arXiv:2302.03081v1 [cs.IT] 6 Feb 2023

置换相似度

LI-AN CHEN 和 ROBERT S. COULTER

数学科学系，特拉华大学，美国特
拉华州纽瓦克 19716

摘要。受构造低差分均匀度双射映射这一问题的启发，我们引入函数的置换相似度这一概念，用以衡量给定映射距离成为置换还有多远。我们证明了若干关于置换相似度的结果，并展示如何利用它构造低差分均匀度的双射。我们还研究了平面函数的置换相似度；众所周知，在奇特征域上，平面函数不是双射，且具有最优差分均匀度。

1. 引言

本文中，$\mathcal{G}$ 表示一个阶为 q 的有限群，运算采用加法记号，但不一定是阿贝尔群；$\mathcal{G}^\star = \mathcal{G} \setminus \{0\}$。阶为 q 的有限域记作 $\mathbb{F}_q$ 和 $\mathbb{F}_q^\star = \mathbb{F}_q \setminus \{0\}$。对于有限集 $\mathcal{S}$，$\#\mathcal{S}$ 表示 $\mathcal{S}$ 的基数。

设函数 $f: \mathcal{G} \to \mathcal{G}$。f 的不同像的集合记作 $\mathrm{Im}(f) := \{f(x) : x \in \mathcal{G}\}$，并记 $V(f) := \#\,\mathrm{Im}(f)$。若 $S \subseteq \mathcal{G}$，则 S 在 f 下的像集记作 $f(S) := \{f(x) : x \in S\}$。对于 $b \in \mathcal{G}$，b 在 f 下的原像集记作 $f^{-1}(b) := \{x \in \mathcal{G} : f(x) = b\}$，并将 f 的均匀度定义为

$$u(f) := \max_{b \in \mathcal{G}} \#f^{-1}(b).$$

若 $\mathrm{Im}(f) = \mathcal{G}$，则称 f 是 $\mathcal{G}$ 上的置换，并用 $\Omega_{\mathcal{G}}$ 表示所有 $\mathcal{G}$ 上置换的集合。众所周知，在函数复合运算下，$\Omega_{\mathcal{G}}$ 是一个群。在有限域 $\mathbb{F}_q$ 上，由于每个函数都可以唯一地表示为关于 $\mathbb{F}_q[x]$、次数至多为 $q-1$ 的多项式，因此，在 $\mathbb{F}_q$ 上经求值后表示一个置换的任何多项式都称为置换多项式（PP）；研究 $\mathbb{F}_q$ 时，我们通常也会直接使用这一术语。

本文旨在衡量定义在 $\mathcal{G}$ 上的非置换函数 f 与置换函数相距多远。一种标准的度量方法是考察 V(f)：其值越大，函数就越接近置换函数。本文在此引入一种衡量这种“距离”的新概念，称为置换相似度。首先，设 f 和 h 是定义在 $\mathcal{G}$ 上的两个函数。f 与 h 的相似度定义为

$$\mathrm{Res}(f,h) = V(f-h).$$

显然，对于任意函数 f，$\mathrm{Res}(f,f) = \#\{0\} = 1$。此外，$\mathrm{Res}(f,h) = \mathrm{Res}(h,f)$，且对于任意常数 $c \in \mathcal{G}$，$\mathrm{Res}(f, h+c) = \mathrm{Res}(f,h)$。现在我们可以介绍本文的核心思想。

定义 1. 对于 $f: \mathcal{G} \to \mathcal{G}$，我们将 f 的置换相似度定义为

$$\text{P-Res}(f) = \min\{\mathrm{Res}(f,h) : h \in \Omega_{\mathcal{G}}\},$$

或者等价地，写作 $f - h = g$，

$$\text{P-Res}(f) = \min\{V(g) : g + f \in \Omega_{\mathcal{G}}\}.$$

直观而言，置换相似度衡量的是，要改变一个函数使其成为置换，所需的不同平移的最小数量。换句话说，可以将 P-Res(f) 视为 V(g) 的最小值，其中 g 遍历所有定义在 $\mathcal{G}$ 上的函数，且满足 $g + f \in \Omega_{\mathcal{G}}$。P-Res(f) 越大，f 就越不像一个置换。特别地，当且仅当 $\text{P-Res}(f) = \mathrm{Res}(f,f) = 1$ 时，f 是一个置换。在

另一方面，当且仅当 P-Res(f) $=\#\mathcal{G}$ 时，f 是常函数。需要注意的是，这一度量不同于前文提到的常见度量。尽管二者存在明确的联系（定义中也体现了这一点），置换相似度似乎比 V(f) 提供了更细致的度量。例如，我们的主要结果部分地表明，置换相似度的上界与 V(f) 成反比。我们注意到，一般而言，对于给定的 f，满足 g $+$f 是一个置换且 V(g) $=$P-Res(f) 的 g 不止一个。据我们所知，有两篇论文—— [5] 和 [14]——引入了类似的概念。本文末尾将讨论置换相似度与这些早期概念之间的不等价性。

对于 P-Res，可以建立非平凡的下界和上界；只要不考虑常值函数和置换这两种极端（且无趣）的情形，这些界就是非平凡的。我们在第 2 节建立了这样的界。我们还证明，这两个界相等，当且仅当 f 是置换，或其原像分布具有某种特定形式。当 u(f) , q $-$V(f) $+1$ 时，下界仍然是紧的；我们给出了两类达到定理 2 下界的函数。在第 3 节中，我们考察函数上几种广泛使用的等价关系，以及 P-Res 在这些关系下的表现。在第 4 节中，我们考察置换相似度与差分均匀度之间的关系；当函数用作 S 盒时，差分均匀度衡量其抵抗差分密码分析的能力。近年来，构造低 DU 的置换多项式这一问题推动了信息安全领域的诸多研究；我们引入置换相似度的主要动机，正是为解决这一问题提供一种新工具。本节阐述了我们认为 P-Res 是一个重要概念的主要理由。特别是，我们指出了定理10，它展示了如何将一个非置换变为置换，同时对差分均匀度的增幅加以界定。本文最后一节将定理 2 中的上界与这些值联系起来

$$N_s(f) = \#\{(x_1, \ldots, x_s) \in \mathcal{G}^s : f(x_i) = f(x_j), \forall 1 \le i, j \le s; x_i = x_j \leftrightarrow i = j\}, \tag{1}$$

其中 f : $\mathcal{G} \to \mathcal{G}$ 且 $2 \le$s $\le$u(f)。我们证明，$\#(\mathcal{G} \setminus \mathrm{Im}(f)) =$q $-$V(f) 可以写成 N_s(f) 之和。这些数已知与 V(f) 密切相关。在 [8], Coulter 和 Senger 针对给定的任意 $2 \le$s $\le$u(f)，给出了 V(f) 关于 N_s(f) 的一个下界。此外，s $=2$ 的情形对于界定 V(f) 及其他相关量尤其有用。一个早期例子由 Carlitz [6] 于 1955 年给出：他将 N_2(f) $+$q 表示为特征和，从而证明了 V(f) 的一个平均下界。关于 N_2(f) 和 N_2(f) $+$q 的较新应用，例如参见 [3, 7, 11]。最后，我们通过证明 P-Res 与 [5] 和 [14] 中定义的其他概念并不等价来结束本文；这些概念涉及有限群上函数的差分算子的双射性。

