某些具有数据保护的函数纠错码的不存在性

Charul Rajput*、B. Sundar Rajan†、Ragnar Freij-Hollanti*、Camilla Hollanti*

*阿尔托大学数学与系统分析系，芬兰{charul.rajput, ragnar.freij, camilla.hollanti}@aalto.fi †印度科学研究院电气通信工程系，印度班加罗尔 bsrajan@iisc.ac.in

arXiv:2603.01049v1 [cs.IT] 1 Mar 2026

摘要

本文研究近期提出的具有数据保护的函数纠错码（*FCCs*）这一概念。这类码为数据提供一定程度的错误保护，并为数据上的目标函数提供更高级别的保护。这些码记为（f：d_d，d_f）-FCC，其中d_d是码的最小距离，d_f 表示函数f：$\mathbb{F}_q^k \to \mathrm{Im}$（$f$）的函数值不同的码字之间的最小距离，且$d_f \geq d_d$。我们根据码字两两之间的距离构造码上的距离图，并给出码无法作为严格（f：d_d，d_f）-FCC 的条件；也就是说，这类码满足$d_f > d_d$。随后，我们考察若干著名的码类，如完美码和最大距离可分（MDS）码，并证明它们无法用作严格（f：d_d，d_f）-FCC。

索引词

纠错、函数纠错码、MDS码、完美码、冗余

I. 引言

函数纠错码（FCC）于 [1]，提出，旨在保护消息向量中的特定函数或属性，而非整个向量本身。在标准通信场景中，发送方通过噪声信道向接收方发送一个消息向量，而接收方只关心该消息的某个函数值。与保证能够可靠恢复完整消息的经典纠错码（ECC）不同，FCC 仅对函数值不同的码字施加距离约束

。这种有针对性的保护方式使 FCC 能够以潜在较低的冗余，可靠地恢复所关注的函数值，尤其是在该函数的像集远小于其定义域时。

自函数纠错码提出以来，已有若干工作针对各种信道模型和函数类研究了其基本极限与构造。在 [1], 中，作者通过正式定义函数纠错码模型，并推导保护一个函数所需冗余的上界与下界，建立了函数纠错码的基本框架。他们还针对某些函数类（例如局部二元函数和汉明重量函数）给出了显式构造，并证明其中一些构造是最优的。该工作主要考虑二元对称信道上的通信。后续工作将函数纠错码的概念推广到其他信道模型与设定。特别地，符号对读信道上的函数纠错码在 [2] 中针对二元情形进行了研究，随后在 [3]中被推广到b符号读信道。在 [4], 中，作者聚焦于线性函数，其中函数的核诱导出定义域的一个自然划分，并利用这一结构来构造函数纠错码并推导冗余界。进一步的工作针对特定函数族（包括汉明重量函数和局部有界函数）推导了改进的界与函数纠错码构造 [5]–[7]。在 [8],中推导了直至对数因子意义下近最优的冗余界，并证明当域大小充分大时这些界是紧的。函数纠错码也在其他距离度量下得到了研究。特别地，Lee度量下的Plotkin型界及相应码构造在[9], [10], 中给出，而具有齐次距离的函数纠错码在 [11]中得到研究。此外，在 [12]中得到了b符号读信道上函数纠错码的Plotkin型界。

在这类研究中，FCCs 的定义旨在只保护函数值，即距离约束仅施加于对应不同函数输出的码字之间。因此，这些码并未明确保证底层数据信息符号所获得的错误保护程度。

然而，在许多实际场景中，人们希望同时保护数据及其函数，并为二者提供不同级别的保护，因为数据的某些属性或函数可能比数据本身更重要。受此启发， [13] 最近引入了具有数据保护的函数纠错码 这一概念。在这一框架下，编码必须满足两个距离约束：最小距离d_d ，以确保数据本身受到错误保护；以及码字之间的（可能更大的）最小距离d_f ，这些码字对应不同的函数值。

当$d_f > d_d$时，该码对函数提供的保护严格强于对数据提供的保护，这类码称为严格 (f: d_d, d_f)-FCC。

虽然已有研究探讨了带数据保护的函数纠错码的构造及其冗余界 [13],，但本文着重研究特定参数下严格FCC的存在性。特别是，一个自然的问题是：经典纠错码中广为人知的最优码族，能否在其已有的数据保护之外，为函数值提供额外保护？本文主要关注这一问题。

