笔记：Basefold 在 List Decoding 下的 Soundness 证明

- Jade Xie jade@secbit.io
- Yu Guo yu.guo@secbit.io

在上一篇文章《Basefold 在 List Decoding 下的 Soundness 证明概览》中，梳理了 [H24] 论文中 soundness 证明的思路，本篇文章将沿着这个思路深入论文中的证明细节，主要是 [H24, Lemma 1] 的证明，其证明了 Basefold 协议在 commit 阶段的 soundness error。

Lemma 1 [H24, Lemma 1] (Soundness commit phase). Take a proximity parameter $\theta = 1 - \left(1 + \frac{1}{2 \cdot m}\right) \cdot \sqrt{\rho}$, with $m \geq 3$. Suppose that a (possibly computationally unbounded) algorithm P^* succeeds the commitment phase with $r \geq 0$ rounds with probability larger than

$$\varepsilon_C = \varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_r, \tag{1}$$

where $\varepsilon_0 = \varepsilon(\mathcal{C}_i, M, \theta)$ is the soundness error from Theorem 3, and

$$\varepsilon_i := \varepsilon(\mathcal{C}_i, 1, B_i, \theta) + \frac{1}{|F|}, \tag{2}$$

with $\varepsilon(\mathcal{C}_i, 1, B_i, \theta)$ being the soundness error from Theorem 4, where $B_i = \frac{|D|}{|D_i|} = 2^i$. Then $(g_0, \ldots, g_M)$ belongs to $\mathcal{R}$.

引理中提到的 [H24, Theorem 3] 就是在 list decoding 下针对 subcode 的 correlated agreement 定理，而 [H24, Theorem 4] 就是 [H24, Theorem 3] 的 weighted 版本。

关系 $\mathcal{R}$ 表示的含义是能得出 P^* 没有作恶，说明其承诺的多项式 $(g_0, \ldots, g_M)$ 既离对应的编码空间距离不超过 θ，同时也满足在查询点 $\vec{\omega} = (\omega_1, \ldots, \omega_n)$ 的值与承诺的值 $v_0, \ldots, v_M$ 是一致的，即

$$\mathcal{R} = \left\{ \begin{array}{c} \exists p_0, \ldots, p_M \in \mathscr{F}[X]^{<2^n} \text{ s.t.} \\ (g_0, \ldots, g_M) : d\left((g_0, \ldots, g_M), (p_0, \ldots, p_M)\right) < \theta \\ \wedge \bigwedge_{k=0}^{M} P_k\left(\omega_1, \ldots, \omega_n\right) = v_k \end{array} \right\}. \tag{3}$$

Lemma 1 说明的就是如果 P^* 在 commit 阶段成功的概率超过了 ε_C，那么我们能相信 P^* 没有作弊，其声称的关系 $\mathcal{R}$ 也是成立的。

在这里，还需要用数学语言去定义 P^* 在 commit 阶段的第 $0 \leq r \leq n$ 轮能成功的含义，这就是 [H24] 论文中给出的 α -good 的概念。从协议本身理解，P^* 能成功，意味着 verifier 拿到 P^* 发送过来的 $f_0, \Lambda_0, f_1, \Lambda_1, f_2, \Lambda_2, \ldots, \Lambda_{r-1}, f_r$，然后进行检查，一是进行 sumcheck 的检查，另一个是在 D_0 中随机选取 x，FRI 的折叠是正确的。首先这里的参数 $\alpha = 1 - \theta \in (0, 1)$，即

$$\alpha = \left(1 + \frac{1}{2 \cdot m}\right) \cdot \sqrt{\rho} \tag{4}$$

用 $\mathcal{F}_i$ 表示和 Reed-Solomon 编码 $\mathcal{C}_i = \mathrm{RS}_{2^{n-i}}[F, D_i]$ 相对应的多项式空间，其中 D_i 就是用映射 π 对 D 作用 i 次，即 $D_i = \pi^i(D), i = 0, \ldots, n$。因此与 $\mathcal{C}'_i \subseteq \mathcal{C}_i$ 相对应的多项式子空间定义为

$$\mathcal{F}'_i = \{p(X) \in \mathcal{F}_i : P(\omega_{i+1}, \ldots, \omega_n) = 0\}. \tag{5}$$

1. sumcheck 检查正确。意味着存在 $p_r(X) \in \mathcal{F}_r$，其对应的多元多项式为 P_r 满足

$$L((\omega_1, \ldots, \omega_r), (\lambda_1, \ldots, \lambda_r)) \cdot P_r(\omega_1, \ldots, \omega_n) = q_{r-1}(\lambda_r) \tag{6}$$

