Basefold 笔记：Random Foldable Codes

前面几篇文章已经提到了 BaseFold 通过引入 *foldable code* 的概念，扩展了 FRI IOPP，并且结合 Sumcheck 协议能够支持做 Multi-linear Polynomial 的 PCS。接下来还剩下一个关键的问题，那就是这样的 *foldable code* 如何显式地进行构造呢？我们想要这样的可折叠编码(*foldable code*)具有以下几个性质：

1. 能够高效编码
2. 无视域的大小，即对于小域也适用
3. 能够适用于多元线性多项式的 PCS

还有对于编码比较重要的一点，就是考虑其编码的最小相对海明距离(Minimum Relative Hamming distance)。如果读者比较熟悉 FRI 协议，想必对其用到的 Reed-Solomon 编码并不陌生，其有一个很好的性质，便是其距离能达到 Singleton bound，即其距离满足 $d = n - k + 1$，这也被称之为属于 Maximum Distance Separable (MDS)编码。这样的编码很好的平衡了编码长度与其纠错能力，即用最少的冗余提供了最强的错误检测与纠错能力，这大大节省了编码的空间。放在 PCS 协议中，验证者能够更加高效的进行检测了。因此从实用角度考虑，我们还希望这样的可折叠编码满足第 4 点：

4. 具有良好的相对最小距离

BaseFold 论文[ZCF23]中就构造了这样一种称为 *Random Foldable Code* (RFCs) 的编码，满足上述的性质。接下来我们看看它是如何做到这几点的。

高效编码算法

这一系列的第一篇文章中其实已经提到了 *foldable linear code* 的概念以及 BaseFold 的编码算法。这里做下简单的回顾。

定义 1 [ZCF23, Definition 5] ((c, k_0, d) - foldable linear codes). 令 $c, k_0, d \in \mathbb{N}$ 以及 $\mathbb{F}$ 表示一个有限域。一个以 $\mathbf{G}_d$ 为生成矩阵的线性编码 $C_d : \mathbb{F}^{k_0 \cdot 2^d} \to \mathbb{F}^{ck_0 \cdot 2^d}$ 被称为是 ***foldable*** 是说：如果存在一系列的生成矩阵 $(\mathbf{G}_0, \ldots, \mathbf{G}_{d-1})$ 以及对角矩阵 $(T_0, \ldots, T_{d-1})$ 以及 $(T'_0, \ldots, T'_{d-1})$ 使得对于任意的 $i \in [1, d]$ 都有

1. 对角矩阵 $T_{i-1}, T'_{i-1} \in F^{ck_0 \cdot 2^{i-1} \times ck_0 \cdot 2^{i-1}}$ 满足对任意的 $j \in [ck_0 \cdot 2^{i-1}]$ 都有 $\mathrm{diag}(T_{i-1})[j] \neq \mathrm{diag}(T'_{i-1})[j]$ 成立；
2. 矩阵 $\mathbf{G}_i \in F^{k_0 \cdot 2^i \times ck_0 \cdot 2^i}$ （按行进行排列）等于

$$\mathbf{G}_i = \begin{bmatrix} \mathbf{G}_{i-1} & \mathbf{G}_{i-1} \\ \mathbf{G}_{i-1} \cdot T_{i-1} & \mathbf{G}_{i-1} \cdot T'_{i-1} \end{bmatrix}. \tag{1}$$

为了高效的构造一个 foldable linear code，采用均匀采样的方式生成，先定义这样的一簇随机可折叠分布(random foldable distributions)。

定义 2 [ZCF23, Definition 9] ((c, k_0) - foldable distributions) 固定有限域 $\mathbb{F}$ 以及 $c, k_0 \in \mathbb{N}$。令 $\mathbf{G}_0 \in \mathbb{F}^{k_0 \times ck_0}$ 是一个满足最大距离可分性的 $[ck_0, k_0]$ 线性编码的生成矩阵，并且设 D_0 为输出 $\mathbf{G}_0$ 的分布，概率为 1。对每个 $i > 0$，我们递归的定义分布 D_i，该分布会采样生成矩阵 $(\mathbf{G}_0, \mathbf{G}_1, \ldots, \mathbf{G}_i)$，其中 $\mathbf{G}_i \in F^{k_i \times n_i}$ 且 $k_i := k_0 \cdot 2^i$，$n_i := ck_i$：

