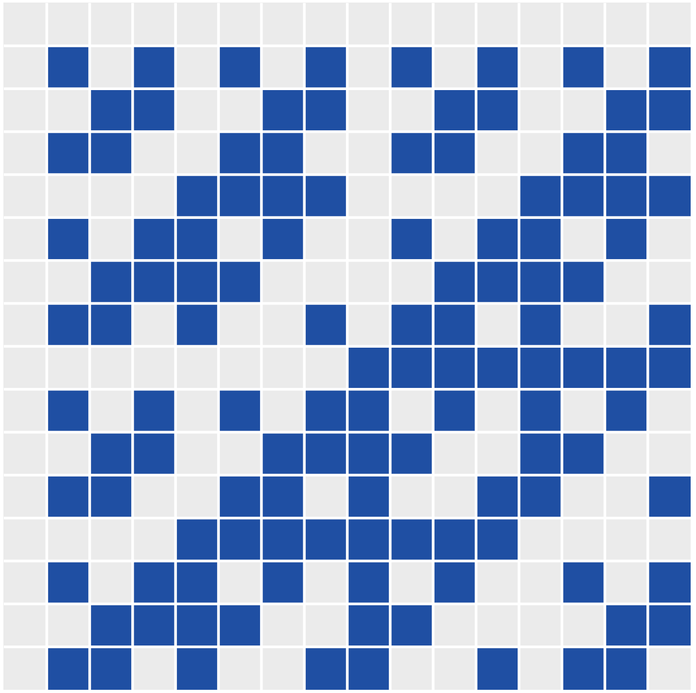
Counterexamples to Beyond-Johnson Proximity Gaps over Binary Fields

Quang Dao *Carnegie Mellon University*

Scott Duke Kominers *Harvard Business School and a16z frontier*

Justin Thaler *a16z frontier and Georgetown University*

Kai Zhe Zheng *Simons Institute for the Theory of Computing*



STOC 2027 Video Submission

Hash-based SNARKs and Proximity Gaps

Prover commits to $f, g : D \to \mathbb{F}_q$

- **claimed Reed–Solomon:** $\deg < K$
- $N = |D|$, rate $\rho = K/N$

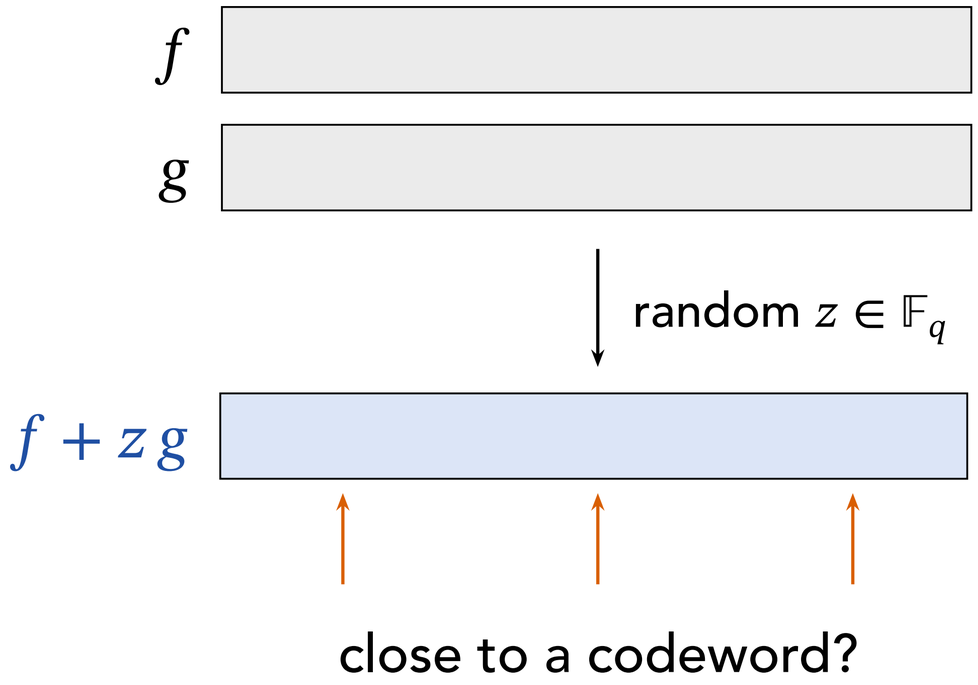
Verifier tests one combination

- $f + z\,g$, random z; then a few queries

Binary fields: additive domains

- $q = 2^m$, D an $\mathbb{F}_2$-subspace of $\mathbb{F}_q$

[Binius, Flock, BinarySpartan, LeanVM, Magnetar]



