式。因此，当且仅当多项式的所有单项式都包含所有变量时，它才是全可除的。若一个多项式运算可由全可除多项式表示，则称该运算为全可除运算。全可除多项式的重要性体现在以下事实中。Bulatov 最先针对 $\mathbb{Z}_{p^2}$ 观察到这一点，但这个简单的论证对 $\mathbb{Z}_8$ 也成立。

引理 3.1. 设 C 是 $P(\mathbb{Z}_8、+、\cdot)$ 的一个子克隆，且包含加法和常数。那么，C 由其完全可除成员生成。

证明。每个 $f(x_1,\dots,x_n) \in C$ 都是全可除多项式运算之和（这些运算涉及不同的变量集合）。我们只需证明这些加项属于 C。设 $f_0 = f(0, x_2, \dots, x_n)$、$f_1 = f - f_0$。那么 $f = f_0 + f_1$、$f_0, f_1 \in C$。多项式 f_0 由 f 中不包含 x_1 的单项式构成，而 f_1 的所有单项式都包含 x_1。接下来，我们根据是否包含 x_2，将 f_0 和 f_1 的单项式拆分。重复这一过程，我们就能将 f 表示为全可除多项式之和，而这些多项式都属于 C。□

上一个证明中的一个加数由所有全可除单项式（包含所有变量）构成。因此我们得到以下结论。

引理 3.2。设 C 是 $P(\mathbb{Z}_8, +, \cdot)$ 的一个子克隆，且包含加法和常数。设 $f \in C$，令 g 为 f 的全可除单项式之和。则 $g \in C$。

现在我们将定义克隆 $M_1 \subseteq P(\mathbb{Z}_8, +, \cdot)$。我们用记号$\mathbf{u} = (u_1, \dots, u_k)$表示元素的 k 元组。任意 n 元运算 $f\colon\ A^n \to A$ 都可以逐点扩展为一个运算 $(A^k)^n \to A^k$，它也记作 f。如果$\mathbf{u}^{(1)}, \dots, \mathbf{u}^{(n)} \in R$ 蕴含 $f(\mathbf{u}^{(1)}, \dots, \mathbf{u}^{(n)}) \in R$，我们就说 n 元运算 $f\colon\ A^n \to A$ 保持关系 $R \subseteq A^k$。

我们发现，使用定义在 $\mathbb{Z}_8$上的 2^k元关系会更方便。我们的 2^k元组将由 P_k（$\{1,\dots,k\}$的幂集）来索引。因此，我们写作$\mathbf{x} = (x_A \mid A \in P_k)$。分量 x_A 可以视为$\mathbf{x}$ 在标准基中的坐标。不过，在我们的定理中，使用另一组基会更方便。对于每个 $A \in P_k$，定义$\mathbf{g}^A = (g^A_B \mid B \in P_k) \in \mathbb{Z}_8^{P_k}$为

$$g^A_B = \begin{cases} 1, \text{ if } A \subseteq B \\ 0, \text{ otherwise.} \end{cases}$$

注意到$\mathbf{g}^\emptyset = \mathbf{1}$为常数 $\mathbf{1}$。在下文中，我们用$\mathbf{g}^m$ 代替$\mathbf{g}^{\{m\}}(m = 1,\dots,k)$，并用$\mathbf{g}^0$ 代替$\mathbf{g}^\emptyset$。

引理 3.3。 每个$\mathbf{x} \in \mathbb{Z}_8^{P_k}$都可以表示为以下形式

$$\mathbf{x} = \sum_{A \in P_k} a_A \mathbf{g}^A,$$

其中

$$a_A = (-1)^{|A|} \sum_{B \subseteq A} (-1)^{|B|} x_B.$$

对每个 $A \in P_k$ 均成立。$\mathbf{x}$ 以这种形式表示是唯一的。

证明。 令 $\mathbf{u} = \sum_{A \in P_k} a_A \mathbf{g}^A$。显然， $u_A = \sum_{B \subseteq A} a_B$ 对每个 $A \in P_k$ 均成立。于是

$$u_A = \sum_{B \subseteq A} (-1)^{|B|} (\sum_{C \subseteq B} (-1)^{|C|} x_C) = \sum_{C \subseteq A} (-1)^{|C|} (\sum_{C \subseteq B \subseteq A} (-1)^{|B|}) x_C = x_A,$$

因为对于 $C \subsetneq A$，我们有 $\sum_{C \subseteq B \subseteq A} (-1)^{|B|} = 0$。

为证明唯一性，假设我们有两个不同的表达式

$$\mathbf{x} = \sum_{A \in P_k} a_A \mathbf{g}^A = \sum_{A \in P_k} b_A \mathbf{g}^A.$$

于是存在一个极小集合 A，使得 $a_A \neq b_A$，进而 $0 = x_A - x_A = \sum_{B \subseteq A} a_B - \sum_{B \subseteq A} b_B = a_A - b_A \neq 0$，这就产生了矛盾。□

使用函数 $\mathbf{g}^A$ 对集合函数进行变换在组合学及其他领域中得到广泛应用，这种变换称为 Möbius 变换。（参见 [10] 或 [2]。）

下面的陈述很容易证明，今后将经常使用而不再给出引用。

引理 3.4。 对于任意 A、$C \in P_k$，在逐点乘法下，$\mathbf{g}^A \cdot \mathbf{g}^C = \mathbf{g}^{A \cup C}$。

设 Z 为 $\mathbb{Z}_8$ 上的 2^4元关系，由所有满足以下条件的元组 $\mathbf{u} = (u_A \mid A \in P_4)$ 组成：

(Z1) $a_{\{2\}} \equiv 2a_{\{1\}}$ (模 4)， $a_{\{4\}} \equiv 2a_{\{3\}}$ (模 4)；(Z2) 当 $|A| \geq 2$时， $a_A \equiv 0$ (模 2)；(Z3) 当 $|A| \geq 2$、$A \cap \{2,4\} \neq \emptyset$时， $a_A \equiv 0$ (模 4)；(Z4) 当 $\{2,4\} \subseteq A$时，$a_A = 0$。