2. Establishing Lower and Upper Bounds for P-Res

我们关于 P-Res 的第一个结果给出了 P-Res 的非平凡下界和上界。

定理 2. 若 f : $\mathcal{G} \to \mathcal{G}$，则

$$u(f) \le \text{P-Res}(f) \le q - V(f) + 1. \tag{2}$$

下界基于以下观察。

引理 3. 设 f : $\mathcal{G} \to \mathcal{G}$。若 g : $\mathcal{G} \to \mathcal{G}$ 满足 g$+$f 是一个置换多项式，则 g 在 f 的每个原像集上都是单射，即对于所有 b $\in$Im(f)，若 x, y $\in$f $^{-1}$(b) 且 x , y，则 g(x) , g(y)。

证明. 设 f, g : $\mathcal{G} \to \mathcal{G}$，使得 g $+$f 是一个置换多项式。若对于某个 b $\in$Im(f)，有 x, y $\in$f $^{-1}$(b) 且 g(x) $=$g(y)，则 (g $+$f)(x) $=$g(x) $+$f (x) $=$g(x) $+$b $=$g(y) $+$f (y) $=$(g $+$f)(y)。由于 g $+$f 是一个置换多项式，这意味着 x $=$ y。□

设 f : $\mathcal{G} \to \mathcal{G}$，并回顾 u(f) $=\max\{\#\, f^{-1}(b) : b \in \mathcal{G}\}$。为证明定理 2 中的下界，取一个元素 b $\in$Im(f)，使得 $\#\, f^{-1}(b) =$u(f)。若 g : $\mathcal{G} \to \mathcal{G}$ 满足 g $+$f 是一个置换，则根据引理 3，g 在 f $^{-1}$(b) 上是单射，这意味着 g 至少有 u(f) 个不同的像。因此，u(f) $\le$P-Res(f)，因为 P-Res(f) $=\min\{$V(g) : g $+$f 是一个置换$\}$。

为证明上界，注意到我们总能构造一个 g，使得 g$+$f $\in \Omega_{\mathcal{G}}$，如下所示。首先，令 $0 \in$Im(g)，并令 g 对每个 b $\in$Im(f)，从原像集 f^{-1}(b) 中恰好映射一个元素到 0。这样就能确保 Im(f) $\subseteq$Im(g $+$f)。此时，定义域和陪域中都还剩下 $\#(\mathcal{G} \setminus \mathrm{Im}(f)) =$q $-$V(f) 个元素未分配

，因此我们可以将定义域中每个未分配的 x 与陪域中每个未分配的 y 配对，并定义 g(x) = y − f (x)。因此，Im(g + f) = $\mathcal{G}$，而 V(g) 至多为 q − V(f) + 1，若所有 y − f (x) 恰好互不相同。于是，P-Res(f) ≤ q − V(f) + 1。至此，定理 2 得证。

对于某些 f，定理 2 中的下界可能与上界重合，因此此时 P-Res(f) = u(f)。接下来，我们证明，这恰好发生在函数为置换，或者除恰好一个元素有多个原像外，其余元素均被单射映射的情形。

定理 4. 设 f : $\mathcal{G} \to \mathcal{G}$。那么，u(f) = q − V(f) + 1 当且仅当 f 是置换，或者存在唯一的 y ∈ Im(f)，使得 # f $^{-1}$(y) = u(f) > 1，并且对所有 b ∈ Im(f) \ {y}，都有 # f $^{-1}$(b) = 1。

证明. 显然，若 f 是置换，则 u(f) = 1 且 q − V(f) = 0，所以此时结论成立。我们关注 f 不是置换的情形，因此可以假设 u(f) > 1 且 q − V(f) > 0。反向证明很容易验证。假设恰好有一个元素 y ∈ Im(f) 的原像多于一个，而 Im(f) \ {y} 中的其他元素都恰好有一个原像。根据定义，u(f) = # f $^{-1}$(y)，因此由所有原像集的不交并为定义域可知，q = u(f) + (V(f) − 1)。

为证明正向结论，考虑 f 的原像分布，该分布由有序的 (u(f) + 1)-元组 (M$_0$(f), M$_1$(f), . . . , M$_{u(f)}$(f)) 定义，其中

$$M_r(f) = \#\{b \in \mathcal{G} : \#f^{-1}(b) = r\}, \text{ for } 0 \le r \le u(f).$$

因此，根据我们的假设，特别有 q − V(f) = M$_0$(f) > 0。分别计算定义域和值域中的元素数量，我们得到

$$q = \sum_{r=1}^{u(f)} rM_r(f), \text{ and } q = \sum_{r=0}^{u(f)} M_r(f). \tag{3}$$

令 (3) 中 q 的两个表达式相等，并将所有 r > 0 对应的 M$_r$(f) 项移到等式一侧，得到

$$\begin{aligned} M_0(f) &= \sum_{r=1}^{u(f)} (r-1)M_r(f) = \sum_{r=2}^{u(f)} (r-1)M_r(f) \\ &= \sum_{r=2}^{u(f)-1} (r-1)M_r(f) + (u(f)-1)M_{u(f)}(f), \end{aligned} \tag{4}$$

其中，若 u(f) = 2，则最后一个表达式中的求和 P$^{u(f)}_{-1\,r=2}$ 视为空和。若 u(f) = q − V(f) + 1，我们可以将 u(f) − 1 = M$_0$(f) 代入 (4) 的最后一项，并与左侧的 M$_0$(f) 合并：

$$0 = \sum_{r=2}^{u(f)-1} (r-1)M_r(f) + M_0(f)\Big(M_{u(f)}(f) - 1\Big). \tag{5}$$

根据定义，所有 M$_r$(f)'s 都是非负整数，且 M$_{u(f)}$(f) ≥ 1。因此，要使 (5) 成立，求和中的每一项都必须为 0。特别地，M$_0$(f)(M$_{u(f)}$(f) − 1) = 0，这意味着 M$_{u(f)}$(f) = 1。此外，如果 u(f) > 2，那么 P$^{u(f)}_{-1\,r=2}$(r − 1)M$_r$(f) = 0 意味着，对于所有 2 ≤ r ≤ u(f) − 1，M$_r$(f) = 0。因此，f 具有所述的原像分布。□

定理 2 中的上界是最坏情况估计，因此我们预计在大多数情况下，P-Res(f) 会更低。不过，这有助于我们将 P-Res(f) 与 N$_s$(f) 联系起来，正如我们将在第 5 节中展示的那样；届时我们将再次使用 (3)，因为它通常对任意 f : $\mathcal{G}$ → $\mathcal{G}$ 都成立。

正如我们即将证明的，即使 u(f), q − V(f) + 1，定理 2 中的下界也可以达到。然而，一般而言，P-Res(f) , u(f)。一个简单的例子来自多项式 f (x) = x^2(1 − x)，定义在 $\mathbb{F}_5$ 上。这里 u(f) = 2，因为有 2 个根，且 f (−1) = f (−2) = 2（而 f (2) = 1）。如果 P-Res(f) 等于 2，那么就存在互不相同的 a、b ∈ $\mathbb{F}_5$，满足 $\mathbb{F}_5$ = {0 + a、0 + b、1 + a、2 + a、2 + b}。现在，将每个元素都平移 −a，得到 $\mathbb{F}_5$ = {0,b − a、1、2、2 + b − a}，这意味着 {b − a、2 + b − a} = {3,4}。然而，(b − a) − (2 + b − a) = −2 ∉{±(3 − 4)} = {±1}，因此这是不可能的。

现在，我们来计算有限域上两类多项式的 P-Res(f)，这些多项式不属于定理 4 中所述的函数类型（因此定理 2 中的下界和上界不同）。每一类都给出了达到定理 2 下界的例子。我们将通过寻找一个合适的

