arXiv:2601.11247v1 [cs.DM] 16 Jan 2026

已知 APN 函数的观察

VALÉRIE GILLOT 和 PHILIPPE LANGEVIN

摘要。我们提出了新的不变量、APN 可扩展性判据以及一种回溯方法，并找到了若干数值事实，支持如下猜想：6 比特 APN 函数的集合仅包含 14 个 CCZ 等价类。

1. 引言

在都柏林举行的 FQ9 有限域会议上，K. A. Browning、J. F. Dillon、M. T. McQuistan 和 A. J. Wolfe 宣布发现了一个几乎完美非线性六维置换 [5]。我们将此置换称为都柏林置换，或等价地将其CCZ等价类称为都柏林*CCZ*等价类。自该消息公布以来，人们尝试构造偶数维的新几乎完美非线性置换，但尚未发现更多实例。

后续研究显著厘清了六维 APN 函数的整体情况。特别是， [7]的结果列出了 14 个不同的 6 比特 APN 函数 CCZ 等价类，其代表元的代数次数至多为三。六维情况下的大量数值搜索、三次 APN 函数的分类[11]，、针对 APN 置换的专项搜索 [3]，以及近期关于切换的研究 [3]都强烈表明，该维数下不存在其他 APN 函数 CCZ 等价类。

猜想 1。 所有 *6*比特*APN*映射均已知。

由于从 $\mathbb{F}_2^6$ 到 $\mathbb{F}_2^6$ 的映射集合规模极其庞大，加之缺乏研究APN映射的一般理论工具，证明猜想 [1]仍然极具挑战性。即使对于布尔函数，目前也没有有效的算法来确定给定函数是否能够作为某个APN映射的坐标。

因此，六维中的任何潜在新例子都至少具有四次代数次数。在本文中，我们给出支持猜想 [1]的数值结果。我们的方法依赖于用于分类布尔函数和向量值函数的新不变量，从而能够深入研究 (6，3)-弯曲函数和 (6，4)-映射的APN扩展，并将其与切换这一概念联系起来。

我们特别关注具有某种特定结构性质的四次APN函数的可能存在性，这一性质由已知的14个CCZ 等价类 [6]的分解所启发。更准确地说，在这14个等价类中，有12个至少包含一个向量值函数的CCZ 等价类，其分量的四阶谱矩集合恰好取两个不同的值。我们提出一种程序，用于分类具有这一规律性的6比特四次函数。为此，我们引入一种新算法，用于检验给定的 $(m,\ m-2)$-函数是否存在APN扩展。

2. 布尔函数

设 $\mathbb{F}_2$ 为阶数为 2 的有限域。设 m 为正整数。我们用 $B(m)$ 表示布尔函数 $f\colon \mathbb{F}_2^m \to \mathbb{F}_2$ 的集合。每个布尔函数都有唯一的代数约化表示：

$$f(x_1, x_2, \ldots, x_m) = f(x) = \sum_{S \subseteq \{1,2,\ldots,m\}} a_S X_S, \quad a_S \in \mathbb{F}_2,\ X_S = \prod_{s \in S} x_s. \tag{1}$$

在这篇关于 $m = 6$ 的短文中，我们用字母 a、b、c、d、e、f表示变量 x_1、..... x_6。 f的次数 是代数形式中满足 $a_S = 1$ 的 S 的最大基数，而满足$a_S = 1$ 的 S 的最小基数则是 f 的赋值 。给定整数 $0 \le s \le t \le m$，我们用记号 $B_s^t(m)$表示由 m 个变量构成、赋值大于或等于 s且次数小于或等于 t的布尔函数空间。

日期: 2026年1月19日。

$f \in B(m)$在$a \in \mathbb{F}_2^m$处的*Walsh*系数为 $\widehat{f}(a) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+a.x}$，其中. 表示通常的标量积。我们用 $\kappa(f)$ 表示 f 的归一化四阶谱矩：

$$\kappa(f) = \frac{1}{q}\kappa_4(f) = \frac{1}{q^3}\sum_{a \in \mathbb{F}_2^m} \widehat{f}(a)^4. \tag{2}$$

Walsh系数满足帕塞瓦尔恒等式：

$$\sum_{a \in \mathbb{F}_2^m} \widehat{f}(a)^2 = q^2, \quad q = 2^m. \tag{3}$$

并给出 f线性度的下界：$\mathrm{lin}(f) := \max_{a \in \mathbb{F}_2^m} |\widehat{f}(a)| \geq 2^{m/2}$，达到该界的布尔函数称为弯曲函数。当且仅当 m 为偶数时，这些函数才存在，并且满足$\kappa(f) = 1$。布尔函数 f 的自相关定义为：

$$f \times f(t) = \sum_{x+y=t} (-1)^{f(x)+f(y)} = \frac{1}{q}\sum_{a \in \mathbb{F}_2^m} \widehat{f}(a)^2 (-1)^{a.t}. \tag{4}$$

如果存在元素 $\mathfrak{s} \in$仿射一般线性群(m)使得$g = f \circ \mathfrak{s}$，则称布尔函数 g 与 f 等价。f的轨道恰好是与 f 等价的所有元素 g 的集合，也就是 f 在仿射一般线性群(m)作用下的轨道。同样，如果存在元素 $\mathfrak{s} \in$仿射一般线性群(m)使得 $\deg(g + f \circ A) \leq 1$，则称 g 与 f 扩展仿射等价。对于维数 6，我们知道 [8, 12] 有 150,356 个布尔函数的 EA 等价类，而对 [4] 限制提升的一种变体给出了一个非常有效的不变量，它在 EA 类之间只产生一次碰撞：

$$ab + bc + cd + bce + abde + abcf + adf \text{ 和 } ac + bc + bd + bce + abde + abcf + adf.$$