本文建立了一个图论框架，用于研究严格（f: d_d, d_f）-FCC 的可行性。为此，我们为任意一个码关联一个图，其顶点为码字，边则由成对的汉明距离决定。我们证明，这些图的连通性对可实现的函数距离 d_f施加了严格限制。特别地，如果一个码的距离图具有足够强的连通性，那么该码就不能作为任何非平凡函数的严格FCC。

利用这一框架，我们根据码的经典参数（例如覆盖半径），推导出严格FCC的一般性不存在结果。作为具体推论，我们证明，两类基础的最优纠错码——完美码和MDS码——对于任何非平凡函数，都不能用作严格（f: d_d, d_f）-FCC。也就是说，这些码无法为函数值提供强于其对数据本身所提供的保护。我们还将这些结果推广到其他覆盖半径已知或可加以界定的码类。本文是在完整版 [13],的基础上扩展而成，新增了一些内容，例如 α-距离图，这是完整版中所给最小距离图的推广；此外还提出了一些新结果，例如引理 1。

A. 贡献与论文结构

本文的主要贡献总结如下。

- 我们研究了 严格 (f: d_d, d_f)-函数纠错码的存在性，其中，为函数值提供的保护严格强于为数据提供的保护。
- 我们引入了码的距离图，并展示了这些图的连通性如何对可实现的函数距离施加基本限制。
- 利用这一框架，我们根据经典码参数（如覆盖半径），推导出严格（f: d_d, d_f）-FCC 不存在的一般性结果。

- 作为具体推论，我们证明，众所周知的最优纠错码族——包括完美码、MDS码，以及满足特定结构条件的线性码——对于任何非平凡函数，都不能充当严格（f: d, d_f）-FCC。

- 我们进一步将这些不存在性结果推广到其他类别的码，这些码的覆盖半径已知或可以确定其界。

本文其余部分安排如下。第二节介绍全文使用的基本定义和概念。第三节回顾具有数据保护的函数纠错码的定义。第四节给出本文的主要结果，我们利用距离图论证，建立严格的（f: d_d, d_f）-FCC 的不存在性结果。最后，第五节总结全文。

记号： 大小为q 的有限域记作 $\mathbb{F}_q$， $\mathbb{F}_q^k$ 表示$\mathbb{F}_q$上的k维向量空间。对于向量u、$v \in \mathbb{F}_q^n$，$d(u, v)$表示u与v之间的汉明距离；对于向量$u \in \mathbb{F}_q^n$，$\mathrm{wt}(u)$表示u的汉明重量。对于整数n 和r，二项式系数记作 $\binom{n}{r} \triangleq \frac{n!}{r!(n-r)!}$。全文中，为方便记号，向量 $\mathbb{F}_q^k$ 有时省略逗号书写，例如 $0110 \in \mathbb{F}_2^4$ 。

——

II. 预备知识

本节介绍码 [14], 的一些基本概念，以及基于文献 [1]中工作的函数纠错码定义。

长度为n 的q元纠错码 (ECC) C 是 $\mathbb{F}_q^n$ 的一个子集，其基数为$M = |C|$。 C的最小距离 记为$d_{\min}(C)$，或简写为d，定义如下：

$$d \triangleq \min_{\substack{c_1, c_2 \in C \\ c_1 \neq c_2}} d(c_1, c_2).$$

这样的码通常称为(n, M, d)码。对于向量$x \in \mathbb{F}_q^n$，x 到码 C的距离定义为

$$d(x, C) \triangleq \min_{c \in C} d(x, c).$$

更一般地，对于两个非空子集 A、$B \subseteq \mathbb{F}_q^n$，子集 A 与 B 之间的距离定义为

$$d(A, B) \triangleq \min_{a \in A, b \in B} d(a, b).$$

定义 1 (覆盖半径**)**。 码 C 的覆盖半径 记为 $R(C)$，定义为

$$R(C) \triangleq \max_{x \in \mathbb{F}_q^n} d(x, C).$$

等价地，$R(C)$ 是最小的整数，使得以 C 的码字为中心、半径为 $R(C)$ 的所有汉明球的并集覆盖整个空间 $\mathbb{F}_q^n$。覆盖半径度量环境空间中任意向量到最近码字的最大距离。