$g \in \mathbb{F}_q[x]$，使得 $g+f$ 是一个置换。我们总可以假设 $g(0) = 0$，因为如果 $g+f$ 是一个置换，那么 $g+f-g(0)$ 也如此，并且 $V(g(x)) = V(g(x) - g(0))$。

我们将考察的是域 $\mathbb{F}_{p^e}$ 上的 p-多项式。这是一类形如 $\sum_{i=0}^{e-1} a_i x^{p^i}$ 的多项式，其中 $a_1, .., a_{e-1} \in \mathbb{F}_{p^e}$，当将其视为域 $\mathbb{F}_p$ 上的向量空间时，可以用来表示 $(\mathbb{F}_{p^e}, +)$ 上的所有线性算子。

定理 5. 如果 $L \in \mathbb{F}_{p^e}[x]$ 是一个 p-多项式，则 $P\text{-}Res(L) = u(L)$。

证明。设 L 是域 $\mathbb{F}_{p^e}$ 上的 p-多项式。由于 L 是从 $\mathbb{F}_{p^e}$ 到自身的线性变换，L 的核 $L^{-1}(0)$ 和像集 Im(L) 都是域 $\mathbb{F}_p$ 上 $\mathbb{F}_{p^e}$ 的子空间，设 $\#L^{-1}(0) = p^{e-k}$ 且 $V(L) = p^k$，其中 $0 \le k \le e$。若 $b \in Im(L)$，且对某个 $x_0 \in \mathbb{F}_{p^e}$ 有 $L(x_0) = b$，则当且仅当 $L(x - x_0) = 0$ 时，$L(x) = b$。因此，$L(x) = b$ 的解的数量与 $L(x) = 0$ 相同。于是，根据定理 2，$u(L) = p^{e-k} \le P\text{-}Res(L)$。

为证明不等式的另一边，我们将构造一个多项式 $g \in \mathbb{F}_{p^e}[x]$，使得 $g+L$ 是一个置换多项式，且 $V(g) = p^{e-k}$。由于 Im(L) 是 $\mathbb{F}_{p^e}$ 的一个子空间，且有 p^k 个元素，因此它是 $\mathbb{F}_{p^e}$ 的一个加法子群，在 $\mathbb{F}_{p^e}$ 中有 p^{e-k} 个加法陪集。设 $C_1, ..., C_{p^{e-k}}$ 为 Im(L) 的陪集，且 c_i 是 C_i 的一个代表元，其中 $1 \le i \le p^{e-k}$。由于 Im(L) 的每个元素都有 p^{e-k} 个不同的原像，我们可以将 $\mathbb{F}_{p^e}$ 划分为 p^{e-k} 个互不相交的子集 $P_1, ..., P_{p^{e-k}}$，每个子集的基数为 p^k，并且从每个 $f^{-1}(b)$ 中恰好取一个元素，其中 $b \in Im(L)$。这样，L 将每个 P_i 单射映射到 Im(L) 上。考虑一个函数 $g \in \mathbb{F}_{p^e}[x]$，它将每个 P_i 上的元素都映射为 c_i，其中 $1 \le i \le p^{e-k}$。那么，对于 $1 \le i \le p^{e-k}$，有 $(g+L)(P_i) = c_i + Im(L) = C_i$。因此，$Im(g+L) = \mathbb{F}_{p^e}$，且 $g+L$ 是一个置换多项式。由于 $V(g) = p^{e-k}$，我们得出 $P\text{-}Res(L) = p^{e-k}$。□

我们要确定 P-Res 的第二类多项式，与奇素数域上的二次特征有关。这类多项式有时也达到定理 2 的下界。

定理 6. 设 $f(x) = x^{(p-1)/2} \in \mathbb{F}_p[x]$, 为奇素数域上的二次特征。 n

$$P\text{-}Res(f) = \begin{cases} u(f) + 1 = \frac{p+1}{2}, & if\ p \equiv 1 \pmod 4; \\ u(f) = \frac{p-1}{2}, & if\ p \equiv 3 \pmod 4. \end{cases} \tag{6}$$

证明. 函数 $f(x) = x^{(p-1)/2} \in \mathbb{F}_p[x]$ 的像 $Im(f) = \{0, 1, -1\}$，且 $\#f^{-1}(1) = \#f^{-1}(-1) = (p-1)/2$。因此，根据定理 2，$u(f) = (p-1)/2 \le P\text{-}Res(f)$。

首先，考虑 $p \equiv 3 \pmod 4$ 的情形。为了证明 (6)，我们将构造一个函数 $g \in \mathbb{F}_p[x]$，使得 $g+f$ 是一个置换多项式，且 $V(g) = u(f) = (p-1)/2$。定义一个基数为 $(p-1)/2$ 的子集 $S \subseteq \mathbb{F}_p$，如下：

$$S = \{0\} \cup \{4t - 1, 4t : 1 \le t \le (p-3)/4\}.$$

设 $g \in \mathbb{F}_p[x]$ 是一个函数，满足 $Im(g) = S$，$g(0) = 0$，并且 g 将 $f^{-1}(1)$ 和 $f^{-1}(-1)$ 分别单射映射到 S 上。那么 $(g+f)(0) = 0$，且

$$\begin{aligned} (g+f)(f^{-1}(1)) &= \{s + 1 : s \in S\} \\ &= \{1\} \cup \{4t, 4t+1 : 1 \le t \le (p-3)/4\} \\ &= \{1\} \cup \{4, 8, \ldots, p-3\} \cup \{5, 9, \ldots, p-2\}, \end{aligned}$$

and

$$\begin{aligned} (g+f)(f^{-1}(-1)) &= \{s - 1 : s \in S\} \\ &= \{-1\} \cup \{4t-2, 4t-1 : 1 \le t \le (p-3)/4\} \\ &= \{p-1\} \cup \{2, 6, \ldots, p-5\} \cup \{3, 7, \ldots, p-4\}. \end{aligned}$$

因此，$g+f$ 是一个置换多项式，且 $P\text{-}Res(f) = (p-1)/2$。

接下来，考虑 $p \equiv 1 \pmod 4$ 的情形。我们先用矛盾法证明 $P\text{-}Res(f) > (p-1)/2$，然后通过举出一个 $g \in \mathbb{F}_p[x]$ 的例子来证明 $P\text{-}Res(f) \le (p+1)/2$，使得 $g+f$ 是一个置换多项式，且 $V(g) = (p+1)/2$。若 $P\text{-}Res(f)$ 为 $(p-1)/2$，则存在 $g \in \mathbb{F}_p[x]$，使得 $g+f$ 是一个置换多项式，$g(0) = 0$，且 $Im(g) = \{y_1 = 0, y_2, ..., y_{(p-1)/2}\}$，其中 y_k 各不相同，且可视为 $\{0, 1, 2, ...p-1\}$ 中的整数。这意味着 $(g+f)(0) = 0$，并且

$$\mathbb{F}_p^\star = (g+f)(\mathbb{F}_p^\star) = \{y_k + 1 : k = 1, \ldots, (p-1)/2\} \cup \{y_k - 1 : k = 1, \ldots, (p-1)/2\}. \tag{7}$$

