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

Antonio Sanso
Ethereum Foundation

Abstract

We give a local modification of the BCIKS20 proof of the Reed–Solomon agreement theorem in the list-decoding regime. By replacing a triple union bound over Y-factors with a single discriminant/subresultant argument applied to the Y-squarefree part of the interpolated polynomial, we improve the error threshold dependence from η^{-7} to η^{-6}, where $\eta = 1 - \sqrt{\rho} - \delta$.

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 the relative distance slack

$$\eta \;:=\; 1 - \sqrt{\rho} - \delta,$$

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

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

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 $i \in [m]$.

Remark 1. *BCIKS20 prove the same statement with $\Big(2 \cdot \min\{\, 1 - \sqrt{\rho} - \delta,\; \sqrt{\rho}/20 \,\}\Big)^{6}$ raised to the 7th power. Our modification removes one factor of D_Y from their union bound over Y-factors. Consequently the threshold improves from η^{-7} to η^{-6}.*

2 Proof Sketch

The proof follows BCIKS20 verbatim up to their condition

$$|S| \;>\; C \cdot D_Y^3 D_X D_{YZ}.$$

We show that it suffices to require

$$|S| \;>\; C \cdot D_Y^2 D_X D_{YZ}.$$

The only change is how we handle "bad" values of z after specializing $X = x_0$ and taking a single Y-factor. Instead of union-bounding across factors, we pass to the Y-squarefree part and control singular fibers with one discriminant bound. The details are in the appendix.

Plugging the known interpolation degree bounds

$$D_Y = \Theta(m\sqrt{\rho}), \quad D_X = \Theta(m\sqrt{\rho}\,n), \quad D_{YZ} = \Theta\Big(\tfrac{m^3}{\sqrt{\rho}}\,n\Big),$$

this change removes one power of m, thus reducing the exponent in η from 7 to 6.

A Appendix: Bounding Bad z via Discriminant

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*

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

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

Proof. Write $d = \deg_Y R$. Then $\mathrm{Disc}_Y(R) = (-1)^{d(d-1)/2}\,\mathrm{Res}_Y(R, \partial_Y R)$, and the Sylvester resultant has Z-degree at most $(2d-1)\deg_Z R$. This yields the claimed bounds. $\square$

Lemma 2 (Squarefree preserves linear factors)**.** *Let K be a field and $F(Y) \in K[Y]$. If $(Y-a) \mid F(Y)$, then $(Y-a) \mid \mathrm{sqfree}(F)$, where $\mathrm{sqfree}(F) := F/\gcd(F, \partial_Y F)$.*

Proof. Write $F = (Y-a)^k G$ with $k \ge 1$ and $\gcd(Y-a, G) = 1$. Then $\partial_Y F = k(Y-a)^{k-1}G + (Y-a)^k \partial_Y G$, so $\gcd(F, \partial_Y F) = (Y-a)^{k-1}$, yielding $\mathrm{sqfree}(F) = (Y-a)G$. $\square$

Lemma 3 (Few bad z)**.** *Let R be as in Lemma 1 and define*

$$B := \{z \in \mathbb{F} : R(Y,z) \text{ is not squarefree in } Y \text{ or } \mathrm{lc}_Y(R)(z) = 0\}.$$

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

Proof. If $R(Y,z)$ has a multiple root, then $\mathrm{Disc}_Y(R)(z) = 0$. If its leading coefficient vanishes, then $\mathrm{lc}_Y(R)(z) = 0$. Thus B is contained in the roots of these two polynomials, and the degree bound follows from Lemma 1. $\square$

Proposition 1 (Improved survival, factor-after-specialization)**.** *Let $Q(X,Y,Z) \in \mathbb{F}[X,Y,Z]$ with $\deg_Y Q \le D_Y$, $\deg_X Q \le D_X$, $\deg_Z Q \le D_{YZ}$. Let $T \subseteq \mathbb{F}$ be the set of "good" z such that $Y - P_z(X) \mid Q(X,Y,z)$ in $\mathbb{F}[X,Y]$. Fix any $x_0 \in \mathcal{L}$ and set*

$$R(Y,Z) \;:=\; \mathrm{sqfree}\big(Q(x_0,Y,Z)\big) \in \mathbb{F}[Z][Y].$$

Let $B \subseteq \mathbb{F}$ be as in Lemma 3 for this R. Then

$$\big|\{\, z \in T \setminus B :\; (Y - P_z(x_0)) \mid R(Y,z) \,\}\big| \;\ge\; |T| - |B| \;\ge\; |T| - 3D_Y D_{YZ}.$$

Moreover, writing $R = \prod_{i=1}^{t} H_i$ *as a product of distinct irreducible factors in* $\mathbb{F}[Z][Y]$ *(so* $\sum_i \deg_Y H_i = \deg_Y R \le D_Y$*), there exists an* $i^\star$ *such that*

$$\bigl|\{\, z \in T \setminus B : \; (Y - P_z(x_0)) \mid H_{i^\star}(Y, z) \,\}\bigr| \;\ge\; \frac{|T| - 3D_Y D_{YZ}}{D_Y}.$$

In particular, if $|T| > C\, D_Y^2 D_{YZ}$ *for a sufficiently large absolute* C*, then the right-hand side is* > 0.

Proof. For any $z \in T$, we have $Q(X, P_z(X), z) \equiv 0$, hence $Q(x_0, P_z(x_0), z) = 0$. If $z \notin B$, then $R(Y, z)$ is a nonzero squarefree polynomial and Lemma 2 implies $(Y - P_z(x_0)) \mid R(Y, z)$. This proves the first inequality. For the second, partition the (simple) roots of $R(Y, z)$ among the factors $H_i(Y, Z)$ and apply the pigeonhole principle using $\sum_i \deg_Y H_i \le D_Y$. □

Consequence for the main argument. Compared to the triple union bound in BCIKS20, Proposition 1 replaces a factor of D_Y by a single discriminant loss $O(D_Y D_{YZ})$ after specializing $X = x_0$ and passing to the Y-squarefree part. With the standard interpolation choices

$$D_Y = \Theta(m\sqrt{\rho}), \quad D_X = \Theta(m\sqrt{\rho}\, n), \quad D_{YZ} = \Theta\Bigl(\tfrac{m^3}{\sqrt{\rho}}\, n\Bigr),$$

this removes one net power of m (equivalently, one power of η^{-1}) from the threshold, improving the exponent from 7 to 6.

References

[BCIKS20] E. Ben-Sasson, D. Carmon, Y. Ishai, S. Kopparty, and S. Saraf. Proximity gaps for Reed–Solomon codes. In *Proceedings of the 61st IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 900–909. IEEE Computer Society, 2020. 10.1109/FOCS46700.2020.00088.