定义 2 （函数纠错码）**.**考虑函数 $f\colon \mathbb{F}_q^k \to Im(f)$。系统编码 $C\colon \mathbb{F}_q^k \to \mathbb{F}_q^{k+r}$ 被定义为一个 (f,t)-函数纠错码（FCC），如果对于任意 $u_1, u_2 \in \mathbb{F}_q^k$，使得 $f(u_1) \neq f(u_2)$，下列条件成立：

$$d(C(u_1), C(u_2)) \geq 2t + 1.$$

III. 具有数据保护的函数纠错码

在本节中，我们给出同时保护数据和函数值的函数纠错码的定义。关于此类码的更多细节，请参见 [13]。

定义 3. 考虑函数 $f\colon \mathbb{F}_q^k \to Im(f)$。编码 $\mathfrak{C}_f\colon \mathbb{F}_q^k \to \mathbb{F}_q^{k+r}$ 被定义为一个 $(f : d_d, d_f)$-函数纠错码（FCC），如果

- 对于任意 $u_1, u_2 \in \mathbb{F}_{kq}$，满足 $u_1 \neq u_2$，

$$d(\mathfrak{C}_f(u_1), \mathfrak{C}_f(u_2)) \geq d_d,$$

- 对于任意 $u_1, u_2 \in \mathbb{F}_{kq}$ 使得 $f(u_1) \neq f(u_2)$，以下条件成立：

$$d(\mathfrak{C}_f(u_1), \mathfrak{C}_f(u_2)) \geq d_f,$$

其中 d_d 和 d_f 是两个非负整数，满足 $d_d \leq d_f$。

以下示例说明了一种具有数据保护功能的函数纠错码。

例 1. 考虑同一个奇偶校验函数 $f\colon \mathbb{F}_2^4 \to \{0, 1\}$，

$$f(u) = \mathrm{wt}(u) \bmod 2 = u_1 \oplus u_2 \oplus u_3 \oplus u_4, \quad u = (u_1, u_2, u_3, u_4).$$

我们利用 *[13]*中给出的两步构造法构造一个$(f: d_d = 3, d_f = 5)$-*FCC*。第一步使用一个 $[7,4,3]$ 汉明码（采用系统编码），第二步使用仅依赖于 $f(u)$ 的 *2* 比特奇偶校验向量，从而得到如下的码。

$[7,4,3]$ 汉明码的奇偶校验位为

$$p_1 = u_1 \oplus u_2 \oplus u_4,\ p_2 = u_1 \oplus u_3 \oplus u_4,\ p_3 = u_2 \oplus u_3 \oplus u_4,$$

而*FCC*奇偶校验位为

$$s_1 = s_2 = f(u) = u_1 \oplus u_2 \oplus u_3 \oplus u_4.$$

现在定义编码 $\mathfrak{C}_f$： $\mathbb{F}_2^4 \to \mathbb{F}_2^9$ 如下

$$\mathfrak{C}_f(u) = (u_1, u_2, u_3, u_4,\ p_1, p_2, p_3,\ s, s).$$

$u \in \mathbb{F}_2^4$	$f(u)$	$(p_1p_2p_3)$	(s,s)	码字
0000	*0*	*000*	*00*	*0000 000 00*
0001	*1*	*111*	*11*	*0001 111 11*
0010	*1*	*011*	*11*	*0010 011 11*
0011	*0*	*100*	*00*	*0011 100 00*
0100	*1*	*101*	*11*	*0100 101 11*
0101	*0*	*010*	*00*	*0101 010 00*
0110	*0*	*110*	*00*	*0110 110 00*
0111	*1*	*001*	*11*	*0111 001 11*
1000	*1*	*110*	*11*	*1000 110 11*
1001	*0*	*001*	*00*	*1001 001 00*
1010	*0*	*101*	*00*	*1010 101 00*
1011	*1*	*010*	*11*	*1011 010 11*
1100	*0*	*011*	*00*	*1100 011 00*
1101	*1*	*100*	*11*	*1101 100 11*
1110	*1*	*000*	*11*	*1110 000 11*
1111	*0*	*111*	*00*	*1111 111 00*

可以验证，对于任意 $u \neq v$，都有 $d(\mathfrak{C}_f(u), \mathfrak{C}_f(v)) \geq 3$。因此，$d_d = 3$成立。如果 $f(u) \neq f(v)$，

那么 $s \neq s'$，最后两个奇偶校验位在两个位置上都不同，因此我们有 $d(\mathfrak{C}_f(u),\ \mathfrak{C}_f(v)) \geq 3+2=5$。因此，$d_f = 5$ 成立。所以，$\mathfrak{C}_f$ 是一个长度为 $(f:\ 3,\ 5)$-*FCC* 的编码9（冗余 $r = 5$）。