Soundness analysis: $f + z\,g$ close for many z $\Rightarrow$ f, g close

Mutual Correlated Agreement

Agreement with the code C

$$\mathrm{agr}(u) = \max_{c \in C} \left| \{ x \in D : u(x) = c(x) \} \right|$$

$$\mathrm{CA}(f, g) = \max_{c, c' \in C} \left| \{ x \in D : f(x) = c(x),\ g(x) = c'(x) \} \right|$$

MCA at threshold T, with error ε

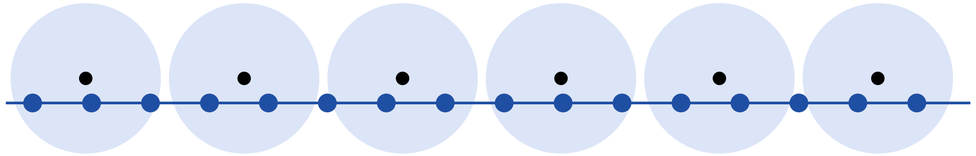
For all f, g, all but an ε fraction of $z \in \mathbb{F}_q$, all $S \subseteq D$:

$$|S| \geq T, \quad (f + z\,g)|_S \in C|_S \implies f|_S, g|_S \in C|_S$$

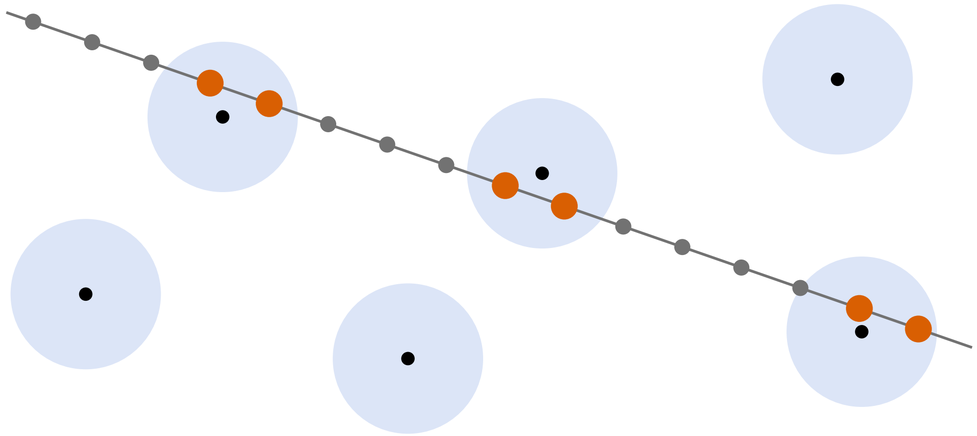
Exceptional challenges, when $\mathrm{CA}(f,g) < T$

$$\mathrm{Bad}_T(f, g) = \left\{ z \in \mathbb{F}_q \ :\ \mathrm{agr}(f + z\,g) \geq T \right\}$$

