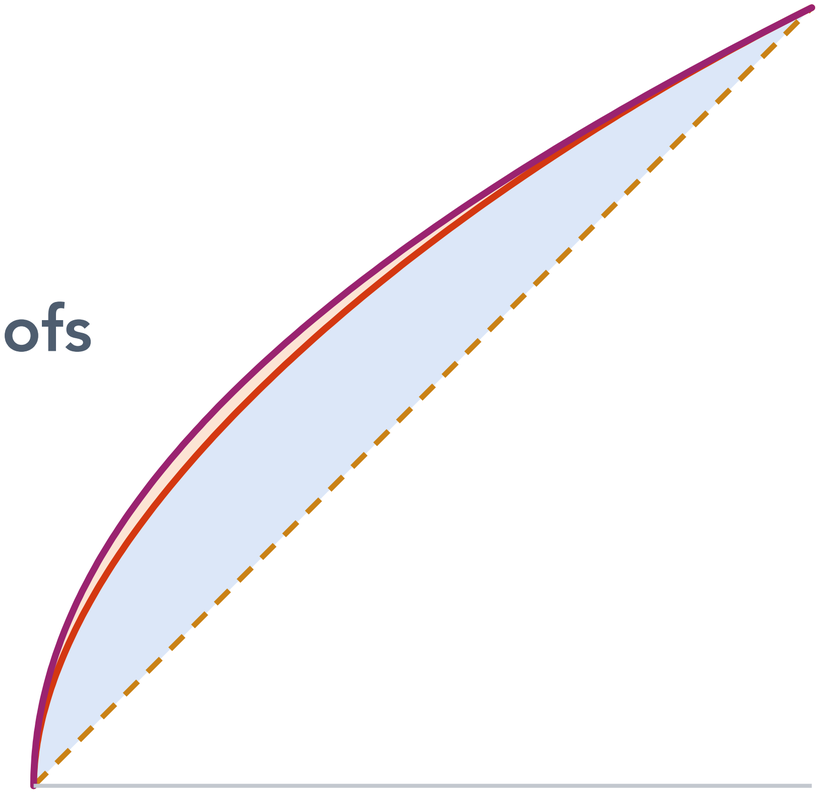
Reed–Solomon Codes Beyond Johnson

Efficient Decoding and Smaller Cryptographic Proofs



Quang Dao, Scott Duke Kominers, Justin Thaler

STOC 2027 Video Submission

Reed–Solomon List Decoding

From the Johnson bound to capacity

Reed–Solomon code

$P \in \mathbb{F}[X]_{<k} \;\mapsto\; (P(\alpha_1), \ldots, P(\alpha_n))$

rate $\rho = k/n$; fixed evaluation points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$

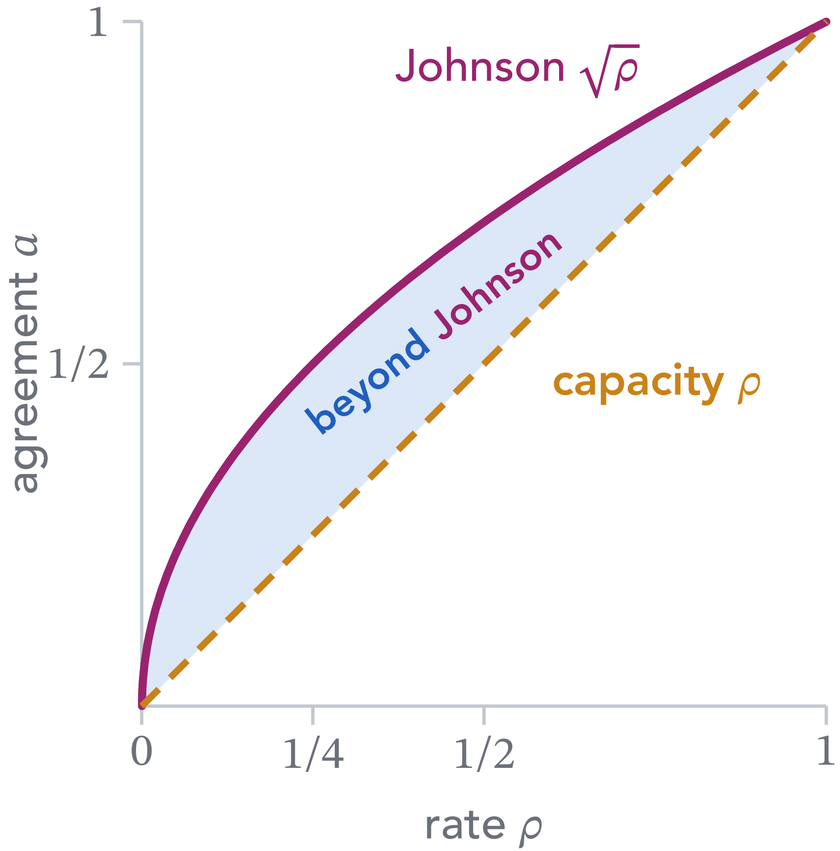
List decoding

Given received word $y \in \mathbb{F}^n$

Goal: output every P agreeing with y in at least an positions

Guruswami–Sudan: $a > \sqrt{\rho}$, the Johnson bound [Sud97, GS99]

Capacity: $a = \rho + \delta$, list size $\mathrm{poly}(n)$



Goal: list decode beyond Johnson on any evaluation set, with an efficient decoder

Mutual Correlated Agreement

Proof systems combine words

Test one random combination

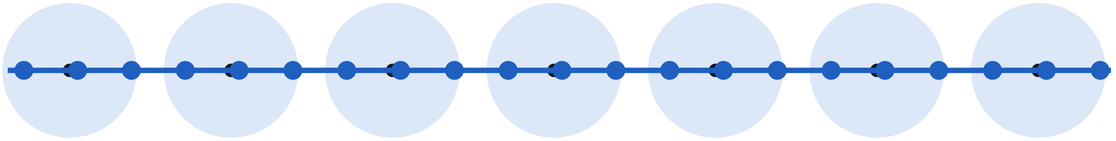
FRI, STIR and WHIR check $f + z\,g$, $z \in \mathbb{F}_q$,
at a few positions [BBHR18, ACFY24a, ACFY24b]

MCA, outside a small set $\mathscr{E}$

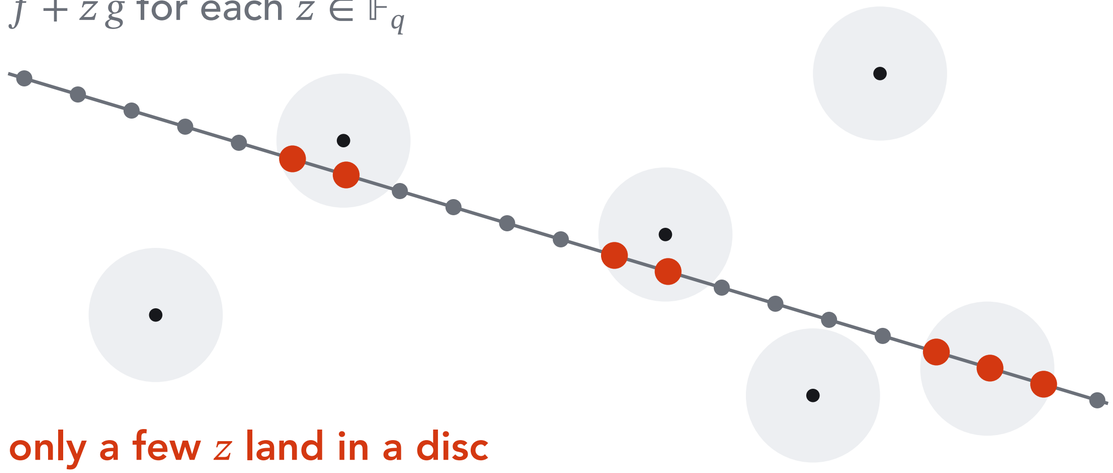
every P close to $f + z\,g$ is $P = F + z\,G$,
with F, G agreeing with f, g wherever
P agrees with $f + z\,g$