1. 采样 $(\mathbf{G}_0, \ldots, \mathbf{G}_{i-1}) \leftarrow D_{i-1}$；
2. 采样 $\mathrm{diag}(T_{i-1}) \leftarrow \$(\mathbb{F}^\times)^{n_{i-1}}$ 并定义 $\mathbf{G}_i$ 为

$$\mathbf{G}_i = \begin{bmatrix} \mathbf{G}_{i-1} & \mathbf{G}_{i-1} \\ \mathbf{G}_{i-1} \cdot T_{i-1} & \mathbf{G}_{i-1} \cdot -T_{i-1} \end{bmatrix}. \tag{2}$$

一旦初始的生成矩阵 $\mathbf{G}_0$ 确定之后，只需从 $\mathbb{F}^\times$ （表示从 $\mathbb{F}$ 去掉 0 元素）均匀采样生成 n_0 个随机数，生成对角矩阵 T_0 的对角元素，就可以得到下一个生成矩阵 $\mathbf{G}_1$，再依次递归下去生成 $(\mathbf{G}_2, \ldots, \mathbf{G}_i)$。在 PCS 中，以均匀采样的方式生成可折叠编码的方式能够帮助实现高效的证明者。

注意上述定义中说到要求初始的 $\mathbf{G}_0$ 是一个满足 MDS 性质线性编码的生成矩阵，在论文 [ZCF23] 脚注中提到，这一点并不是必须要满足的，添加该性质只是为了后文简化对编码距离的分析，其实关于距离的分析对于任意的线性编码都是成立的。

协议 1 Enc_d **[ZCF23, Protocol 1]: BaseFold 编码算法**

输入：原消息 $\mathbf{m} \in \mathbb{F}^{k_d}$

输出：$\mathbf{w} \in \mathbb{F}^{n_d}$ 使得 $\mathbf{w} = \mathbf{m} \cdot \mathbf{G}_d$

参数：$\mathbf{G}_0$ 以及对角矩阵 $(T_0, T_1, \ldots, T_{d-1})$

1. If $d = 0$ (即 $\mathbf{m} \in \mathbb{F}^{k_0}$): (a) 返回 $\mathrm{Enc}_0(\mathbf{m})$
2. else (a) 分解 $\mathbf{m} := (\mathbf{m}_l, \mathbf{m}_r)$ (b) 令 $\mathbf{l} := \mathrm{Enc}_{d-1}(\mathbf{m}_l)$ ，$\mathbf{r} := \mathrm{Enc}_{d-1}(\mathbf{m}_r)$ 以及 $\mathbf{t} = \mathrm{diag}(T_{d-1})$ (c) 返回 $(\mathbf{l} + \mathbf{t} \circ \mathbf{r}, \mathbf{l} - \mathbf{t} \circ \mathbf{r})$

通过分析协议 1 ，可以看出编码得到 C_d 只需要 $\frac{dn_d}{2}$ 域乘法与 dn_d 域加法，即需要 $0.5n \log n$ 域乘法和 $n \log n$ 的域加法，总体来说编码复杂度是 $O(n \log n)$ 的。至此我们已经介绍了 BaseFold 给出的 Random linear Foldable Codes 的显式构造，且验证了其确实是高效编码的。

多项式拯救世界：基于多项式的编码

接下来我们来看看 *Random Foldable Code* 的第 2 个和第 3 个性质：

2. 无视域的大小，即对于小域也适用
3. 能够适用于多元线性多项式的 PCS

前面提到过 Reed-Solomon 编码能够达到 Singleton 界限，但是其仅在字母表比较大(即 $q \gg n$)的情况下才能实现这种显著的特性。好在我们可以扩展 Reed-Solomon 编码，称之为 Reed-Muller 编码，这样我们就从一元多项式编码进入到了多元多项式编码的世界。这使得我们能够在小域上($q \ll n$) 适用了，虽然这其中会失去一点距离和纠错能力的平衡，但是这是值得的。

在 [ZCF23] 的附录 D 中告诉我们 *Random Foldable Code* 就是截断的 Reed-Muller 编码(Punctured Reed-Muller Codes)的一个特例。这样 *Random Foldable Code* 就可以无视域的大小，同时由于进入到了多元多项式的世界，也就能够适用于多元线性多项式的 PCS 了。

我们知道 Reed-Solomon 编码的编码空间是由不超过一个次数 d 的一元多项式组成的集合，那 Reed-Muller 编码其实就是从一元多项式扩展到了多元多项式，其编码空间就是多元多项式的总次数不超过 d 的集合。