disc: agreement $\geq T$ with a codeword



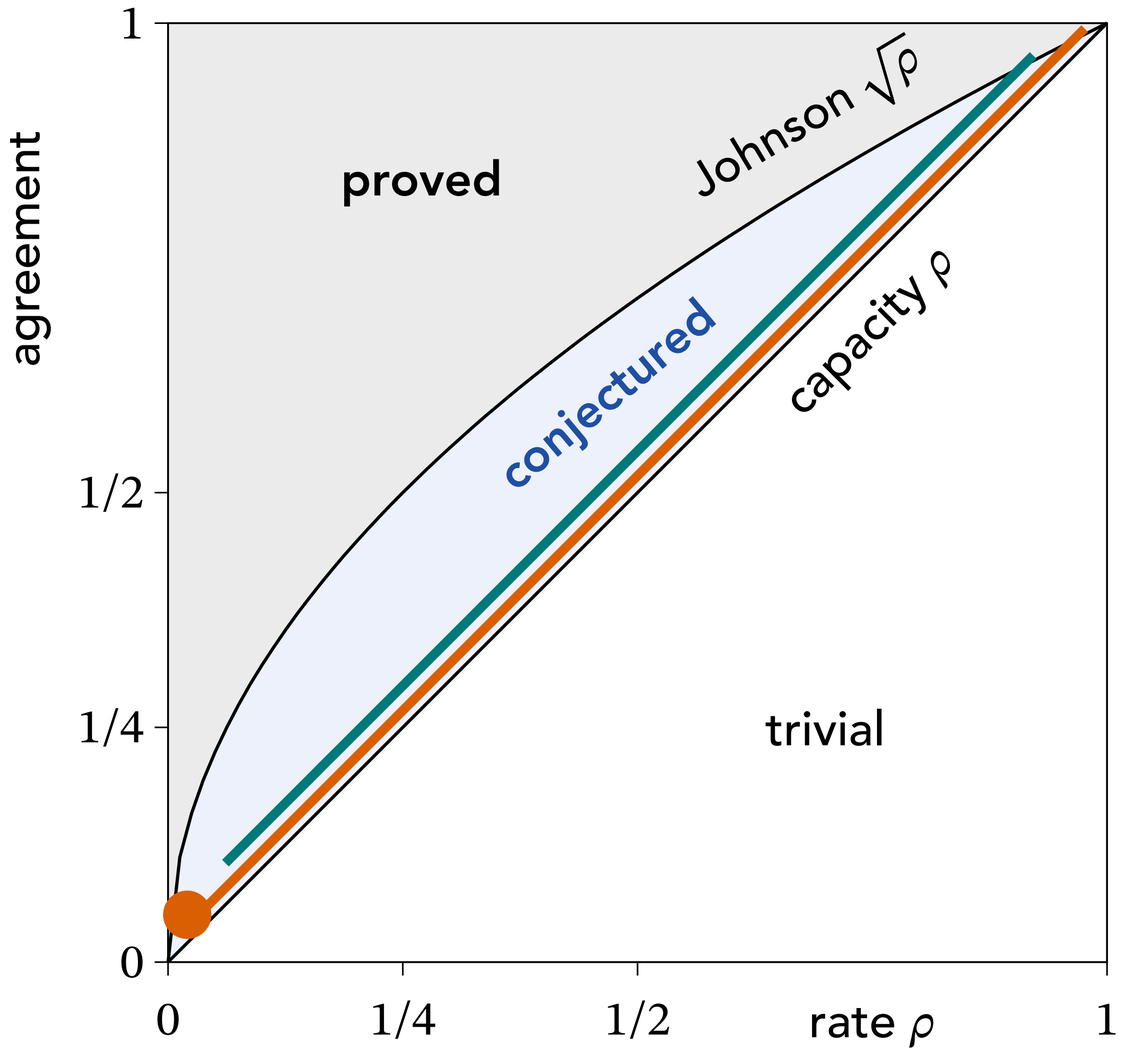
f, g close: every z is close



otherwise: only a few z are close

MCA fails: some (f,g) has $\mathrm{CA}(f,g) < T$ and $|\mathrm{Bad}_T(f,g)| > \varepsilon\, q$

Prior Work on Proximity Gaps



Proved above Johnson

in every field: error $O_\eta(N/q)$

a few positions below: $O(N^6)$ challenges

[BCIKS, BCHKS; Jo26]

Conjectured to capacity

refuted only as agreement approaches capacity, or at rate $\rho \to 0$

[BCIKS 8.4, WHIR 4.12; CS, DG, KKH]

