Improving the BCIKS20 List-Decoding Bound: From Exponent 7 to 6

Antonio Sanso
Ethereum Foundation

Abstract

We give a modification of the BCIKS20 proof in the list-decoding regime. The original analysis loses two powers of the Y-degree parameter D_Y at the "cleanup" step (their Eq. (5.14)), via the product $d_H \cdot d$ when working per factor H. We reorganize around the squarefree part $R = \mathrm{sqfree}(Q(x_0, Y, Z))$ and apply a global discriminant bound, so that only $\deg_Y R \cdot \deg_Z R$ appears. This collapses the loss from $D_Y^2 D_{YZ}$ to $D_Y D_{YZ}$ and removes the extra d_H multiplier. Crucially, we leave the earlier lower bound (5.13) unchanged and we keep the per-factor use of Lemma A.1 in §5.2.7 and Appendix C, so all downstream arguments remain intact with additional slack.

1 Introduction

Let $\mathbb{F}$ be a finite field, $\mathcal{L} \subseteq \mathbb{F}$ a set of evaluation points with $|\mathcal{L}| = n$, and $\mathrm{RS}[\mathbb{F}, \mathcal{L}, d]$ the Reed–Solomon code of degree $< d$ and rate $\rho := d/n$. Define $\eta := 1 - \sqrt{\rho} - \delta$, where δ is the decoding radius.

Theorem 1 (List-agreement with exponent 6)**.** *Fix $m \geq 2$ and δ with $\frac{1-\rho}{2} < \delta < 1 - \sqrt{\rho}$. For functions $f_1, \ldots, f_m : \mathcal{L} \to \mathbb{F}$ and random $r \in \mathbb{F}$, set $W(r) = \sum_{j=1}^{m} r^{j-1} f_j$. If*

$$\Pr_{r \leftarrow \mathbb{F}}\Big[\, \Delta\big(W(r), \mathrm{RS}[\mathbb{F}, \mathcal{L}, d]\big) \leq \delta \,\Big] \;>\; \mathrm{err}^{\dagger}((, d, , , \rho), \delta, m) \;:=\; \frac{(m-1)\, d^2}{|\mathbb{F}| \cdot \Big(2 \cdot \min\{\, 1 - \sqrt{\rho} - \delta,\; \sqrt{\rho}/20 \,\}\Big)^6},$$

then there exists $u \in \mathrm{RS}[\mathbb{F}, \mathcal{L}, d]$ and $S \subseteq \mathcal{L}$ with $|S| \geq (1-\delta)n$ such that $f_i|_S = u|_S$ for all $i \in [m]$.

2 Equation (5.8) and (5.13)

From Claim 5.4 and equation (5.3) in [BCIKS20], one has

$$|S| \;>\; \frac{(1 + \frac{1}{2m})^7 m^7}{3\rho^{3/2}}\, n^2 \;\geq\; 2 D_Y^3 D_X D_{YZ}. \tag{5.8}$$

Remark 1 (On the standing hypothesis)**.** *Equation (5.8) in [BCIKS20] lower-bounds $|S|$ by a quantity $\geq 2D_Y^3 D_X D_{YZ}$. Our patched analysis needs only $|S| \geq 2D_Y^2 D_X D_{YZ}$, but we* keep (5.8) and (5.13) unchanged*. This ensures compatibility with §5.2.7 and App. C, where Lemma A.1 requires a per-factor multiplier d_H. The effect of the patch is only to improve the subtraction of "bad z" after (5.13).*

By Claim 5.7 there exist R, H with

$$|S_{x_0,R,H}| \;\geq\; \frac{|S|}{D_Y} \;>\; 2 D_Y^2 D_X D_{YZ}. \tag{5.13}$$

We emphasize that (5.13) remains as in the original proof.

3 Discriminant lemmas for cleanup

Lemma 1 (Discriminant degree). *Let $R(Y,Z) \in \mathbb{F}[Z][Y]$ be squarefree in Y with $\deg_Y R \le D_Y$ and $\deg_Z R \le D_{YZ}$. Then*

$$\deg_Z \mathrm{Disc}_Y(R) \;\le\; (2\deg_Y R - 1)\deg_Z R \;\le\; (2D_Y - 1)D_{YZ},$$

and

$$\deg_Z\big(\mathrm{lc}_Y(R)\big) \le D_{YZ}.$$

Lemma 2 (Few bad z via discriminant). *Fix x_0 and set $R(Y,Z) := \mathrm{sqfree}\big(Q(x_0,Y,Z)\big)$. Let*

$$B \;:=\; \big\{z :\; \mathrm{Disc}_Y(R)(z) = 0 \quad \text{or} \quad \mathrm{lc}_Y(R)(z) = 0\big\}.$$

Then

$$|B| \;\le\; (2D_Y - 1)D_{YZ} + D_{YZ} \;\le\; 3D_Y D_{YZ}.$$

4 Patched version of (5.14) and the uniqueness step

Proposition 1 (Patched cleanup). *With B as in Lemma 2, define $S' := S_{x_0,R,H} \setminus B$. Then*

$$\boxed{|S'| \;\ge\; \tfrac{|S|}{D_Y} \;-\; c\,D_Y D_{YZ}}$$

for an absolute constant c (e.g. $c = 3$).