   根据 $q_i(X)$ 与 $\Lambda_i(X)$ 之间的关系，可以得到 P_r 需要满足

$$\begin{aligned} L((\omega_1, \ldots, \omega_r), (\lambda_1, \ldots, \lambda_r)) \cdot P_r(\omega_{r+1}, \ldots, \omega_n) &= q_{r-1}(\lambda_r) \\ &= L((\omega_1, \ldots, \omega_r), (\lambda_1, \ldots, \lambda_r)) \cdot \Lambda_{r-1}(\lambda_r) \end{aligned} \tag{1}$$

2. 折叠正确。需要满足

$$\left| \left\{ x \in D_0 : \begin{array}{c} (f_0, \ldots, f_r) \text{ satisfy all folding checks along } x \\ \wedge f_r(\pi^r(x)) = p_r(\pi^r(x)) \end{array} \right\} \right| \geq \alpha \cdot |D_0| \tag{2}$$

这里只有当在 D_0 中满足 folding check 的 x 的比例大于 α，经过 π^r 映射，到最后 verifier 才会通过。

当满足 1 和 2 两个条件时，就说这样的 $(f_0, \Lambda_0, f_1, \Lambda_1, f_2, \Lambda_2, \ldots, \Lambda_{r-1}, f_r)$ 对于 $(\lambda_0, \ldots, \lambda_r)$ 来说 α -good 的。

Lemma 1 证明

Lemma 1 的证明采用的是数学归纳法，先证明当 $r = 0$ 时结论是成立的，这里用到了 [H24, Therorem 3]。接着假设 Lemma 1 在 $0 \leq r < n$ 时成立，证明 Lemma 1 在 $r + 1$ 时结论也成立，在这个过程中就用到了带权重的 [H24, Theorem 4]，其证明思路与上篇文章介绍的思路类似。例如在第 $r + 1$ 轮，用随机数 λ_{r+1} 折叠之后得到 f_{r+1} 满足的条件入手，其离对应的编码空间距离比较近，并满足 sumcheck 约束，先推导出对应的 f'_{r+1} 满足一些条件，这样就能使用针对 subcode 的 correlated agreement 定理了。应用定理的结论，进而得到在折叠之前的 $f_{r,0}$ 与 $f_{r,1}$ 满足的性质，以此再得出 f_r 满足的性质。此时应用归纳假设，能得到在第 r 轮满足引理的条件，从而得出在第 r 轮的结论成立，也就证明了在第 $r + 1$ 轮引理成立。

证明：首先证明当 $r = 0$ 时引理是成立的。已知的条件是 P^* 在 commit 阶段成功的概率大于 $\varepsilon(\mathcal{C}_0, M, \theta)$，想证明得到的结论是 $(g_1, \ldots, g_M) \in \mathcal{R}$。根据条件以及 α -good 的定义，可以得到以大于 $\varepsilon(\mathcal{C}_0, M, \theta)$ 的概率 P^* 提供的 f_0 对 λ_0 来说是 α -good 的，那么对于考虑折叠之前的多项式 $g'_k = g_k - v_k$，距离对应的 subcode $\mathcal{C}'_0 \subseteq \mathcal{C}_0$ 不超过 θ (也就说明一致的地方大于 α)的概率为

$$\Pr\left[\lambda_0 : \exists p'_0 \in \mathcal{F}'_0 \text{ s.t. agree}\left(\sum_{k=0}^{M} g'_k \cdot \lambda_0^k, p'_0(X)\right) \geq \alpha\right] > \varepsilon(\mathcal{C}_0, M, \theta) \tag{7}$$

这里考虑的是多项式 $g'_k = g_k - v_k$ 而不是 g_k 的目的是，能让我们的分析进入线性子码 $\mathcal{C}'_0$ 的范围内，这样我们就能用 [H24, Theorem 3]，得到存在多项式

$$p'_0(X), \ldots, p'_M(X) \in \mathcal{F}'_0 \tag{8}$$

以及存在集合 $D'_0 \subseteq D$，满足

1. $|D'_0|/|D| \geq \alpha$
2. $p'_k(X)|_{D'_0} = g'_k(X)|_{D'_0}$

现在找到了多项式 $p'_0(X), \ldots, p'_M(X)$，那么对于多项式

$$p'_0(X) + v_0, \ldots, p'_M(X) + v_M \in \mathcal{F}_0 \tag{9}$$

就满足

$$(p'_k(X) + v_k)|_{D'_0} = (g'_k(X) + v_k)|_{D'_0} = g_k(X)|_{D'_0} \quad 0 \leq k \leq M \tag{10}$$