Proved below Johnson

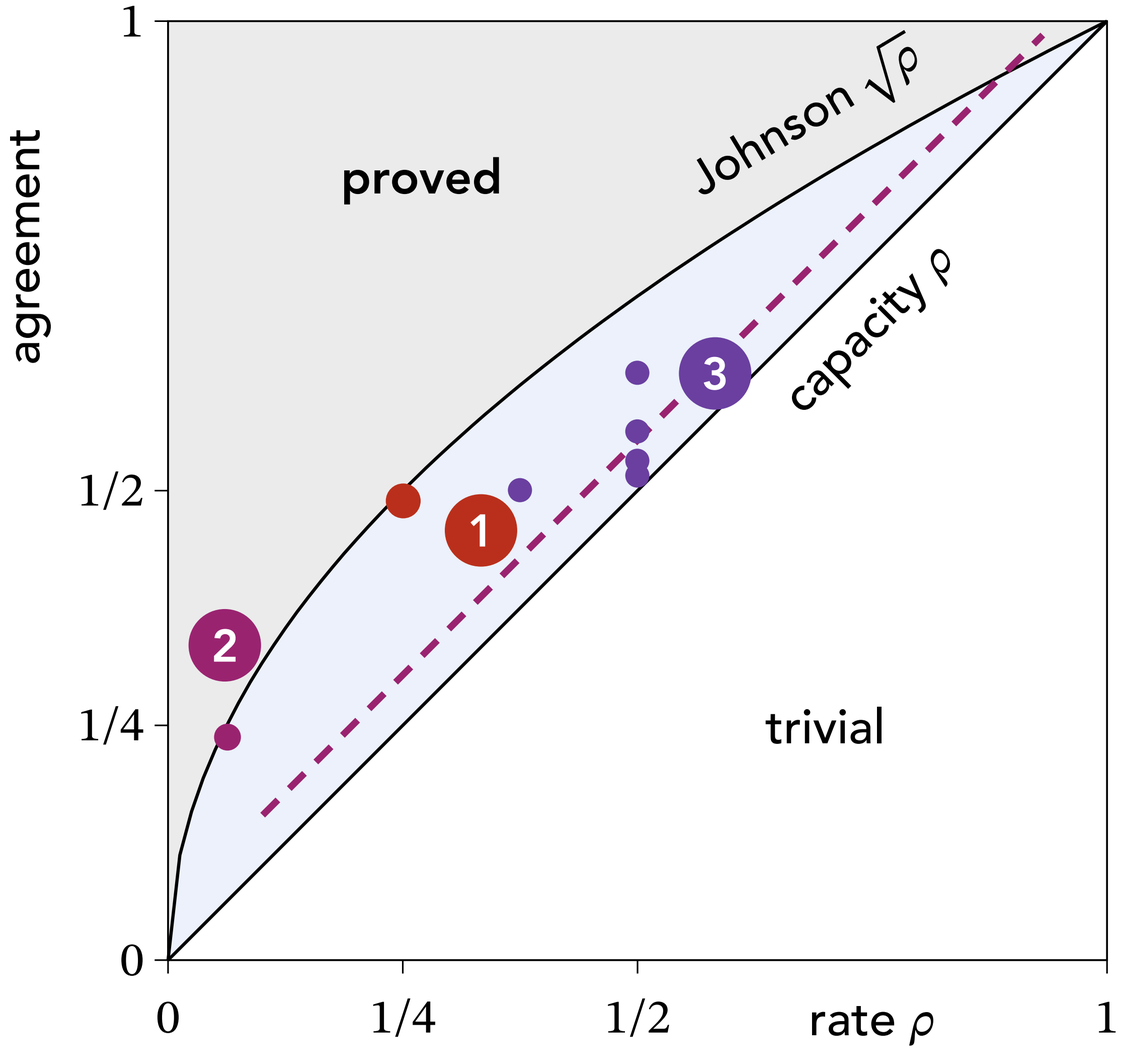
in large characteristic, or at random or explicit points

[BCPZZ, Jeronimo, DKT; GG; AGG, subspace designs]

On binary additive domains (that SNARKs rely on), do gaps hold below Johnson?

Our Results

D : binary additive domain



1 Gold construction

dense D, **rate** $1/4$, **at** $1/2 - o(1)$:
$N^{\Omega(\log N)}$ exceptional z

every rate: superpolynomially many

2 Subspace locators

every D, **rate** $1/16$, **at** $N/4 - 1$:
$(N-1)(N-2)/6$ exceptional z

every rate: every z, if $q \leq N^a$

3 Decision trees

every D, **rate** $1/2$, **at** $1/2 + 2^{-h-1}$:
$\Omega_h(\min\{N^{2^h-h-1}, q/N\})$ exceptional z

rate $3/8$, **at** $1/2$: cubically many

All results are verified in Lean.