Proof. From Claim 5.7 and (5.13), $|S_{x_0,R,H}| \ge |S|/D_Y$. Subtracting the at most $|B| \le cD_Y D_{YZ}$ values of z from Lemma 2 gives the result. □

The uniqueness step (patched)

In §5.2.6 of [BCIKS20], after obtaining (5.14) they apply Lemma A.1 to the power-series expansions $P_z(X) = \sum_t \pi_z(\alpha_t)(X - x_0)^t$. To conclude that all higher coefficients α_t vanish, they require

$$|S'| \;>\; d_H\,\Lambda(\beta_t),$$

where $d_H = \deg_Y(H)$ and $\Lambda(\beta_t) \le (2D_X - 1)\,dD$ by Claim A.2, with $d = \deg_Y(R)$ and $D = \deg_Z(R)$. Thus the original proof enforced

$$|S'| \;\ge\; d_H\,d\,D\,(2D_X - 1). \tag{Uniq-BCIKS}$$

With Proposition 1, our set S' is strictly larger, since we subtract only $O(D_Y D_{YZ})$ rather than $O(D_Y^2 D_{YZ})$. Hence it suffices to require

$$\boxed{|S'| \;\ge\; d\,D\,(2D_X - 1)} \tag{Uniq-patched}$$

without the extra d_H multiplier. Because $d \le D_Y$ and $D \le D_{YZ}$, this condition follows from the weaker standing assumption $|S| \ge 2D_Y^2 D_X D_{YZ}$. This is the precise point where the exponent improves from 7 to 6.

Remark 2 (On later sections). *In §5.2.7 and App. C, BCIKS apply Lemma A.1 inside the extension $\mathbb{F}_q(Z)[T]/(H_e)$, which intrinsically carries a multiplier $d_H = \deg_Y H$. We do not attempt to remove d_H there. Instead we note that since our patched Proposition 1 gives a* larger *surviving set S', all subsequent inequalities (such as $|S_x^0| > d_H\Lambda(\beta)$) remain true with more slack. Thus the downstream arguments are unchanged.*

5 Consequences for the FRI protocol

The analysis in [BCIKS20] was motivated by the soundness of the FRI (Fast Reed–Solomon IOPP) protocol. The key parameter is the *list-agreement bound*: if a prover's function $f : \mathcal{L} \to \mathbb{F}$ agrees with too many low-degree polynomials on a large set S, then f must essentially be a codeword. The size of S that forces uniqueness determines the soundness error of FRI.

Exponent 7 in BCIKS. In the original analysis, the threshold

$$|S| \gtrsim D_Y^3 D_X D_{YZ}$$

translated into a soundness error that scales like η^{-7} in the distance parameter $\eta = 1 - \sqrt{\rho} - \delta$. This was the dominant term in the FRI soundness exponent.

Patched exponent 6. With our global discriminant cleanup, the threshold improves to

$$|S| \gtrsim D_Y^2 D_X D_{YZ},$$

so the soundness error decays as η^{-6}. This strictly strengthens the FRI analysis: for the same number of verifier queries, the cheating probability is smaller by a factor of η. Equivalently, to achieve a target soundness error (say 2^{-128}), the verifier may use fewer queries.

Asymptotic and practical impact. For typical cryptographic regimes, η is on the order of $1/\log n$, so the improvement from exponent 7 to exponent 6 yields a nontrivial reduction in proof size or query complexity. Conceptually, it shows that the BCIKS20 analysis was not tight, and that the FRI soundness exponent can be sharpened without altering the protocol.

Outlook. It remains an open question whether further algebraic refinements could push the exponent even lower. Any such improvement would immediately transfer to tighter soundness guarantees for FRI and related RS-based IOPPs.

Acknowledgments. We are grateful to Dan Carmon for insightful discussions and clarifications.

References

[BCIKS20] E. Ben-Sasson, D. Carmon, Y. Ishai, S. Kopparty, and S. Saraf. Proximity gaps for Reed–Solomon codes. In *FOCS 2020*, pp. 900–909. IEEE, 2020. See §5.2.4–5.2.6 and Appendix A for the degree bookkeeping behind Eqs. (5.13)–(5.14).