$p'_0(X) + v_0$ 对应的多元线性多项式 $P_k \in F[X_1, \ldots, X_n]$ 也满足 $P_k(\vec{\omega}) = v_k$，因此 $(g_1, \ldots, g_M) \in \mathcal{R}$。

现在假设引理在 $0 \leq r < n$ 时是成立的，想证明在 $r + 1$ 时引理依然成立。根据引理的条件，在第 $r + 1$ 轮，P^* 在 commit 阶段成功的概率超过 $(\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_r) + \varepsilon_{r+1}$。记 $\text{tr}_r = (\lambda_0, f_0, \Lambda_0, \ldots, \lambda_r, f_r, \Lambda_r)$ 组成的集合为 $\mathfrak{T}$，因此在

$$\Pr[\mathfrak{T}] > \varepsilon_0 + \ldots + \varepsilon_r \tag{11}$$

的条件下，P^* 成功的概率大于 ε_{r+1}，即

$$\Pr\left[\lambda_{r+1} : \begin{matrix}\exists f_{r+1} \text{ s.t. } (\lambda_0, f_0, \Lambda_0, \ldots, \lambda_r, f_r, \Lambda_r, f_{r+1}) \\ \text{is } \alpha\text{-good for } (\lambda_0, \ldots, \lambda_{r+1})\end{matrix}\right] > \varepsilon_{r+1} \tag{12}$$

由 α - good 的定义可以得到，对于满足 α -good 的 λ_{r+1}，存在一个满足 sumcheck 约束的多项式 $p_{r+1} \in \mathcal{F}_{r+1}$，使得

$$\text{agree}_{\nu_r}((1 - \lambda_{r+1}) \cdot f_{r,0} + \lambda_{r+1} \cdot f_{r,1}, p_{r+1}) \geq \alpha \tag{3}$$

这里的 ν_r 是一个子概率测度，其 density 函数定义为，对 $y \in D_{r+1}$ 有

$$\delta_r(y) := \frac{|\{x \in \pi^{-(r+1)}(y) : (f_0, \ldots, f_r) \text{ satisfies all folding checks along } x\}|}{|\pi^{-(r+1)}(y)|} \tag{13}$$

这里解释下式 (3) 表示的实质上就是 α -good 定义中的式 (2)。根据 agree 函数的定义，式 (3) 等价于

$$\frac{\nu_r(\{y \in D_{r+1} : ((1-\lambda_{r+1}) \cdot f_{r,0} + \lambda_{r+1} \cdot f_{r,1})(y) = p_{r+1}(y)\})}{|D_{r+1}|} \geq \alpha \tag{14}$$

先将在 D_{r+1} 中满足折叠关系的 y 组成一个集合，记为 S_{r+1}，再用 ν_r 函数对这个集合进行计算。

$$\begin{aligned}
\nu_r(S_{r+1}) &= \sum_{y \in S_{r+1}} \delta_r(y) \\
&= \sum_{y \in S_{r+1}} \frac{|\{x \in \pi^{-(r+1)}(y) : (f_0, \ldots, f_r) \text{ satisfies all folding checks along } x\}|}{|\pi^{-(r+1)}(y)|} \\
&= \sum_{y \in S_{r+1}} \frac{|\{x \in \pi^{-(r+1)}(y) : (f_0, \ldots, f_r) \text{ satisfies all folding checks along } x\}|}{2^{r+1}} \\
&:= \sum_{y \in S_{r+1}} \frac{|S_{y,0}|}{2^{r+1}} \\
&= \frac{\sum_{y \in S_{r+1}} |S_{y,0}|}{2^{r+1}}
\end{aligned} \tag{15}$$

因此

$$\begin{aligned}
\text{agree}_{\nu_r}((1-\lambda_{r+1}) \cdot f_{r,0} + \lambda_{r+1} \cdot f_{r,1}, p_{r+1}) &= \frac{\nu_r(S_{r+1})}{|D_{r+1}|} \\
&= \frac{\sum_{y \in S_{r+1}} |S_{y,0}|}{2^{r+1} \cdot |D_{r+1}|} \\
&= \frac{\sum_{y \in S_{r+1}} |S_{y,0}|}{|D_0|}
\end{aligned} \tag{16}$$