不变量 J 在 $B(m-1)$ 上的限制提升 J' 是一个定义在 $B(m)$ 上的不变量，定义如下。对于每个 $u \in \mathbb{F}_2^m$，我们记

$$H_u := \{\, x \in \mathbb{F}_2^m \mid u.x = 0 \,\}, \qquad \overline{H}_u := \{\, x \in \mathbb{F}_2^m \mid u.x = 1 \,\}$$

为与 u 正交的仿射超平面及其补集。将 f 限制到这些超平面上，可知$f|_{H_u}$和 $f|_{\overline{H}_u}$属于 $B(m-1)$。对于每个 $u \in \mathbb{F}_2^m$，我们考虑多重集 $R_f(u) := \{\!\{ J(f_{|H_u}), J(f_{|\overline{H}_u}) \}\!\}$，以及分布 $J'(f) := \{\!\{ R_f(u) | u \notin \mathbb{F}_2^m \}\!\}$，它是定义在 $B(m)$ 上的不变量。在我们的实现中，多重集$R_f(u)$动态地对应一个数值，以得到数值函数；而傅里叶系数的分布就是我们所说的 J的导数傅里叶提升。对于 $m = 5$，扩展仿射等价类的数量为 206。通过 $\omega(f)$为这些等价类编号，可以得到 ω的限制提升；它在 B_2^6(6) 上取 150 355 个不同的值。我们的实现用 18 秒计算出所有成员的不变量。

3. 向量值函数

在该笔记中，向量值（m，n）函数是从 $\mathbb{F}_2^m$ 到 $\mathbb{F}_2^n$ 的映射，由 n 个线性无关的坐标布尔函数定义，使得 $F(x) = \big(f_1(x)\ f_2(x).....,\ f_n(x)\big)$。对于任意 $0 \neq b \in \mathbb{F}_2^n$，布尔函数 $x \mapsto F_b(x) = b.F(x)$ 是 F 的一个分量，我们将非零分量的集合记为 comp(F)。具有相同分量空间（模仿射函数）的两个函数称为合同函数。我们称 $F' :\ \mathbb{F}_2^m \to \mathbb{F}_2^n$ 通过 G 与 F 连接，即 k-连接，如果

$$\mathrm{comp}(G) = \mathrm{comp}(F') \cap \mathrm{comp}(F), \quad \dim \mathrm{comp}(G) = n - k.$$

当我们考察向量值函数 F 的布尔分量空间 comp(F) 时，一方面，我们关注其等价类的集合 $C_F := \{\omega(f) \mid f \in \mathrm{comp}(F)\}$；另一方面，我们关注所有归一化四阶谱矩的集合 $K_F := \{\kappa(f) \mid 0 \neq f \in \mathrm{comp}(F)\}$。对于这两个集合，我们还研究其基数及值分布。注意，$\sharp K_F \leq \sharp C_F$。我们尤其关注 $\kappa(f)$ 取一个或两个值的向量值函数。若 $C_F = 1$，则称 F 为齐次；若 $C_F = 2$，则称其为双齐次。若向量值函数 F 的四阶谱矩有 k 个层级，则 K_F 的基数为 k。

例 1. 如果 m 为奇数，那么 $\mathbb{F}_{2^m}$ 中幂函数 x^3 的所有非零分量都等价；它是一个齐次映射，$\sharp C_F = 1$，因此 $\sharp K_F = 1$。

次数	κ	类	次数	κ	类	次数	κ	类
2	1.0000	1	5	1.6562	13	6	1.6211	11
3	1.0000	3	5	1.7500	17	6	1.7148	10
4	1.7500	8	5	1.8438	84	6	1.8086	56
4	1.9375	54	5	1.9375	213	6	1.9023	161
5	1.4688	8	6	1.2461	4	6	1.9961	444

表1. 4阶归一化矩小于2的15个

我们称 $F:\ \mathbb{F}_2^m \to \mathbb{F}_2^n$ 是 $g:\ \mathbb{F}_2^m \to \mathbb{F}_2^k$ 对 $G:\ \mathbb{F}_2^m \to \mathbb{F}_2^{n-k}$ 的扩展，当且仅当空间 comp(G) 是 comp(F) 的余维为 k 的子空间，且 comp(F) $=$comp(G) $\oplus$comp(g)。如果存在一个仿射 (m,m)-置换 A 和一个仿射 (n,n)-置换 B，使得 deg($G+B\circ F\circ A$) ≤ 1，我们就称 F 和 G 仿射等价。为了对 6 位向量值函数进行数值探索，我们构造如下不变量。对于一个向量值 (5，6)-函数 F，我们将 F 的复合所定义的不变量记为多重集:

$$\mathfrak{j}(F) = \{\!\{\omega(f) \mid f \in \mathrm{comp}(F)\}\!\}$$

是一个EA不变量。该不变量的限制提升，记作j′，是一个很好的不变量，在已知的6比特几乎完美非线性函数集合上取714个不同值。碰撞涉及三个次数为2的函数。(m，n)函数 F在(a，b)处的Walsh系数 $\in \mathbb{F}_2^m \times \mathbb{F}_2^n$，是其分量 F_b的Walsh系数:

$$\widehat{F}(a,b) = \widehat{F_b}(a) = \sum_{x\in\mathbb{F}_2^m} (-1)^{F_b(x)+a.x}.$$

次数和线性度扩展到(m，n)函数 F:

$$\deg(F) := \max_{f\in\mathrm{comp}(F)} \deg(f), \quad \mathrm{lin}\,(F) := \max_{0\neq f\in\mathrm{comp}(F)} \mathrm{lin}\,(f)$$

一个 $(m,\ n)$函数称为 弯曲 函数，当且仅当其所有非零分量都是弯曲函数。这样的函数存在，当且仅当 m 为偶数且 $n \le m/2$。对于 $m=2k$和 $n>k$，若一个 $(m,\ n)$函数 F具有最多数量的弯曲分量 $2^n - 2^{n-k}$，则称其为 $(m,\ n)$-MNBC 函数，见 [1],。我们知道，在维数 6 中，(6,3)弯曲函数恰有13个EA 等价类。