Impact on Binary-Field SNARKs

Gold construction

dense additive domain: as in Binius64

$$> 2^{-29.9}$$

128-bit challenge field

$N = 2^{27}$, inside a 32-bit base field

rate $1/4$, agreement 0.494 (Johnson 0.5)

Decision trees

every additive domain: even sparse ones, as in LeanVM and Flock

$$> 2^{-27}$$

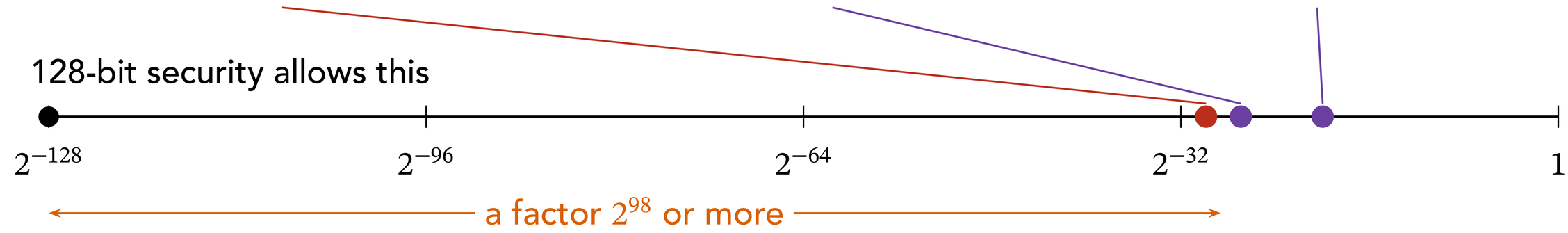
256-bit challenge field

$N = 2^{22}$, any base field (LeanVM: 64-bit)

rate $1/2$, agreement $17/32 = 0.531$ (Johnson 0.707)

$$\geq 2^{-20}$$

192-bit challenge field



Rate $1/8$, BBHR 2018: an analysis can certify at most 57.17 of its 60 bits

None of these systems relies on proximity gaps below Johnson.

Decoding Lists

No polynomial list-size bound at any fixed agreement below Johnson

Dense additive domains, field of size $O(N)$

- **rate** $1/4$: one word agrees with $N^{\Omega(\log N)}$ codewords on $1/2 - o(1)$ of D
- D at least an eighth of its field: $N^{(1/8-o(1))\log_2 N}$ codewords
- **every fixed rate** ρ: superpolynomial lists at an agreement strictly between ρ and $\sqrt{\rho}$