对于 n, d, q 且 $d < q$ ，定义 Reed-Muller 编码为([GJX15])

$$\mathrm{RM}_q(n, d) := \{(F(\mathbf{u}))_{\mathbf{u} \in \mathbb{F}_q^n} : F \in \mathbb{F}_q[X_1, \cdots, X_n], \deg(F) \leq d\}. \tag{3}$$

Reed-Muller code 表示的是总次数不超过 d 的 n 元多项式在 $\mathbb{F}_q^n$ 上的取值的集合。编码 $\mathrm{RM}_q(n, d)$ 的长度为 q^n ，维数为 $\binom{n+d}{n}$ 。

从字面上来理解 Punctured Reed-Muller 编码，其就是 Reed-Muller code 的一个截断。具体来说就是估计的点 $\mathbf{u}$ 不取到所有的 $\mathbf{F}_q^n$ ，只取到其中的一部分，设其为 $\mathcal{T} = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_N\}$ ，通常的 Punctured Reed-Muller code 的定义允许这个集合 $\mathcal{T}$ 是多重集合 （multiset），即允许其中有重复元素，这里不做该要求。记 $\mathrm{RM}_q(n, d)|_{\mathcal{T}}$ 为 $\mathbb{F}_q$ - 线性码：

$$\mathrm{RM}_q(n, d)|_{\mathcal{T}} := \{(F(\mathbf{u}_1), F(\mathbf{u}_2), \cdots, F(\mathbf{u}_N)) : F \in \mathbb{F}_q[X_1, \cdots, X_n], \deg(F) \leq d\}. \tag{4}$$

这就被称为 punctured Reed-Muller code ([GJX15])。通过定义也可以发现其就是 Reed-Muller 编码的一个子集，只是选取了其中的 N 个点，这和字面上的“截断的(punctured)”也是相符的。

有了上述关于 punctured Reed-Muller code 的概念，我们来看看论文 [ZCF23] 附录 D 中给出的下面这个引理，它告诉我们 foldable linear codes 就是 punctured Reed-Muller codes 的一个特例。

引理 1 [ZCF23, Lemma 11] (Foldable Punctrured Reed-Muller Codes). 令 C_d 是一个可折叠的线性编码 (foldable linear code) ，其生成矩阵是 $(\mathbf{G}_0, \ldots, \mathbf{G}_{d-1})$ ，对角矩阵为 $(T_0, \ldots, T_{d-1})$, $(T'_0, \ldots, T'_{d-1})$ 。那么存在一个子集 $D \subset \mathbb{F}^d$ 使得 $C_d = \{(P(\mathbf{x}) : \mathbf{x} \in D) : P \in \mathbb{F}[X_1, \ldots, X_d]\}$ ，即 C_d 中的每个码字都是一个多元线性多项式 P 在 D 中的每个点的取值。

证明：用归纳法证明。为了叙述的简单，考虑 C_0 是重复码。对于最基本的情况， $\mathrm{Enc}_0(m) = m \| \ldots \| m$ 是一个次数为 0 的多项式 $P \equiv m$ 在 c 个不同点的 evaluation。假设对于 $i < d$ ，存在一个集合 D_i 使得 $C_i = \{(P(\mathbf{x}) : \mathbf{x} \in D_i) : P \in \mathbb{F}[X_1, \ldots, X_i]\}$ 。不失一般性，通过任意分配一个整数 $j \in [1, c \cdot 2^i]$ 给 D_i 中的每个元素来进行索引。根据这个顺序，将 x_j 表示为 D_i 中的第 j 个元素。

令 $t = \mathrm{diag}(T_i), t' = \mathrm{diag}(T_i'), n_i = c \cdot 2^i, \mathbf{v} \in \mathbb{F}^{2^{i+1}}$ ，令 $P \in \mathbb{F}[X_1, \ldots, X_{i+1}]$ 表示是以 $\mathbf{v}$ 中的元素为系数的多项式。最后，令 $P_l, P_r \in \mathbb{F}[X_1, \ldots, X_i]$ 使得 $P(X_1, \ldots, X_{i+1}) = P_l(X_1, \ldots, X_i) + X_{i+1} P_r(X_1, \ldots, X_i)$ 。则有