4. 几乎完全函数

设 F 是一个 $(m,\ n)$-函数。对于 $0\neq u\in\mathbb{F}_2^m$、 $v\in\mathbb{F}_2^n$，我们用 $N_F(u,\ v)$ 表示方程 $F(x+u)+F(x) = v$ 在 $\mathbb{F}_2^m$ 中的解的数量。注意，如果 x 是一个解，那么 $x+u$ 也是一个解。因此， $N_F(u,\ v)$ 是偶数。

$$N_F(u,v) = \frac{1}{2^{m+n}} \sum_{a\in\mathbb{F}_2^m, b\in\mathbb{F}_2^n} \widehat{F_b}(a)^2 (-1)^{a.u}(-1)^{b.v} = \frac{1}{2^n}\sum_{b\in\mathbb{F}_2^n} F_b \times F_b(u)(-1)^{b.v}. \tag{5}$$

$(m,\ n)$-函数 F 的差分均匀度 为 $\Delta_F := \max_{u\in\mathbb{F}_2^m\setminus\{0\},\ v\in\mathbb{F}_2^n} N_F(u,\ v)$。一个 $(m,\ m)$-函数 F 是几乎完全非线性 （apn），当且仅当它满足以下等价性质之一:

(i) F 的差分均匀度为 $\Delta_F = 2$;

(ii) 对所有 2-平坦 $\{x,y,z,t\}\subseteq\mathbb{F}_2^m$， $F(x)+F(y)+F(z)+F(t)\neq 0$;

(iii) $\sum_{0\neq f\in\mathrm{comp}(F)} \kappa(f) = 2(q-1)$, where $q=2^m$.

（iii）表明，几乎完美非线性函数至少有一个分量，其归一化谱矩不超过 2。在维数 6 中，66 个次数小于或等于 4 的 EA 等价类满足这一性质（见表 1）。

引理 1。 若 F 在偶数维中是几乎完美非线性，则 $\sharp K_F \ge 2$。

证明。 若 f 是 F 的一个非零分量，且满足 $\sharp K_F = 1$，则由 (iv) 可知 $\kappa(f) = 2$。根据费马小定理， $q^3 \equiv q$ 模 3，且 $\widehat{f}(a)^4 \equiv \widehat{f}(a)_2$模 3。应用帕塞瓦尔恒等式，可得 $\kappa(f) \equiv q$模 3，这意味着 m为奇数。□

标签	Code 64	次数			Γ-秩
1	AAA0AEK2AUIoMcOmASMvUCS5FDB2dfTsAYqG7zfvWa0Mh9NpEOncu0DkXJ8Tx/Un	1	66	18	1170
2	AAAkA4YEAgw0WO+CAICuE0eK9VPDv/FxASQmrBjtYq4ulvdzUOG47Zx3xLTNIKyU	1	66	18	1174
3	AAAEAYIUAQg0We+yA4yOU0uKtF/Tvf1BACQWbBDdIa4uFP9zE+mYLphHhLjN4KyE	1	66	24	1170
4	AAABAoQJAhI82PuyAXDzMDv3z3sb5VGpZVhspNBU1YF9zGTDLQwM30s4UczIuOpK	1	9	3	1166
5	AAAkAw8oAow8qymaAQSmU06+1NXLLDV5ACQ2zBfJEukqdHB/cOeo7ZFDtXfBgquA	1	69	16	1172
6	AAAkAYwMA4o0iC6+AwaOEsuiVdnLzjxFAK4WTBbtcuMatHNDQqysHlVTZbT1s2Wo	0	10	15	1300
7	AAAEAIw8Ao4U2W+aAYOSo4WC1FD3rTtRASg2bBLVUuMy5LRncWy8vtx39frN4Sew	1	15	3	1158
8	AAAkAQsYAYQsSauCAgim0E6uldXLDrdRACgGzh/JUOka1/pHc+eYbp1jtX/h4SGI	1	63	27	1170
9	AAAkAosgA4g8CSO6AYK28MaOtNHDTbV5AKwejB/5UmES1vJ3EW+IbhNT9XnpgiWw	1	15	3	1170
10	AAAkAw8oAIoEC6WKAgaeEUiWlNXbj7tRA64mLBPh0Gky9/R3UO2IbxFLFXP5Iq+4	1	1	1	1146
11	AAAEAwgUAoQ8OW+iAICO0MWq9dvLHX1hAqoGbBTNgiYe1HtbU2+Y7pxnJDz9oSyM	1	5	7	1166
12	AAAkAYQsA4o0SyquAIyes8O6td3jT7ZVACY+bBTtUuk6d/97Qa6Un1drpbr9MmeQ	1	66	24	1168
13	AAAgAIQ4AEY8COKmAwaKM0GelRnzrX5lAyUG7B/lI+ESxPtzgiuMXdJjNLb942+Q	1	1	1	1102
14	AAAgAoYQAEQ0qGiuAwaKEcG+lRv7LXZlA6cGTBXlgesyZPN7ICOkf9BDNDb1wW+4	1	69	22	1172

表2. 根据 EA 类的次数分布和 Γ-秩识别出的 14 个已知 6 比特几乎完美非线性函数 CCZ 等价类的代表元 Code-64

偶数维中不存在只有一个 4 阶谱矩的几乎完美非线性函数，因此我们自然会在下一节考察具有两个 4 阶谱矩的几乎完美非线性函数。这里我们引入“具有两个谱值的函数”这一术语，用来指称满足 $\sharp K_F = 2$的向量值函数 F

。对于几乎完美非线性向量值函数 F，我们引入称为 计数函数 的布尔函数。对于由 $v \in \mathbb{F}_2^m$ 定义的给定 $u \in \mathbb{F}_2^m$,

$$n_u^F(v) = \begin{cases} 1, & \text{if } N_F(u,v) = 2; \\ 0, & \text{if } N_F(u,v) = 0. \end{cases}$$

