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 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 of degree parameters $d_H \cdot d$ (with $d_H = \deg_Y H$ for the chosen factor and $d = \deg_Y R$ for the squarefree part). We replace that per-factor degeneracy bound by a single discriminant bound on the Y-squarefree product, which collapses the loss from $D_Y^2 D_{YZ}$ to $D_Y D_{YZ}$. Keeping the same pigeonhole step (their Claim 5.7), this lowers the overall threshold from $D_Y^3 D_X D_{YZ}$ to $D_Y^2 D_X D_{YZ}$, improving the η-exponent from 7 to 6.

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 $i \in [m]$.

Remark 1 (Where D_Y^2 arises in BCIKS)**.** *In Section 5.2.4 (Claim 5.7) they factor $Q(x_0, Y, Z)$ into at most D_Y irreducible Y-factors H_{ij} and use pigeonhole to get $|S_{x_0,R,H}| \geq |S|/D_Y$ (their Eq. (5.13)); this costs one D_Y. Immediately after, in Eq. (5.14), they subtract the number of "bad" z for the chosen H by bounding*

$$|S'| \;\geq\; |S_{x_0,R,H}| \;-\; (\deg W + d_H\,\Lambda(\xi)) \;\geq\; |S_{x_0,R,H}| \;-\; d_H \cdot d \cdot D,$$

where $d_H = \deg_Y H$, $d = \deg_Y R$ (with R the Y-squarefree part), and $D = \deg_Z R$ (notations from Appendix A). Relaxing $d_H \leq D_Y$, $d \leq D_Y$, $D \leq D_{YZ}$ yields the $D_Y^2 D_{YZ}$ term. No *factor is counted twice; the quadratic comes from the* product *$d_H \cdot d$, not from enumerating H_{ij} twice.*

2 Patch: global discriminant cleanup at the (5.14) step

We keep the BCIKS interpolation, the choice of a good x_0 (Claim 5.6), and the pigeonhole step (Claim 5.7). The only change is the cleanup that follows (5.13).

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*

$$\deg_Z \mathrm{Disc}_Y(R) \;\le\; (2\deg_Y R - 1)\deg_Z R \;\le\; (2D_Y - 1)D_{YZ}, \quad \textit{and} \quad \deg_Z\big(\mathrm{lc}_Y(R)\big) \le D_{YZ}.$$

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

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

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

Proposition 1 (Patched version of (5.14)). *With B as above and the H chosen by pigeonhole (Claim 5.7), define $S' := S_{x_0,R,H} \setminus B$. Then*

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

for an absolute constant c (e.g. $c = 3$ from Lemma 2).

Proof. By Claim 5.7, $|S_{x_0,R,H}| \ge |S|/D_Y$. Removing B discards at most $|B| \le cD_Y D_{YZ}$ values of z by Lemma 2. □

Remark 2 (Why bad z must be removed). *If many z correspond to multiple roots (inseparable fibers) or degree drops, one cannot promote "$Y - P_z(x_0)$ divides $H(Y,z)$ for many z" to a global factor $Y - \Gamma(Z)$ dividing $H(Y,Z)$. A standard counterexample over characteristic p is $H(Y,Z) = (Y-Z)^2 + (Z^p - Z)$, for which $(Y-Z) \mid H(Y,z)$ for every $z \in \mathbb{F}_p$, yet $Y - Z \nmid H(Y,Z)$.*

Consequence for the threshold

BCIKS need $|S'| \ge 2\,d_H\,d\,D\,D_X$ (as assembled in §5.2.5 using Appendix A). With Proposition 1,

$$\frac{|S|}{D_Y} \;-\; c\,D_Y D_{YZ} \;\ge\; 2\,d_H\,d\,D\,D_X.$$

In the worst case $d_H \le D_Y$, $d \le D_Y$, $D \le D_{YZ}$, this is implied by

$$|S| \;\ge\; 2\,D_Y^2\,D_X\,D_{YZ} \;+\; c\,D_Y^2\,D_{YZ} \;=\; O\big(D_Y^2 D_X D_{YZ}\big),$$

improving BCIKS's $O(D_Y^3 D_X D_{YZ})$. This is precisely the point Dan raised: using $(|S| - |B|)/D_Y$ still yields D_Y^3 *unless* $|B| = O(D_Y D_{YZ})$; Lemma 2 provides exactly that.

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 §5.2.4–5.2.5 and Appendix A for the degree bookkeeping behind Eqs. (5.13)–(5.14).