定义 4 (最优冗余)。 最优冗余记为 $r_f(k:d_d,d_f)$，定义为存在一个具有编码函数 $\mathfrak{C}_f$: $\mathbb{F}_q^k \to \mathbb{F}_q^{k+r}$ 的 $(f:d_d,d_f)$-*FCC* 时，r 的最小值。

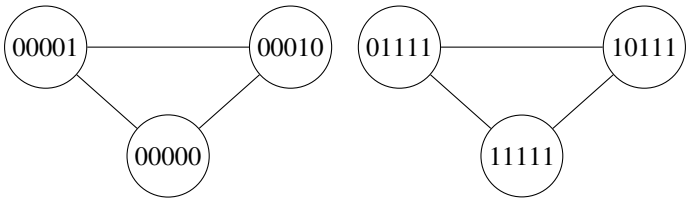
IV. 严格 (f: d_d, d_f)-FCC 的不存在性

若一个 (f: d_d, d_f)-FCC 满足严格 (f: d_d, d_f)-*FCC* 的条件，即 $d_f > d_d$，则称其为严格 (f : d_d, d_f)-FCC，因为当 $d_f = d_d$ 时，该情形可归约为纠错码。本节定义码 C 的 α-距离图，并借此证明某些类型的码不能用作严格 (f: d_d, d_f)-FCC。

定义 5 (α-距离图)。 设 C 是一个码。 C 的 α-距离图 记为 $G_\alpha(C)$，它是一个图，顶点集为 C；两个不同的顶点 $c_1,c_2 \in C$ 相邻，当且仅当 $d(c_1,c_2) \leq \alpha$，其中 $\alpha \geq d_{\min}(C)$，而 $d_{\min}(C)$ 表示码 C 的最小距离。

特别地，当 $\alpha = d_{\min}(C)$ 时， α-距离图称为最小距离图 ，记作 $G(C) = G_{d_{\min}}(C)$。显然，只要 $\alpha \leq \alpha'$，$G_\alpha(C)$ 就是 $G_{\alpha'}(C)$ 的子图。因此，如果 $G_\alpha(C)$ 是连通的，那么 $G_{\alpha'}(C)$ 也连通。此外，如果 $d_{\max}$ 表示任意两个码字之间的最大距离，那么 $G_{d_{\max}}(C)$ 就是完全图。

例 2. 设 $C = \{00000, 00001, 00010, 01111, 10111, 11111\} \subset \mathbb{F}_2^5$. 与 $\alpha = 2 > d_{\min}(C)$ 对应的 α-距离图，即 $G_2(C)$ ，仅当两点间距离小于或等于 *2* 时才有边。



以下定理说明，了解 α-距离图如何用于判定某个码是否能在特定参数下作为 (f: d_d, d_f)-FCC。

定理 1. 设 C 是一个 (n,q^k,d) 码。若 α-距离图 $G_\alpha(C)$ 是连通图，则 C 不可能是任意满足 f: $\mathbb{F}_q^k \to Im(f)$ 且 $|Im(f)| \geq 2$、$d_f > \alpha$ 的 $(f:d,d_f)$-*FCC*。

证明。 假设$G_\alpha(C)$是连通的，并设 C是一个 (f: d, d_f)，其中 $d_f > \alpha$，对应函数f: $\mathbb{F}_q^k \to \mathrm{Im}(f)$，且 $|\mathrm{Im}(f)| \geq 2$。对每个 $a \in \mathrm{Im}(f)$，定义如下集合

$$C_a = \{c_u \in C : \ f(u) = a\},$$

其中，c_u表示与消息向量 $u \in \mathbb{F}_q^k$对应的码字。若 $|\mathrm{Im}(f)| \geq 2$且 $d_f > \alpha$，则根据 (f: d, d_f)-FCC 要求，任意满足 $a \neq b$ 的 $x \in C_a$和 $y \in C_b$都必须满足 $d(x, y) \geq d_f > \alpha$。因此，$G_\alpha(C)$ 中不同的 C_a和 C_b之间不存在边，所以划分 $\{C_a : a \in \mathrm{Im}(f)\}$将图分离，这与 $G_\alpha(C)$ 的连通性矛盾。因此，C不可能是一个 (f: d, d_f)-FCC。

□

定理 1 可以很容易地推广到其 α-距离图具有多个连通分量的码。

定理 2. 设 C 是一个(n, q^k, d) 码。若 α-距离图 $G_\alpha(C)$ 有 Q 个连通分量，则对于任意满足 $|Im(f)| \geq Q + 1$且 $d_f > \alpha$的 $f: \mathbb{F}_q^k \to Im(f)$， C都不可能是一个$(f: d, d_f)$-FCC。