由于并集 (7) 中的两个集合的基数均为 (p − 1)/2，因此它们必定不相交，且构成 $\mathbb{F}_p^\star$ 的一个划分。由于$\{y_1 \pm 1\} = \{1, p-1\}$，我们必有 $y_k \pm 1 \notin \{0, 1, p-1\}$，其中 $k = 2, \ldots, (p-1)/2$，这意味着

$$\{y_k \pm 1 : k = 2, \ldots, (p-1)/2\} = \{2, \ldots, p-2\}, \tag{8}$$

and

$$\{y_2, y_3, \ldots, y_{(p-1)/2}\} \cap \{0, 1, 2, p-2, p-1\} = \emptyset.$$

由于 0 和 $p-1$ 不属于 $\{y_2, y_3, \ldots, y_{(p-1)/2}\}$，因此将 $\mathbb{Z}$ 中的元素视为元素时，(8) 仍然成立。将 (8) 两边的元素在 $\mathbb{Z}$ 中求和，得到

$$\sum_{k=2}^{(p-1)/2} (y_k + 1) + (y_k - 1) = 2 \sum_{k=2}^{(p-1)/2} y_k = 2 + 3 + \cdots + (p-2) = \frac{p(p-3)}{2}.$$

这与 $p(p-3)/2$ 在 $p \equiv 1 \bmod 4$ 时为奇数这一事实矛盾。因此，P-Res(f) $> (p-1)/2$。为证明 P-Res(f) $\le (p+1)/2$，令 $g \in \mathbb{F}_p[x]$ 满足 $g(0) = 0$ 且

$$g(f^{-1}(1)) = \{0\} \cup \{4t - 1, 4t : 1 \le t \le (p-5)/4\} \cup \{p-3\},$$

$$g(f^{-1}(-1)) = \{0\} \cup \{4t - 1, 4t : 1 \le t \le (p-5)/4\} \cup \{p-2\}.$$

因此 $V(g) = (p+1)/2$。$g + f$ 的像为 $(g+f)(0) = 0$,

$$\begin{aligned}(g+f)(f^{-1}(1)) &= \{1\} \cup \{4t, 4t+1 : 1 \le t \le (p-5)/4\} \cup \{p-2\} \\ &= \{1\} \cup \{4, 8, \ldots, p-5\} \cup \{5, 9, \ldots, p-4\} \cup \{p-2\},\end{aligned}$$

and

$$\begin{aligned}(g+f)(f^{-1}(-1)) &= \{-1\} \cup \{4t-2, 4t-1 : 1 \le t \le (p-5)/4\} \cup \{p-3\} \\ &= \{p-1\} \cup \{2, 6, \ldots, p-7\} \cup \{3, 7, \ldots, p-6\} \cup \{p-3\}.\end{aligned}$$

因此，$g + f$ 是一个置换多项式，且 P-Res(f) $\le (p+1)/2$。由此可得 P-Res(f) $= (p+1)/2$. □

3. 置换相似度的不变量

现在我们来探讨 P-Res 的潜在不变量。首先回顾一些较为广为人知的函数关系。

设 f,g: $\mathcal{G} \to \mathcal{G}$。

- 若存在某个 $\varphi \in \Omega_{\mathcal{G}}$，使得 $f \circ \varphi = g$，则称 f 与 g 右等价。
- 类似地，若存在某个 $\varphi \in \Omega_{\mathcal{G}}$，使得 $\varphi \circ f = g$，则称 f 与 g 左等价。

现在设 $f, g \in \mathbb{F}_q[x]$。

- 若存在仿射置换 A1、A2 和仿射函数 A3，使得

$$g = A_2 \circ f \circ A_1 + A_3.$$

  如果 $A_3 = 0$，则称 f 和 g 仿射等价。
- 一种更一般的等价关系 CCZ等价，由 Carlet、Chaprin 和 Zinoviev 在 [4] 中定义，其使用 f 的图 $\in \mathbb{F}_q[x]$: $G_f = \{(x, f(x)) : x \in \mathbb{F}_q\}$。如果存在仿射置换 A: $\mathbb{F}^2{}_q \to \mathbb{F}^2{}_q$，使得 $A(G_f) = G_g$，则称多项式 f、g CCZ等价。CCZ等价是 EA等价的推广；关于这一点，请参阅 Budaghyan、Carlet 和 Pott [2], , 其中给出了若干对 CCZ等价但非 EA等价的函数示例。

我们首先考虑左等价和右等价。

引理 7. 设 f: $\mathcal{G} \to \mathcal{G}$ 且 $\varphi \in \Omega_{\mathcal{G}}$。则

$$\mathrm{Im}(f) = \mathrm{Im}(f \circ \varphi), \tag{9}$$

从而,

$$V(f) = V(f \circ \varphi). \tag{10}$$

此外，对于任意 $b \in \mathcal{G}$,

$$\#f^{-1}(b) = \#(f \circ \varphi)^{-1}(b).$$

证明。第一个断言由以下事实得出： $\varphi(\mathcal{G}) = \mathcal{G}$。我们有

$$\mathrm{Im}(f) = f(\mathcal{G}) = f(\varphi(\mathcal{G})) = (f \circ \varphi)(\mathcal{G}) = \mathrm{Im}(f \circ \varphi).$$

第二个断言是因为

$$\begin{aligned}(f \circ \varphi)^{-1}(b) &= \{a \in \mathcal{G} : f(\varphi(a)) = b\} \\ &= \{\varphi^{-1}(c) \in \mathcal{G} : f(c) = b\} \\ &= \varphi^{-1}\left(\{c \in \mathcal{G} : f(c) = b\}\right).\end{aligned}$$

由于 φ^{-1} 也是一个置换，我们有

$$\#(f \circ \varphi)^{-1}(b) = \#\{c \in \mathcal{G} : f(c) = b\} = \#f^{-1}(b).$$

□

推论 8. 设 $f : \mathcal{G} \to \mathcal{G}$ 且 $\varphi \in \Omega_{\mathcal{G}}$。那么

$$\text{P-Res}(f) = \text{P-Res}(f \circ \varphi),$$

即，P-Res 是右不变的。

证明。设 $f, h : \mathcal{G} \to \mathcal{G}$ 且 $\varphi \in \Omega_{\mathcal{G}}$。根据引理 7，$V(f - h) = V((f - h) \circ \varphi) = V(f \circ \varphi - h \circ \varphi)$。如果 h 是 $\mathcal{G}$ 上的一个置换，那么 $h \circ \varphi$ 也是。因此，

$$\begin{aligned}\text{P-Res}(f) &= \min\{V(f - h) : h \in \Omega_{\mathcal{G}}\} \\ &= \min\{V(f \circ \varphi - h) : h \in \Omega_{\mathcal{G}}\} = \text{P-Res}(f \circ \varphi).\end{aligned}$$

□

对于左等价，我们仍有

$$V(f) = V(\varphi \circ f) \tag{11}$$

对于任意 $f : \mathcal{G} \to \mathcal{G}$ 以及 $\varphi \in \Omega_{\mathcal{G}}$，因为

$$\mathrm{Im}(\varphi \circ f) = \{\varphi(f(a)) : a \in \mathcal{G}\} = \varphi(\mathrm{Im}(f)).$$