$z \in \mathscr{E}$: cancellation creates extra agreements

$F + z\,G$: shared agreement, every z



$f + z\,g$ for each $z \in \mathbb{F}_q$



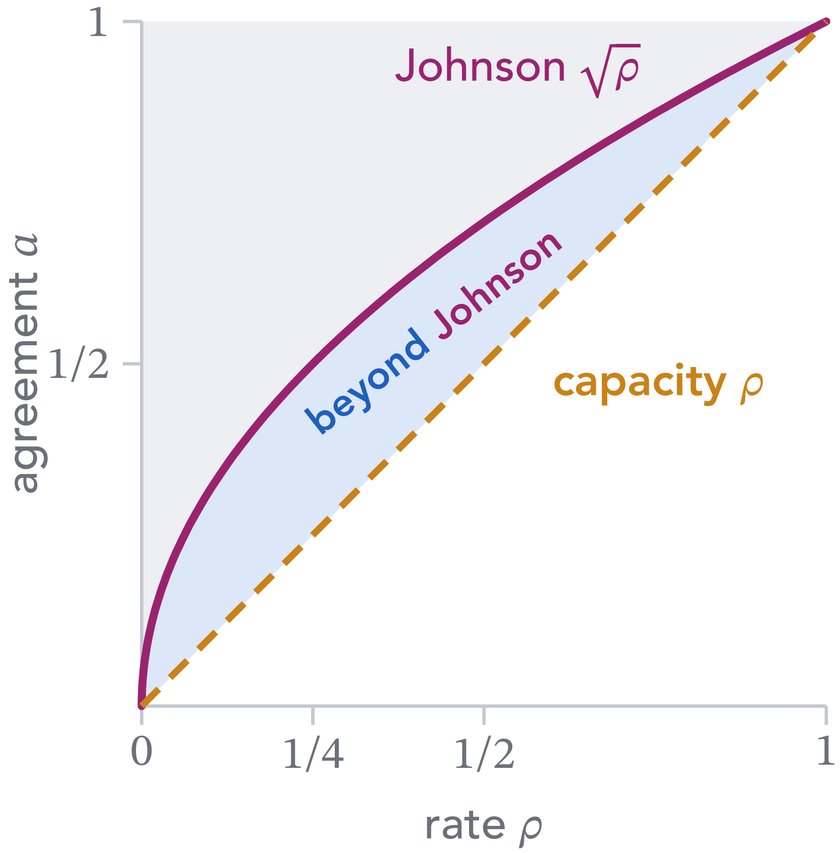
only a few z land in a disc

Soundness: s queries contribute about $(A/n)^s$, plus list size and $|\mathscr{E}|/q$
A lower threshold A saves queries, if the two algebraic terms still meet the target

Prior Work and Two Gaps

Bounds to capacity, but not yet for proof systems

- [ ] **Up to Johnson: MCA established**
  [BCI+23, BCH+26, Hab25, BCGM25]
- [ ] **To capacity, 2026: hidden derivatives**
  list decoding over prime fields [BCP+26a, Nas26]
  and MCA [Zhe26, Jer26]
  unified exposition, every rate directly [HKS26]
- **Gap 1: explicit bounds**
  list sizes and MCA errors at practical n, q
- **Gap 2: decoding at $q = 2^{\Theta(\lambda)}$**
  extractors list decode [BGK+23, ACFY24a, ACFY24b]
  need $\mathrm{poly}(n, \log q)$, not $\mathrm{poly}(q)$ [BCP+26a, Jer26]



Can we decode beyond Johnson efficiently over cryptographically large fields, and obtain agreement bounds strong enough to reduce proof sizes in existing systems?

One Derivative Beats Johnson

Gap 1: explicit bounds below Johnson at every rate

One hidden derivative

every close P satisfies $Q(X, P, P') = 0$ [Nas26, BCP+26a]

counting its independent conditions gives $a_1(\rho)$

$a_1(\rho) < \sqrt{\rho}$ at every rate; $a_1 \sim \sqrt{\rho/2}$ as $\rho \to 0$

Above $a_1(\rho) + \eta_1$, on any evaluation set

list size $O_\rho(n\,\eta_1^{-2})$, MCA count $O_\rho(n^2\eta_1^{-4})$

linear and quadratic in n: small enough for proof systems

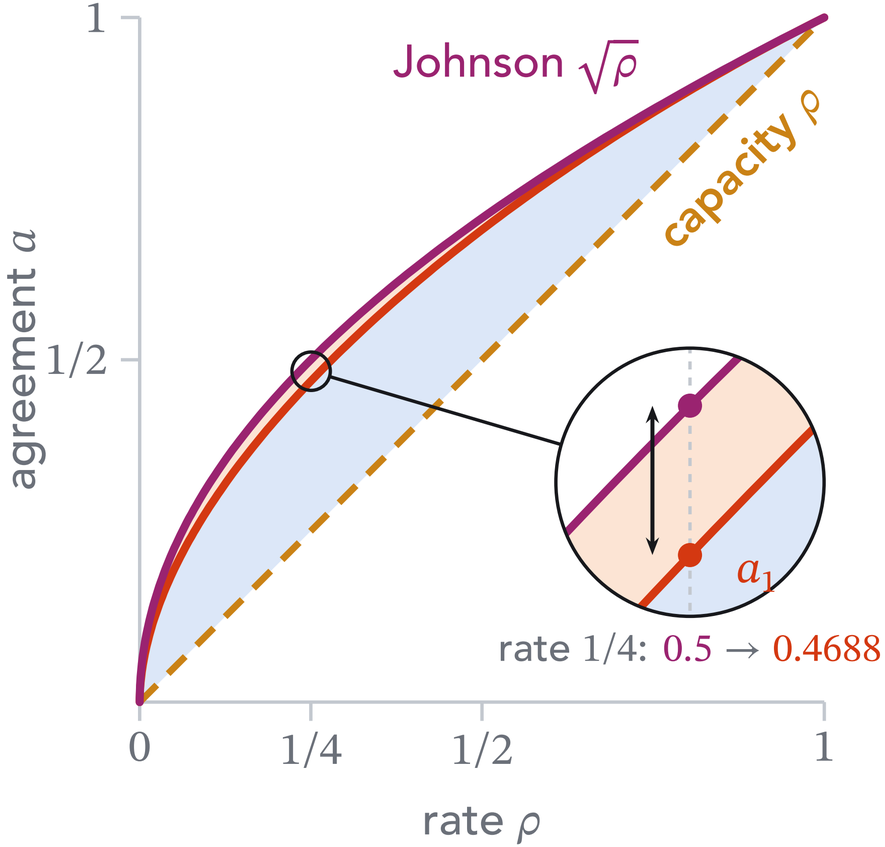
Related work below Johnson

same a_1 for $\rho \geq 0.18$, list size $O_\rho(n)$, no MCA [Gab26]

MCA, a fixed number of extra errors [Jo26b]

MCA, counts exponential in n [Cho26]

capacity: derivative order growing as $\delta \to 0$ [Zhe26, Jer26]



List and MCA Bounds

On any n distinct evaluation points; MCA error = count/q

Agreement	List size	MCA exceptional count
Above Johnson $a = \sqrt{(k-1)/n} + \eta_0$ every characteristic	$O_\rho(\eta_0^{-1})$ classical [GS99]	$O_\rho(n\,\eta_0^{-3})$ previously $O_\rho(n\,\eta_0^{-5})$ [BCH+26] with savings from [Bit26a, jie26a]
One derivative $a = a_1(\rho) + \eta_1$ char 0 or $p > \max\{k-1, O_\rho(1/\eta_1)\}$	$O_\rho(n\,\eta_1^{-2})$ previously: the row above if $a > \sqrt{\rho}$, else the row below, $\delta = a - \rho$ concurrently $O_\rho(n)$, large p [Gab26]	$O_\rho(n^2\eta_1^{-4})$ previously likewise
Up to capacity $a \geq \rho + \delta,\ n \geq N(\delta)$ char 0 or $p > k-1$	$C_\delta\, n^{d(\delta)}$ $d(\delta) = \lceil e^{1.5/\delta} \rceil$ for $\delta < 6/25$, else 1 previously [BCP+26a] order $\exp(O_\rho(\delta^{-1}\log\delta^{-1}))$	$C_\delta\, n^{d(\delta)+1}$ previously $n^{O_{\rho,\delta}(1)}$, prime fields [Zhe26]; $n^{O_\delta(1)}$, prime $q \geq n$ or large p [Jer26]

To capacity: one cutoff weighting Y_j by j, refining [BCP+26a], coinciding with later exposition [HKS26]; enlarge the message space only at low rate, similar to Jeronimo [Jer26]

Efficient Decoding

Gap 2: deterministic time $\mathrm{poly}(n, \log q)$, specialized to each agreement threshold

Agreement	Decoding time (bit operations)	Previously
Above Johnson $a = \sqrt{(k-1)/n} + \eta_0$ every characteristic	$\tilde{O}_{\rho,a}(n \log q)$	$\mathrm{poly}(n, \log q)$ [CHK26]
One derivative $a = a_1(\rho) + \eta_1$ char 0 or $p > \max\{k-1, O_\rho(1/\eta_1)\}$	$\tilde{O}_{\rho,a}(n^3 \log q)$ for $p > k-1$	the row above if $a > \sqrt{\rho}$, else the row below
Up to capacity $a \geq \rho + \delta,\ n \geq N(\delta)$ char 0 or $p > k-1$	$n^{O(d(\delta))}\, \tilde{O}_\delta(\log q)$ for $p > k-1,\ n \geq N_\delta$	$\mathrm{poly}(n, q)$ prime $q \geq C_{\rho,\delta}\, n$ [BCP+26a] prime $q \geq n$ [Jer26]

Deterministic: agreement with y is imposed first, with no root finding

Fields in a polynomial basis, $\mathbb{F}_q = \mathbb{F}_p[t]/(f(t))$, with $q \geq n$

Smaller Proofs, Checked in Lean

Query counts at each system's security target (including grinding)

System	Proof	Shipped	Johnson floor	Ours	Measured saving
ProveKit	Passport, BN254 field	127	119	109	79.4 KB (11.1%)
ZisK	Compressed final proof	54	53	51	13.2 KB (4.63%)
LambdaVM	CPU subproof	219	217	208	59.8 KB (4.85%)

First proof-size reductions in existing systems from provable bounds beyond Johnson!