$$
\begin{aligned}
\mathrm{Enc}_{i+1}(\mathbf{v}) &= \mathrm{Enc}_i(\mathbf{v}_l) + \mathrm{diag}(T_i) \circ \mathrm{Enc}_i(\mathbf{v}_r) \quad \| \quad \mathrm{Enc}_i(\mathbf{v}_l) + \mathrm{diag}(T_i) \circ \mathrm{Enc}_i(\mathbf{v}_r) \\
&\quad \text{(由Protocol1编码算法得)} \\
&= (P_l(\mathbf{x}_1), \ldots, P_l(\mathbf{x}_n)) + \mathrm{diag}(T_i) \circ (P_r(\mathbf{x}_1), \ldots, P_r(\mathbf{x}_n)) \\
&\| \quad (P_l(\mathbf{x}_1), \ldots, P_l(\mathbf{x}_n)) + \mathrm{diag}(T_i') \circ (P_r(\mathbf{x}_1), \ldots, P_r(\mathbf{x}_n)) \\
&\quad \text{(由归纳假设可得)} \\
&= (P_l(\mathbf{x}_1) + t_1 P_r(\mathbf{x}_1), \ldots, P_l(\mathbf{x}_n) + t_n P_r(\mathbf{x}_n), P_l(\mathbf{x}_1) + t_1' P_r(\mathbf{x}_1), \ldots, P_l(\mathbf{x}_n) + t_n' P_r(\mathbf{x}_n)) \\
&\quad \text{(由Hadmard积的定义得)} \\
&= (P(\mathbf{x}_1, t_1), \ldots, P(\mathbf{x}_n, t_n), P(\mathbf{x}_1, t_1'), \ldots, P(\mathbf{x}_n, t_n')) \\
&\quad \text{(由}P\text{的定义得)}
\end{aligned} \tag{5}
$$

因此，令 $D_{i+1} = \{(\mathbf{x}_1, t_1), \ldots, (\mathbf{x}_n, t_n), (\mathbf{x}_1, t_1'), \ldots, (\mathbf{x}_n, t_n')\}$ ，对于 $i+1$ 时引理也成立。因此由归纳法得证。 □

良好的相对最小距离

最后，我们关注 *Random Foldable Code* (RFCs) 满足的第 4 个性质：

4. 具有良好的相对最小距离

论文[ZCF23]中证明了 RFCs 最小海明(Hamming distance)的紧的界限（“紧的”界限意味着实际是能够达到的界限）。例如，一个在 256 位有限域上具有消息长度 2^{25} 和码率 $\frac{1}{8}$ 的 RFC，其相对最小距离以压倒性概率为 0.728 。而对于码率为 $\frac{1}{8}$ 的 code ，其能够达到的最大的相对最小 Hamming 距离大约是 $1 - \frac{1}{8} = 0.875$ ，可以看到 0.728 还是比较接近 0.875 的。这在实际中是比较实用的，并且这也意味着以压倒性概率(overwhelming probability)，均匀采样的 foldable code（能够实现高效的PCS证明者）也具有良好的相对最小距离（能够实现高效的PCS验证者）。

上面说到的以“压倒性的概率”，这是由于我们在编码的过程中引入的分布 $(\mathbf{G}_0, \ldots, \mathbf{G}_d) \leftarrow D_d$ 导致的。当均匀的从 $\mathbb{F}^\times$ 中采样生成对角矩阵 T_i ，并令 $T_i' = -T_i$ ，那么在选取的 $(T_1, \ldots, T_d)$ 基础上，以压倒性的概率(overwhelming probability) 得到的 C_d 的相对最小距离等于

$$
1 - \left(\frac{\epsilon_{\mathbb{F}}^d}{c} + \frac{\epsilon_{\mathbb{F}}}{\log |\mathbb{F}|} \sum_{i=0}^{d} (\epsilon_{\mathbb{F}})^{d-i} \left(0.6 + \frac{2 \log(n_i/2) + \lambda}{n_i} \right) \right) \tag{1}
$$

其中，c 是码率的倒数，$\epsilon_{\mathbb{F}} = \frac{\log |\mathbb{F}|}{\log |\mathbb{F}| - 1.001}$ ，n_i 是编码的长度，d 是消息长度的对数，λ 是安全参数。如果选取 $\lambda = 128$ ，意思是 (c, k_0, d) - random foldable linear codes 能够以至少为 $1 - 2^{-128}$ 的概率达到上述的相对最小距离。