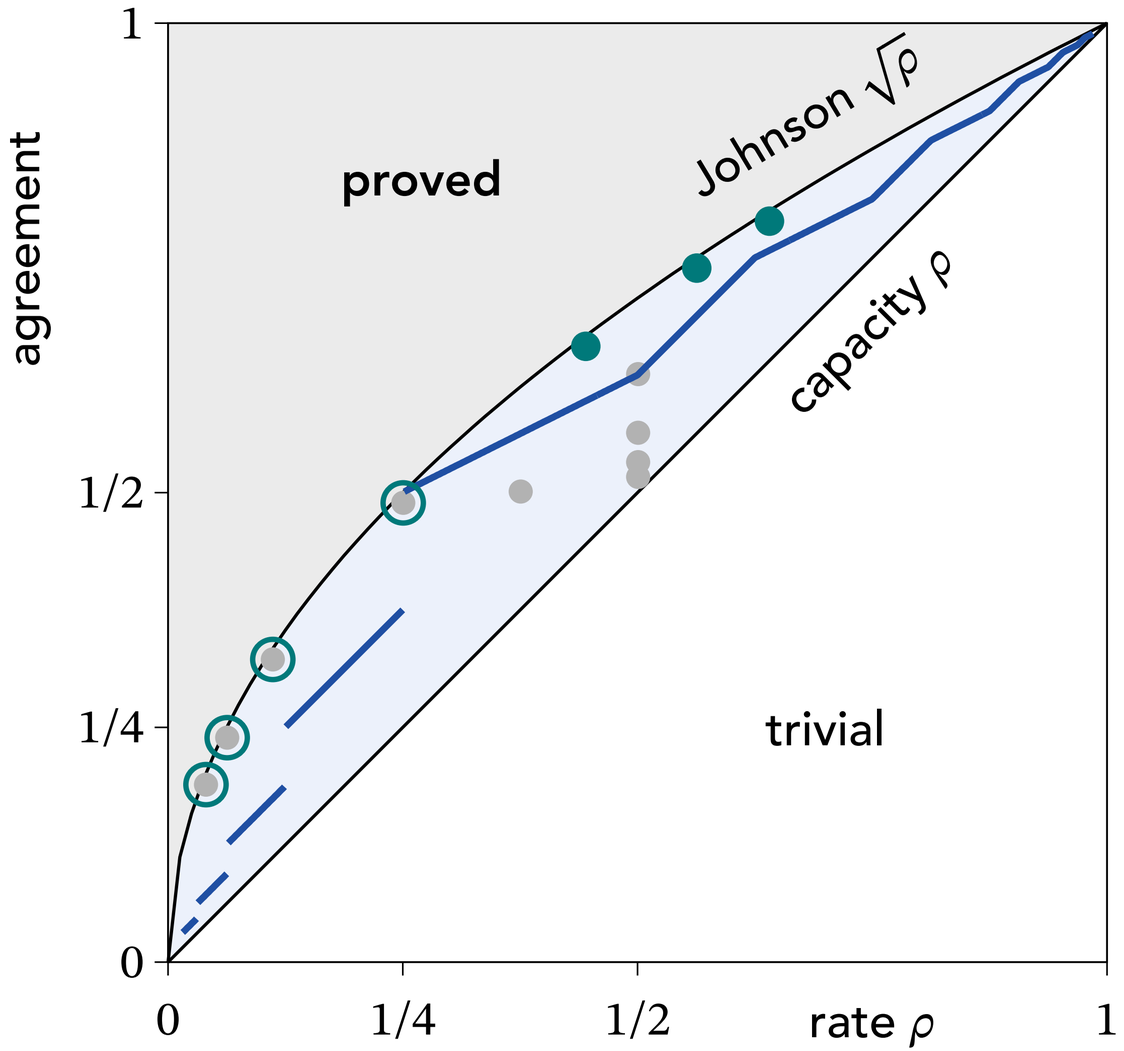
Every characteristic p, rate $1/b^2$, b a power of p

- on $\mathbb{F}_{b^{2n}}$, the word $x^{N/b}$ agrees with $N^{\Omega_b(\log N)}$ codewords on $1/b - \Theta_b(N^{-1/4})$ of D
- Johnson is $\sqrt{\rho} = 1/b$: $b = 2^k$ gives rate 4^{-k} near Johnson, over a field of size N

Earlier lower bounds, and concurrent independent work

- **Earlier:** superpolynomial lists at vanishing rate [GR, BKR]; linear-size lists at Johnson [JH]
- **Zhu:** the same lists at rate $1/4$ on full binary fields
- **Alrabiah–Goyal–Guruswami:** lists just beyond Johnson on $\mathbb{F}_{b^{4t}}$, rates $1/b^2$ and $(1 - 1/b)^2$

Concurrent Counterexamples



- our results (from previous slide)

Zhu arXiv 2610.15815

full field $\mathbb{F}_{2^h}$, every rate: $2^{h^2/8-O(h)}$ codewords

neither envelope contains the other:

his is higher on $(1/4,1/2)$ for odd h,

ours is near Johnson at 4^{-k} when $2k \mid h$

Alrabiah–Goyal–Guruswami

full field $\mathbb{F}_{b^{4t}}$, b a prime power:

- rate $1/b^2$, as ours, by the same identity
- rate $(1-1/b)^2$, new for $b > 2$

prime fields: polynomial lists beyond Johnson

ECCC TR26-304 [AGG26]

Only ours: every suitable additive domain, exceptional challenges for gaps and MCA