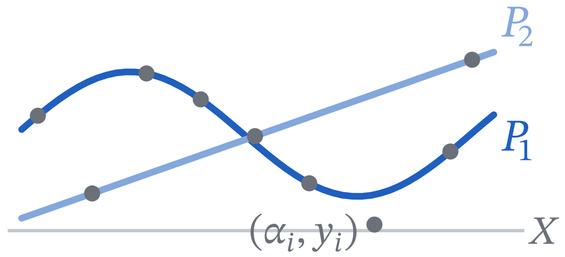
challenge fields of about 254 and 192 bits, where first-order bounds apply

Johnson floor: the fewest queries whose query term alone meets the target at Johnson

Verified in Lean: the list and MCA bounds, and the parameter checks behind this table
Not formalized: the decoders and their running times

Proof Outline for List Sizes and MCA Counts

1 Interpolate one equation → 2 Parameterize its solutions → 3 Count close messages



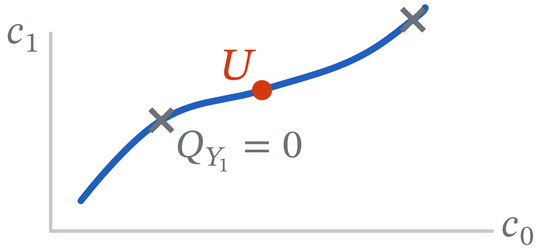
$Q(X, P, P') = 0$ for every close P

exists: more unknowns than conditions

$\deg Q(X, P, P') < mA$, but mA roots

no derivative: above $\sqrt{\rho}$ [GS99]

derivative Y_1: below $\sqrt{\rho}$ [Nas26, BCP+26a]



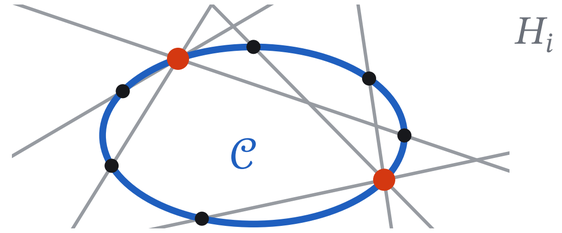
$P(x_0 + T) = c_0 + c_1 T + \sum_{j \geq 2} \phi_j(c_0, c_1)\, T^j$

(c_0, c_1) on the curve $Q(x_0, c_0, c_1) = 0$

each c_j is forced: divide by $j\, Q_{Y_1}$

symbolic c_0, c_1 [Kop15, Zhe26]

singular: an equation without P' [Nas26]



$N \leq \Delta\, \lambda_{\text{agr}}, \qquad \lambda_{\text{agr}} = \dfrac{n - D}{A - D}$

close: on at least A of the n planes H_i

degree Δ: at most Δ points per H_i

dimension r: one factor λ_{agr} each

agreements cut the family [Zhe26, Jer26]

Our improvements: sharper counts in all three steps

1 One Hidden Derivative

agreement $a_1(\rho) + \eta_1$, below $\sqrt{\rho}$: lists of size $O_\rho(n/\eta_1^2)$

the exact count of conditions per point; each factor of Q counted once

2 MCA Beyond Johnson

the same agreement: $O_\rho(n^2/\eta_1^4)$ exceptional challenges

sharper degrees and thresholds in the transfer; degree in Z independent of n, as in [Zhe26]

3 Up to Capacity

agreement $\rho + \delta$: $d = \lceil e^{1.5/\delta} \rceil$ derivatives, lists $C_\delta\, n^d$, MCA $C_\delta\, n^{d+1}$

weight Y_j by j; one order at every rate; explicit degrees $O(n^d)$

The Vanishing Argument

Step 1. One equation for every close message

One polynomial for every close message

$Q(X, Y_0, Y_1) \neq 0$: $Q(X, P, P') = 0$ for every P with $\geq A$ agreements

every close message then solves one differential equation

$$Q = \sum q_{xj_0j_1} X^x Y_0^{j_0} Y_1^{j_1} \quad \text{over} \quad x + D(j_0 + j_1) < mA, \qquad D = k - 1$$

$\deg P \leq D$, so every monomial gives $\deg X^x P^{j_0} (P')^{j_1} < mA$

Vanishing by counting roots

$R = Q(X, P, P')$: #{roots of R} $\geq$ mA $>$ $\deg R$ $\Longrightarrow$ $R = 0$

$(X - \alpha_i)^m \mid R$ at each of the A agreements; $\deg R < mA$ by the support of Q

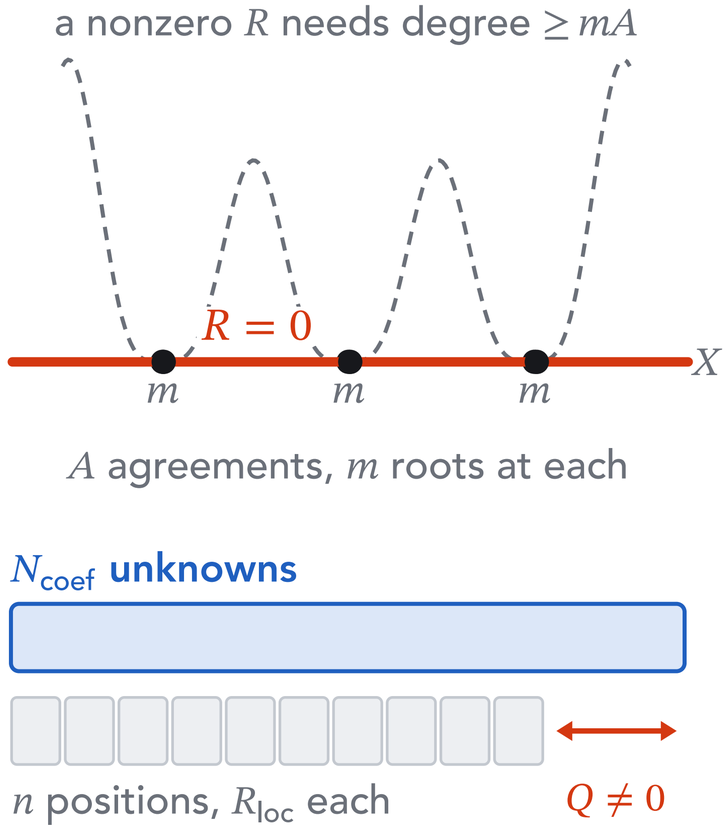
the order-m vanishing must be imposed without $P'(\alpha_i)$: next slide

Find Q by linear algebra

N_{coef} unknowns $>$ $n\,R_{\text{loc}}$ conditions $\Longrightarrow$ $Q \neq 0$ exists

Without Y_1 this is Guruswami–Sudan, which stops at $\sqrt{\rho}$ [GS99].

The threshold is decided by R_{loc} (Improvement 1).

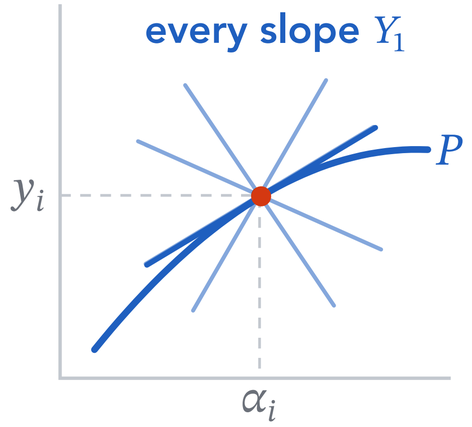


Interpolation with a Hidden Derivative

Step 1. Impose the roots without the slope $P'(\alpha_i)$

Naskręcki, BCPZZ: a variable Y_1 for P' [Nas26, BCP+26a]

the value y_i at α_i is received; the slope $P'(\alpha_i)$ is not



Backward Taylor at an agreement $P(\alpha_i) = y_i$

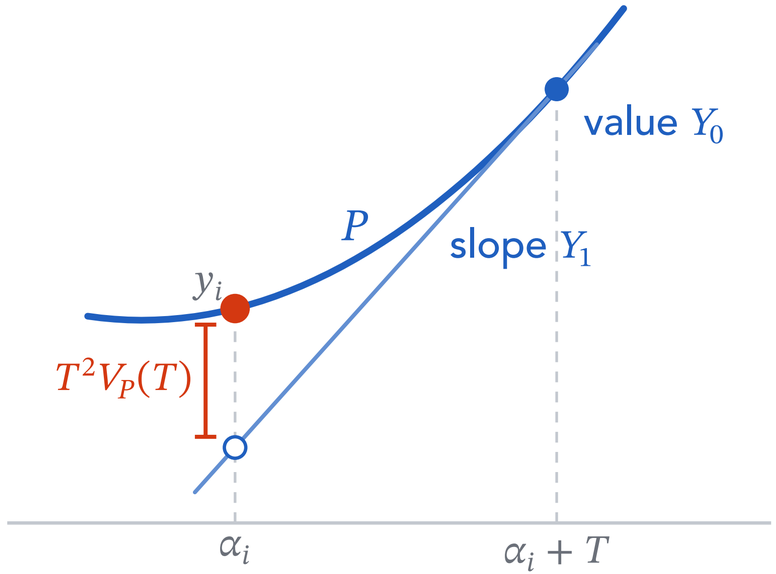
$$P(\alpha_i + T) = y_i + T\,P'(\alpha_i + T) + T^2\,V_P(T)$$

the slope is taken at $\alpha_i + T$, not at α_i (Lemma 3.5)

Conditions at position i, for every slope

$$Q(\alpha_i + T,\ y_i + TY_1 + T^2V,\ Y_1) \equiv 0 \pmod{T^m}$$

an identity in the variables Y_1 and V (Definition 3.6)



Substitute $Y_1 = P'(\alpha_i + T)$ and $V = V_P(T)$

$(X - \alpha_i)^m \mid Q(X, P, P')$ at every agreement (Lemma 3.7)

Many of these conditions are dependent: this is Improvement 1.