然而，除非 $f \in \Omega_{\mathcal{G}}$ 也成立，否则 (9) 的类似结论显然并非普遍成立。事实上，若 f 不是置换，那么对于 $c \in \mathrm{Im}(f), G$，我们总能定义一个置换 φ，使得 $\varphi(c) \in G \setminus \mathrm{Im}(f)$，因此 $\mathrm{Im}(f), \mathrm{Im}(\varphi \circ f)$。（事实上，可以确定 $\mathrm{Im}(f) = \mathrm{Im}(\varphi \circ f)$ 成立的精确条件，但这里略去，因为这与我们理解置换相似度无进一步关联。）由此可见，P-Res 不是左不变的。在 $\mathbb{F}_7$ 上很容易构造一个小反例。令 $f(x) = x^2 \in \mathbb{F}_7[x]$，并令 $\varphi = (0)(1)(2345)(6)$（采用循环记号）。很容易验证，$(\varphi \circ f)(0) = 0, (\varphi \circ f)(\{1,6\}) = 1, (\varphi \circ f)(\{3,4\}) = 3, (\varphi \circ f)(\{2,5\}) = 5$。特别地，$\varphi \circ f$ 固定 $\{0,1,3,5\}$ 中的每个元素，并将一个 $\in \{2,4,6\}$ 映射到 $7 - a$。令 g 为定义在 $\mathbb{F}_7$ 上的函数，它将 $\{0,1,3,5\}$ 映射到 0，并将 $\{2,4,6\}$ 映射到 1。于是 $(\varphi \circ f + g)\{0,1,3,5\} = \{0,1,3,5\}$，且 $(\varphi \circ f + g)(\{2,4,6\}) = \{2,4,6\}$，因此 $\varphi \circ f + g$ 是一个置换。故 $\text{P-Res}(\varphi \circ f) \le V(g) = 2$。然而，根据下文的定理 13，$\text{P-Res}(f) > 2$。所以 $\text{P-Res}(f), \text{P-Res}(\varphi \circ f)$。

如果 $\varphi \in \Omega_{\mathcal{G}}$ 满足：对所有 x、$y \in \mathcal{G}$，都有 $\varphi(x - y) = \varphi(x) - \varphi(y)$，那么，采用与推论 8 证明中类似的论证，我们可以证明，对于 $f : \mathcal{G} \to \mathcal{G}$，$\text{P-Res}(f) = \text{P-Res}(\varphi \circ f)$。这引出以下定理。

定理 9. 对于 $f \in \mathbb{F}_q[x]$，以及仿射置换 $A_1, A_2 \in \mathbb{F}_q[x],$，我们有

$$\text{P-Res}(f) = \text{P-Res}(A_1 \circ f \circ A_2),$$

也就是说，P-Res 是一个仿射不变量。

证明。设 $f, h \in \mathbb{F}_q[x]$ 和 A_1, A_2 是 $\mathbb{F}_q$ 上的仿射置换。首先，由 (10) 和 11)，我们有 $V(f - h) = V(A_1 \circ (f - h) \circ A_2)$。令 $A_1 = L_1 + c_1, A_2 = L_2 + c_2$，其中 L_1, L_2 是线性化置换，$c_1, c_2 \in \mathbb{F}_q$ 是常数。于是对于 $x \in \mathbb{F}_q$，有

$$\begin{aligned}(A_1 \circ (f - h) \circ A_2)(x) &= A_1(f(A_2(x)) - h(A_2(x))) \\ &= L_1(f(A_2(x))) - L_1(h(A_2(x))) + c_1 \\ &= A_1(f(A_2(x))) - L_1(h(A_2(x))).\end{aligned}$$

由于 Ω 在复合运算下是一个群，因此 $\Omega = \{h \in \Omega\} = \{L_1 \circ h \circ A_2 : h \in \Omega\}$。因此，

$$\begin{aligned}\text{P-Res}(f) &= \min\{V(f-h) : h \in \Omega\} \\ &= \min\{V(A_1 \circ (f-h) \circ A_2) : h \in \Omega\} \\ &= \min\{V(A_1 \circ f \circ A_2 - h) : h \in \Omega\} \\ &= \text{P-Res}(A_1 \circ f \circ A_2).\end{aligned}$$

□

一般来说，P-Res(f) 既不是 EA 不变量，也不是 CCZ 不变量。例如，设 $f(x) = x \in \mathbb{F}_{p^e}[x]$，$g(x) = \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x)$，其中 $e > 1$。由于 $g = f + \sum_{i=1}^{e-1} x^{p^i}$，这两个函数 EA 等价，因此也 CCZ 等价。然而，P-Res(f) = 1，因为它是置换；而 P-Res(g) > 1，因为它不是置换。

4. 置换相似度与差分均匀度

对于非零的 $a \in \mathcal{G}$，f 在方向 a 上的差分算子定义为

$$\Delta_{f,a} := f(x+a) - f(x),$$

f 的差分均匀度（DU）定义为

$$\delta_f := \max_{a \in \mathcal{G}^\star} u(\Delta_{f,a}).$$

DU 的概念最初由 Nyberg [13]提出。DU 越低，f 用作密码系统中 S 盒时抵抗差分攻击的能力就越强。最理想的函数是在有限域上具有最优（可能的最低）DU 的置换多项式。当 q 为偶数时，由于 $\Delta_{f,a}(x) = b$ 当且仅当 $\Delta_{f,a}(x+a) = b$，因此对于任意 $(a, b) \in \mathbb{F}_q^\star \times \mathbb{F}_q$，方程 $\Delta_{f,a}(x) = b$ 的解的个数总是偶数。因此，最优函数是 2-DU 函数；这类函数称为几乎完美非线性（APN）函数。已知一些 APN 置换的例子。然而，当 $q = 2^n$ 且 n 为偶数时，目前只知道一个 APN 置换的例子——见 Browning、Dillon、McQuistan 和 Wolfe [1] ——而构造 APN 函数和 APN 置换仍是该领域的核心研究问题。当 q 为奇数时，可以构造 1-DU 多项式，这类多项式称为平面多项式。等价地，函数 f 是平面函数，当且仅当 f 的每个差分算子都是置换多项式。显然，这类函数确实存在：容易看出，在特征不为 2 的任意域上，多项式 x^2 是平面函数。然而，对于任意 $a \in \mathbb{F}_q^\star$，$f(x+a) - f(x) = 0$ 必有解，因此平面函数不可能是置换。事实上，文献 [8] 证明，若 f 在 $\mathbb{F}_q$ 上是平面函数，则 V(f) 不会大于大约 $q - \sqrt{q}$。因此，在奇特征下，我们的问题转化为构造具有近乎最优 DU 的置换。

本节的首个结果表明，当 $\mathcal{G}$ 是阿贝尔群时，给定两个函数 f、g，函数 g + f 的 DU 由 f 的 DU 和 V(g) 控制。

定理10. 若 $\mathcal{G}$ 是有限阿贝尔群，且 f、$g : \mathcal{G} \to \mathcal{G}$，则

$$\delta_{g+f} \le \delta_f \cdot (V(g)^2 - V(g) + 1).$$

特别地，如果 V(g) = P-Res(f)，那么

$$\delta_{g+f} \le \delta_f \cdot (\text{P-Res}(f)^2 - \text{P-Res}(f) + 1). \tag{12}$$

证明。设$\mathcal{G}$是一个有限阿贝尔群，且 $f, g : \mathcal{G} \to \mathcal{G}$。注意，由于$\mathcal{G}$是阿贝尔群，$\Delta_{g+f,a}(x) = g(x+a) + f(x+a) - g(x) - f(x) = \Delta_{g,a}(x) + \Delta_{f,a}(x)$。因此，对于 $b \in \mathcal{G}$,

$$\begin{aligned}
\#\Delta_{g+f,a}^{-1}(b) &= \#\{x : \Delta_{g+f,a}(x) = b\} \\
&= \#\bigcup_{z\in\mathcal{G}} \{x : \Delta_{g,a}(x) = z \text{ and } \Delta_{f,a}(x) = b - z\} \\
&= \sum_{z\in\mathcal{G}} \#\Big(\{x : \Delta_{g,a}(x) = z\} \cap \{x : \Delta_{f,a}(x) = b - z\}\Big) \\
&\le \sum_{z\in \mathrm{Im}(\Delta_{g,a})} \#\{x : \Delta_{f,a}(x) = b - z\} \\
&\le \delta_f \cdot V(\Delta_{g,a})
\end{aligned}$$