Common Mechanism: Pole Reduction

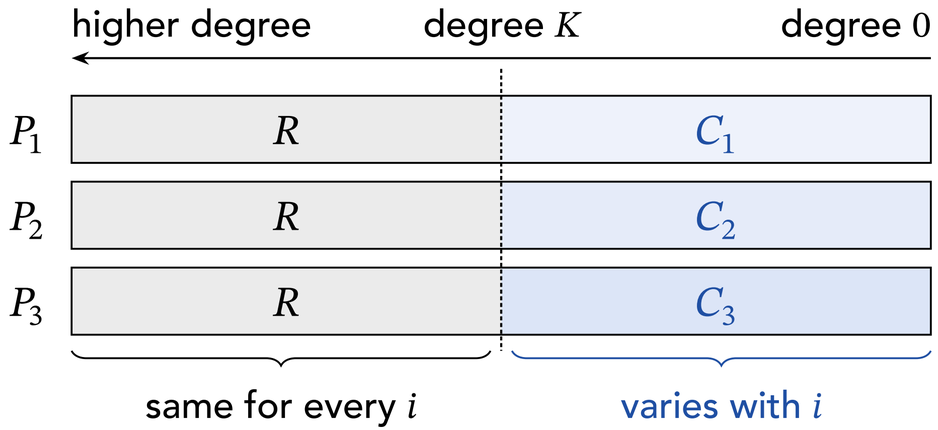
1. One family, one pair

[BKR]; division by a linear factor [BCHKS, Crites–Stewart]

Start: a family with shared high coefficients

$$P_i = R + C_i \qquad i = 1, \ldots, L$$

each P_i has $\geq T$ roots in D $\quad$ C_i distinct, deg $C_i \leq K < T$



Pick a pole $\beta \notin D$, divide by $X - \beta$

TWO FIXED INPUTS

$$f(x) = \frac{R(x)}{x - \beta} \qquad g(x) = \frac{1}{x - \beta}$$

FOR EACH MEMBER i

$$z_i = C_i(\beta)$$ challenge

$$H_i(X) = -\frac{C_i(X) - C_i(\beta)}{X - \beta}$$ codeword, deg $H_i < K$

$$f + z_i\, g - H_i = \frac{R}{x-\beta} + \frac{z_i}{x-\beta} + \frac{C_i - z_i}{x-\beta} = \frac{P_i}{x-\beta} \quad \text{on } D \quad \Longrightarrow \quad \operatorname{agr}(f + z_i\, g) \geq T$$

Common Mechanism: Pole Reduction

2. Why the pair is a counterexample

$$f(x) = \frac{R(x)}{x-\beta} \qquad g(x) = \frac{1}{x-\beta}$$

THE TWO INPUTS, TOGETHER: FAR

$$\mathrm{CA}(f, g) = \mathrm{agr}(g) = K$$

EVERY COMBINATION $z_i = C_i(\beta)$: CLOSE

$$\mathrm{agr}(f + z_i\, g) \;\geq\; T \;>\; K$$

At least K: interpolate both inputs on any K points.

At most K: g agrees with each h of degree below K on at most K points. Each such point is a root of $(X-\beta)\,h(X) - 1$, which is -1 at β and has degree $\leq K$.

On D, $f + z_i\, g - H_i = P_i/(x-\beta)$, with $\deg H_i < K$. The codeword H_i agrees with $f + z_i\, g$ at every root of P_i in D, and P_i has at least T of them.

$\Longrightarrow$ every z_i $(i = 1, \ldots, L)$ lies in $\mathrm{Bad}_T(f, g)$

Most challenges are distinct

Two members collide at no more than K poles: $C_i(\beta) = C_j(\beta)$ makes β a root of $C_i - C_j \neq 0$, of degree at most K.