上式中分子 $\sum_{y \in S_{r+1}} |S_{y,0}|$ 表示的含义正是在 D_0 中满足第 $r+1$ 次折叠正确，同时 $(f_0, \ldots, f_r)$ 折叠检查也是正确的。(3) 式就变为

$$\sum_{y \in S_{r+1}} |S_{y,0}| \geq \alpha \cdot |D_0| \tag{17}$$

这与 α -good 定义中式 (2) 是完全一致的。接下来根据在上篇文章中介绍的 soundness 证明思路，由于 $p_{r+1}(X)$ 对应的多元线性多项式 P_{r+1} 满足 sumcheck 约束，因此满足

$$\begin{aligned}
L((\omega_1, \ldots, \omega_{r+1}), (\lambda_1, \ldots, \lambda_{r+1})) \cdot P_{r+1}(\omega_{r+2}, \ldots, \omega_n) &= q_r(\lambda_{r+1}) \\
&= L((\omega_1, \ldots, \omega_{r+1}), (\lambda_1, \ldots, \lambda_{r+1})) \cdot \Lambda_r(\lambda_{r+1})
\end{aligned} \tag{18}$$

推出

$$\begin{aligned}
L((\omega_1, \ldots, \omega_r), (\lambda_1, \ldots, \lambda_r)) \cdot L(\omega_{r+1}, \lambda_{r+1}) \cdot P_{r+1}(\omega_{r+2}, \ldots, \omega_n) \\
= L((\omega_1, \ldots, \omega_r), (\lambda_1, \ldots, \lambda_r)) \cdot L(\omega_{r+1}, \lambda_{r+1}) \cdot \Lambda_r(\lambda_{r+1})
\end{aligned} \tag{19}$$

对于 λ_{r+1} 的选择，有 $1/|F|$ 的概率使得 $L(\omega_{r+1}, \lambda_{r+1}) = 0$，得出上式成立。因此除了 $1/|F|$ 的概率，依然有超过

$$\varepsilon_{r+1} - \frac{1}{|F|} = \varepsilon(\mathcal{C}_{i+1}, 1, B_{r+1}, \theta) \tag{20}$$

的概率，使得多项式 $p'_{r+1} = p_{r+1} - \Lambda_r(\lambda_{r+1}) \in \mathcal{F}'_{r+1}$，以及 $f'_{r,0} = f_{r,0} - \Lambda_r(0)$，$f'_{r,1} = f_{r,1} - \Lambda_r(1)$ 满足

$$\text{agree}_{\nu_r}((1-\lambda_{r+1}) \cdot f'_{r,0} + \lambda_{r+1} \cdot f'_{r,1}, p'_{r+1}) \geq \alpha \tag{21}$$

上面满足的条件可以写为

$$\Pr\left[\lambda_{r+1} : \begin{array}{c} \exists p'_{r+1} \in \mathcal{F}'_{r+1} \text{ s.t.} \\ \text{agree}_{\nu_r}((1-\lambda_{r+1}) \cdot f'_{r,0} + \lambda_{r+1} \cdot f'_{r,1}, p'_{r+1}) \geq \alpha \end{array}\right] > \varepsilon(\mathcal{C}_{i+1}, 1, B_{r+1}, \theta) \tag{22}$$

这也就满足了 [H24, Theorem 4] 带权重的 correlated agreement 定理的条件，因此可以得到存在多项式 $p'_{r,0}(X), p'_{r,1}(X) \in \mathcal{F}'_{r+1}$，以及集合 $A_{r+1} \subseteq D_{r+1}$ 满足：

1. $\nu_r(A_{r+1}) \geq 1-\theta$
2. $p'_{r,0}(X)|_{A_{r+1}} = f'_{r,0}(X)|_{A_{r+1}}, p'_{r,1}(X)|_{A_{r+1}} = f'_{r,1}(X)|_{A_{r+1}}$

现在已经找到了多项式 $p'_{r,0}(X), p'_{r,1}(X)$，因此存在多项式

$$p_{r,0}(X) = p'_{r,0}(X) + \Lambda_r(0), \quad p_{r,1}(X) = p'_{r,1}(X) + \Lambda_r(1) \in \mathcal{F}_{r+1} \tag{23}$$

而

$$f_{r,0}(X) = f'_{r,0}(X) + \Lambda_r(0), \quad f_{r,1}(X) = f'_{r,1}(X) + \Lambda_r(1) \tag{24}$$