由于$G_\alpha(C)$的连通性在 α 增大时得以保持，因此在应用定理1时，只需确定使$G_\alpha(C)$变为连通的 α 的最小值。这一选择对函数距离d_f给出了最强的排除，因为 α的任何更大值都会对d_f的可行值产生更弱的约束。此外，由于 $\alpha \geq d$，其中d是 C的最小距离，确立最小距离图$G_d(C)$的连通性会对函数距离d_f给出尽可能最强的限制。

以下引理给出了 α-距离图连通的一个条件。

引理 1. 设 C 是覆盖半径为 $R(C)$ 的码。则满足 $\alpha \geq 2R(C)+1$ 的 α-距离图 $G_\alpha(C)$ 是连通的。

证明. 设 $C = A \cup B$ 是将C 划分为两个非平凡部分，使得 $d(A,B) = \delta$。设 $a^* \in A$ 与$b^* \in B$ 满足 $d(a^*, b^*) = \delta$。选取一个向量 $x \in \mathbb{F}_q^n$ 满足

$$d(x, a^*) = \left\lceil \frac{\delta}{2} \right\rceil, \qquad d(x, b^*) = \left\lfloor \frac{\delta}{2} \right\rfloor.$$

于是,

$$d(x, A) \leq d(x, a^*) = \left\lceil \frac{\delta}{2} \right\rceil, \quad d(x, B) \leq d(x, b^*) = \left\lfloor \frac{\delta}{2} \right\rfloor.$$

根据三角不等式，对于任意的 $a \in A$，我们有

$$\delta \le d(a,b^*) \le d(a,x) + d(x,b^*) = d(a,x) + \left\lfloor \frac{\delta}{2} \right\rfloor,$$

这给出 $d(a,x) \ge \left\lceil \frac{\delta}{2} \right\rceil$。因此，$d(x,A) = \left\lceil \frac{\delta}{2} \right\rceil$。类似地，我们可以得到 $d(x,B) = \left\lfloor \frac{\delta}{2} \right\rfloor$。进一步根据覆盖半径的定义，我们有

$$R(C) \ge \max_{x' \in \mathbb{F}_q^n} d(x',C) \ge d(x,C) = \min\{d(x,A), d(x,B)\} = \left\lfloor \frac{\delta}{2} \right\rfloor.$$

因此，$\delta \le 2R(C)+1$。这意味着任意两个非连通分量之间的最小距离至多为 $2R(C)+1$。因此，若我们构造图 $G^{2R(C)+1}(C)$，将距离小于或等于 $2R(C)+1$ 的码字相连，则 $G^{2R(C)+1}(C)$ 是连通的。因此，任何满足 $\alpha \ge 2R(C)+1$ 的 $G_\alpha(C)$ 都是连通的。□

利用定理 1 和引理 1，我们得到以下结果。

推论 1. 设 C 是一个覆盖半径为 $R(C)$ 的 (n,q^k,d) 码。那么，对于任意 $f\colon \mathbb{F}_q^k \to Im(f)$ 满足 $|Im(f)| \ge 2$ 且 $d_f > 2R(C)+1$，C 都不可能是一个 $(f:d,d_f)$-*FCC*。

A. 完美码与*MDS*码的最小距离图

在本小节中，我们证明，对于ECC的两类最优码族，最小距离图是连通的：1）完美码和2）MDS码。

1) 完美码：长度为n、最小距离为d 的纠错码 C 的大小的汉明界在 [15] 中给出如下。

$$M \le \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i}.$$

达到汉明界的码称为完美码。若$d = 2t+1$，则称其为完美t错误纠正码。由于完美t错误纠正码的覆盖半径恰好为t，由引理 1，我们得到如下结果。

定理 3. 完美 t 错误纠正码的最小距离图是连通的。

由定理 1 和定理 3，可得以下推论。

推论 2. 设 f: $\mathbb{F}_q^k \to Im(f)$ 是一个函数。则对于一个(f: d_d, d_f)-*FCC*，其中 $d_f > d_d$，我们有

$$r_f(k : d_d, d_f) \geq n - k + 1,$$

其中 n 是满足 $q^{n-k} = \sum^{\lfloor \frac{d_d-1}{2} \rfloor}_{i=0} \binom{n}{i}(q-1)^i$. 的整数。