该结果源于这样一个事实：$\mathrm{Im}(\Delta_{g,a}) = \{g(x+a) - g(x) : x \in \mathcal{G}\}$ 必须是 $\{g_1 - g_2 : g_1, g_2 \in \mathrm{Im}(g)\}$ 的子集，而该集合至多包含 $V(g)(V(g)-1)+1$ 个元素。□

当 f 为平面函数时，(12) 可简化为 $\delta_{g+f} \le \text{P-Res}(f)^2 - \text{P-Res}(f) + 1$。因此，定理10表明，寻找置换相似度较低的平面函数，是构造近最优差分均匀置换的一种途径。如前所述，通常存在多个 g，使得 g+f 是置换且 $V(g) = \text{P-Res}(f)$；通过计算很容易验证（这也完全在意料之中），不同的 g 会产生差分均匀度不同的置换 g + f。基于这些观察，本节最后将考察平面函数的置换相似度。

对于平面函数 f，已知 $V(f) \ge (q+1)/2$，参见例如任意 [7, 12, 15]。利用 (2) 中的上界可立即得到

引理11. 如果 $f \in \mathbb{F}_q[x]$ 是平面的，那么

$$\text{P-Res}(f) \le \frac{q+1}{2}.$$

为确定下界，我们将自身限制在一类特殊的平面函数上；即所谓的二对一函数，这意味着 $f(0) = 0$，且 f 在非零元素上是二对一的。所有已知的平面函数类都由这类平面函数组成，并且这一限制已在多个地方用于获得重要结果，例如参见 [9] 或 [15]。我们首先证明，当一个 d对一函数满足 $\text{P-Res}(f) = u(f)$ 时的一个必要条件。

引理12. 设 $f \in \mathbb{F}_q[x]$。假设 $f(0) = 0$，且 f 在 $\mathbb{F}_q^\star$上是 d对一的。如果 $\text{P-Res}(f) = u(f) = d$，那么存在一个 d元子集 $\{c_1, c_2, \ldots, c_d\} \subseteq \mathbb{F}_q$，使得对于所有 $x, y \in \mathbb{F}_q^\star$，$f(x) - f(y) \notin \{c_i - c_j : 1 \le i, j \le d, i \ne j\}$。

证明。设 $f \in \mathbb{F}_q[x], f(0) = 0$，且 f 在 $\mathbb{F}_q^\star$ 上为 d 对 1。若 $\text{P-Res}(f) = u(f) = d$，则存在函数 $g \in \mathbb{F}_q[x]$，使得 g + f 是一个置换多项式，且 $V(g) = d$。我们还可以假设 $g(0) = 0$，记 $\mathrm{Im}(g) = \{c_1 = 0, c_2, \ldots\ldots, c_d\}$。对于 $1 \le i \le d$，定义 $P_i = \{x \in \mathbb{F}_q^\star : g(x) = c_i\}$，即 g 在 $\mathbb{F}_q^\star$ 上的原像集合。这些集合 P_i 构成一个 $\mathbb{F}_q^\star$ 的划分，因此 $\sum_{i=1}^{d} \#P_i = q - 1$。

根据引理 3，g 在每个 $f^{-1}(b)$ 上都是单射，其中 $b \in \mathrm{Im}(f)$。由于对于所有 $b \in \mathrm{Im}(f) \setminus \{0\}$，$\#f^{-1}(b) = d$，$f^{-1}(b)$ 必须恰好包含来自每个 P_i 的一个元素，其中 $1 \le i \le d$。由于 $\#(\mathrm{Im}(f) \setminus \{0\}) = (q-1)/d$ 且 $\sum_{i=1}^{d} \#P_i = q - 1$，通过对元素计数可知，对于所有 $1 \le i \le d$，$\#P_i = (q-1)/d$，并且每个 P_i 都恰好包含来自每个 $f^{-1}(b)$ 的一个元素，其中 $b \in \mathrm{Im}(f) \setminus \{0\}$。因此，$f(P_i) = \mathrm{Im}(f) \setminus \{0\}$。

由于 g + f 是置换多项式，且 $(g+f)(0) = 0$，我们可以按如下方式划分 $\mathbb{F}_q^\star$:

$$\mathbb{F}_q^\star = \bigsqcup_{i=1}^{d} (g+f)(P_i) = \bigsqcup_{i=1}^{d} \{c_i + f(x) : x \in \mathbb{F}_q^\star\}.$$

特别是，这个并集中的任意两个集合都不相交。因此，对所有 x、y $\in \mathbb{F}_q^\star$以及 i、j，$c_i + f(x) \ne c_j + f(y)$，这意味着

$$f(x) - f(y) \ne c_j - c_i.$$

□

定理 13. 设 $q > 5$ 是奇素数或奇素数幂。若 $f \in \mathbb{F}_q[x]$ 是平面函数，$f(0) = 0$ 且 f 在 $\mathbb{F}_q^\star$ 上是二对一的，则 P-Res$(f) > 2$。

证明。设 f 是一个二对一平面函数，且 $f(0) = 0$。由于 f 是平面的，对于 $a \in \mathbb{F}_q^\star$，$f(x+a) - f(x)$ 是一个置换多项式。若 P-Res$(f) = 2$，则由引理12，存在两个元素，其中一个可以是 0，另一个为 $c \in \mathbb{F}_q^\star$，使得对于任意固定的 $a \in \mathbb{F}_q^\star$ 和 $x \notin \{0, -a\}$，都有 $f(x+a) - f(x) \neq \pm c$。但由于 $f(x+a) - f(x)$ 是一个置换多项式，$f(x+a) - f(x) = \pm c$ 必有解。因此，对所有 $a \in \mathbb{F}_q^\star$，0 必须是 $f(x+a) - f(x) = c$ 或 $f(x+a) - f(x) = -c$ 的一个解，这意味着 $f(a) = c$ 或 $f(a) = -c$。由此可得 $f(\mathbb{F}_q^\star) = \{\pm c\}$。然而，由于 f 在 $\mathbb{F}_q^\star$ 上是二对一的，$\#f(\mathbb{F}_q^\star) = (q-1)/2$。因此，当 $(q-1)/2 > \#\{\pm c\} = 2$ 时，这是不可能的。□

5. 置换相似度与一些已知的双射性度量

在本节最后，我们将说明定理 2 中的上界可以与式 (1) 中定义的 $N_s(f)$ 的值联系起来。这也表明，在未知 $N_s(f)$ 全部取值的情况下，如何确定 P-Res 的上界估计。