For 对于所有 $u \in \mathbb{F}_2^m \setminus \{0\}$，计数函数 n_u^F 是平衡的，且 Walsh 系数为:

$$\forall b \in \mathbb{F}_2^m \setminus \{0\}, \quad \widehat{n_u^F}(b) = -F_b \times F_b(u) \quad \text{and} \quad \widehat{n_u^F}(0) = 0. \tag{6}$$

F的图: $\mathbb{F}_2^m \to \mathbb{F}_2^n$是集合 $\Gamma(F) = \{(x,\ F(x)) \mid x \in \mathbb{F}_2^m\} \subset \mathbb{F}_2^m \times \mathbb{F}_2^n$。如果两个映射$F, G$的图的布尔指示函数在 $B(m+n)$ 中仿射等价，则称它们*CCZ*等价；也就是说，存在 $A \in$ 仿射一般线性群$(m+n)$中的一个仿射变换，将 $\Gamma(F)$ 映射到 $\Gamma(G)$。

已知的 6 比特几乎完美非线性映射的次数为 2、3 或 4。它们分为 716 个EA类，归为 14 个CCZ类，见 [6]。总共有 534 个映射的次数为 3。这 14 个类的最大次数均为 4，最小次数均为 2，但 Edel-Pott 的三次函数除外 [7]。

利用 EA类的次数分布和 Γ-秩，可以识别这 14 个已知类。然而，CCZ 不变量并不多，因此寻找一组数值不变量作为判别集是一个有趣的问题。在 [10]，中指出， Γ-秩和 Δ-秩的组合可取 10 个值。接下来，我们定义布尔函数上的 3 个新的有用仿射不变量，以便区分几乎完美非线性映射的图。

不变量	$X_{2,0}$	$\mathfrak{V}$	Γ-秩	Δ-秩	$\mathfrak{T}_9$
数值	6	5	9	3	3
时间（秒）	1.24	0.21	56	42	2080

表 3. 14 个已知类的不变量累计计算成本。

不变量 1（乘法）。 对于布尔函数 f： $\mathbb{F}_2^m \to \mathbb{F}_2$，我们将 $X_{p,\,q}^f$ 记为将 $g \in RM(0,p)$ 映射到投影至 $B_p^m(m)$ 的乘积 gf的乘法自同态。$X_{p,\,q}^f$ 的核的维数是一个数值不变量，称为乘法不变量，记作$X_{p,\,q}$。例如，$X_{2,\,0}$ 在 *14* 个已知类的图上取 *6* 个值。

不变量 2（赋值）。 我们通过考察布尔函数 f的傅里叶系数分布，动态地构造一个不变量。对于每个整数 $v \in \{\infty, 0, 1, \ldots, m\}$，令 ψ_v表示赋值为 v的 *Walsh*系数的示性函数。给定一个不变量 j，我们将赋值不变量定义为以下元组：

$$\mathfrak{V}(f) = \big(\mathrm{j}(\psi_\infty), \mathrm{j}(\psi_0), \ldots, \mathrm{j}(\psi_m)\big).$$

不变量 3 (类换位**)**。 形式为 $T_{\phi,\, u}$： $x \mapsto x + \phi(x) \cdot u$ 的二次函数集合，其中 $q \in RM(2,\ m)$ 和 $u \in \mathbb{F}_2^m$，在群仿射一般线性群(m)的作用下保持稳定。$stab^r(f)$ 中这类函数的元素数量定义了一个不变量，记为 $\mathfrak{T}_r$。

问题 1。 这些不变量的组合能够区分 *14* 个已知类；如果没有 $\mathfrak{T}_2$，则会出现 *1* 次碰撞。挑战在于寻找一种更快的区分解，以绕过从 *13* 个类增加到 *14* 个类时的瓶颈。

5. 已知 APN 的观察

已知的 6比特APN 函数的代数次数为 2、3 或 4，它们分布在 716 个 EA 等价类和 14 个 CCZ 等价类中 [6]。其中有 534 个三次函数等价类，并且每个 CCZ 等价类至少包含一个三次代表元和一个四次代表元。除 Edel-Pott 类外，每个 CCZ 等价类都包含一个二次代表元 [7]。

问题 1. 是否存在 *14* 个已知类之外的几乎完美非线性函数?

5.1. **几乎完美非线性映射的分量**。 二次函数的研究由 [11], 完成，而四次函数的研究似乎仍遥不可及。由于次数不是 CCZ 不变量，问题在于是否存在几乎完美非线性函数 F，使得

$$4 \le \deg_{\min}(F) := \min_{F \underset{\mathrm{CCZ}}{\sim} G} \deg(G)?$$

已知几乎完美非线性函数的分量中只出现了 37 个布尔函数 EA 等价类，这一点相当引人注目，见表 几乎完美非线性函数，表 4，对应 8 个归一化矩。

事实 1. 几乎完美非线性函数的分量集合缩减至 *37* 个元素。

κ	♯			**分布**
1.00	4	4	0	$596_1\ 8230_3\ 6951_6\ 1546_9$
1.75	4	8	17	$2112_{12}\ 2214_{13}\ 476_{14}\ 176_{22}\ 36_{23}\ 34_{27}$
2.50	15	216	4454	$968_{10}\ 1224_{11}\ 12_{20}\ 4_{21}72_{24}\ 144_{25}\ 20_{26}\ 72_{28}\ 8_{29}\ 8_{30}\ 4_{32}\ 4_{33}\ 6830_4\ 7014_5\ 1380_8$
3.25	4	191	3261	$152_{15}\ 216_{16}\ 168_{17}\ 8_{31}$
4.00	4	86	1056	$780_0\ 72_{18}\ 52_{19}\ 1689_2\ 1796_7$
4.75	1	17	258	12_{36}
8.50	1	3	8	24_{35}
16.00	1	1	0	4_{34}