2) MDS 码：长度为n且最小距离为d 的纠错码 C 的大小满足 Singleton界，如 [15]所示：

$$M \leq q^{n-d+1},$$

等价地，对于$k = \log_q M$，$d \leq n - k + 1$。以等号达到 Singleton界的码称为最大距离可分（*MDS*）码。特别地，当且仅当$M = q^{n-d+1}$时，$(n, M, d)_q$ 码是 MDS 码。

为了证明 MDS 码的最小距离图是连通的，我们使用以下引理。

引理 2. 设 C 是一个参数为$(n, M, d)_q$的 *MDS* 码，且 $u, v \in C$。那么存在 $u' \in C$使得

1) $d(u,u') = d$（即，u' 是图 $G(C)$中的 u 的邻居）；
2) $d(u', v) \leq d(u,v) - 1$。

如果 $d(u,v) = d$，则码字 v 本身就是 u'。

证明。令 $S = \{i \in [n] : u_i \neq v_i\}$，且 $S^c = [n] \setminus S = \{i \in [n] : u_i = v_i\}$。则 $|S| = d(u, v) \geq d = n - k + 1$，因此 $|S^c| = n - |S| \leq k - 1$。选取集合 $J \subseteq [n]$，使得 $|J| = k$ 且 $S^c \subseteq J$（即，J 包含 u 和 v 的所有相同位置，并从 S 中再选取 $k - |S^c|$ 个位置）。那么 $|J^c| = n - k = d - 1$，并且

$$|J \cap S| = k - |S^c| = k - (n - d(u, v)) = d(u, v) - (d - 1).$$

任取$j \in J \cap S$，并定义向量$t \in \mathbb{F}_q^J$如下：$t_j = v_j \neq u_j$，且对所有$i \in J \setminus \{j\}$，有$t_i = u_i$。根据 MDS投影性质（对任意 $|J| = k$，投影 $\pi_J : C \to \mathbb{F}_q^J$ 是双射），存在唯一的$u' \in C$满足 $\pi_J(u') = t$。现在，我们有以下结论。

1) $d(u,u') = d$. u 和u' 可能不同的坐标为：单个索引$j \in J$（被强制为不同），以及J^c 中的索引（不受约束）。因此

$$d(u, u') \leq 1 + |J^c| = 1 + (d - 1) = d.$$

由于$u' \neq u$ 且d 是 C 的最小距离，我们必须有$d(u,u') = d$。

2) $\mathrm{d}(\mathrm{u}', \mathrm{v}) \leq \mathrm{d}(\mathrm{u}, \mathrm{v}) - 1$。我们统计 u' 和 v 之间确定相同的位置。在 $\mathrm{S}^c \subseteq \mathrm{J}$ 上令 $\mathrm{t}_i = \mathrm{u}_i = \mathrm{v}_i$，因此对所有 $\mathrm{i} \in \mathrm{S\,c}$，都有 $\mathrm{u}'_i = \mathrm{v}_i$；这给出了 $|\mathrm{S\,c}| = \mathrm{n} - \mathrm{d}(\mathrm{u}, \mathrm{v})$ 个相同位置。此外，我们在 j 处强制令 $\mathrm{u}'_j = \mathrm{v}j$，从而多得到一个相同位置。因此，相同位置的数量至少为 $\mathrm{n} - \mathrm{d}(\mathrm{u}, \mathrm{v}) + 1$，于是

$$d(u', v) \leq n - (n - d(u, v) + 1) = d(u, v) - 1.$$

这就证明了两个结论。 □

定理 4. 任意 *MDS* 码的最小距离图都是连通的。

证明。 令 $G(C)$ 为 C 的最小距离图，且 u、$v \in C$。我们将通过沿边移动并逐步缩短与 v 的距离，在 $G(C)$ 中构造一条从顶点 u 到 v 的路径。令 $x_0 = u$，并对点对 (x_0, v) 应用引理 2，得到 $x_1 \in C$，满足

$$d(x_0, x_1) = d \quad \text{and} \quad d(x_1, v) \leq d(x_0, v) - 1.$$

若 $d(x_1, v) = 0$，则我们已经到达 v；否则 $d(x_1, v) \geq d$。再次对 (x_1, v) 使用引理 2，得到 x_s。重复此过程，我们得到一个序列 $x_0, x_1, x_2, \ldots$，其中 C 满足

$$d(x_i, x_{i+1}) = d \qquad \text{and} \qquad d(x_{i+1}, v) \leq d(x_i, v) - 1.$$