设 $f: \mathcal{G} \to \mathcal{G}$。回顾一下，对于 $0 \le r \le u(f)$，$M_r(f)$ 表示在 f 下恰有 r 个原像的 $b \in \mathcal{G}$ 的数量，如定理 4 的证明中所定义。通过计算每个原像集中的所有可能 s 元组，我们得到

$$N_s(f) = \sum_{r=s}^{u} (r)_s M_r(f), \tag{13}$$

其中 $(r)_s = r(r-1)(r-2)\cdots(r-s+1)$。文献 [8] 给出的以 $N_s(f)$ 表示的 $V(f)$ 下界意味着

$$V(f) \ge q - \frac{N_2(f)}{2}. \tag{14}$$

将此应用于定理 2 中的上界，可得

$$\text{P-Res}(f) \le \frac{N_2(f)}{2} + 1.$$

这个界很有用，因为人们通常可能只掌握 $N_2(f)$ 的信息。但如果掌握了关于较大 s 对应的 $N_s(f)$ 的更多信息，就可以得到更强的界。事实上，我们可以使用所有满足 $2 \le s \le u(f)$ 的 $N_s(f)$，而不只是选取一个 s。下面我们证明，$q - V(f) = M_0(f)$ 实际上是一个涉及所有 $N_s(f)$ 的和。

定理 14. 设 $f: \mathcal{G} \to \mathcal{G}$。那么

$$M_0(f) = \sum_{s=2}^{u(f)} \frac{N_s(f)}{s!}(-1)^s. \tag{15}$$

特别地，

$$\frac{N_2(f)}{2!} - \frac{N_3(f)}{3!} \le M_0(f) \le \frac{N_2(f)}{2!}, \tag{16}$$

其中，当且仅当对所有 $r \ge 4$ 都有 $M_r(f) = 0$ 时，下界成立；当且仅当对所有 $r \ge 3$ 都有 $M_r(f) = 0$ 时，上界成立（后一种情况下两个界相等）。

证明。考虑原像分布的普通生成函数 $P_f(z) \in \mathbb{C}[z]$

$$P_f(z) = \sum_{r=0}^{u(f)} M_r(f) z^r. \tag{17}$$

由 (3)，$P_f(1) = q$，并且

$$\frac{d}{dz} P_f(z)\Big|_{z=1} = \sum_{r=1}^{u(f)} r M_r(f) z^{r-1}\Big|_{z=1} = q.$$

此外，由（13）可知，对于 $2 \le s \le u(f)$，

$$\frac{d^s}{dz^s} P_f(z)\Big|_{z=1} = \sum_{r=s}^{u(f)} r(r-1)\cdots(r-s+1) M_r(f) z^{r-s}\Big|_{z=1} = N_s(f).$$

因此，

$$P_f(z) = q + q(z-1) + \sum_{s=2}^{u(f)} \frac{N_s(f)}{s!}(z-1)^s. \tag{18}$$

显然，由（17）可得 $P_f(0) = M_0(f)$。因此，在（18）中令 $z = 0$，即可得到（15）。

为了证明（16）中的界，我们希望通过截去（15）中的若干项来估计 $M_0(f)$。假设对于某个 $3 \le c \le u(f)$，我们只取前 $s = 2, \ldots, c-1$ 项。将（13）代入（15）的尾项，得到

$$\begin{aligned} \sum_{s=c}^{u(f)} \frac{N_s(f)}{s!}(-1)^s &= \sum_{s=c}^{u(f)} (-1)^s \sum_{r=s}^{u(f)} \binom{r}{s} M_r(f) \\ &= \sum_{r=c}^{u(f)} M_r(f) \sum_{s=c}^{r} \binom{r}{s} (-1)^s. \end{aligned} \tag{19}$$

由于 $\sum_{s=0}^{r} \binom{r}{s}(-1)^s = (1-1)^r = 0$，

$$\sum_{s=c}^{r} \binom{r}{s}(-1)^s = -\sum_{s=0}^{c-1} \binom{r}{s}(-1)^s.$$

这个和是一个关于 r 的 $c-1$ 次多项式，r^{c-1} 的系数为 $(-1)^c(c-1)!$。我们断言，这个多项式的根为 $r = 1$、2、…、$c-1$。事实上，由于 $\binom{r}{s} = 0$ if $r < s$，对于任意 $1 \le r_0 \le c-1$，

$$-\sum_{s=0}^{c-1} \binom{r_0}{s}(-1)^s = -\sum_{s=0}^{r_0} \binom{r_0}{s}(-1)^s = -(1-1)^{r_0} = 0.$$

因此，

$$-\sum_{s=0}^{c-1} \binom{r}{s}(-1)^s = \frac{(-1)^c}{(c-1)!} \prod_{i=1}^{c-1} (r-i),$$

且（19）等于

$$\sum_{s=c}^{u(f)} \frac{N_s(f)}{s!}(-1)^s = \frac{(-1)^c}{(c-1)!} \sum_{r=c}^{u(f)} M_r(f) \prod_{i=1}^{c-1} (r-i).$$

因此，对于所有 $c \le r \le u(f)$，$M_r(f)$ 的系数具有相同的符号（-1）^{c}。由于对于所有 $0 \le r \le u(f)$，$M_r(f) \ge 0$，尾项 $P^{u(f)}s=c\ Ns(f)\ s!\ (-1)^s \ge 0$ 在 c 为偶数时等于 ≤ 0，在 c 为奇数时等于 ≤ 0。特别地，当 $c = 3$ 且 $c = 4$ 时，我们得到（16）。当且仅当 $P^{u(}f)s=c\ Ns(f)\ s!\ (-1)^s = (-1)c\ (c-1)!\ P_{u(f)}r=c\ M_r(f)\ Q_{i=1}^{c-1}(r-i) = 0$ 时，这些界成立。但是，由于各项 $M_r(f)$ 的系数符号都相同，当且仅当对于所有 $c \le r \le u(f)$，$M_r(f) = 0$ 时，该和为 0。□

注意，由于 $V(f) = q - M_0(f)$，(15) 和 (16) 等价于

$$V(f) = q - \sum_{s=2}^{u(f)} \frac{N_s(f)}{s!}(-1)^s,$$

and

$$q - \frac{N_2(f)}{2!} \le V(f) \le q - \frac{N_2(f)}{2!} + \frac{N_3(f)}{3!}.$$

因此，我们得到了 (14) 的另一种证明，这与 [8] 中的证明不同。

根据定理 14，定理 2 的上界等价于

$$\text{P-Res}(f) \le 1 + \sum_{s=2}^{u(f)} \frac{N_s(f)}{s!}(-1)^s.$$

此外，定理 14 的证明表明，即使我们没有关于 $N_s(f)$ 的全部信息，仍可以通过将求和截断到偶数 s 来得到一个较弱的界。例如，

$$\text{P-Res}(f) \le 1 + \frac{N_2(f)}{2!} - \frac{N_3(f)}{3!} + \frac{N_4(f)}{4!}.$$

置换相似度与先前概念的不等价性。本文最后，我们希望讨论 P-Res 与文献中两种先前概念之间是否等价或存在联系这一问题。

为了研究函数所有微分算子的整体双射性， [5] 和 [14]中的两篇论文分别定义了两种不同的概念。后来 Fu、Feng、Wang 和 Carlet [10]证明，这两种概念相差一个常数的加法和乘法后等价。在本附录中，我们将说明，尽管 P-Res 与这些概念相似，但并不等价。 [5] 和 [14] 中的原始定义针对的是两个有限阿贝尔群$\mathcal{G}_1$ 和$\mathcal{G}_2$ 之间的函数，这两个群不一定相同。由于大多数情况下我们关注的是从一个群到自身的函数，因此这里只讨论$\mathcal{G}_1 = \mathcal{G}_2 = \mathcal{G}$ 且含有 q 个元素的情形。