表 4. 已知几乎完美非线性函数的分量分布。

备注 1。 利用已知的 *37* 个分量的信息，可以更轻松地在大型数据集中检测新的 *APN* 函数。

5.2. **计数函数**。 已知 APN 函数的计数函数共有 13 个布尔函数仿射等价类。可以观察到，它们的次数均为 ≤ 4，且始终至少有一个次数为 1 的函数，没有三次函数。

事实 2。 已知的 *6* 比特几乎完美非线性函数至少包含一个仿射计数函数。

我们应用关系6，可以看出，所有可能的 6 比特几乎完美非线性函数的计数函数，其次数为 6，都是五次函数。这一事实为广受认同的观点提供了佐证：

猜想2。 *APN*映射的次数小于 m。

乘法。	deg	**1**	**2**	**4**
13	2	63		
3	3	13	50	
3	3	15	48	
1	3	21	42	
114	3	3	60	
219	3	5	58	
117	3	7	56	
31	3	9	54	
2	4	7		56

表 5. 几乎完美非线性函数和计数函数次数汇总。

5.3. **低级映射。**

命题1。 所有类型为(1、4) 的*6*比特*APN*函数都是二次的。

证明。 一个 6比特APN 函数的分量空间 F 类型为 (1,4) 包含 56 个弯曲函数，构成一个秩为 6 的系统。由于弯曲函数的代数次数至多为 3，因此我们得到 $\deg(F) \leq 3$，并且所有 APN三次函数已在 [11]中完成分类。 □

包含著名都柏林置换的 CCZ 等价类分裂为 13 个不同的等价类。下表给出了对分量函数更细致的分析。

#	次数			四阶谱矩			
	2	3	4	1	1.75	2.5	4.0
1	63			42[1]			21[1]
2		7	56		56[1]		7[1]
5	1	62		30[2]		24[2]	9[3]
2		31	32	12[2]	32[3]	12[2]	7[2]
1		31	32	12[1]	32[2]	12[2]	7[2]
2		31	32	12[2]	32[2]	12[2]	7[2]

存在具有两个谱值的几乎完美非线性函数。CCZ等价类分为 13 个 EA等价类 [6], 3 ，其中有一些具有两个谱值，见第 1 行和第 2 行。此表还给出了分量的次数和谱值分布，并列明了 EA等价类的数量。例如，第 2 行有 2 个 EA等价类，其中一个包含都柏林置换；7 个分量是三次函数，56 个是四次函数。

此外，谱矩为 1.75 的 56 个分量属于 [1] EA等价类，谱矩为 4.0 的 7 个分量属于 [1]。在 14 个已知类之外，是否存在双谱值几乎完美非线性函数? 我们决定通过扩张过程寻找其他例子。若向量值几乎完美非线性函数 F 的归一化

其分量的四阶谱矩取两个不同的值 α 和 β。在这种情况下，

$$\alpha A + \beta B = 2(q-1), \quad A + B = q - 1; \tag{7}$$

其中 A （分别为 B的分量数量， f 其中 F 满足 $\kappa(f) = \alpha$ （分别为 $\kappa(f) = \beta$）。我们假设 $\alpha < \beta$，并称 F 为类型 (α, β) 的函数。利用布尔函数的分类，在 κ个值中，我们找到了 62 个满足 7 的可能对，其中涉及次数小于或等于 4 的函数:

α	A	deg	♯	β	B	deg	♯
1.0	42	23.	4	4.0	21	234	86
1.0	60	23.	4	22.0	3	.3.	1
1.0	56	23.	4	10.0	7	.3.	1
1.0	49	23.	4	5.50	14	.34	29
1.0	21	23.	4	2.50	42	.34	216
1.0	57	23.	4	11.50	6	.34	5
1.0	35	23.	4	3.250	28	.34	191
1.0	15	23.	4	2.3125	48	.34	214
1.0	51	23.	4	6.250	12	..4	13
1.0	47	23.	4	4.9375	16	..4	37
1.0	39	23.	4	3.6250	24	..4	67
1.0	7	23.	4	2.1250	56	..4	49
1.0	55	23.	4	8.8750	8	..4	2

α	A	deg	♯	β	B	deg	♯
1.750	56	..4	8	4.0	7	234	86
1.750	42	..4	8	2.50	21	.34	216
1.750	60	..4	8	7.0	3	.34	3
1.750	51	..4	8	3.0625	12	.34	321
1.750	35	..4	8	2.3125	28	.34	214
1.750	59	..4	8	5.6875	4	..4	25
1.750	21	..4	8	2.1250	42	..4	49
1.750	49	..4	8	2.8750	14	..4	119
1.750	57	..4	8	4.3750	6	..4	34
1.9375	56	..4	54	2.50	7	.34	216
1.9375	60	..4	54	3.250	3	.34	191
1.9375	42	..4	54	2.1250	21	..4	49
1.9375	62	..4	54	5.8750	1	..4	19

注2。 请注意，不存在具有超过 *32* 个弯曲分量的类型为 （1、 β）的函数。事实上，弯曲分量的秩必然为 *6*，这将意味着该函数是三次函数。然而，几乎完美非线性三次函数已经被完全分类。

6. 切换已知的几乎完美非线性函数

回顾一下，平坦集是一个四元集 $\{x, y, z, t\} \subset \mathbb{F}_2^m$，满足 $x + y + z + t = 0$，且 $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ 是几乎完美非线性的，当且仅当 $F(x) + F(y) + F(z) + F(t) \neq 0$ 对所有 2-平坦 $\{x, y, z, t\}$ 都成立。给定一个整数 $k \leq m$ 和 $G\colon \mathbb{F}_2^m \to \mathbb{F}_2^{m-k}$，我们定义