Improvement 1: One Hidden Derivative

Step 1. Count the conditions at one position

Notation: $x_+ = \max(x,0)$

The allowed monomials $X^x Y_0^{j_0} Y_1^{j_1}$ of Q: N_{coef} unknowns

$x + D(j_0 + j_1) < mA$ — inherited from the vanishing argument: $\deg Q(X, P, P') < mA$

$j_1 \le B_\partial, \qquad j_0 + j_1 \le B_{\text{jet}}$ — new: degree at most B_∂ in Y_1, at most B_{jet} in Y_0, Y_1 together

---

Counted naively: $Y_0 = y_i + TU$, U free

at T^s, one condition per $U^a Y_1^b$ ($a \le s$, $b \le B_\partial$)

conditions $\sum_{s<m} (s+1)(B_\partial + 1) = (B_\partial + 1)\, m(m+1)/2$

unknowns $\sum_t (\min(t, B_\partial) + 1)\, (mA - Dt)_+$

against Johnson ($B_\partial = 0$): the conditions grow by $B_\partial + 1$,
the unknowns at degree $t < B_\partial$ only by $t + 1 \Longrightarrow$ no gain

Where the conditions collide

the conditions see Y_0 only through $y_i + TY_1 + T^2V$:

$L_i = Y_0 - y_i - (X - \alpha_i) Y_1 \longmapsto T^2 V$

$(X - \alpha_i)^e L_i^j \longmapsto T^{e+2j} V^j \equiv 0$ once $e + 2j \ge m$

these products meet every condition at α_i [Nas26]
dependencies at T^s exist once $2s \ge m$ and $s + B_\partial \ge m$

$$\text{rank} \;\le\; R_{\text{loc}} = \sum_{s<m} \left[(s+1)(B_\partial + 1) - (2s - m + 1)_+ (s + B_\partial - m + 1)_+ \right]$$

$m = 6$, $B_\partial = 2$: 13 of 63 dependent



The count R_{loc} has no B_{jet}: take $B_{\text{jet}} \approx mA/D$, every power of Y_0 the support allows, at no cost in conditions
so the N_{coef} unknowns outnumber the $n\, R_{\text{loc}}$ conditions once the agreement exceeds an explicit $a_1(\rho)$

Improvement 2: MCA Beyond Johnson

Step 1 for a received line $f + zg$: one equation in X, Z, Y_0, Y_1

From lists to MCA: one equation for the whole line

lists: $Q(X, P, P') = 0$ for every P close to y

MCA: $Q(X, z, P, P') = 0$ for every z and every P close to $f + zg$

The same interpolation, with Z a variable [BCIKS23, Zhe26]

$$Q(\alpha_i + T,\ f_i + Zg_i + TY_1 + T^2V,\ Y_1) \equiv 0 \pmod{T^m}$$

solve over $F(Z)$ once $N_{\text{coef}} > nR_{\text{loc}}$, then clear denominators: but of what degree in Z?

New for MCA: the surplus sets the degree in Z

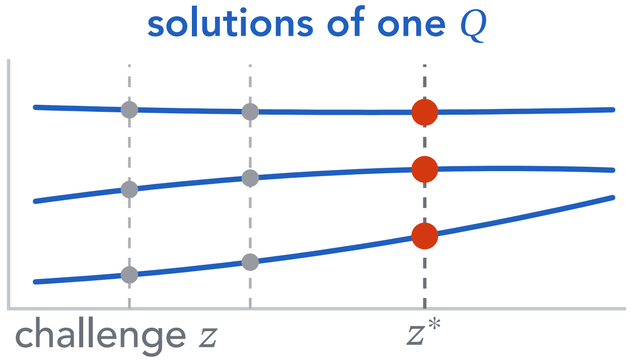
for $\deg_Z Q \le H$, each condition has degree at most $H + B_{\text{jet}}$ in Z,
so the scalar unknowns outnumber the scalar equations once

$$N_{\text{coef}}(H+1) \ > \ nR_{\text{loc}}(H + B_{\text{jet}} + 1) \quad \Longleftrightarrow \quad (H+1)\big(N_{\text{coef}} - nR_{\text{loc}}\big) > nR_{\text{loc}}B_{\text{jet}}$$

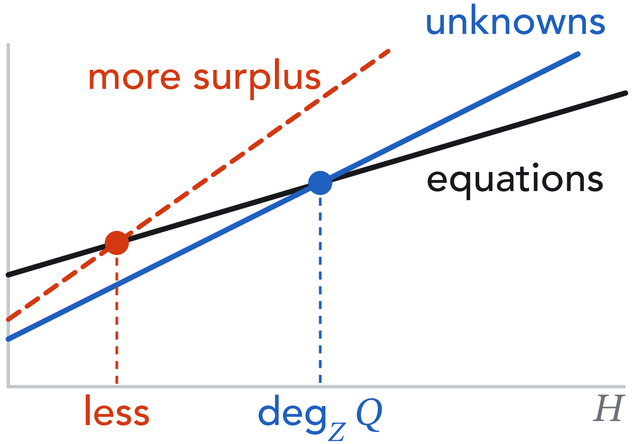
$$\deg_Z Q \ \le \ \left\lfloor \frac{nR_{\text{loc}}\, B_{\text{jet}}}{N_{\text{coef}} - nR_{\text{loc}}} \right\rfloor \ \le \ \left\lceil \frac{B_{\text{jet}}}{\gamma - 1} \right\rceil \quad \text{if } N_{\text{coef}} \ge \gamma\, nR_{\text{loc}}$$

at agreement $a_1(\rho) + \eta_1$: $\deg_Z Q = O_\rho(1/\eta_1^2)$, independent of n (Lemma 3.16)

$\deg_Z Q$ enters the number of bad challenges linearly; $O(n)$ in [Jer26]



slice at z^*: the list for $f + z^*g$



Solutions as Taylor Coefficients

Step 2. From one equation to a family of candidates

Expand a solution P around a generic point x_0

$$P(x_0+T) = c_0 + c_1 T + c_2 T^2 + c_3 T^3 + \cdots, \qquad P'(x_0+T) = c_1 + 2c_2 T + 3c_3 T^2 + \cdots$$

Read off $Q(X, P, P') = 0$ one power of T at a time [Kop15]

T^0: $\quad Q(x_0, c_0, c_1) = 0$

T^1: $\quad 2c_2\, Q_{Y_1} = -\,Q_X - c_1 Q_{Y_0}$

T^{j-1}: $\quad j\, c_j\, Q_{Y_1} =$ a polynomial in $c_0, \ldots, c_{j-1}$

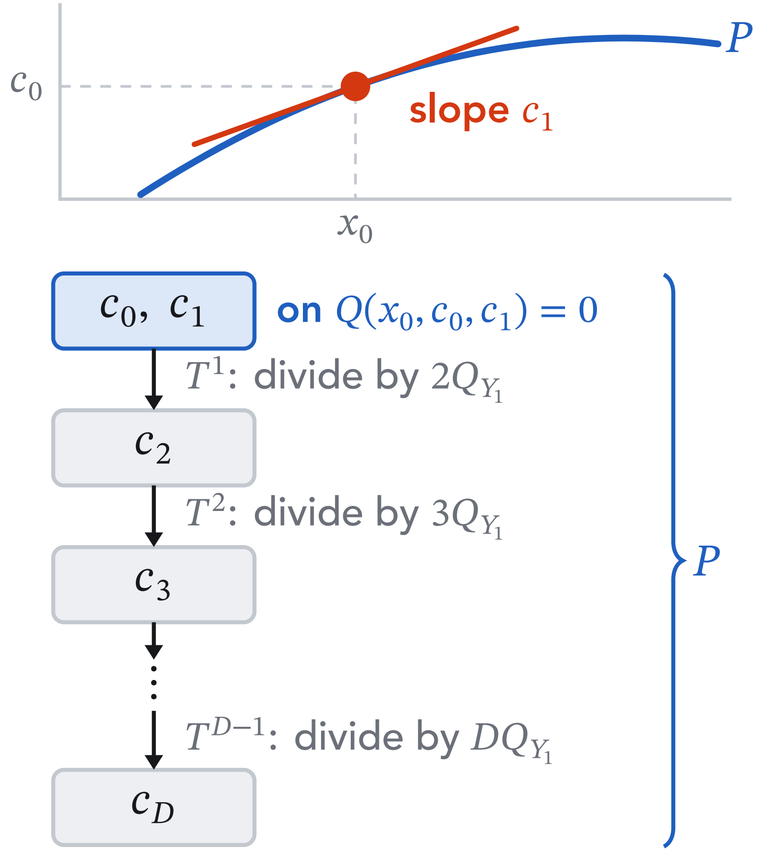
partials at (x_0, c_0, c_1); c_j first enters through P', as jc_jT^{j-1}: hence jQ_{Y_1}

Regular: the separant $Q_{Y_1}(X, P, P')$ is not identically 0 [Zhe26]

$$c_j = \phi_j(c_0, c_1) \quad (2 \le j \le D), \qquad P(X) = \sum_{j \le D} c_j (X - x_0)^j$$

with x_0 a new variable, the separant is nonzero at x_0; needs $p > D$

singular ($\equiv 0$ along P): an equation without Y_1, counted separately [Nas26]



Every close P solves the equation (Step 1); a regular one is the image of its point (c_0, c_1) on the curve.
Not every image is close: Step 3 counts the close ones on this one curve of messages, by its degree.

