

Math Companion to Soundcalc

December 4, 2025

1 Notation and Preliminaries

1.1 Fields

Fields of size q are denoted as \mathbb{F}_q or simply \mathbb{F} .

1.2 Reed-Solomon codes

We use the following notation:

- $RS[\mathbb{F}, S, \rho]$: Reed-Solomon code over the field \mathbb{F} with evaluation domain S and rate ρ .
- $\deg(f)$: degree of the polynomial f .

2 FRI

This section contains the soundness formula for the FRI protocol.

2.1 FRI protocol analysis

- m_J — Johnson parameter.
- r_{FRI} — number of FRI rounds.
- Folding factors $\widehat{\text{folds}} = [k_0, k_1, \dots, k_{r_{FRI}-1}]$;
- t — number of queries.
- θ .
- $b_{\text{grind}, Q}$ — grinding parameter for the query phase.
- n — witness size.
- b_{hash} — number of bits in the hash function output.
- b_{proof} — proof size in bits.
- s_{batch} — batch size.

2.2 Fixed constants

We fix the following constants for the soundness calculator:

- $m_J = 16$. Set in

```
fri.py/get_johnson_parameter_m()
```

-

2.3 Soundness formula

Query phase error:

$$\epsilon_{\text{query}} = (1 - \theta)^t \cdot 2^{-b_{\text{grind}, Q}} \quad (1)$$

The query phase error without grinding is computed as per [?] ¹

2.4 Proof size

This calculation is performed in

`fri.py/get_FRI_proof_size_bits()`

. The FRI proof contains two parts: Merkle roots, and one "openings" per query, where an "opening" is a Merkle path for each folding layer. For each layer we count the size that this layer contributes, which includes the root and all Merkle paths.

Initial round: one root and one path per query. We assume that for the initial functions, there is only one Merkle root, and each leaf i for that root contains symbols i for all initial functions.

Folding rounds: we assume that "siblings" for the following layers are grouped together in one leaf. This is natural as they always need to be opened together.

The proof size is calculated as follows:

$$b_{\text{proof}} = b_{\text{hash}} + t \cdot MP\left(\underbrace{\frac{n}{\text{folds}[0]}}_{\text{Initial round}}, s_{\text{btch}}, |\mathbb{F}|, b_{\text{hash}}\right) + \\ + \underbrace{\sum_{1 \leq i \leq r_{\text{FRI}} - 2} \left(b_{\text{hash}} + t \cdot MP\left(\frac{n}{\prod_{1 \leq j \leq i} \text{folds}[j]}, s_{\text{btch}}, |\mathbb{F}|, b_{\text{hash}}\right) \right)}_{\text{Folding rounds but last}} + \\ + \underbrace{\left(b_{\text{hash}} + t \cdot MP\left(\frac{n}{\text{folds}[r_{\text{FRI}} - 1] \prod_{1 \leq j \leq r_{\text{FRI}} - 1} \text{folds}[j]}, s_{\text{btch}}, |\mathbb{F}|, b_{\text{hash}}\right) \right)}_{\text{Last folding round}} \quad (2)$$

where $MP(n, s, q, b)$ is the Merkle path size calculated as

$$MP(n, s, q, b) = \underbrace{sq}_{\text{leaf size}} + \underbrace{sq}_{\text{sibling}} + \underbrace{\lceil \log_2 n \rceil \cdot b}_{\text{co-path}} \quad (3)$$

¹Code refers to (7) and Th2 of [Hab22]