下面来看看 (1) 式的结果是如何得到的。我们现在的目标是想分析可折叠的随机编码(Foldable Random Codes) C_d 的相对最小距离。对于一个线性编码，其最小距离等于其中非零码字的最小 Hamming weight (Hamming weight 的意思就是一个向量中非零分量的个数)，这是因为

$$
d = \min_{\substack{\vec{c_1} \neq \vec{c_2} \\ \vec{c_1}, \vec{c_2} \in C_d}} \Delta(\vec{c_1}, \vec{c_2}) = \min_{\substack{\vec{c_1} \neq \vec{c_2} \\ \vec{c_1}, \vec{c_2} \in C_d}} wt(\vec{c_1} - \vec{c_2}) = \min_{\vec{c} \neq \vec{0}, \vec{c} \in C_d} wt(\vec{c}) \tag{6}
$$

由于是线性编码，因此上式中的 $\vec{c_1} - \vec{c_2}$ 也是 C_d 中的一个码字，从而最后一个等式成立。那么我们想证明对于任意非零消息，即 $\forall \vec{m} \neq \vec{0}$ ，编码之后的码字 $\mathrm{Enc}_d(\vec{m})$ 中没有太多的零分量，不妨设最多为 t_d 个，用 $\mathrm{nzero}(\cdot)$ 来表示一个向量中零分量的个数， 则我们想要说明

$$
\forall \vec{m} \neq \vec{0}, \quad \mathrm{nzero}(\mathrm{Enc}_d(\vec{m})) \leq t_d \tag{2}
$$

用 n_d 表示码字 $\mathrm{Enc}_d(\vec{m})$ 的长度，那么由 (2) 可得到

$$\forall \vec{m} \neq \vec{0}, \quad wt(\mathrm{Enc}_d(\vec{m})) \geq n_d - t_d \tag{7}$$

因此 C_d 能够达到的相对最小距离就为

$$\Delta(C_d) = \frac{\min_{\vec{c}\neq\vec{0}, \vec{c}\in C_d} wt(\vec{c})}{n_d} = \frac{n_d - t_d}{n_d} = 1 - \frac{t_d}{n_d} \tag{3}$$

(1) 式的结果就是通过 (3) 式计算而来的，现在剩下的任务就是分析 t_d 具体等于多少了，也就是对于任意非零的消息，编码之后的码字中的零分量的个数有多少。

借助归纳法

借助于强有力的工具——归纳法，我们来分析 t_d 。假设以压倒性的概率（基于对角矩阵 $T_0, \ldots, T_{i-1}$ 的选择），对于任意的非零消息 $\vec{m} \in \mathbb{F}^{k_i} \ \{0^{k_i}\}$ ，编码之后的 $\mathrm{Enc}_i(\vec{m})$ 最多有 t_i 个零分量。我们来分析 $i+1$ 的情况。对于任意的非零消息 $\vec{m} = (\vec{m}_l, \vec{m}_r) \in \mathbb{F}^{2k_i}$ ，

$$\begin{aligned}
\mathrm{Enc}_{i+1}(\vec{m}) &= (\vec{m}_l, \vec{m}_r) \begin{bmatrix} \mathbf{G}_i & \mathbf{G}_i \\ \mathbf{G}_i \cdot T_i & \mathbf{G}_i \cdot -T_i \end{bmatrix} \\
&= (\vec{m}_l \mathbf{G}_i + \vec{m}_l \mathbf{G}_i \cdot T_i, \vec{m}_l \mathbf{G}_i - \vec{m}_l \mathbf{G}_i \cdot T_i) \\
&= (\mathrm{Enc}_i(\vec{m}) + \mathrm{Enc}_i(\vec{m}) \circ \mathrm{diag}(T_i), \mathrm{Enc}_i(\vec{m}) - \mathrm{Enc}_i(\vec{m}) \circ \mathrm{diag}(T_i)) \\
&:= (\mathbf{M}_l \| \mathbf{M}_r)
\end{aligned} \tag{8}$$

也就是看看向量 $(\mathbf{M}_l \| \mathbf{M}_r)$ 中零分量的个数有多少。将 $\mathbf{M}_l$ 与 $\mathbf{M}_r$ 分开表示，即为

$$\begin{aligned}
\mathbf{M}_l &= \mathrm{Enc}_i(\vec{m}_l) + \mathrm{Enc}_i(\vec{m}_r) \circ \mathrm{diag}(T_i) \\
\mathbf{M}_r &= \mathrm{Enc}_i(\vec{m}_l) - \mathrm{Enc}_i(\vec{m}_r) \circ \mathrm{diag}(T_i)
\end{aligned} \tag{9}$$