Counting by Agreement

Step 3. Bound the close messages on the curve

From Step 2: the regular solutions lie on one curve $\mathscr{C}$ of messages

$$\mathscr{C} = \text{image of } \{Q(x_0, c_0, c_1) = 0\}, \qquad \deg \mathscr{C} = \Delta \le 4D\, B_{\text{jet}} B_\partial$$

each squarefree factor of Q counted once; B_∂ kept apart from B_{jet} (Lemmas 5.3, 5.5)

Agreement at α_i is a hyperplane of messages [Zhe26]

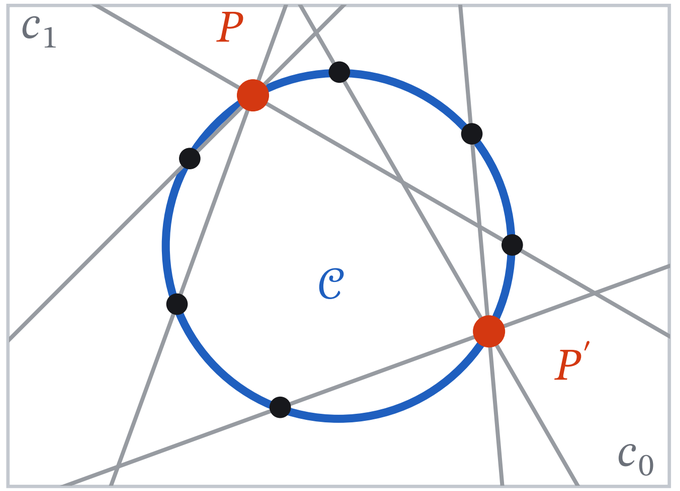
$$H_i = \{P : P(\alpha_i) = y_i\}, \qquad \mathscr{C} \not\subset H_i \implies |\mathscr{C} \cap H_i| \le \Delta$$

$\mathscr{C}$ lies in at most D of the H_i: any $k = D + 1$ of them meet in a single point

Count the agreements of the N close P on $\mathscr{C}$ two ways

each close P lies on A of the H_i, and at most D of these contain $\mathscr{C}$;
each other H_i holds at most Δ points of $\mathscr{C}$:

$$N(A - D) \;\le\; \Delta\,(n - D) \quad\implies\quad N \le \Delta\,\frac{n - D}{A - D} = \Delta\,\lambda_{\text{agr}}$$



$n = 6$ lines, $k = 2$

no line contains $\mathcal{C}$: $N \le 2 \cdot 6/3 = 4$

regular close P: at most $\lambda_{\text{agr}}\Delta$; singular: roots in Y_0 of an equation without Y_1, of degree at most $2B_{\text{jet}}B_\partial + B_{\text{jet}}$

$$|\text{List}(y, A)| \;\le\; 4D\lambda_{\text{agr}}B_{\text{jet}}B_\partial + 2B_{\text{jet}}B_\partial + B_{\text{jet}} \;=\; O_\rho(n/\eta_1^2) \qquad \text{(Theorem 5.1)}$$

Improvement 2: MCA Beyond Johnson

Step 3. Count the exceptional challenges

Want: one witness pair for each close P, unless $z \in \mathscr{E}$

$$P = F_0 + zG_0, \qquad S_z(P) = S(F_0, G_0)$$

P agrees with $f + zg$ exactly where F_0 agrees with f and G_0 with g

Witness graphs: each pair traces a line $z \mapsto (z, F_0 + zG_0)$ [Zhe26, Jer26]

point: a pair (z, P), with P close to $f + zg$

every point is on a line: interpolate f and g on k agreements of P

good line: at least L agreements common to all its points; L halfway from D to A

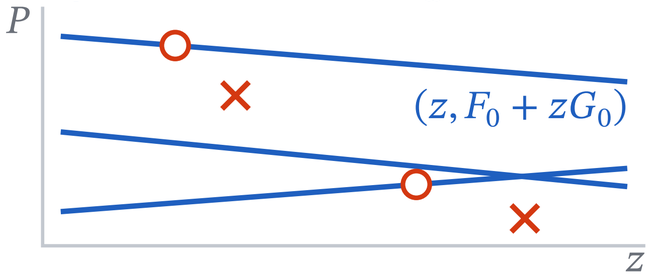
Count both failures by agreement, as for lists (Lemma 4.2)

$$|\mathscr{E}| \le \underbrace{2\lambda_{\text{agr}}^2 J_1}_{\times} + \underbrace{2\lambda_{\text{agr}}\Delta \cdot n}_{\circ}$$

×: close pairs lie on a surface of degree J_1; list count twice: surface → curves → points

∘: at most $2\lambda_{\text{agr}}\Delta$ good lines, by the list count at threshold L; at most n extra agreements on each

points (z, P); blue: good lines



MCA fails at z only if:

× a close (z, P) on no good line

∘ on one, with an agreement outside the common set

$J_1 = O(n\Delta \deg_Z Q)$ (Lemma 5.5); surplus: $\deg_Z Q$ independent of n, so $J_1 = O(n^2)$, not $O(n^3)$

Result: $|\mathscr{E}| = O_\rho(n^2/\eta_1^4)$ at agreement $a_1(\rho) + \eta_1$, below Johnson (Theorem 5.2)

Before: Jo, h errors beyond Johnson, $O_{r,h}(n^6)$ [Jo26b]; Chojecki, exponential in n [Cho26]

Improvement 3: Up to Capacity

The same three steps, with d hidden derivatives

	First order	Order d
Step 1	$Y_0 = y_i + TY_1 + T^2V$ agreement above $a_1(\rho)$	$Y_0 = y_i + TY_1 - T^2Y_2 + \cdots \pm T^dY_d + T^{d+1}V$ [BCP+26a] weight Y_l by l: $\sum_l l j_l \le W$ any $a = \rho + \delta$ once $d \ge d(\delta) = \lceil e^{1.5/\delta} \rceil$ (Thm. 8.1)
Step 2	$c_2, \ldots, c_D$ from (c_0, c_1): a curve of degree $O(n)$	$c_{d+1}, \ldots$ from the jet $(c_0, \ldots, c_d)$: a family of dimension $\le d$, degree $O(n^d)$ singular: pass to the separant, at most B_{jet} times
Step 3	$\lvert \text{List} \rvert = O_\rho(n/\eta_1^2)$ $\lvert \mathscr{E} \rvert = O_\rho(n^2/\eta_1^4)$	$\lvert \text{List} \rvert \le C_L n^d$, $\lvert \mathscr{E} \rvert \le C_E n^{d+1}$ (Prop. 8.7) one factor λ_{agr} per dimension (Lemma 4.1)

An explicit order

$d(\delta) = \lceil e^{1.5/\delta} \rceil$ at $a = \rho + \delta < \rho + 6/25$
BCPZZ: $\exp(O_\rho(\delta^{-1} \log \delta^{-1}))$
one $\log(1/\delta)$ fewer [BCP+26a]

One order at every rate

below rate δ^2, we enlarge the messages as Jeronimo does [Jer26]
also every rate: Mishra [Mis26]

Same support as HKS [HKS26]

our count keeps the degree left for X, Y_0 per derivative monomial: hence the explicit order

Deterministic Decoding: Obstacles and Approach

Goal: the whole list, deterministically, in time polynomial in n and $\log q$

Obstacle 1: root finding

Guruswami–Sudan: the messages are the roots $Y = P(X)$ of $Q(X, Y)$

Deterministic root finding in $\mathrm{poly}(\deg, \log q)$ is open: fast decoders are Las Vegas [JNSV17, NRS17]

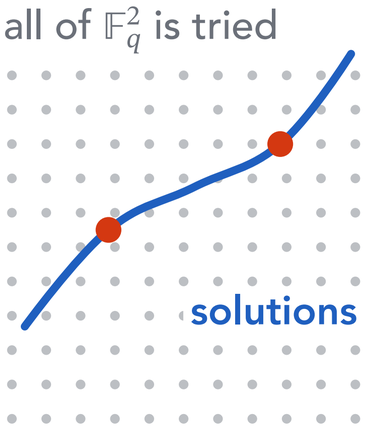
Order zero avoids it with the received values; CHK: $\mathrm{poly}(n, \log q)$ above Johnson [AP00, CHK26]

Obstacle 2: a family, not a finite set

$Q(X, P, P') = 0$ has a curve of solutions, one per (c_0, c_1) (Part III)

Kopparty, BCPZZ, Jeronimo try every $(c_0, c_1) = (P(x_0), P'(x_0)) \in \mathbb{F}_q^2$ [Kop15, BCP+26a, Jer26]