14 个已知几乎完美非线性的 CCZ 等价类														
标签	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ea	25	19	91	19	3	13	91	3	92	85	85	91	13	86
切换类	16275 5945	12369 2133	59241 8263	12369 1699	1953 193	8463 1111	59241 8493	1953 65	59892 8315	55335 8188	55335 7878	59241 8170	8463 1584	55986 7341
apns	41626	85271	154303	63682	6069	34076	154832	2928	156167	154780	147546	161340	55048	144378
类	519	700	704	694	473	701	704	353	706	703	704	704	688	706

G 的 2-平坦集：

$$\mathfrak{F}_G := \{\{x,y,z,t\} \mid G(x)+G(y)+G(z)+G(t)=0\}$$

可见，G 通过 g：$\mathbb{F}_2^m \to \mathbb{F}_2^k$ 映射 $x \mapsto \big(G(x)\ g(x)\big)$ 的扩展 $F:=(G,g)$ 是几乎完美非线性，当且仅当

$$\forall \{x,y,z,t\} \in \mathfrak{F}_G \qquad g(x)+g(y)+g(z)+g(t) \neq 0.$$

换句话说，记作 $T=\mathbb{F}_2^n \setminus \{0\}$，$g$ 是在线性自同态作用下 T^N 的原像：

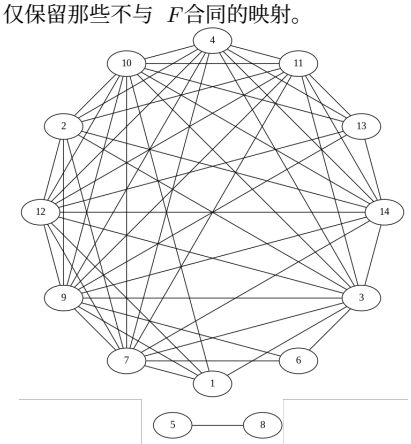
$$Ш(g) := (\ldots, g(x)+g(y)+g(z)+g(t), \ldots) \in \mathbb{F}_2^N, \quad N=|\mathfrak{F}_G|$$

G 的几乎完美非线性扩展的确定：$\mathbb{F}_2^m \to \mathbb{F}_2^{m-}$ 是一项可以通过求解线性方程组完成的简单任务，而当 $k>1$ 时则会变得更加困难。给定一个几乎完美非线性函数 F，可以通过切换构造新的函数，更一般地，还可以找出所有与 F 1-连通的映射。如果存在与 F 1-连通的 $F' \not\equiv F$，我们就称 F 可通过 G 进行 1-切换。

引理 2。一个几乎完美非线性映射 F：$\mathbb{F}_2^m \to \mathbb{F}_2^m$ 可通过 G 进行 *1*-切换，当且仅当 维数 $K(G) > 2m$.

证明。 □

现在，我们说明如何利用不变量证明，已知的 716 个 几乎完美非线性 映射的集合在 1-连通下是闭合的。对于每个已知几乎完美非线性函数的 EA 类 F，我们构造 S中所有 63 个余维为 1 的子空间 $\mathrm{comp}(F)$，考虑 G：$\mathbb{F}_2^6 \to \mathbb{F}_2^5$，其支撑集为 S，并使用引理 2仅保留那些不与 F合同的映射。



标签	ea	sub	apn	类	维数				
					1	2	3	4	5
1	25	1575	100	60	12			22	
2	19	1197	453	206	355		26		4
3	91	5733	1175	457	644	34	69	44	16
4	19	1197	474	243	35	41	79		24
5	3	189	66	4	66				
6	13	819	162	67	162				
7	91	5733	1319	526	813	28	94	22	16
8	3	189	66	5	66				
9	92	5796	1584	516	813	152	97	44	
10	85	5355	1413	507	690	121	75	44	16
11	85	5355	1434	504	758	124	116		16
12	91	5733	1427	492	791	93	94	22	16
13	13	819	336	163	108	114			
14	86	5418	1589	458	773	183	150		

结果汇总于上表。对于具有给定标签的每个 CCZ 等价类，我们列出 EA 等价类的数量、待扩展的子函数数量、通过扩展得到的几乎完美非线性函数数量，以及最终的 EA 等价类数量。最后五列记录了过程中出现的维数 $K(G)$ 的重数。

事实3. 已知 *APN* 函数集合在 *1*-切换下封闭。*CCZ* 等价类的 *1*-连接图有 *14* 个顶点，且包含两个连通分支。

7. 通过回溯进行切换

为确定 G：$\mathbb{F}_2^m \to \mathbb{F}_2^{m-2}$ 到 g：$\mathbb{F}_2^m \to \mathbb{F}_2^2$ 的几乎完美非线性扩张，我们采用回溯方法，并精心选择初始化。我们考虑一个秩为 $2m-1$ 的系统，该系统由 comp(*F*) 的一个基和 $m+1$ 个线性无关的仿射函数组成，并配有一组“主元” $\{p_k\}_{k=1}^{2m-1}$，使得 $\phi_i(p_j) = \delta i,\ j$。这样，我们便可将搜索范围限制在于整组主元上取值为零的函数；而且，如果 p 不是主元，则还可以进一步假设 $g(p) \in 00, 01$。对于 $m=6$，必须在剩余的 53 个向量上实例化 g。这项计算工作量巨大，需要采用基于位运算的实现，并在大量核心上并行运行。

一个向量值函数定义了 $\begin{bmatrix}6\\2\end{bmatrix} = 615$ 个余维 2 子函数，因此我们需要执行 466，116 个回溯过程。为了加快这一过程，我们在计算所有 APN 扩展之前，将不变量 J 应用于某个 CCZ 等价类的 (6，4)-子函数集合。

表 6. 14 个已知 APN 函数的 CCZ 等价类

14 个已知 APN 的 CCZ 等价类														
num	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ea	25	19	91	19	3	13	91	3	92	85	85	91	13	86
sub	16275	12369	59241	12369	1953	8463	59241	1953	59892	55335	55335	59241	8463	55986
筛选	5945	2133	8263	1699	193	1111	8493	65	8315	8188	7878	8170	1584	7341
apns	41626	85271	154303	63682	6069	34076	154832	2928	156167	154780	147546	161340	55048	144378
类别	519	700	704	694	473	701	704	353	706	703	704	704	688	706