设 $\mathbf{t} = \mathrm{diag}(T_i)$ ，对每一个 $j \in [1, n_i]$ ，设 $A_j = \mathrm{Enc}_i(\vec{m}_l)[j]$ ， $B_j = \mathrm{Enc}_i(\vec{m}_r)[j]$ ，定义一个函数：

$$f_j(x) = A_j + xB_j \tag{4}$$

如果 $f_j(\mathbf{t}[j]) = 0$ 或者 $f_j(-\mathbf{t}[j]) = 0$ ，就说明 $\mathbf{M}_l[j] = 0$ 或者 $\mathbf{M}_r[j] = 0$ ，也就找到了编码之后的零分量。先从 A_j ， B_j 是否为零来分析 $f_j(x)$ 是否为零，分为以下几种情况：

	$A_j = 0$	$A_j \neq 0$
$B_j = 0$	$f_j(x) \equiv 0$	$f_j(x) = A_j \neq 0$
$B_j \neq 0$	$f_j(x) = xB_j$	$f_j(x) = A_j + xB_j$

首先考虑第一种情况，那就是 $A_j = B_j = 0$ ，可以发现无论 x 取什么值，$f_j(x) \equiv 0$ ，此时 $\mathbf{M}_l[j] = 0$ 并且 $\mathbf{M}_r[j] = 0$ 。满足这样的指标 $j \in [n_i]$ 也有多少呢？我们用一个集合 $S \subseteq [n_i]$ 来表示，并且由归纳假设知道 $|S| \leq t_i$ ，用 $m_{i+1}(S)$ 来表示那些非零的消息能满足 $A_j = B_j = 0$ ，即

$$S = \{j \in [1, n_i] : A_j = B_j = 0\}. \tag{10}$$

在这种情况下，$\mathbf{M}_l[j] = \mathbf{M}_r[j] = 0$ ， 那么 $(\mathbf{M}_l \| \mathbf{M}_r)$ 中已经找到了有 $2|S|$ 个分量为零了。

考虑第 2 种情况，$A_j \neq 0, B_j = 0$ ，此时 $f_j(x) = A_j \neq 0$ ，这种情况下肯定找不到零分量。

下面考虑表格中的最后一行，$B_j \neq 0$ ，此时指标 j 肯定不在 S 中，我们定义一个指标集合 $\urcorner S^* \subseteq \urcorner S$ 使得

$$\urcorner S^* = \{j \in [1, n_i] \backslash S, B_j \neq 0\} \tag{11}$$

对于每一个 $j \in \urcorner S^*$ ，定义一个随机变量

$$X_j = 1\{f_j(\mathbf{t}[j]) = 0\} + 1\{f_j(-\mathbf{t}[j]) = 0\} \tag{12}$$

其中的 $1(\cdot)$ 表示一个指示函数，如果括号中的条件成立则为 1，否则为 0。那么 X_j 的值就反映了对于一个 $j \in \urcorner S^*$，向量 $\mathbf{M}_l$ 与 $\mathbf{M}_r$ 在 j 这个位置上总共有几个分量为零，其可能的取值就有 $\{0,1,2\}$ 个。首先，可以发现，X_j 是一个独立的 Bernulli 试验，因为 $\mathbf{t}[j]$ 是从 $\mathbb{F}^\times$ 中独立采样的。令 $z_j \in \mathbb{F}^\times$，使得 $f_j(z_j)=0$。那么当 $\mathbf{t}[j]=z_j$ 时，$1\{f_j(\mathbf{t}[j])=0\}=1$，而当 $\mathbf{t}[j]=-z_j$ 时，$1\{f_j(-\mathbf{t}[j])=0\}=1$。接下来分析 X_j 的取值：

1. $X_j=2$。此时说明 $f_j(\mathbf{t}[j])=0$ 且 $f_j(-\mathbf{t}[j])=0$，说明 $\mathbf{t}[j]=z_j=-z_j$，这说明 $z_j=0$，这是不可能的，因为 $z_j \in \mathbb{F}^\times$。
2. $X_j=1$。此时说明 $f_j(\mathbf{t}[j])=0$ 或 $f_j(-\mathbf{t}[j])=0$，此时 $\mathbf{t}[j]=z_j$ 或者 $\mathbf{t}[j]=-z_j$，其发生的概率为 $\frac{2}{|\mathbb{F}|-1}$。
3. $X_j=0$。说明 $\mathbf{t}[j] \neq z_j$ 并且 $\mathbf{t}[j] \neq -z_j$，其发生的概率自然为 $1-\frac{2}{|\mathbb{F}|-1}$。