设 M_1 是保持关系 Z 的所有环多项式构成的克隆。

包含加法和常数的环多项式的每个克隆都由其完全可除成员生成。因此，我们的首要目标是刻画 M_1 的完全可除成员。正如上一节所示， $\mathbb{Z}_8$ 上完全可除的 n 元多项式运算的一般形式为

$$f(\mathbf{x}) = x_1 x_2 \dots x_n \sum_{\alpha \in I_n} b_\alpha \mathbf{x}^\alpha, \tag{3.1}$$

其中， I_n 是由 $\{0,1,2\}^n$ 中所有至多有两个非零分量的 n 元组构成的集合。

很容易看出，加法保持 Z。

引理 3.5。运算 $f(x) = 2x_1x_2\dots x_n$ 对每个 $n \geq 1$ 都保持 Z。

证明。我们需要证明，当每个 i 都满足$\mathbf{u}^{(i)} \in Z$时， $f(\mathbf{u}^{(1)},\dots,\mathbf{u}^{(n)}) \in Z$。考虑$\mathbf{u}^{(i)}$的如下形式

$$\mathbf{u}^{(i)} = \sum_{A\in\mathcal{P}(4)} a_A^{(i)}\mathbf{g}^A,$$

其中，对于 $\{2,4\}\subseteq A$，有 $a_A^{(i)} = 0$。于是

$$f(\mathbf{u}^{(1)},\dots,\mathbf{u}^{(n)}) = \sum_{A\in\mathcal{P}(4)} a_A\mathbf{g}^A,$$

其中

$$a_A = \sum\{2a_{A_1}^{(1)}\cdot a_{A_2}^{(2)}\cdot\ldots a_{A_n}^{(n)} \mid A_1\cup\dots\cup A_n = A\}.$$

显然，每个 a_A 都是偶数，因此满足 (Z2)。根据 (Z1)，所有 $a_{\{2\}}^{(i)}$ 和 $a_{\{4\}}^{(i)}$ 都是偶数。因此，$a_{\{2\}}$ 和 $a_{\{4\}}$ 都能被 4 整除，所以 $f(\mathbf{u}^{(1)},\dots,\mathbf{u}^{(n)})$ 满足 (Z1)。由于每个包含 2 或 4 的 $a_A^{(i)}$，只要 A 就是偶数，因此得到 (Z3)。最后，若 $\{2,4\}\subseteq A$，则表达式 a_A 中的每一项都包含某个 i,j 的 $2a_{\{2\}}^{(i)}a_{\{4\}}^{(j)}$，因此 $a_A = 0$，故 (Z4) 成立。□

所有偶系数多项式运算都属于由加法和所有运算 $2x_1\dots x_n$ 生成的克隆。因此，我们得到如下结论。

引理 3.6. 所有 b_α 均为偶数的 *(3.1)* 形式的运算都保持 Z。

现在我们证明逆命题。一元情形需要单独处理。

引理 3.7. 运算 $f(x) = ax^3+bx^2+cx$ 保持 Z，当且仅当 a 和 b 都是偶数。

证明. 所有线性运算显然都保持 Z。因此， f 保持 Z，当且仅当 $g(x) = ax^3+bx^2$ 保持它。

首先，假设 g 保持 Z。令 $\mathbf{u} = \mathbf{g}^{\{1\}}+2\mathbf{g}^{\{2\}}$。显然，$\mathbf{u}\in Z$，所以$g(\mathbf{u})\in Z$。容易计算得出， $g(\mathbf{u}) = (a+b)\mathbf{g}^{\{1\}}+4b\mathbf{g}^{\{2\}}+(2a+4b)\mathbf{g}^{\{1,2\}}$。由 (Z3) 得到 $2a+4b\equiv 0$ (模 4)，因此 a 是偶数。由 (Z1) 得到 $2(a+b)\equiv 4b\equiv 0$ (模 4)，因此 b 是偶数。

反之由引理 3.6 可得。 □

引理 3.8. 设 f 形式的对象保持 Z。假设对于每个 α，都有 $n\geq 2$, $b_\alpha\in\{0,1\}$。那么对于每个 α，都有 $b_\alpha = 0$。

证明. 令 $\mathbf{u}^{(1)} = \mathbf{g}^{\{1\}} + 2\mathbf{g}^{\{2\}}$、$\mathbf{u}^{(2)} = \mathbf{g}^{\{3\}} + 2\mathbf{g}^{\{4\}}$，并令 $\mathbf{u}^{(i)} = \mathbf{g}^{\emptyset} = \mathbf{1}$（常值元组），其中 $i = 3, \ldots, n$。显然，对于每个 i，都有 $\mathbf{u}^{(i)} \in Z$，因此 $f(\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(n)}) \in Z$。令 $g(x_1, x_2) = f(x_1, x_2, 1, 1, \ldots, 1)$。那么 g 是一个二元多项式，可表示为

$$g(\mathbf{x}) = x_1 x_2 \sum_{\alpha \in I_2} c_\alpha \mathbf{x}^\alpha.$$

我们有 $g(\mathbf{u}^{(1)}, \mathbf{u}^{(2)}) = f(\mathbf{u}^{(1)}, \ldots\ldots, \mathbf{u}^{(n)}) \in Z$。显然，

$$c_{(\alpha_1, \alpha_2)} = b_{(\alpha_1, \alpha_2, 0, \ldots, 0)}$$

当且仅当 $\alpha_1, \alpha_2 \neq 0$。

将 $g(\mathbf{u}^{(1)}, \mathbf{u}^{(2)})$ 表示为 $\sum_{A \in P_n} d_A \mathbf{g}^A$ 的形式需要进行相当多的计算。我们有 $(\mathbf{u}^{(1)})^2 = \mathbf{g}^{\{1\}} + 4\mathbf{g}^{\{1,2\}} + 4\mathbf{g}^{\{2\}}$，$(\mathbf{u}^{(1)})^3 = \mathbf{g}^{\{1\}} + 2\mathbf{g}^{\{1,2\}}$，$(\mathbf{u}^{(2)})^2 = \mathbf{g}^{\{3\}} + 4\mathbf{g}^{\{3,4\}} + 4\mathbf{g}^{\{4\}}$，$(\mathbf{u}^{(2)})^3 = \mathbf{g}^{\{3\}} + 2\mathbf{g}^{\{3,4\}}$。因此，

$$(\mathbf{u}^{(1)})^3 (\mathbf{u}^{(2)})^3 = (\mathbf{g}^{\{1\}} + 2\mathbf{g}^{\{1,2\}})(\mathbf{g}^{\{3\}} + 2\mathbf{g}^{\{3,4\}}) = \tag{3.2}$$

$$= \mathbf{g}^{\{1,3\}} + 2\mathbf{g}^{\{1,3,4\}} + 2\mathbf{g}^{\{1,2,3\}} + 4\mathbf{g}^{\{1,2,3,4\}}.$$