A power of q, however small the list: fine if $n = q$, not if $n \ll q$



Ours: impose the agreements before extracting any candidate

1. a center x_0:
(c_0, c_1) fix P

→

2. keep $U = (c_0, c_1)$
unknown: a family $\tilde{P}_U$

→

3. agreements leave
finitely many U

→

4. read P off the y_i
in a finite algebra

Kopparty's recurrence | Zheng, Jeronimo | removes obstacle 2 | removes obstacle 1

Order Zero: A Separable Equation

Above Johnson, no derivative. Step 1: from Q to a polynomial h with distinct roots

Start: Guruswami–Sudan gives $Q(X, Y)$ with $Q(X, P(X)) = 0$ for every close P

Q has X-degree $O(n)$ and Y-degree at most $\ell = O_{\rho,a}(1)$; $Y - P(X)$ divides Q
Fast interpolation computes Q in $\tilde{O}_{\rho,a}(n)$ operations [JNSV17]

1a. Want: a factor $\bar{Q}$ of Q with no repeated roots in Y

why: Step 2 divides by $\partial_Y \bar{Q}$ at each root, and it is 0 at a repeated root

how: $R = Q / \gcd(Q, \partial_X Q, \partial_Y Q)$ one copy of each factor of Q

$\bar{Q} = R / \gcd(R, \partial_Y R)$ drops factors with only repeated roots

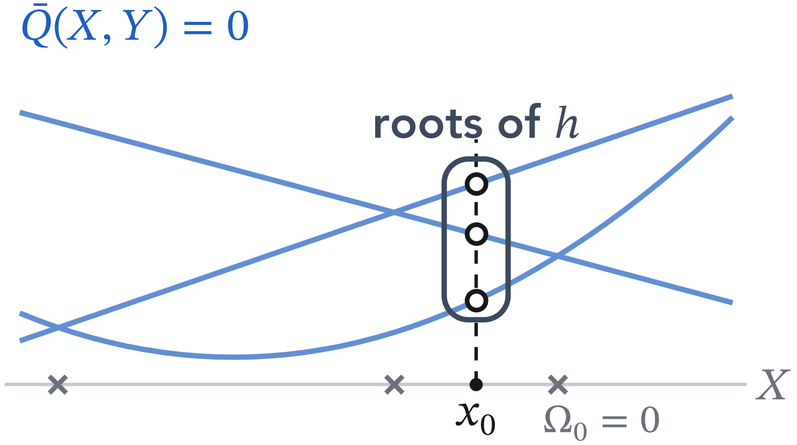
$\Longrightarrow$ $\bar{Q}$ keeps every factor $Y - P(X)$ of Q [Lec08]

1b. Want: a point x_0 where $h(U) = \bar{Q}(x_0, U)$ has distinct roots

why: Step 2 rebuilds each close P from one number, its value $P(x_0)$
if two branches of $\bar{Q} = 0$ cross at x_0, that value does not say which one is P

how: $\Omega_0 = \mathrm{lc}_Y(\bar{Q}) \cdot \mathrm{Res}_Y(\bar{Q}, \partial_Y \bar{Q})$

$\Omega_0(x) = 0$ exactly when a root of $\bar{Q}(x, Y)$ goes to infinity, or is also a root of $\partial_Y \bar{Q}$
$\Omega_0 \neq 0$ by 1a, of degree $D = O(n)$: it is nonzero at one of any $D + 1$ points
compute Ω_0 (a small determinant), evaluate it at $D + 1$ points at once $\Longrightarrow$ pick x_0 with $\Omega_0(x_0) \neq 0$



After Step 1:
h has distinct roots;
for every close P,
$P(x_0)$ is one of them
$\tilde{O}_{\rho,a}(n \log q)$ bits

Order Zero: All Roots in One Algebra

Above Johnson, no derivative. Step 2: from h to every close P at once

Start: $h(U) = \bar{Q}(x_0, U)$ has distinct roots $\zeta_1, \ldots, \zeta_d$, and $P(x_0)$ is one of them (Step 1)

2a. If we knew $c_0 = P(x_0)$, then we could rebuild P

how: $\tilde{P} = c_0 + \tau_1 T + \tau_2 T^2 + \cdots + \tau_{k-1} T^{k-1}$ unknowns $\tau_1, \ldots, \tau_{k-1}$

$\bar{Q}(x_0 + T, \tilde{P}) \equiv 0 \bmod T^k$ solve for one τ_j at a time

at T^j, τ_j appears only as $\bar{Q}_Y(x_0, c_0)\,\tau_j$: divide by $\bar{Q}_Y(x_0, c_0) \neq 0$ (1b)

$\Longrightarrow$ one solution, $P(x_0 + T)$: shift back to get P, since $\deg P < k$

2b. We do not: run 2a once in $\mathscr{A}$, at every root of h at once

why: we do not know which root is $P(x_0)$, and the roots may lie outside E

how: $c_0 \longmapsto U \in \mathscr{A} = E[U]/h$ $a(U) \in \mathscr{A} \leftrightarrow (a(\zeta_1), \ldots, a(\zeta_d))$

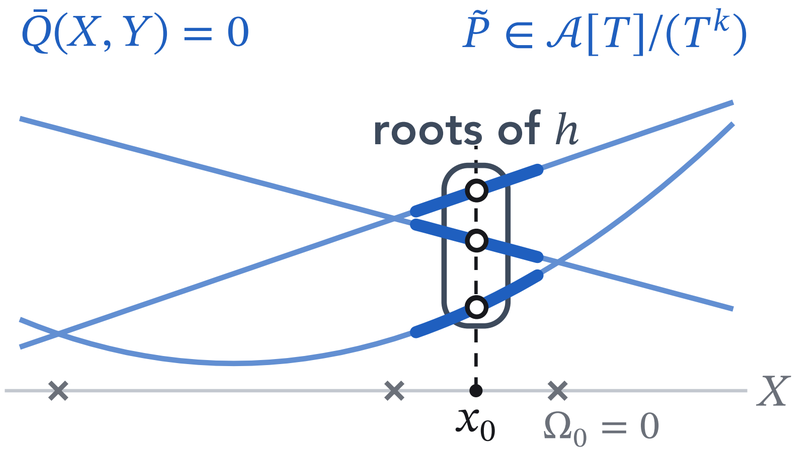
the same recurrence, dividing by $\bar{Q}_Y(x_0, U)$: invertible in $\mathscr{A}$, nonzero at every root

$\Longrightarrow$ one $\tilde{P} \in \mathscr{A}[T]/(T^k)$; setting $U = P(x_0)$ gives P, for every close P

the only divisor is $\bar{Q}_Y(x_0, U)$, never j: no condition on the characteristic

No Step 3: the candidates are already finite

at most $d \leq \ell$ candidates, one per root of h $\Longrightarrow$ nothing left to filter



No root of h is computed:
all of them live in $\mathscr{A}$

$\tilde{O}(n)$ to expand $\bar{Q}$ at x_0,

$\tilde{O}(k)$ to lift [vdH02]

Step 4 picks the messages

Order Zero: Messages from the Received Values

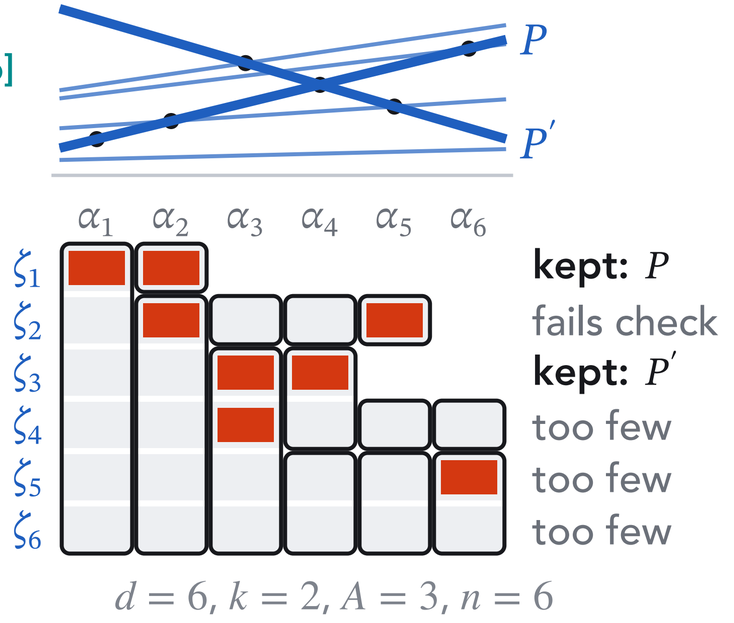
Above Johnson, no derivative. Step 4: from $\tilde{P}$ to the list, with no root

Start: $\tilde{P} \in \mathscr{A}[X]_{<k}$; **setting** $U = \zeta_j$ **gives candidate** j **(Step 2)**

Want: the close messages among the candidates, with no root of h

why: fast root finding is randomized [JNSV17]; received values avoid it [AP00, CHK26]

1 $e_i \leftarrow \tilde{P}(\alpha_i) - y_i \in \mathscr{A}$ for all i, by one multipoint evaluation
2 factors $\leftarrow \{(h, \emptyset)\}$: a factor g of h and a list L of positions
3 for $i = 1, \ldots, n$, and each factor (g, L):
4 split it into $(\gcd(g, e_i),\ L \cup \{i\})$ and $(g/\gcd(g, e_i),\ L)$
5 if a new factor has $|L| = k$: $P \leftarrow$ the interpolant of $(\alpha_j, y_j)_{j \in L}$
6 output P if it agrees with y in at least A positions, and drop the factor