首先，在 [5], 中，Carlet 和 Ding 引入了 f 的不平衡度和导数不平衡度；此时定义域和陪域的大小不一定相等，从而推广了双射性的概念。f 的不平衡度定义为：从陪域中均匀随机选取 b 时，# f^{-1}(b) 的方差。当 f :$\mathcal{G} \to \mathcal{G}$ 时，我们有

$$Nb_f = \sum_{b\in\mathcal{G}} \left(\#f^{-1}(b) - 1\right)^2 = \sum_{b\in\mathcal{G}} \left(\#f^{-1}(b)\right)^2 - q,$$

且 f 的导数不平衡度定义为

$$NB_f = \sum_{a\in\mathcal{G}^\star} Nb_{\Delta_{f,a}}.$$

其次，在 [14], Panario、Sakzad、Stevens 和 Wang 引入了 f 的歧义度，用以衡量 $\Delta_{f,a}$ 的整体单射性。设 α_i(f) =#{(a, b) $\in \mathcal{G}^\star \times \mathcal{G}$: #$\Delta_f^{-1}$,a(b) =i}。f 的歧义度定义为

$$A(f) = \sum_{0\le i\le q} \alpha_i(f)\binom{i}{2}.$$

在计算 α_i(f) 时，每次固定一个 a $\in \mathcal{G}^\star$，A(f) 也可以看作各行歧义度之和：P $_{a\in\mathcal{G}^\star}$。

$$A_{r=a}(f) = \sum_{b\in\mathcal{G}} \binom{\#\Delta_{f,a}^{-1}(b)}{2}.$$

文献 [10]证明了 NB$_f$ 与 A(f) 等价。特别地，当 f : $\mathcal{G} \to \mathcal{G}$ 时，A(f) =NB $_f$/2。事实上，两者也都可以用 $N_2(\Delta_{f,a})$ 表示如下：

$$\begin{aligned} N_2(f) &= \#\{(x,y) : f(x) = f(y), x \neq y\} = \#\{(x,y) : f(x) = f(y)\} - q \\ &= \sum_{b\in\mathcal{G}} \#\{(x,y) : f(x) = f(y) = b\} - q \\ &= \sum_{b\in\mathcal{G}} \left(\#f^{-1}(b)\right)^2 - q \\ &= Nb_f. \end{aligned}$$

因此，NB $_f$ =P $_{a\in\mathcal{G}^\star}$Nb$_{\Delta_{f,a}}$ =P $_{a\in\mathcal{G}^\star}$N$_2$($\Delta_{f,a}$)。另一方面，

$$\begin{aligned} A_{r=a}(f) &= \sum_{b\in\mathcal{G}} \binom{\#\Delta_{f,a}^{-1}(b)}{2} \\ &= \sum_{r=2}^{u(f)} \binom{r}{2} \#\{b \in \mathcal{G} : \#\Delta_{f,a}^{-1}(b) = r\} \\ &= \sum_{r=2}^{u(f)} \binom{r}{2} M_r(\Delta_{f,a}) \\ &= \frac{N_2(\Delta_{f,a})}{2}. \end{aligned}$$

因此，A(f) =P $_{歧义度\in\mathcal{G}^\star}A_{r=a}$(f) =P $_{歧义度\in\mathcal{G}^\star}$ $\frac{N_2(\Delta_{f,\ 歧义度})}{2}$。

根据定义，P-Res(f)、NB$_f$和A(f)之间一个显而易见的区别是，P-Res(f)关注的是f自身的双射性，而NB$_f$和A(f)关注的是f的差分算子的双射性。此外，即使考察的是同一个函数，P-Res($\Delta_{f,\ a}$)也取决于所有N$_s$($\Delta_{f,\ a}$)，而Nb$_{\Delta_{f,\ a}}$和A$_{r=a}$(f)则都基于N$_2$($\Delta_{f,\ a}$)。事实上，可能存在两个P-Res不同但N$_2$相同的函数。例如，在 $\mathbb{F}_7$ 上定义两个函数f、h：

$$f(x)=\begin{cases}0 & \text{when } x=0,1,\\ 2 & \text{when } x=2,3,\\ 4 & \text{when } x=4,5,\\ 6 & \text{when } x=6,\end{cases}\qquad \text{and}\qquad h(x)=\begin{cases}0 & \text{when } x=0,1,2,\\ x & \text{when } x=3,4,5,6.\end{cases}$$

原像分布为 (M$_0$(f)，M$_1$(f)，M$_2$(f)，M$_3$(f)) =(3, 1, 3, 0) 和 (M$_0$(h)，M$_1$(h)，M$_2$(h)，M$_3$(h)) =(2,4,0,1)。两个函数都具有 N$_2$(f) = N$_2$(h) = 6。然而，P-Res(h) = 3 根据定理2和定理4，而 P-Res(f) =2，因为通过添加函数即可将其变为恒等函数

$$g(x)=\begin{cases}0 & \text{when } x=0,2,4,6,\\ 1 & \text{when } x=1,3,5.\end{cases}$$

References

1. K.A. Browning、J.F. Dillon、M.T. McQuistan 和 A.J. Wolfe，《六维中的几乎完美非线性置换》，《有限域：理论与应用》，《当代数学》，第518卷，美国数学会，普罗维登斯，RI，2010年，第33–42页。2. L. Budaghyan、C. Carlet 和 A. Pott，《几乎弯曲和几乎完美非线性多项式的新类》，《IEEE信息论汇刊》52（2006），第3期，1141–1152。3. C. Carlet，《利用像集大小给出差分均匀函数非线性度的界及其与仿射函数的距离》，《IEEE信息论汇刊》67（2021），第12期，8325–8334。4. C. Carlet、P. Charpin 和 V. Zinoviev，《适用于 DES 类密码系统的码、弯曲函数和置换》，《设计、码与密码学》15（1998），第2期，125–156。5. C. Carlet 和 C. Ding，《S 盒的非线性度》，《有限域及其应用》13（2007），第1期，121–135。6. L. Carlitz，《有限域中系数为有限域元素的多项式的不同值数量》，《日本学士院纪要》31（1955 年），第3期，119–120。7. R.S. Coulter 和 R.W. Matthews，《有限域上函数类的不同值数量》，《有限域及其应用》17（2011），220–224。8. R.S. Coulter 和 S. Senger，《有限定义域上函数类的不同值数量》，《组合年刊》18（2014），第2期，233–243。9. C. Ding 和 J. Yuan，《一族斜哈达玛差集》，《组合理论杂志A辑》113（2006），1526–1535。10. S. Fu、X. Feng、Q. Wang 和 C. Carlet，《函数的导数不平衡度与歧义度》，《IEEE信息论汇刊》65（2019），第9期，5833–5845。11. L. Kölsch、B. Kriepke 和 G.M. Kyureghyan，《完美非线性映射的像集》，《设计、码与密码学》（2022）。12. G.M. Kyureghyan 和 A. Pott，《关于平面映射的一些定理》，《有限域算术：第二届国际研讨会论文集，WAIFI 2008》（J. von zur Gathen、J.L. Imanã 和 C.K. Koç 编），《计算机科学讲义》，第5130卷，2008年，第117–122页。13. K. Nyberg，《用于密码学的差分均匀映射》，《密码学进展——EUROCRYPT ’93》，《计算机科学讲义》，施普林格，1993年，第55–64页。14. D. Panario、A. Sakzad、B. Stevens 和 Q. Wang，《置换的两个新度量：歧义度和亏损度》，《IEEE信息论汇刊》57（2011），第11期，7648–7657。15. W. Qiu、Z. Wang、G. Weng 和 Q. Xiang，《来自预半域的伪帕利图与斜哈达玛差集》，《设计、码与密码学》44（2007），49–62。