类似地，我们得到

$$(\mathbf{u}^{(1)})^3 (\mathbf{u}^{(2)})^2 = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{1,3,4\}} + 4\mathbf{g}^{\{1,4\}} + 2\mathbf{g}^{\{1,2,3\}}, \tag{3.3}$$

$$(\mathbf{u}^{(1)})^2 (\mathbf{u}^{(2)})^3 = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{1,2,3\}} + 4\mathbf{g}^{\{2,3\}} + 2\mathbf{g}^{\{1,3,4\}}, \tag{3.4}$$

$$(\mathbf{u}^{(1)})^2 (\mathbf{u}^{(2)})^2 = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{1,3,4\}} + 4\mathbf{g}^{\{1,2,3\}} + 4\mathbf{g}^{\{1,4\}} + 4\mathbf{g}^{\{2,3\}}, \tag{3.5}$$

$$(\mathbf{u}^{(1)})^3 \mathbf{u}^{(2)} = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{1,2,4\}} + 2\mathbf{g}^{\{1,2,3\}} + 2\mathbf{g}^{\{1,4\}}, \tag{3.6}$$

$$\mathbf{u}^{(1)} (\mathbf{u}^{(2)})^3 = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{2,3,4\}} + 2\mathbf{g}^{\{1,3,4\}} + 2\mathbf{g}^{\{2,3\}}, \tag{3.7}$$

$$(\mathbf{u}^{(1)})^2 \mathbf{u}^{(2)} = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{1,2,3\}} + 4\mathbf{g}^{\{2,3\}} + 2\mathbf{g}^{\{1,4\}}, \tag{3.8}$$

$$\mathbf{u}^{(1)} (\mathbf{u}^{(2)})^2 = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{1,3,4\}} + 4\mathbf{g}^{\{1,4\}} + 2\mathbf{g}^{\{2,3\}}, \tag{3.9}$$

$$\mathbf{u}^{(1)} \mathbf{u}^{(2)} = \mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{2,4\}} + 2\mathbf{g}^{\{1,4\}} + 2\mathbf{g}^{\{2,3\}}. \tag{3.10}$$

现在我们有

$$g(\mathbf{u}^{(1)},\mathbf{u}^{(2)})=\sum_{A\in P_n} d_A\mathbf{g}^A=\sum_{i,j=1}^{3} c_{(i-1,j-1)}(\mathbf{u}^{(1)})^i(\mathbf{u}^{(2)})^j.$$

元组 $\mathbf{g}^{\{1,2,3,4\}}$ 只出现在 (3.2) 中，因此 $d_{\{1,2,3,4\}}=4c_{(2,2)}$。根据条件 (Z4)，我们有 $4c_{(2,2)}=d_{\{1,2,3,4\}}=0$，因此 $c_{(2,2)}$ 是偶数。由于 $c_{(2,2)}=b_{(2,2,0,\dots,0)}\in\{0,1\}$，我们得到 $b_{(2,2,0,\dots,0)}=0$。由对称性可知，只要 α 有任意两个分量等于 2，就有 $b_\alpha=0$。元组 $\mathbf{g}^{\{1,2,4\}}$ 只出现在 (3.6) 中，因此 $d_{\{1,2,4\}}=4c_{(2,0)}$。根据条件 (Z4)，我们有 $4c_{(2,0)}=d_{\{1,2,4\}}=0$，因此 $c_{(2,0)}$ 是偶数。（我们目前还不能断言 $c_{(2,0)}=0$。）元组 $\mathbf{g}^{\{1,2,3\}}$ 出现在多个地方，因此我们得到

$$d_{\{1,2,3\}}=2c_{(2,2)}+2c_{(2,1)}+4c_{(1,2)}+4c_{(1,1)}+2c_{(2,0)}+4c_{(1,0)}.$$

由条件 (Z3)，$d_{\{1,2,3\}}\equiv 0$（模 4）。由于 $c_{(2,2)}=0$ 和 $c_{(2,0)}$ 是偶数，我们得到 $c_{(2,1)}$ 是偶数。由于 $c_{(2,1)}=b_{(2,1,0,\dots,0)}\in\{0,1\}$，我们有 $c_{(2,1)}=b_{(2,1,0,\dots,0)}=0$。由对称性，当 α 同时包含 2 和 1 时，$b_\alpha=0$。

接下来，

$$c_{(2,0)}=\sum\{b_\alpha\mid \alpha_1=2,\ \alpha_2=0\}.$$

我们已经证明，除 $b_{(2,0,0,\dots,0)}$ 外，所有加数都为零。因此，$c_{(2,0)}=b_{(2,0,\dots,0)}\in\{0,1\}$。由于 $c_{(2,0)}$ 是偶数，我们得到 $b_{(2,0,\dots,0)}=0$。由对称性，当 α 包含 2 时，$b_\alpha=0$。

截至目前，我们已有 $c_{(2,2)}=c_{(2,1)}=c_{(1,2)}=c_{(2,0)}=c_{(0,2)}=0$。此外，$\mathbf{g}^{\{2,4\}}$仅出现在 (3.10) 中，因此 $d_{\{2,4\}}=4c_{(0,0)}$。根据 (Z4)，$c_{(0,0)}$ 为偶数。对于 $d_{\{2,3\}}$，我们得到

$$d_{\{2,3\}}=4c_{(1,1)}+4c_{(1,0)}+2c_{(0,1)}+2c_{(0,0)}.$$

由于（根据 (Z3)），$d_{\{2,3\}}$ 是 4 的倍数，且$c_{(0,0)}$ 为偶数，所以 $c_{(0,1)}$ 也必为偶数。通过类似的论证（使用 $d_{\{1,4\}}$），我们证明 $c_{(1,0)}$ 为偶数。现在我们有

$$d_{\{1,3\}}=c_{(1,1)}+c_{(1,0)}+c_{(0,1)}+c_{(0,0)}. \tag{3.11}$$

由于（根据 (Z2)）$d_{\{1,3\}}$ 为偶数，$c_{(1,1)}$ 也为偶数。然而，$c_{(1,1)}=b_{(1,1,0,\dots,0)}\in\{0,1\}$，因此 $b_{(1,1,0,\dots,0)}=0$。由对称性，当 α 有两个分量等于 1 时，$b_\alpha=0$。