由于 $d(x_i, v)$ 是一个非负整数，且每一步都会减小，因此经过有限步后，我们会到达某个 x_j，使得 $d(x_j, v) = d$。接下来应用引理 2，得到 $x_{j+1} = v$，使得 $d(x_j, v) = d$。因此 $u = x_0, x_1, \ldots, x_j, v$ 是 $G(C)$ 中从 u 到 v 的一条路径。因此，$G(C)$ 是连通的。

□

由定理 1 和定理 4，可得以下推论。

推论 3. 设 $f\colon \mathbb{F}_q^k \to \mathrm{Im}(f)$ 是一个函数。假设存在一个 *MDS* $(n, q^k, d)_q$ 码，即 $n = k + d - 1$。那么，对于一个 $(f : d, d_f)$-*FCC*，若 $d_f > d$，则有

$$r_f(k : d, d_f) \geq n - k + 1 = d.$$

B. 线性码的最小距离图

在本小节中，我们给出一类最小距离图连通的线性码。

引理 3。 设 C 是一个定义在 $\mathbb{F}_q$ 上、最小距离为 d 的线性码，令 W_d 表示 C 中所有汉明重量为 d 的码字组成的集合。那么，当且仅当最小距离图 $G(C)$ 连通时， C 由其最小重量码字张成，即 $C = \langle W_d \rangle$。

证明。 由于 C 是线性的，对于所有u、$v \in C$，有$d(u,v) = \mathrm{wt}(u - v)$。假设 $C = \langle W_d \rangle$。令$u \in C$，则存在码字$w_1, w_2, \ldots\ldots$、$w_t \in W_d$，使得

$$u = w_1 + w_2 + \cdots + w_t.$$

从零码字开始，依次加上$w_1, w_2, \ldots\ldots$、w_t，每一步都相当于加上一个最小重量码字，因此沿着$G(C)$的一条边移动。经过t 步后，我们到达u。因此，每个码字都通过$G(C)$中的一条路径与零码字连通。由于 C 是线性的，因此任意两个码字都连通，所以$G(C)$是连通的。

反过来，假设 $C \neq \langle W_d \rangle$。令 $C' = \langle W_d \rangle$，它是 C的真子码。现在我们证明$G(C)$不连通。若x、$y \in C$ 在$G(C)$中相邻，则

$$x - y \in W_d \subseteq C',$$

这意味着x 和y 属于 C' 的同一个陪集。因此，属于 C' 不同陪集的顶点之间不存在边，而$G(C)$ 分解为由 C' 的陪集索引的连通分量。因此，$G(C)$ 不连通。

□

由定理 1 和引理 3，可得以下推论。

推论 4. 设 C 是一个由其最小重量码字张成的 $[n,k,d]$ 线性码，其定义在 $\mathbb{F}_q$ 上。那么，对于任何满足 $f: \mathbb{F}_q^k \to \mathrm{Im}(f)$ 且 $|\mathrm{Im}(f)| \geq 2$、$d_f > d$ 的 f， C 都不可能是一个 $(f: d, d_f)$-*FCC*。

C. 某些其他码类的 α-距离图

有若干类码的覆盖半径是已知的。此外，即使只是覆盖半径的上界，也足以满足我们的目的。特别地，根据推论 1，若码 C 的覆盖半径满足$R(C) \leq x$，则对于任何满足 $\mathbb{F}_q^k \to \mathrm{Im}(f)$ 且 $|\mathrm{Im}(f)| \geq 2$、$d_f > 2x + 1$ 的函数f: $\mathbb{F}_q^k \to$， C 都不可能是一个 (f: d, d_f)-FCC。

- **准完美码：** 设$C_0 \subseteq \mathbb{F}_{nq}$为一个完美（$n$，$q_k$，$2t+1$）码。一个具有 $|C| = |C_0| = q_k$的码 $C \subseteq \mathbb{F}_{n+1q}$称为准完美码，如果在一个坐标上对 C 进行删 puncturing得到 C_0，即存在一个坐标

i 使得

$$\pi_i(C) = C_0,$$

其中， π_i 表示删除i个坐标的删余映射。经典示例包括扩展汉明码和扩展戈莱码。准完美码的覆盖半径为$t + 1$，这一结果在文献中已广为人知 [14]。

- **一阶 Reed-Muller 码：** 对于长度为 2_m 的二元一阶 Reed-Muller 码 RM(1,m)，其覆盖半径已被精确确定，表达式如下：

$$R(\mathrm{RM}(1, m)) = 2^{m-1} - 2^{\lceil m/2 \rceil - 1}.$$

这一结果在 [14] 中得到证明。

文献 [16] 给出了 Reed-Muller 码 RM(r,m) 覆盖半径的一般上界。在[17], 中，作者证明了一个 [n,k,d] 线性码在 $\mathbb{F}_q$ 上的对偶距离为$d^{\perp}$时，其覆盖半径满足

$$R(C) \leq n - \sum_{i=0}^{d^{\perp}-2} \left\lceil \frac{n-i}{q} \right\rceil.$$