$d = 6, k = 2, A = 3, n = 6$

orange: agrees at α_i; frames: factors of h

$e_i(\zeta_j) = 0$ exactly when candidate j agrees at α_i: $\gcd(g, e_i)$ keeps those roots of g

every candidate of (g, L) agrees with y on L; at $|L| = k$, all equal P (degree below k)

$\tilde{O}((n+k)\,d)$ operations in E: at each i the factors have total degree d (Lemma 9.2)

With Steps 1–2: deterministic $\tilde{O}_{\rho,\eta_0}(n \log q)$ at a fixed gap η_0 above Johnson (Corollary 9.4)

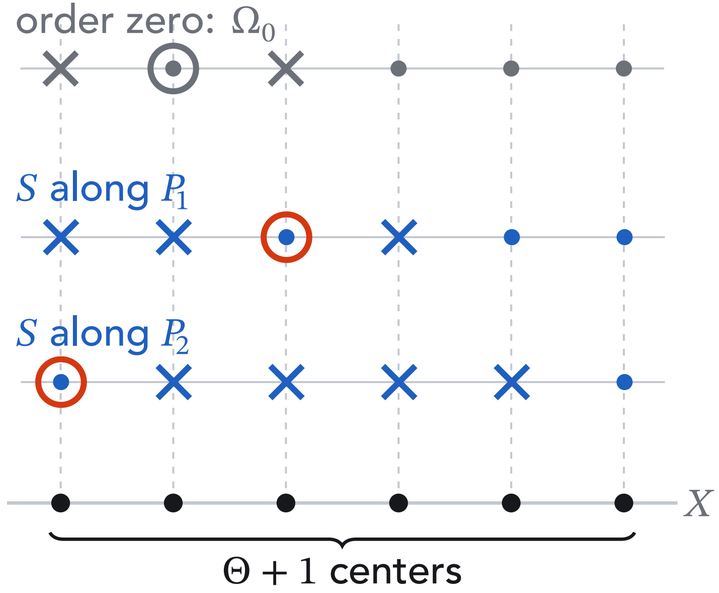
CHK: $\mathrm{poly}(n, \log q)$ at every agreement above Johnson, however small the gap [CHK26]

First Order: A Stage and a Center

Beyond Johnson, one derivative. Step 1: from Q to a stage $\bar{Q}$ and centers

Start: Improvement 1 gives $Q(X, Y_0, Y_1)$ with $Q(X, P, P') = 0$ for every close P

similar to order zero: X-degree $O(n)$, and degree at most $B_{\text{jet}} = O_{\rho,a}(1)$ in Y_0, Y_1



1a. Want: an equation $\bar{Q}$ that P solves, with separant $\bar{Q}_{Y_1}(X, P, P') \neq 0$

why: Step 2 divides by the separant, similar to $\bar{Q}_Y$ at order zero

new: gcd no longer suffices with differential equations

how: $Q_0 = Q, \qquad Q_{j+1} = \partial Q_j / \partial Y_1$ once Y_1 is gone: $\partial / \partial Y_0$

each P corresponds to exactly one Q_j: the first such that Q_{j+1} is nonzero along P

we do not know which $Q_j \implies$ run Steps 2–4 for every Q_j, at most $B_{\text{jet}} + 1$ of them

1b. Want: a center x_0 where the separant of P is nonzero

why: Step 2 divides by it at $U = (P(x_0), P'(x_0))$, similar to order zero

how: $S(X) = \bar{Q}_{Y_1}(X, P, P') \neq 0, \qquad \deg S \leq \Theta = O(n)$

Θ: a degree bound for the separant along every $P \implies S \neq 0$ at one of any $\Theta + 1$ centers

new: S depends on the unknown P, unlike $\Omega_0 \implies$ run Steps 2–4 at all $\Theta + 1$ centers

After Step 1: each close P is regular at one of $O(n)$ centers

order zero: one center for all

First Order: A Curve of Candidates

Beyond Johnson, one derivative. Step 2: from $\bar{Q}$ to a curve of candidates

Start: P solves the stage $\bar{Q}$, and its separant is nonzero at x_0 (Step 1)

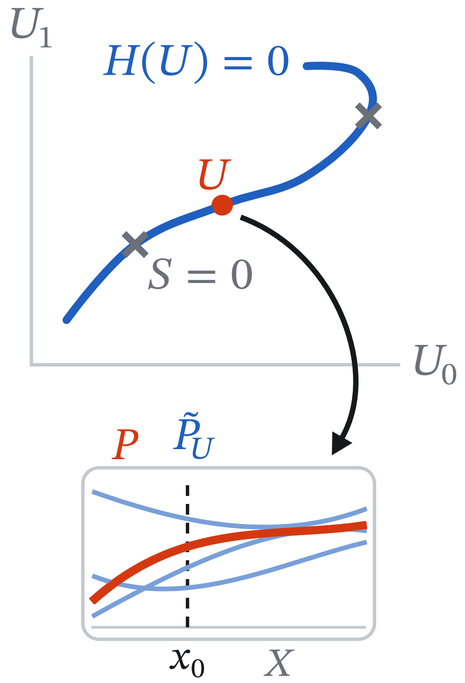
2a. If we knew $U = (P(x_0), P'(x_0))$, then we could rebuild P

how: $\tilde{P} = U_0 + U_1 T + \tau_2 T^2 + \cdots + \tau_{k-1} T^{k-1}$ unknowns $\tau_2, \ldots, \tau_{k-1}$

$\bar{Q}(x_0 + T, \tilde{P}, \tilde{P}') \equiv 0 \bmod T^{k-1}$ solve for one τ_j at a time

at T^{j-1}, to solve for τ_j, we divide by $j \cdot S(U)$, where $S(U) = \bar{Q}_{Y_1}(x_0, U)$ [Kop15]

new: two starting numbers, not one, and a division by $j < k \implies$ needs $p > k - 1$



2b. We do not: run 2a once, on the curve $H(U) = \bar{Q}(x_0, U) = 0$

why: similar to order zero, we do not know which point is $(P(x_0), P'(x_0))$ [Zhe26, Jer26]

how: write as a fraction $\tau_j(U) = N_j(U)/B_0(U)$, $B_0 = S^{2k}$, $\deg N_j = O(k)$

new: a curve has infinitely many candidates, and contains points where $S(U)$ vanishes

$\implies$ we cannot divide there: τ_j stays a fraction

order zero: $\bar{Q}_Y(x_0, U)$ was nonzero at every candidate, so τ_j was a polynomial

Step 3 is new: cut the curve by agreement

agreement equations cut the curve to finitely many points, with no root computed

After Step 2: each close P is the candidate at its own U

$\tilde{O}(n + k^2)$ per center (Lemma 9.5)

First Order: Cutting by Agreements

Beyond Johnson, one derivative. Step 3: from a curve to finitely many points

Start: the curve $h(u, v) = 0$ of Step 2, monic in v, where $s \neq 0$

Want: the points of the curve where many agreement equations hold

new: represent these points implicitly, as the roots of one polynomial $G(u)$

3a. Want: agreement at α_i as an equation on the curve

how: $g_i = \sum_{j<k} N_j (\alpha_i - x_0)^j - y_i B_0 = 0$

proper agreement: $g_i = 0$ at the point, but $g_i \not\equiv 0$ on its component [Jer26]

at most $k-1$ of the g_i vanish on a component $\Longrightarrow$ at least $t = A - k + 1$ are proper

3b. Want: a detector $\nu_i(u)$, zero at the proper agreements at α_i

why: the plain $\mathrm{Res}_v(h, g_i)$ is identically 0 when $g_i \equiv 0$ on a component

how: ν_i = lowest nonzero ζ-coefficient of $\mathrm{Res}_v(h, \zeta - g_i)$

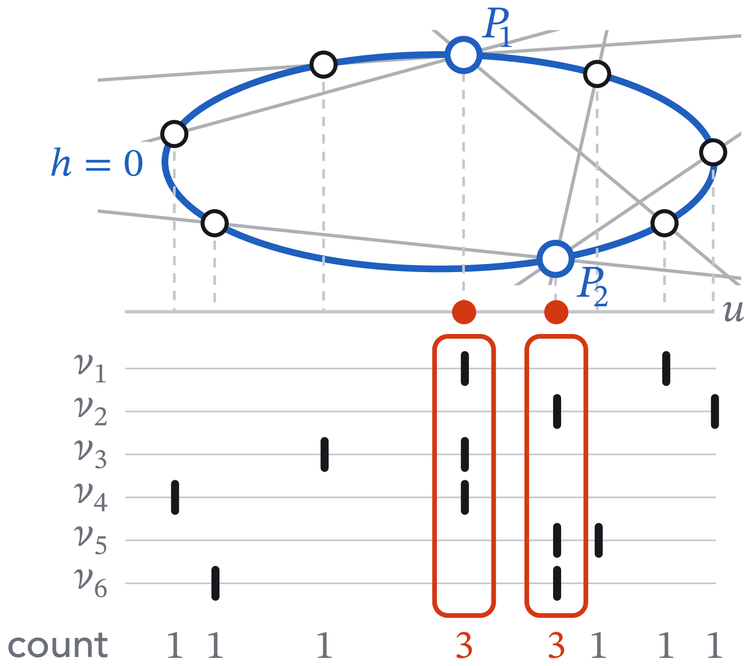
$\mathrm{Res}_v(h, \zeta - g_i) \in E[u, \zeta]$: above each u, its roots in ζ are the values of g_i

at $\zeta = 0$ it is $\mathrm{Res}_v(h, g_i)$; the lowest nonzero coefficient ignores where $g_i \equiv 0$