现在我们来考虑

$$c_{(1,0)}=\sum\{b_\alpha\mid \alpha_1=1,\ \alpha_2=0\}.$$

我们已经证明，除了 $b_{(1,0,0,\dots,0)}$ 之外，所有加数都为零。因此，$c_{(1,0)}=b_{(1,0,\dots,0)}\in\{0,1\}$。由于 $c_{(1,0)}$ 是偶数，我们得到 $b_{(1,0,\dots,0)}=0$。由对称性可知，只要 α 含有 1，就有 $b_\alpha=0$。

还需证明 $b_{(0,0,\dots,0)} = 0$。我们有

$$c_{(0,0)} = \sum\{b_\alpha \mid \alpha_1 = 0,\ \alpha_2 = 0\} = b_{(0,0,\dots,0)},$$

因为所有其他加数均为零。根据我们的假设，$b_{(0,0,\dots,0)} \in \{0,1\}$。因此，$b_{(0,0,\dots,0)} = 0$，证明完毕。□

定理 3.1。设 f 由（*3.1*）定义，其中 $n \geq 2$。则 f 保持 Z 当且仅当每个 b_α 都是偶数。

证明。每个形如（3.1）的 f 都可以表示为以下和式

$$f(\mathbf{x}) = x_1x_2\dots x_n \sum_{\alpha\in I_n} c_\alpha \mathbf{x}^\alpha + x_1x_2\dots x_n \sum_{\alpha\in I_n} k_\alpha \mathbf{x}^\alpha, \tag{3.12}$$

其中每个 c_α 都是偶数，且每个 k_α 属于 $\{0,1\}$。假设 f 保持Z。根据引理 3.6，（3.12）中的第一项也保持 Z。加法也保持 Z，因此 $x_1x_2\dots x_n \sum_{\alpha\in I_n} k_\alpha \mathbf{x}^\alpha$ 保持 Z。根据引理 3.8，（3.12）中的第二项为零，因此 $f(\mathbf{x}) = x_1x_2\dots x_n \sum_{\alpha\in I_n} c_\alpha \mathbf{x}^\alpha$。

逆向蕴含由引理 3.6 得出。 □

因此，我们研究具有以下形式的全可除多项式

$$f = 2x_1\dots x_n(\sum_{\alpha\in I_n} b_\alpha \mathbf{x}^\alpha),. \tag{3.13}$$

这种形式还可以进一步简化。由于等式

$$2(x^2 + x)(y^2 + y) = 0$$

对于每个 $x, y \in \mathbb{Z}_8$，我们可以用次数较低的单项式替换所有 $b_\alpha \mathbf{x}^\alpha$，其中 α 有两个非零分量。由此可知，由 (3.13) 定义的运算等于由以下形式的多项式定义的运算

$$f = 2x_1\dots x_n(\sum_{i=1}^{n} a_i x_i^2 + \sum_{i=1}^{n} b_i x_i + c). \tag{3.14}$$

等式 $4x^3 = 4x^2 = 4x$ 对所有 $x \in \mathbb{Z}_8$ 均成立，这意味着，如果同时将某些 a_k 或 b_k 替换为 $a_k - 2$（或分别替换为 $b_k - 2$），并将 c 替换为 $c + 2$，则形式为 (3.14) 的 f 不变。此外，如果将 c 替换为 $c + 4$，f 也不变。因此，从现在起，我们假设在 (3.14) 中

$$a_i, b_i \in \{0,1\} \text{ for every } i \text{ and } c \in \{0,1,2,3\}.$$

下文中，令 $\mathcal{G}_1$ 表示所有这种形式的多项式的集合（对每个 $n \geq 1$）。此外，令 $\mathcal{G}_0$ 表示所有形如（3.14）的多项式的集合，使得 $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i + c$ 为偶数。

引理 3.9。令 f 为形如（*3.14*）且满足 $n \geq 2$ 的一个运算。那么，当且仅当 f 保持关系时，$f \in \mathcal{G}_0$

$$M = \{\mathbf{x} \in Z \mid a_{\{1,3\}} \equiv 0 \pmod 4\}.$$

证明。假设 $f \in \mathcal{G}_0$、$\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(n)} \in M$。由于 $M \subseteq Z$ 且 f 保持 Z，我们得到 $f(\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(n)}) \in Z$。$M$ 的附加条件得到满足，因为显然 $\mathrm{rng}(f) \subseteq \{0, 4\}$。

反过来，假设 $f \in \mathcal{G}_1 \setminus \mathcal{G}_0$。于是 $g = f + 2x_1 \ldots x_n \in \mathcal{G}_0$。根据本证明的第一部分，$g$ 保持 M。因此，f 保持 M 当且仅当 $2x_1 \ldots x_n$ 保持 M。令 $\mathbf{u}^{(1)} = \mathbf{g}^{\{1\}} + 2\mathbf{g}^{\{2\}}$、$\mathbf{u}^{(2)} = \mathbf{g}^{\{3\}} + 2\mathbf{g}^{\{4\}}$，以及 $\mathbf{u}^{(i)} = \mathbf{g}^{\emptyset} = \mathbf{1}$（常值元组），其中 $i = 3, \ldots, n$。显然，对于每个 i，$\mathbf{u}^{(i)} \in M$，并且

$$2\mathbf{u}^{(1)} \ldots \mathbf{u}^{(n)} = 2\mathbf{g}^{\{1,3\}} + 4\mathbf{g}^{\{1,4\}} + 4\mathbf{g}^{\{2,3\}} \notin M,$$