对于 14 个 CCZ 等价类中的每个函数 F，我们生成了与 F等价的函数的分量空间的所有余维 2 子空间。我们使用不变量 j 对这些子空间进行筛选，并通过回溯确定所有扩展。这在分量层面得到 37 个等价类。在包含 1，362，046 个 APN 函数的集合上，我们的不变量取 714 个不同的值。

事实 4. 已知几乎完美非线性的集合在 *2*-交换下封闭。

8. 两层

构造所有$(\alpha,\ \beta)$ 几乎完美非线性映射对于一个可容许对而言已经是非常困难的任务。我们决定将搜索范围限制为包含两个等价类的两层向量值函数，其中一个是三次类，另一个是二次类。在这种情况下，三次类构成一个等空间，并且有四种可能的配置，具体描述见表7。类型为(1.75，4）的两层 Dublin 类属于这一类别。

表 7。4 数值空间相容。

α	A	次数	♯等价类	β	B	次数	♯等价类
1.0000	(7)	23...	4	2.1250	(56)	..4..	49
1.7500	(56)	..45.	25	4.0000	(7)	23...	6
1.9375	(56)	..4..	54	2.5000	(7)	.3...	5
1.9375	(62)	..4..	54	5.8750	(1)	..4..	19

从三次函数 g 和四次函数 h 出发，满足 $56\times\kappa(g)+7\times\kappa(h)=126$，我们分几步构造几乎完美非线性扩张。第一步，我们建立相容三次函数列表 L，再从中提取在 h 的稳定子作用下的一组代表元 R：

$$L:=\{f\in \textsc{orbit}(g)\mid f+h\in \textsc{orbit}(h)\},\qquad R:=L\backslash \textsc{stab}(h).$$

然后，我们构造所有子空间的列表

$$V:=\{\langle f_1,f_2,f_3\rangle\mid f_1\in R,\quad f_2\in L,\quad f_3\in L\}.$$

接下来，我们通过取 (6，4)-函数 (f_1，f_2，f_3，h) 来构造候选列表 $\langle f_1,\ f_2,\ f_3\rangle$，只保留满足引理 3 和引理 8所给可扩张性判据的候选项。如果候选集过大，则使用不变量 J对其进行筛选。最后，应用回溯过程完成构造。

$g\backslash f$	1				2				3				4			
0	5	448	0	-	13	236	0	-	4	16	0	-	13	152	64	-
1	16	2168	0	-	152	5652	136	0	77	1004	0	-	181	1770	70	0
2	0	0	0	-	43	0	0	-	50	512	0	-	76	63	0	-
3	0	0	0	-	105	0	0	-	104	0	0	-	210	0	0	-
4	0	0	0	-	802	1660	0	-	958	7136	0	-	2604	4685	0	-
5	0	0	0	-	272	0	0	-	584	4448	0	-	1856	551	0	-
$g\backslash f$	5				6				7				8			
0	5	178	240	-	5	24	0	-	17	48	0	-	12	62	0	-
1	22	112	0	-	131	1416	0	-	420	1951	8	0	397	1786	70	-
2	9	7	0	-	37	0	0	-	436	488	10	0	824	803	40	**12**
3	2	0	0	-	102	0	0	-	1166	0	0	-	1822	0	0	-
4	131	0	0	-	2132	154	0	-	29290	2537	0	-	47184	12699	0	-
5	62	11	0	-	1122	0	0	-	50988	11861	0	-	89576	61126	57	-

通过添加一些坐标函数，可以得到 F 的扩张 G；在这种情况下，comp(F) 成为 G 的分量空间的一个子空间。

引理 3。 如果一个 (m,n)-函数 F 具有几乎完美非线性扩张，那么 $\Delta_F \le 2^{m-n+1}$。

向量型（$m,$ $m-2$）函数 F 存在几乎完美非线性扩张，当且仅当对于所有（$x,$ $y,$ $z,$ t）$\in Q_F$ 方程组 f 二次方程：

$$g(x)+g(y)+g(z)+g(t)\neq 0 \Leftrightarrow \big(g(x)+g(y)+g(z)+g(t)\big)^3=1. \tag{8}$$

在 $\mathbb{F}_2^4$ 中有解。我们注意到 $\big(g(x)+g(y)+g(z)+g(t)\big)^3$ 等于：

$$x^3+y^3+z^3+t^3+xy(x+y)+xz(x+z)+xt(x+t)+yz(y+z)+yt(y+t)+zt(z+t).$$

因此，我们可以将系统（8）转换为一个仿射系统 S_F，其中包含 N 个方程和 $q(q+1)/2$ 个未知数，引入 q 布尔变量 x^3，以及 $q(q-1)/2$ 变量 $xy(x+y)$，其中 $q=2^m$。

引理 4. 如果仿射系统 S_F 无解，那么 F 没有几乎完美非线性扩张。

如果一个（$m, m-2$）-向量值函数满足引理 3 和引理 4 的条件，我们就称它通过了扩展检验。尽管这是一项艰巨的任务，但可以使用以下过程来“分类”所有作为 (6, 3)-向量值三次函数的四次扩展的（α,β）型几乎完美非线性函数。设 $\mathcal{E}$ 为一组（m,n）-函数。我们将 Ext($\mathcal{E}$) 定义为满足引理 3、具有（F,f）型且属于（α,β）类型的扩展集合，并通过不变量 $\mathfrak{Z}$ 进行“筛选”。从 $\mathcal{E}_0$ 开始：$=\{h\}$，其中 deg(h) $=4$ 且 $\kappa(f)=\alpha$，我们构造 $\mathcal{E}_1=$Ext($\mathcal{E}_0$)、 $\mathcal{E}_2=$Ext($\mathcal{E}_1$)和 $\mathcal{E}_3=$Ext($\mathcal{E}_2$)。我们保留通过扩展检验的 (6, 4)-函数，并通过回溯算法进行搜索，以识别几乎完美非线性扩张，进而找到二层几乎完美非线性函数。