根据 correlated agreement 给出的结论 2，可以得到

$$p_{r,0}(X)|_{A_{r+1}} = f_{r,0}(X)|_{A_{r+1}}, \quad p_{r,1}(X)|_{A_{r+1}} = f_{r,1}(X)|_{A_{r+1}} \tag{25}$$

对于 $p_{r,0}(X), p_{r,1}(X)$ 相对应的多元线性多项式 $P_{r,0}$ 以及 $P_{r,1}$，根据 $\mathcal{F}'_r$ 的定义，可以得到

$$\begin{aligned} P_{r,0}(\omega_{r+2}, \ldots, \omega_n) &= \Lambda_r(0) \\ P_{r,1}(\omega_{r+2}, \ldots, \omega_n) &= \Lambda_r(1) \end{aligned} \tag{26}$$

将集合 A_{r+1} 中的点通过 π 的逆映射得到 $A_r = \pi^{-1}(A_{r+1}) \subseteq D_r$，在这些点一定满足 f_r 和

$$p_r(X) = p_{r,0}(X^2) + X \cdot p_{r,1}(X^2) \in \mathcal{F}_r \tag{27}$$

是一致的。对于与 $p_r(X)$ 相对应的多元线性多项式 P_r，其满足

$$\begin{aligned} P_r(\omega_{r+1}, \omega_{r+2}, \ldots, \omega_n) &= (1-\omega_{r+1}) \cdot P_{r,0}(\omega_{r+2}, \ldots, \omega_n) + \omega_{r+1} \cdot P_{r,1}(\omega_{r+2}, \ldots, \omega_n) \\ &= (1-\omega_{r+1}) \cdot \Lambda_r(0) + \omega_{r+1} \cdot \Lambda_r(1) \\ &= L(\omega_{r+1}, 0) \cdot \Lambda_r(0) + L(\omega_{r+1}, 1) \cdot \Lambda_r(1) \end{aligned} \tag{28}$$

由此可以得到在第 r 轮的 sumcheck 是满足的：

$$\begin{aligned} &L(\omega_1, \ldots, \omega_r, \lambda_1, \ldots, \lambda_r) \cdot P_r(\omega_{r+1}, \omega_{r+2}, \ldots, \omega_n) \\ &\quad = L(\omega_1, \ldots, \omega_r, \lambda_1, \ldots, \lambda_r) \cdot L(\omega_{r+1}, 0) \cdot \Lambda_r(0) \\ &\quad\quad + L(\omega_1, \ldots, \omega_r, \lambda_1, \ldots, \lambda_r) \cdot L(\omega_{r+1}, 1) \cdot \Lambda_r(1) \\ &\quad = q_r(0) + q_r(1) \\ &\quad = q_{r-1}(\lambda_r) \end{aligned} \tag{29}$$

现在得到了在第 r 轮的 sumcheck 是满足的，接下来需要考虑折叠关系是否满足。考虑 $x \in \pi^{-1}(A_r)$，有

$$\begin{aligned} &\frac{|\{x \in \pi^{-r}(A_r) : \text{all folding checks hold for } f_0, \ldots, f_r\}|}{|D_0|} \\ &= \frac{1}{|D_0|} \cdot \sum_{y \in A_{r+1}} \delta(y) \cdot |\pi^{-(r+1)}(y)| \\ &= \frac{2^{r+1}}{|D_0|} \cdot \sum_{y \in A_{r+1}} \delta(y) \\ &= \frac{1}{|D_{r+1}|} \cdot \sum_{y \in A_{r+1}} \delta(y) \\ &= \nu_r(A_{r+1}) \end{aligned} \tag{30}$$

前面通过 correlated agreement 定理已经得到 $\nu_r(A_{r+1}) \geq \alpha$，因此在 D_0 中的 x 能满足 folding check 的比例超过 α。综合在第 r 轮的 sumcheck 约束以及折叠关系，得到 $(f_0, \Lambda_0, \ldots, f_r, \Lambda_r)$ 对于 $(\lambda_0, \ldots, \lambda_r)$ 是 α -good 的。由于产生这样的 trace 的集合的概率

$$\Pr[\mathfrak{T}] > \varepsilon_0 + \ldots + \varepsilon_r \tag{31}$$

因此其满足引理的条件，由归纳假设，在第 r 轮引理成立，因此可以得到结论，$(g_0, \ldots, g_M) \in \mathcal{R}$，至此就证明了在第 $r+1$ 轮引理也是成立的。从而得证引理成立。 □

References

- [H24] Ulrich Haböck. "Basefold in the List Decoding Regime." *Cryptology ePrint Archive*(2024).