因此，$2x_1 \ldots x_n$ 和 f 不保持 M。 □

4. The subclones of M_1

对于每个 $f \in \mathcal{G}_1$，令 $C(f)$ 表示由 f、加法以及（一元）常值运算共同生成的 $\mathbb{Z}_8$ 上的克隆。现在我们研究这些克隆之间的等式和不等式。

我们为 $\mathbb{Z}_8$ 上的一些 n 元（$n \geq 1$）多项式引入以下记号。

$$r_n = x_1 x_2 \ldots x_n;$$
$$t_n = \begin{cases} x_1 x_2 \ldots x_n (x_1 + \cdots + x_n), & \text{if } n \text{ is even} \\ x_1 x_2 \ldots x_n (x_1 + \cdots + x_n + 1), & \text{if } n \text{ is odd.} \end{cases}$$
$$s_n = \begin{cases} x_1 x_2 \ldots x_n (x_1 + \cdots + x_n), & \text{if } n \text{ is odd} \\ x_1 x_2 \ldots x_n (x_1 + \cdots + x_n + 1), & \text{if } n \text{ is even.} \end{cases}$$
$$p_n = x_1^2 x_2 \ldots x_n;$$
$$q_n = x_1^3 x_2 \ldots x_n;$$
$$w_n = x_1 x_2 \ldots x_n (x_1^2 + 1);$$
$$u_n = x_1 x_2 \ldots x_n (x_1 + 1);$$
$$v_n = x_1 x_2 \ldots x_n (x_1 + x_2).$$

（运算 v_1 未定义。）运算 $2r_n$、$4r_n$、$2t_n$、$2s_n$、$2p_n$、$2q_n$、$2w_n$、$2u_n$ 和 $2v_n$ 属于 $\mathcal{G}_1$。其中，$4r_n$、$2t_n$、$2w_n$、$2u_n$ 和 $2v_n$ 属于 $\mathcal{G}_0$。注意，$4t_n$、$4w_n$、$4u_n$ 和 $4v_n$ 均为零。

引理 4.1。设 $f \in \mathcal{G}_1$ 具有（*3.14*）的形式。

(i) *If $a_i = 1$ for some i, then $4r_k \in C(f)$ for every $k \leq n + 2$;*

(ii) 若对于某个 i 有 $b_i = 1$，则对于每个 $k \leq n+1$，$4r_k \in C(f)$；

证明。(i) 我们可以假设 $a_1 = 1$，并将 f 写成如下形式

$$f = 2x_1^3 x_2 \dots x_n + 2x_1 \dots x_n (\sum_{i=2}^{n} a_i x_i^2 + \sum_{i=1}^{n} b_i x_i + c).$$

现在我们进行代换 $x_1 := x_1 + x_{n+1} + x_{n+2}$（其他变量不变）。代换后，我们得到一个属于 $C(f)$ 的多项式运算 g。多项式 g 包含一个可被 $x_1 x_2 \dots x_{n+2}$ 整除的单项式，即

$$2 \cdot (6x_1 x_{n+1} x_{n+2}) \cdot x_2 \dots x_n = 4r_{n+2}.$$

由引理 3.2，我们得到 $4r_{n+2} \in C(f)$。对所有 $i > k$ 代入 $x_i = 1$ 后，我们得到对于每个 $k \leq n+2$ 都有 $4r_k \in C(f)$。

(ii) 由于 (i)，我们可以假设对于所有 i 和 $b_1 = 1$ 都有 $a_i = 0$。于是

$$f = 2x_1^2 x_2 \dots x_n + 2x_1 \dots x_n (\sum_{i=2}^{n} b_i x_i + c).$$

经过代换 $x_1 := x_1 + x_{n+1}$，我们得到一个多项式运算 $g \in C(f)$，它包含一个可被 $x_1 \dots x_{n+1}$ 整除的单项式，即

$$2 \cdot (2x_1 x_{n+1}) x_2 \dots x_n = 4r_{n+1}.$$

因此，对于每个 $k \leq n+1$，$4r_k \in C(f)$。

□

因此，若 f 是 $\mathcal{G}_1$中的任意非零元素，则 $C(f)$包含 $4r_n$。因此，若 f 至少有一个 a_i 或 b_i 非零，则 $C(f) = G(g)$，对于

$$g = 2x_1 \dots x_n (\sum_{i=1}^{n} a_i x_i^2 + \sum_{i=1}^{n} b_i x_i + c - 2).$$

因此，我们只需在讨论中纳入运算 $4r_n$，即 $c = 2$。在所有其他情况下，我们可以假设 $c \in \{0, 1\}$。

引理 4.2. 对于每个 $n \geq 1$, $2r_n \in C(2r_{n+1})$, $4r_n \in C(4r_{n+1})$,$2t_n \in C(2t_{n+1})$, $2s_n \in C(2s_{n+1})$,$2p_n \in C(2p_{n+1})$, $2q_n \in C(2q_{n+1})$, $2u_n \in C(2u_{n+1})$, 以及 $2w_n \in C(2w_{n+1})$。对于每个 $n \geq 2$, $2v_n \in C(2v_{n+1})$。

证明. 所有结论均可通过代入 $x_{n+1}=1$ 得到证明。只有当 n 为偶数时的 $2t_n$ 情形，以及当 n 为奇数时的 $2s_n$ 情形，还需要进一步论证。在这些情形下，我们有 $2t_{n+1}(x_1,\dots,x_n,1) = 2t_n+4r_n$ 和 $2s_{n+1}(x_1,\dots,x_n,1) = 2s_n+4r_n$，因此$2t_n\in C(2t_{n+1})$和 $2s_n\in C(2s_{n+1})$可由引理 4.1 得出。□

引理 4.3。 设 $f\in\mathcal{G}_1$ 由 *(3.14)* 给出。假设对于某个 i，有 $a_i\neq 0$。那么 $2u_n\in C(f)$。

证明。 我们可以假设 $a_1=1$，并写作 $f=2x_1\dots x_n(x_1^2+b_1x_1+h(x_2,\dots,x_n))$。我们计算

$$\begin{gathered}f(x_1+1,x_2,\dots,x_n)-f(x_1,\dots,x_n)=\\ =2x_1\dots x_n((x_1+1)^2+b_1(x_1+1)+h(x_2,\dots,x_n))+\\ +2x_2\dots x_n((x_1+1)^2+b_1(x_1+1)+h(x_2,\dots,x_n))+\\ -2x_1\dots x_n(x_1^2+b_1x_1+h(x_2,\dots,x_n))=\\ =2x_1\dots x_n(2x_1+1+b_1)+2x_2\dots x_n((x_1+1)^2+b_1(x_1+1)+h(x_2,\dots,x_n)).\end{gathered}$$