3c. Want: the values of u where at least t detectors vanish

how: $G = \mathrm{rad}(\nu_{\geq t}), \qquad \deg G \leq \sum_i \deg \nu_i / t = O(nk/t)$

$\nu_{\geq t}$: zero where at least t of the ν_i vanish; Batcher's network, $(\gcd, \mathrm{lcm})$ comparators [Bat68]



union: all 8 values, $O(nk)$

threshold $t = 2$: 2 values, $O(nk/t)$

Kept: the tower $(E[u]/G)[v]/h$,
dimension $O(nk/t)$: Step 4, next

First Order: Splitting Towers

Beyond Johnson, one derivative. Step 4: the same algorithm, in a tower

Start: $\tilde{P}$ over $\mathscr{A} = (E[u]/G)[v]/h$, of dimension $O(nk/t)$ (Step 3)

a point of $\mathscr{A}$ is a root β of G with a root of $h(\beta, v)$, and gives one candidate

Want: the close messages, by the order-zero read-off

the read-off needs one operation: split a factor into $e_i = 0$ and e_i invertible

$\Longrightarrow$ returns exactly the close messages, in $\tilde{O}((n+k)\dim \mathscr{A})$ operations (Lemma 9.2)

new: in a tower, $\gcd(h, e_i)$ no longer gives this split: one reason in v, one in u

4a. In v (mod h): repeated roots

new: branches of $h = 0$ can meet above a root β of G, so $h(\beta, v)$ can repeat a root

why: $\gcd(h, e)$ can take too few copies of a repeated root: the rest land where $e \neq 0$

how: $\gcd(h, e^b \bmod h) = \prod_{e(\gamma)=0} (v-\gamma)^{m_\gamma}$ with $b = \deg_v h \geq m_\gamma$ for all γ

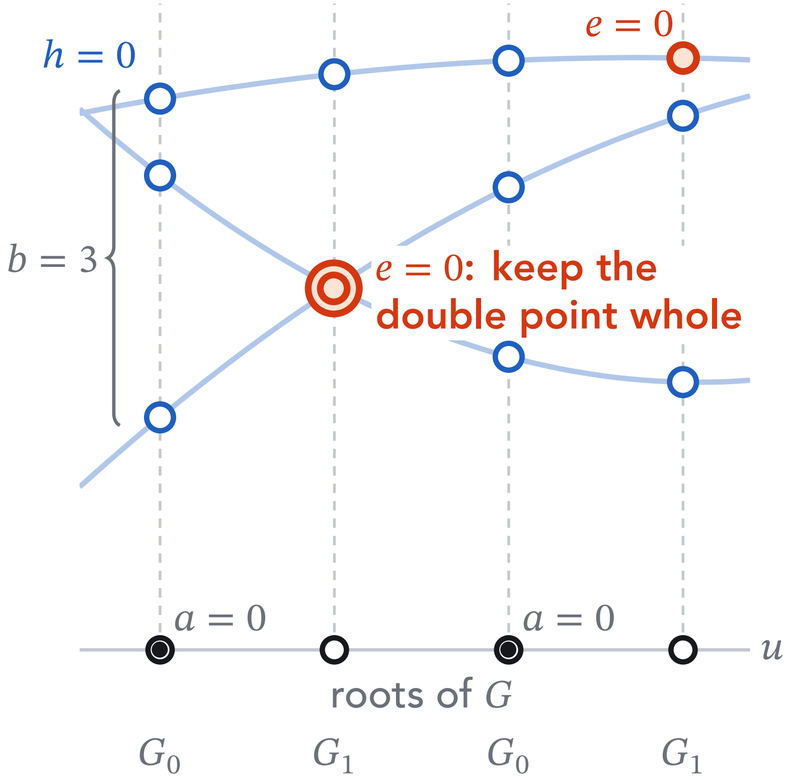
4b. In u (mod G): zero divisors

new: each gcd in v has coefficients in $E[u]/G$, and divides by leading coefficients a

why: a can vanish at some roots of G but not others: neither 0 nor invertible

how: $G_0 = \gcd(G, \tilde{a})$: $a = 0$, $G_1 = G/G_0$: a invertible [DMSX05]

the gcd then runs separately mod G_0 and mod G_1, without computing any root of G



First order: $O(n)$ centers, $\tilde{O}(n^2)$ each

$\Longrightarrow$ $\tilde{O}_{\rho,a}(n^3 \log q)$, $p > k-1$

Corollary 9.9

Higher Order: Square Systems

Beyond Johnson, $r \geq 2$ derivatives. Only step 3 changes; the other steps carry over

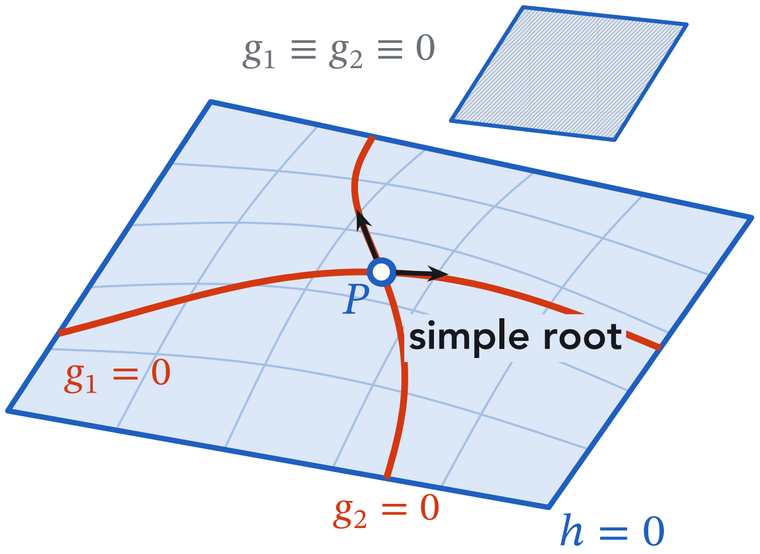
Start: Steps 1–2 similar to first order, with $r+1$ initial values: the family $h = 0$ has dimension r

3. Want: finitely many points that include every close point

why: one agreement equation lowers the dimension by one: we need r at once

how: $h = 0, \quad g_i = 0 \ \ (i \in J), \quad |J| = r$ $\quad r+1$ equations, $r+1$ unknowns

new: the agreements of P are unknown $\implies$ try all n^r subsets J per center



3a. Want: for each close P, some J makes P a simple root, hence isolated

how: $dg_i(\xi) = B_0 \dot{\tilde{P}}_\xi(\alpha_i)$ $\quad \xi$: a direction along $h = 0$ at P

$\dot{\tilde{P}}_\xi$: the change of $\tilde{P}$ as its initial values move along ξ, of degree below k

$dg_i(\xi) = 0$ at k agreements $\alpha_i \implies \dot{\tilde{P}}_\xi$ has k roots, so $\dot{\tilde{P}}_\xi = 0$ and $\xi = 0$

$\implies$ some r of the dg_i are independent: with $h = 0$, P is a simple root (Lemma 9.10)

3b. Want: every isolated root, as a finite algebra [Roj99]

how: $\{\psi(\theta) : F_{\text{iso}}(\theta) = 0\} \supseteq \{\text{isolated roots}\}$ $\quad$ Rojas: input the square system, output F_{iso} and $\psi_1, \ldots, \psi_{r+1}$

output $E'[\theta]/G_{\text{iso}}$, over an extension E' of E. Single variable $\theta \implies$ Step 4 similar to order zero

> **Higher order: $O(n)$ centers, n^r systems each $\implies$ $n^{O(r+1)}\,\tilde{O}(\log q)$ (Theorem 9.11)**
> every rate, order $d(\delta)$: $n^{O(\exp(1.5/\delta))}\,\tilde{O}_\delta(\log q)$ (Theorem 9.14)

Summary and Open Problems

1. **Beyond Johnson with one hidden derivative; capacity at every rate with order $d(\delta) = \lceil e^{1.5/\delta} \rceil$**
2. **Deterministic list decoding in $\mathrm{poly}(n, \log q)$ at each of these thresholds**
3. **Smaller proofs: ProveKit 11.1%, ZisK 4.63%, LambdaVM 4.85%; bounds verified in Lean**

Characteristic

[DKTZ26, BKR10]

fails at $p = 2$ **ours:** $p > k - 1$

?

characteristic p

Which characteristic is required?

Our Johnson bound holds for every p

Exponent of n

[AGG26]

at least $\delta^{-1/2}$ **ours:** $e^{1.5/\delta}$

?

exponent of n, gap δ fixed

Can it be polynomial in $1/\delta$?

Gap $1/\log n$: n^c exceptional [KKH26]

MCA error in n

[ABF26]

at least τn **ours:** n^2

?

MCA error $\times\, q$

Can the first-order bound be linear?

At the Johnson bound, linear is optimal