V. 结论

本文确立了具有数据保护的严格 (f: d_d, d_f)-函数纠错码不存在的结果，其中要求对函数值的保护强于对数据的保护。通过分析与码相关联的距离图，我们确定了排除这类严格FCC存在可能性的连通性条件。

我们提出的基于图的方法使我们能够将严格FCC的可行性与纠错码的经典参数联系起来。具体而言，我们证明，完美码和MDS码等最优码族无法为函数值提供严格高于数据的保护。这些结果凸显了具有数据保护的FCC固有的结构性限制。

致谢

本工作得到了瓦伦贝里人工智能、自主系统与软件计划向阿尔托大学和查尔姆斯理工大学（项目负责人A. Graell i Amat和C. Hollanti）提供的联合项目资助，并另外得到了科学与工程研究委员会（SERB）所属

印度政府科学技术部（DST）通过J.C. Bose国家奖学金向B. Sundar Rajan教授提供的资助。

参考文献

[1] A. Lenz、R. Bitar、A. Wachter-Zeh 和 E. Yaakobi，《函数纠错码》，IEEE信息论汇刊，第69卷，第9期，第5604–5618页，2023年9月。[2] Q. Xia、H. Liu 和 B. Chen，《适用于符号对读信道的函数纠错码》，IEEE信息论汇刊，第70卷，第11期，第7807–7819页，2024年11月。[3] A. Singh、A. K. Singh 和 E. Yaakobi，《适用于 b 元符号读取信道的函数纠错码》，arXiv预印本 arXiv:2503.12894，2025年。[4] R. Premlal 和 B. S. Rajan，《论函数纠错码》，IEEE信息论汇刊，第71卷，第8期，第5884–5897页，2025年8月。[5] Y. Zhang、Z. Xu、X. Zhang 和 G. Ge，《函数纠错码的最优冗余》，IEEE信息论汇刊，第71卷，第12期，第9458–9467页，2025年12月。[6] C. Rajput、B. S. Rajan、R. Freij-Hollanti 和 C. Hollanti，《适用于局部有界函数的函数纠错码》，载于2025年IEEE信息论研讨会（ITW）论文集，澳大利亚悉尼，2025年，第851–856页。[7] G. K. Verma、A. Singh 和 A. K. Singh，《适用于局部（λ,ρ, b）函数的函数纠错 b 符号码》，IEEE信息论汇刊，第72卷，第1期，第331–341页，2026年1月。[8] H. Ly 和 E. Soljanin，《论有限域上函数纠错码的冗余》，载于2025年第13届编码专题国际研讨会（ISTC）论文集，美国加利福尼亚州洛杉矶，2025年，第1–5页。[9] G. K. Verma 和 A. K. Singh，《论 Lee 度量下的函数纠错码》，arXiv预印本 arXiv:2507.17654v2，2025年。[10] H. K. Hareesh、R. Ummer N. T. 和 B. S. Rajan，《李度量信道的类Plotkin界及显式函数纠错码构造》，arXiv预印本 arXiv:2508.01702v3，2025年。[11] H. Liu 和 H. Liu，《具有齐次距离的函数纠错码》，arXiv预印本 arXiv:2507.03332，2025年。[12] S. Sampath H. 和 B. S. Rajan，《论适用于 b 元符号读取信道的函数纠错码的 Plotkin 界》，载于2025年IEEE信息论研讨会（ITW）论文集，澳大利亚悉尼，2025年，第698–703页。[13] C. Rajput、B. S. Rajan、R. Freij-Hollanti 和 C. Hollanti，《具有数据保护的函数纠错码》，arXiv预印本 arXiv:2511.18420，2025年。[14] J. H. Lint，《编码理论导论》。施普林格，柏林、海德堡，1992年。[15] R. Hill，《编码理论入门课程》。牛津大学出版社，1986年。[16] G. D. Cohen 和 S. N. Litsyn，《关于 Reed-Muller码的覆盖半径》，IEEE信息论汇刊，第40卷，第2期，第542–548页，1994年3月。[17] H. Janwa 和 H. F. Mattson，《关于线性码覆盖半径的一些上界及其应用》，设计、编码与密码学，第18卷，第1–3期，第163–181页，1999年。