略去不含x_1的多项式 $2x_2\dots x_n(1+b_1+h(x_2,\dots,x_n))$，可见 $C(f)$ 包含

$$2x_1\dots x_n(2x_1+1+b_1+x_1+2+b_1)=2u_n+2x_1\dots x_n(2x_1+2b_1+2).$$

求和项 $2x_1\dots x_n(2x_1+2b_1+2) = 4x_1\dots x_n(x_1+b_1+1)$ 为零或 $4r_n$，因此属于 $C(f)$。于是 $2u_n\in C(f)$ 也如此。□

引理 4.4。 设 $f\in\mathcal{G}_1$ 由 *(3.14)* 给出。假设对于某个 i，有 $a_i\neq 0$。那么 $2w_n\in C(f)$ 或 $2q_n\in C(f)$。

证明。 我们可以假设 $a_1=1$。首先，我们证明 $C(f)$ 包含如下形式的 $g\in\mathcal{G}_1$

$$g=2x_1\dots x_n(x_1^2+\sum_{i=1}^n b_i'x_i+c'). \tag{4.1}$$

我们需要消去除 a_1 之外的所有非零 a_i。我们假设 $a_2=1$。然后我们将 $x_1:=x_1+x_2$ 代入 f，其他变量保持不变。我们得到 $C(f)$ 的一个元素，它是以下各项之和

$$f_1=2x_1\dots x_n((x_1+x_2)^2+x_2^2+\sum_{i=3}^n a_ix_i^2+b_1x_2+\sum_{i=1}^n b_ix_i+c)$$

and

$$f_2=2x_2^2x_3\dots x_n((x_1+x_2)^2+x_2^2+\sum_{i=3}^n a_ix_i^2+b_1x_2+\sum_{i=1}^n b_ix_i+c).$$

f_2 的某些单项式不含 x_1。略去它们之后，我们得到多项式

$$f_3 = 2x_2^2 x_3 \dots x_n(x_1^2 + 2x_1x_2 + b_1x_1) = 2x_1 \dots x_n(x_1x_2 + 2x_2^2 + b_1x_2),$$

并且我们仍有 $f_1 + f_3 \in C(f)$。利用恒等式

$$2x_1^2x_2^2 = -2x_1^2x_2 - 2x_1x_2^2 - 2x_1x_2$$

我们有

$$f_3 = 2x_1 \dots x_n(-x_1 - x_2 - 1 + 2x_2^2 + b_1x_2).$$

此外，单项式 $2x_1 \dots x_n \cdot 2x_1x_2$ 和 $2x_1 \dots x_n \cdot 2x_2^2$ 都等于 $4r_n$。因此我们有

$$f_1 = 2x_1 \dots x_n(x_1^2 + 2 + 2 + \sum_{i=3}^{n} a_ix_i^2 + b_1x_2 + \sum_{i=1}^{n} b_ix_i + c),$$

$$f_3 = 2x_1 \dots x_n(-x_1 - x_2 - 1 + 2 + b_1x_2).$$

和 $g_1 = f_1 + f_3$ 属于 $C(f)$，并且可以写成以下形式

$$g_1 = 2x_1 \dots x_n(x_1^2 + \sum_{i=3}^{n} a_ix_i^2 + \sum_{i=1}^{n} b_i'x_i + c').$$

重复这一过程，我们得到所需形式（4.1）的 $g \in C(f)$。

根据引理 4.3，$2u_{n,\ i} = 2x_1 \dots x_n(x_i + 1)$ 对每个 i 都属于 $C(f)$。因此，

$$h = g - \sum_{i=1}^{n} 2b_i'u_{n,i} = 2x_1 \dots x_n(x_1^2 + c' - \sum_{i=1}^{n} b_i') = 2w_n + 2dr_n = 2q_n + 2(d+1)r_n,$$

其中 $d = c' - \sum_{i=1}^{n} b_i' - 1$也属于 $C(f)$。若 d为偶数，则 $2dr_n \in C(f)$，因此 $2w_n \in C(f)$也成立。若 d 为奇数，则 $2(d+1)r_n \in C(f)$，且 $2q_n \in C(f)$。□

引理 4.5。对于每个 $n \geq 2$, $C(2w_n) = C(2v_{n+1})$ 均成立。

证明。首先，我们将证明可以通过运算 $2v_{n+1}$得到 $2w_n$。由于$n \geq 2$，我们可以代入 $x_{n+1} := x_1$。我们有

$$2v_{n+1}(x_1, x_2, \dots, x_n, x_1) = 2x_1^3x_2 \dots x_n + 2x_1^2x_2^2 \dots x_n.$$

第一项等于 $2w_n(x_1, \dots\dots, x_n) - 2r_n(x_1, \dots\dots, x_n)$。对于第二项，我们使用等式 $2x_1^2x_2^2 = 6x_1^2x_2 + 6x_1x_2^2 + 6x_1x_2$，并得到

$$2x_1^3x_2 \dots x_n + 6x_1^2x_2 \dots x_n + 6x_1x_2^2 \dots x_n + 6x_1x_2 \dots x_n =$$

$$= 2w_n(x_1, x_2, \ldots, x_n) + 6v_n(x_1, x_2, \ldots, x_n) + 4r_n(x_1, x_2, \ldots, x_n).$$

根据引理 4.1，多项式 $4r_n$ 属于 $C(2v_{n+1})$。此外，$2v_n \in C(2v_{n+1})$，因此克隆 $C(2v_{n+1})$也包含函数 $2w_n$。

反过来，我们证明 $2v_{n+1} \in C(2w_n)$。我们有

$$2w_n(x_1 + x_{n+1}, x_2, \ldots, x_n) = 2(x_1 + x_{n+1})x_2 \ldots x_n((x_1 + x_{n+1})^2 + 1).$$