对 (1.75,4) 这一对使用以？为参数的过程时，有 8 个四次类可用于初始化构造过程，其中 4 个会产生 APN 函数。回溯阶段之后得到的 506880 个 APN 函数不一定具有两个谱值，但所有 16384 个 (1.75,4) 型函数最终都与都柏林置换 CCZ-等价。

事实 5. 都柏林类在 （1.75，4） 型双齐次二层映射中是唯一的。

9. EXTENSION OF BENT

根据 [13], ，我们知道有 13 个 (6，3)-弯曲函数等价类。不变量 J 能区分 13 个弯曲函数等价类中的 9 个。通过添加一个如下定义的不变量 K，可以得到一个判别不变量。

对于一个 (m，n)-向量值函数 F，我们考虑从 $B_s^t(m)$ 到 $(m,\ n)_{s+2}^t$ 的映射，它将 $f_c(k,\ m)$ 映射为 f_F。这个映射的核的维数是不变量 K，它在 (6，3)-弯曲函数上取六个值。该不变量可与 J结合，得到一个用于区分弯曲函数的判别不变量。顺便一提，同一不变量在所有已知 APN 函数的集合上取 715 个值。

每个 APN 函数的支撑集包含 1,395 个三维子空间。考察已知 APN 函数的所有三维子空间时，我们发现其中有 3,455 个是弯曲空间。

表 8. APN 函数分量中弯曲三维空间的数量

♮-弯曲	0	8	16	21	24	44	48	60	74	75	140
重数。	504	99	78	1	21	2	2	2	4	2	1

进一步详细考察后发现，这些子空间依赖于五个弯曲等价类。因此，14 个（6,3）-弯曲等价类中有 8 个没有出现在已知 APN 函数的支撑集中。因此，弄清这一情况十分重要。我们所描述的回溯算法足够高效，可以计算出 13 个弯曲等价类的所有 APN 扩张。作为第一步，我们计算所有 3×8 阶梯形矩阵；共有

$$\begin{bmatrix}8\\3\end{bmatrix}+\begin{bmatrix}8\\3\end{bmatrix}^2+1=108{,}206$$

这样的矩阵。为了判断一个 (6，3)-弯曲函数是否存在 APN 扩展，可以独立运行 108，206 次回溯过程。计算结果证实，(6，3)-弯曲函数中有 8 个等价类无法进行 APN 扩展。其余 5 个等价类产生了 150 个 EA 等价类（没有新的 CCZ 等价类），分布如下：

表 9. 弯曲等价类的 APN 扩张：150 个等价类

code	1	2	3	5	6
♮-解	13441	58426	61720	103	776
♮-类	3	12	13	54	111

事实 6. 所有 *(6,3)*-弯曲函数的几乎完美非线性扩展均已知。

10. 结论

我们的研究是理解 6比特APN函数的重要一步，为已知的 14 个 CCZ 等价类的完备性提供了有力支持。然而，在研究过程中，我们意识到，要彻底解决双层情形，仍有许多可能性有待探索。

参考文献

[1] Amar Bapić、Enes Pasalic、Alexandr Polujan 和 Alexander Pott。具有超过 Nyberg 界的最多弯曲分量的向量布尔函数。《设计、码与密码学》，92 3 531 552, 2024 3 ( ): – 。Jules Baudrin、[2] Pierre Galissant 和 Léo Perrin。x, 。doi。[3] Christof Beierle、Marcus Brinkmann 和 Gregor Leander。低维中的线性自等价 APN 置换。《IEEE 信息论汇刊》，67 7 4863 4875, 2021 1 ( ): – 。Eric Brier 和 Philippe Langevin。九个变量的布尔三次函数分类。载于 2003 年 IEEE 信息论研讨会，“索邦大学”，法国巴黎，2025 2003 2 。K. A. Browning、[4] J. F. Dillon、M. T. McQuistan 和 A. J. Wolfe。六维中的一个 APN 置换。载于《有限域：理论与应用》，Contemp. Math. 第 518 卷，页码 33 – 42。美国数学会，2010 1 。[5] 罗德岛州普罗维登斯，。Marco Calderini。低维中已知 APN 函数的 EA 等价类。《密码学通信》，( ):821 840, 2020 1, 4, 5, 6 – 。[6] Yves Edel 和 Alexander Pott。一个新的非二次几乎完美非线性函数。《数学与通信进展》，12 5 3 1 59 81, 2009 1, 4, 5 ( ): – 。Valérie Gillot 和 Philippe Langevin。[7] $B\ s\ t\ m$ 2022 http://langevin.univ-tln.fr/data/bst/ 2 (, ,) 的分类，。[8] Valérie Gillot 和 Philippe Langevin。Reed–Muller 码某些陪集的分类。《密码学与通信》，15:1129–1137，2023。doi:10.1007/s12095-023-00652-4。[9] Nikolay Kaleyski。APN 函数和 AB 函数的 EA 等价与 CCZ 等价不变量。密码学电子印本文库，论文 2021 300, 2021 4/ 。Philippe Langevin、Zülfükar Saygi 和 Efim Saygi。有限域 gf( ) 上六维 APN 三次函数的分类，。[10] [11] [12] R 1, 6 57 195 403 414, 1991 2 James A. [13] Maiorana。Reed–Muller 码 ( ) 的陪集分类。《数学计算》，( ): – 。Alexander Poujan。《示例分析》。博士论文，马格德堡奥托·冯·格里克大学，2021。可见于 http://dx.doi.org/10.25673/37956。9

Imath，土伦大学电子邮件地址：
{valerie.gillot,philippe.langevin}@univ-tln.fr