当 j 取遍 $\urcorner S^*$，将所有的 X_j 相加，就得到了此时 $(\mathbf{M}_l \| \mathbf{M}_r)$ 中零分量的个数，即 $X=\sum_{j\in\urcorner S^*} X_j$。

至此，我们就分析完了表格中的所有情况，那么可以得到

$$\mathrm{nzero}(\mathrm{Enc}_{i+1}(\vec{m})) = 2|S| + X \tag{13}$$

下面就是分析 $|S|$ 和这个 X 了，想证明对于任意非零消息 $\vec{m} \in \mathbb{F}^{2k_i}\backslash\{0^{2k_i}\}$，编码之后的 $\mathrm{Enc}_{i+1}(\vec{m})$ 以压倒性的概率最多有 t_{i+1} 个零分量。现在分析 $\mathrm{Enc}_{i+1}(\vec{m})$ 至少有 $2t_i+l_i$ 个零分量的概率：

$$\begin{aligned}
\Pr[\mathrm{nzero}(\mathrm{Enc}_{i+1}(\vec{m})) \geq 2t_i+l_i] &= \Pr[2|S|+X \geq 2t_i+l_i] \\
&= \Pr[X \geq 2t_i+l_i-2|S|] \\
&= \Pr[\sum_{j\in\urcorner S^*} X_j \geq 2t_i+l_i-2|S|] \\
&\leq \sum_{j=2t_i+l_i-2|S|}^{|\urcorner S^*|} \binom{|\urcorner S^*|}{i} \cdot (\frac{2}{|\mathbb{F}|-1})^i \cdot (1-\frac{2}{|\mathbb{F}|-1})^{|\urcorner S^*|-i} \\
&\quad (\text{由二项式定理得} \binom{|\urcorner S^*|}{i} \leq 2^{|\urcorner S^*|}) \\
&\leq |\urcorner S^*| \cdot 2^{|\urcorner S^*|} (\frac{2}{|\mathbb{F}|-1})^{2t_i+l_i-2|S|} \\
&\leq |\urcorner S| \cdot 2^{|\urcorner S|} \cdot (\frac{2}{|\mathbb{F}|-1})^{2t_i+l_i-2|S|} \quad (\urcorner S^* \subseteq \urcorner S) \\
&= |[1,n_i]\backslash S| \cdot 2^{|[1,n_i]\backslash S|} \cdot (\frac{2}{|\mathbb{F}|-1})^{2t_i+l_i-2|S|} \\
&= (n_i-|S|) \cdot 2^{n_i-|S|} \cdot (\frac{2}{|\mathbb{F}|-1})^{2t_i+l_i-2|S|} \\
&\quad (\text{设} |\mathbb{F}| \geq 2^{10}, \text{可得} \frac{2}{|\mathbb{F}|-1} \leq \frac{2.002}{|\mathbb{F}|}) \\
&\leq n_i \cdot 2^{n_i-|S|} \left(\frac{2.002}{|\mathbb{F}|}\right)^{2t_i+l_i-2|S|}
\end{aligned} \tag{14}$$

我们注意到，指标集合 $S \subseteq [1,n_i]$，如果任意选取集合 S，对于每一个指标 $i \in [1,n_i]$，都有两种可能，那就是选取或者不选取进集合 S，那么集合 S 的选取总共就有 2^{n_i} 种。当我们取遍了集合 S 的所有的可能，那么将这些 S 形成的 $m_{i+1}(S)$ 并起来 $\cup_{S\subseteq[1,n_i]} m_{i+1}(S)$，就能覆盖在 $\mathbb{F}^{k_{i+1}}=\mathbb{F}^{2k_i}$ 中的所有消息了。论文 [ZCF23] 引理 2 告诉我们 $m_{i+1}(S)$ 集合的大小最多为 $\mathbb{F}^{t_i-|S|}$。那么取遍所有 2^{n_i} 种可能的 S 集合，每个集合 S 中最多有 $\mathbb{F}^{t_i-|S|}$ 个消息 $\vec{m} \in \mathbb{F}^{2k_i}$。通过将所有 S 并起来的方式，联合每个 S 大小的界限，可以得到当 l_i 足够大时，即 $|\mathbb{F}|^{l_i} \gg 2^{n_i}$ 时，$n_i \cdot 2^{n_i-|S|}\left(\frac{2.002}{|\mathbb{F}|}\right)^{2t_i+l_i-2|S|}$ 会足够的小，此时对于任意的非零向量 $\vec{m} \in \mathbb{F}^{2k_i}$，都有 $\mathrm{nzero}(\mathrm{Enc}_{i+1}(\vec{m})) \leq 2t_i+l_i$，即 $\mathrm{Enc}_{i+1}(\vec{m})$ 中最多有 $2t_i+l_i$ 个零分量。