这个多项式的全可除部分属于 $C(2w_n)$，且等于

$$2x_1x_2 \ldots x_{n+1}(x_{n+1} + 2x_{n+1} + x_1 + 2x_1) = 2v_{n+1} + 4x_1x_2 \ldots x_{n+1}^2 + 4x_1^2x_2 \ldots x_{n+1}.$$

由于 $4x_1^2 = 4x_1$ 和 $4x_{n+1}^2 = 4x_{n+1}$，我们有 $4x_1x_2 \ldots x_{n+1}^2 + 4x_1^2x_2 \ldots x_{n+1} = 0$，所以 $2v_n \in C(2w_n)$。□

引理 4.6。对于每个 $n \geq 1$，$2w_n \in C(2q_n)$ 以及 $2r_n \in C(2q_n)$。

证明。由于 $2r_1 = 2x_1$ 是线性的，我们有 $2r_1 \in C(2q_1) \cap C(2w_1)$，且 $C(2q_1) = C(2w_1)$。现在假设 $n \geq 2$。运算 $2(x_1+x_2)^3x_3 \ldots x_{n+1}$ 属于 $C(2q_n)$。这个多项式的全可除部分为 $6x_1 \ldots x_{n+1}(x_1 + x_2) = -2v_{n+1}$。因此，$2v_{n+1} \in C(2q_n)$。根据引理 4.5，$2w_n \in C(2q_n)$。由于 $2r_n = 2w_n - 2q_n$，我们还得到 $2r_n \in C(2q_n)$。□

因此，我们得到下面的引理。

引理 4.7。设 $f \in \mathcal{G}_1$ 由（*3.14*）给出。假设对于某个 i，有 $a_i \neq 0$。那么 $2w_n \in C(f)$。

定理 4.1。设 $f \in \mathcal{G}_1$ 由（*3.14*）给出。假设对于某个 i，有 $a_i \neq 0$。如果 $f \in \mathcal{G}_0$，那么 $C(f) = C(2w_n)$。如果 $f \in \mathcal{G}_1 \setminus \mathcal{G}_0$，那么 $C(f) = C(2q_n)$。

证明。设 f 是 n元的，由（3.14）给出。我们已经知道，对于每个 i，运算$2w_{n,i} = 2x_1 \ldots x_n(x_i^2 + 1)$和$2u_{n,i} = 2x_1 \ldots x_n(x_i + 1)$都属于 $C(2w_n)$。于是还有

$$g = \sum_{i=1}^{n} 2a_i w_{n,i} + \sum_{i=1}^{n} 2b_i u_{n,i}$$

属于 $C(2w_n)$。显然，

$$g = 2x_1 \ldots x_n(\sum_{i=1}^{n} a_i x_i^2 + \sum_{i=1}^{n} b_i x_i + d),$$

其中 $d = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$。因此，$f = g + 2x_1 \ldots x_n(c - d)$。然后，$g \in C(2w_n) \subseteq C(2q_n)$，且 $2r_n \in C(2q_n)$ 蕴含 $f \in C(2q_n)$。所以，我们有 $C(2w_n) \subseteq C(f) \subseteq C(2q_n)$。

如果 $f \in \mathcal{G}_0$，则数值 $c-d$ 为偶数，因此 $2x_1 \dots x_n(c-d) \in C(2w_n)$。所以，$f \in C(2w_n)$。

若 $f \notin \mathcal{G}_0$，则 $d-c$ 为奇数，且 $2r_n = f - g - 2(d-c+1)r_n \in C(f)$。此外，$2q_n = 2w_n - 2r_n \in C(f)$。□

定理 4.2. 假设对所有 i， $f \in \mathcal{G}_1$, $a_i = 0$，且对某个 j， $b_j = 1$。令 $K = \{j \mid b_j = 1\}$。则

(i) 若 $K = \{1, \dots, n\}$，则 $f = 2t_n$ 或 $f = 2s_n$; *(ii)* 若 $1 \le |K| < n$，则 $2v_n \in C(f)$; *(iii)* 若 $1 \le |K| < n$ 且 $|K|$ 为偶数，则 $C(f) = C(2v_n)$ 或 $C(f) = C(2v_n) \vee C(2r_n)$; *(iv)* 若 $1 \le |K| < n$ 且 $|K|$ 为奇数，则 $C(f) = C(2u_n)$ 或 $C(f) = C(2p_n)$。

证明。记 $|K| = k$。不失一般性地， $K = \{1, \dots, k\}$，这意味着

$$f = 2x_1 \dots x_n(x_1 + \dots + x_k)$$

or

$$f = 2x_1 \dots x_n(x_1 + \dots + x_k + 1).$$

因此，(i) 显然成立。

(ii) 我们有

$$f(x_1, \dots, x_n) + f(x_2, \dots, x_n, x_1) =$$
$$= 2v_n(x_1, x_{k+1}, x_2, \dots, x_n) + 4x_1 \dots x_n(x_2 + x_3 + \dots + x_k) + 4mx_1 \dots x_n,$$

其中 $m \in \{0, 1\}$ 取决于 f的形式。对于每个 i，根据引理 4.1，有 $4x_1 \dots x_n x_i = 4r_n \in C(f)$。因此， $2x_1 \dots x_n(x_1 + x_{k+1}) \in C(f)$，所以 $2v_n$ 也包含于 $C(f)$ 中。

(iii) 如果 $|K|$为偶数，则要么

$$f = 2v_n(x_1, x_2, \dots, x_n) + 2v_n(x_3, x_4, \dots, x_n, x_1, x_2) + \dots +$$

$$+2v_n(x_{k-1}, x_k, \dots, x_n, \dots, x_{k-2}),$$

or

$$f = 2v_n(x_1, x_2, \dots, x_n) + 2v_n(x_3, x_4, \dots, x_n, x_1, x_2) + \dots +$$
$$+2v_n(x_{k-1}, x_k, \dots, x_n, \dots, x_{k-2}) + 2r_n.$$

在第一种情况下，我们有 $f \in C(2v_n)$，因此（结合 (ii)） $C(f) = C(2v_n)$。在第二种情况下，我们有 $f \in C(2v_n) \vee C(2r_n)$，因此 $C(f) \subseteq C(2v_n) \vee C(2r_n)$。同一等式蕴含 $2r_n \in C(f)$（因为 $2v_n \in C(f)$），因此 $C(2v_n) \vee C(2r_n) \subseteq C(f)$。

(iv) 若 $|K|$为奇数，则有以下两种情况之一:

$$f = 2u_n + 2v_n(x_2, x_3, \dots) + 2v_n(x_4, x_5, \dots) + \dots + 2v_n(x_{k-1}, x_k, \dots),$$

or

$$f = 2p_n + 2v_n(x_2, x_3, \dots) + 2v_n(x_4, x_5, \dots) + \cdots + 2v_n(x_{k-1}, x_k, \dots).$$

由 (ii) 可知， $2v_n \in C(f)$，且 $2v_n \in C(2u_n)$、 $2v_n \in C(2p_n)$。因此，在第一种情况下，我们得到 $C(2u_n) = C(f)$；在第二种情况下，得到 $C(f) = C(p_n)$。□

因此，区间 $\langle P(\mathbb{Z}_8, +) M_1\rangle$ 中的每个克隆都由其形如 $2t_n$, $2u_n$, $2v_n$, $2s_n$, $2p_n$, $2q_n$, $2r_n$ 和 $4r_n$的成员生成。注意，不再需要运算 $2w_n$，因为对于 $n \geq 2$， $C(2w_n) = C(2v_{n+1})$，且 $C(2w_1) = C(2q_1)$。

由于由每种类型的运算生成的克隆构成一个递增链n（例如， $C(2t_2) \subseteq C(2t_3) \subseteq C(2t_4) \subseteq \dots$），我们得到以下结果。

定理 4.3。 $\langle P(\mathbb{Z}_8, +) M_1\rangle$ 中的每个克隆都可以表示为以下连接形式

$$C(2t_{n_1}) \vee C(2u_{n_2}) \vee C(2v_{n_3}) \vee C(2s_{n_4}) \vee C(2p_{n_5}) \vee C(2q_{n_6}) \vee C(2r_{n_7}) \vee C(4r_{n_8}).$$

在此连接中，我们允许出现 $n_i = 0$ （以及 $n_3 = 1$），这表示相应的连接项不存在；也允许出现 $n_i = \infty$，这表示该克隆包含相应类型的所有运算。

当然，有些连接项可能是冗余的，因此克隆的上述形式表达式并不唯一。在本文后续部分，我们将给出一种算法，用于比较两个这种形式的克隆，从而完成对区间 $\langle P(\mathbb{Z}_8, +) M_1\rangle$ 的描述。

References

[1] *E. Aichinger, P. Mayr*：阶为 pq 的群上的多项式克隆。Acta Math. Hungar. **114** (2007), 267–285.[2] *M. Boczek, O. Hutník, M. Kleinová*：通过基和变换表示 Choquet 积分的一则注记。Fuzzy Sets and Systems**481** (2024).[3] *A. A. Bulatov*：包含群 $\mathbb{Z}_{p^2}$ 和 $\mathbb{Z}_p \times \mathbb{Z}_p$的 Mal'tsev 运算的多项式克隆。Multiple-valued Logic. **22** (2002), 193–221. [4] *A. A. Bulatov*：模的多项式约化 I：粗分类。Multiple-Valued Logic. **3** (1998), 135–154. [5] *A. A. Bulatov*：模的多项式约化 II：本原函数和幂零函数代数。Multiple-Valued Logic. **3** (1998), 173–193. [6] *A. Bulatov, P. Idziak*：小集合上的 Mal'tsev 克隆计数。Discrete Mathematics. (2003), 59–80.[7] *G. P. Gavrilov*：包含多项式类的多值逻辑闭类。Diskretnaya Matematika. **9** (1997), 12–23. [8] *G. P. Gavrilov*：多值逻辑多项式类的上结构。Diskretnaya Matematika. **8** (1996), 90–97. [9] *M. Goldstern, M. Pinsker*：无限集合上克隆概述。Algebra Universalis. **59** (2008). [10] *M. Grabisch*：决策中的集合函数、博弈与容量。Springer. **46** (2016), ISBN: 9783319306889.

[11] *A.A. Krokhin, K. L. Safin, E. V. Sukhanov*：多项式闭类格的结构。Diskretnaja Math.. 9 (1997), 24–40. [12] *P. Mayr*：无平方因子群上的多项式克隆。Internat. J. of Algebra and Computation. 18 (2008), 759–777. [13] *M. Ploščica, I. Varga*：环上相容运算的克隆 $\mathbb{Z}_{p^k}$。Journal of Multiple-Valued Logic and Soft Computing. 26 (2020), 45–60. [14] *E. L. Post*：数理逻辑的二值迭代系统。普林斯顿大学出版社。Annals of Mathematics Studies. (1942 267 285 9780691095707), – . ISBN: : 多项式模 k的闭类上结构。Diskretnaya Matematika. 1 (1989), 3–15. [15] *A. B. Remizov* [16] *I. Rosenberg*：含有仿射本质运算的素基数宇宙上的克隆。Tatra Mountains Mathematical Publications. 5 (1995), 201–215.[17] *I. G. Rosenberg*： ¨关于多值逻辑中的函数完备性。有限集上多元函数的结构。Rozpravy ˇCeskoslovensk´e Akademie Vˇed, ˇRada Matematiky a Pˇr´ırod- n´ıc h Vˇed. 80 (1970). [18] *A. A. Salomaa*：有限代数中的无穷生成运算集。Annales Universitatis Turkuensis, Series A I. 74 (1964), 13.[19] *Á. Szendrei*：阿贝尔群的幂等约化。Acta Scientiarum Mathematicarum. 38 (1976), 170–182. ˇ*Authors' addresses*: *Miroslav Ploščica*，自然科学学院，萨法里克大学，Jesenn´a 5，04154 Koˇsice 电子邮箱：miroslav.ploscica@upjs.sk https://ploscica.science.upjs.sk，ˇ*Radka Schwartzová*，自然科学学院，萨法里克大学，Jesenn´a 5，04154 Koˇsice 电子邮箱：radka.schwartzova@student.upjs.sk，ˇ*Ivana Varga*，自然科学学院，萨法里克大学，Jesenn´a 5，04154 Koˇsice 电子邮箱：ivana.varga@student.upjs.sk。