论文 [ZCF23] 中以定理的形式给出了更加具体的描述。

定理 1 [ZCF23, 定理 2] 固定任意的有限域 $\mathbb{F}$，其中 $|\mathbb{F}| \geq 2^{10}$，设 $\lambda \in \mathbb{N}$ 是安全参数。对于一个分量元素在 $\mathbb{F}$ 中的向量 $\mathbf{v}$，用 $\mathrm{nzero}(\mathbf{v})$ 表示向量 $\mathbf{v}$ 中零分量的个数。对于任意的 $d \in \mathbb{N}$，设 D_d 是 (c,k_0)-可折叠的分布，设对每一个 $i \leq d$，$k_i=k_0 2^i, n_i=ck_i$。那么

$$\Pr_{(\mathbf{G}_0,\ldots,\mathbf{G}_d)\leftarrow D_d}\left[\exists \mathbf{m}\in\mathbb{F}^{k_d}\backslash\{\mathbf{0}\}, \mathrm{nzero}(\mathrm{Enc}_d(\mathbf{m}))\geq t_d\right]\leq d\cdot 2^{-\lambda} \tag{5}$$

其中，$t_0=k_0$ 以及对每一个的 $i\in[d]$， $t_i=2t_{i-1}+l_i$，

$$l_i:=\frac{2(d-1)\log n_0+\lambda+2.002t_{d-1}+0.6n_d}{\log|\mathbb{F}|-1.001}. \tag{15}$$

(5) 式告诉我们 $\mathrm{Enc}_d(\mathbf{m})$ 中零分量个数极大概率小于 t_d，因为如果超过 t_d，其概率可忽略不计。由于 t_i 的值给出的是一个迭代的式子，即 $t_i=2t_{i-1}+l_i$，因此可以通过迭代式求和得到 t_d，那么可以得到能够达到的最大的在 C_d 中的相对 0 的个数 $Z_{C_d}=\frac{t_d}{n_d}$，再计算 $1-Z_{C_d}$ 即可得到 C_d 能够达到的最小的相对 Hamming 距离 Δ_{C_d}，其结果就为 (1) 式：

$$1-\left(\frac{\epsilon_{\mathbb{F}}^d}{c}+\frac{\epsilon_{\mathbb{F}}}{\log|\mathbb{F}|}\sum_{i=0}^{d}(\epsilon_{\mathbb{F}})^{d-i}\left(0.6+\frac{2\log(n_i/2)+\lambda}{n_i}\right)\right). \tag{16}$$

由迭代式 $t_i=2t_{i-1}+l_i$ 也可以发现，随着 i 的增加，t_i 比 $2t_{i-1}$ 还多 l_i，从 i 到 $i+1$，编码长度每次增加一倍，因此码字中能达到的最大的 0 分量的相对个数在增加，因此能达到的最小相对 Hamming 距离在减少。如果 Δ_{C_d} 比较大，那么通过这种迭代方式得到的 C_i，可以得到极大概率有 $\Delta_{C_0}\geq\Delta_{C_1}\geq\ldots\geq\Delta_{C_d}$，从 $i=d$ 到 $i=0$，可以看到这种编码方式不会减小 Δ_{C_d}，在 IOPP 协议中，如果开始的最小相对 Hamming 距离比较大，那么到最后极大概率有 Δ_{C_0} 也依然会比较大，这一点在分析 IOPP 的 soundness 中也起了比较重要的作用。

References

- [ZCF23] Hadas Zeilberger, Binyi Chen, and Ben Fisch. "BaseFold: efficient field-agnostic polynomial commitment schemes from foldable codes." Annual International Cryptology Conference. Cham: Springer Nature Switzerland, 2024.
- [GJX15] Venkatesan Guruswami, Lingfei Jin, and Chaoping Xing. “Efficiently List-Decodable Punctured Reed-Muller Codes”. In: IEEE Transactions on Information Theory 63 (2015), pp. 4317–4324. url: https://api.semanticscholar.org/CorpusID: 14176561.