Averaging over the $q - N$ poles, some pole gives $\left|\mathrm{Bad}_T(f, g)\right| \;\geq\; \left|\{C_i(\beta)\}_{i \leq L}\right| \;\geq\; \frac{1}{2} \min\left\{L, \frac{q-N}{K}\right\}$



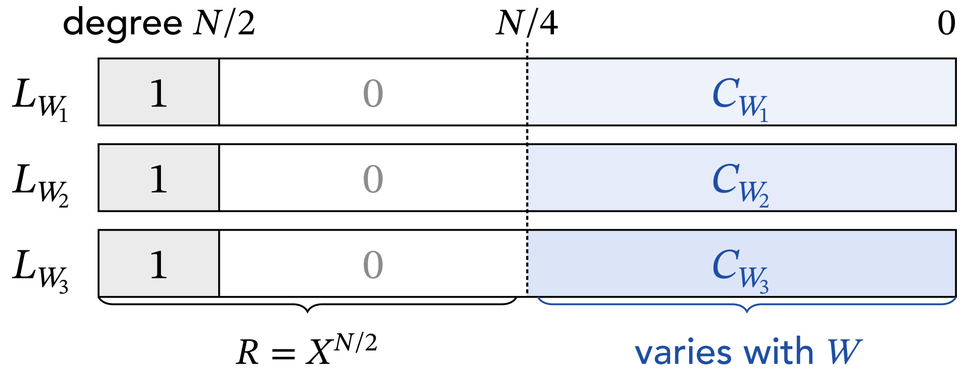
Common Mechanism: Pole Reduction

3. Example: hyperplanes

Linearized locators: a gap below the top

$$L_W = X^{N/2} + a_W X^{N/4} + (\deg \le N/8)$$

W: one of the $2N-2$ affine hyperplanes of D, $|W| = N/2$



Pole reduction with $K = N/4$, $T = N/2$

TWO FIXED INPUTS

$$f(x) = \frac{x^{N/2}}{x-\beta} \qquad g(x) = \frac{1}{x-\beta}$$

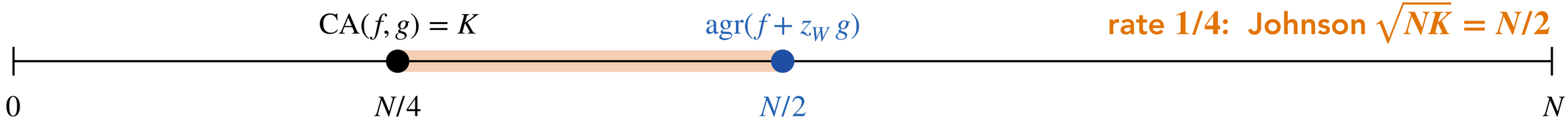
FOR EACH HYPERPLANE W

$$z_W = C_W(\beta) \qquad f + z_W\, g - H_W = \frac{L_W}{x-\beta}$$

$f + z_W\, g$ agrees with a codeword on all of W

All $2N-2$ challenges are distinct, and they are the only ones at agreement $N/2$.

[BGKS] used the same locators at rate $1/8$, with agreement above Johnson.



Common Mechanism: Pole Reduction

4. Comparison between hyperplanes and our other constructions

Input: L polynomials $P_i = R + C_i$, each with T roots in D, $\deg C_i < K$

Output: a pair at rate $\rho = K/N$, with at least half of $\min\{L, (q-N)/K\}$ bad challenges at agreement T/N

Johnson: at agreement $\sqrt{\rho} + \eta$, there are at most $\mathrm{poly}(N, 1/\eta)$ bad challenges [BCIKS]

FAMILY	DOMAIN	RATE ρ	AGREEMENT	JOHNSON	SETS L
Hyperplanes the example from the previous slide	any	$1/4$	$1/2$	$1/2$	$2N-2$
Gold construction zero sets of quadratic forms	dense	$1/4$	$1/2 - \Theta(N^{-1/4})$	$1/2$	$N^{\Omega(\log N)}$
Subspace locators codimension-two subspaces	any	$1/16$	$1/4 - 1/N$	$< 1/4 - 2/N$	$\approx N^2/6$
Decision trees unions of affine subspaces picked out by a decision tree	any	$1/2$	$1/2 + 2^{-h-1}$	$1/\sqrt{2}$	$\Theta_h(N^{2^h-h-1})$

$\Longrightarrow$ **each of our other constructions gives many more sets, at a cost in rate, agreement or domain**

Gold Construction

1. Keep the property of hyperplanes that pole reduction uses

Linearized locators have constant derivative

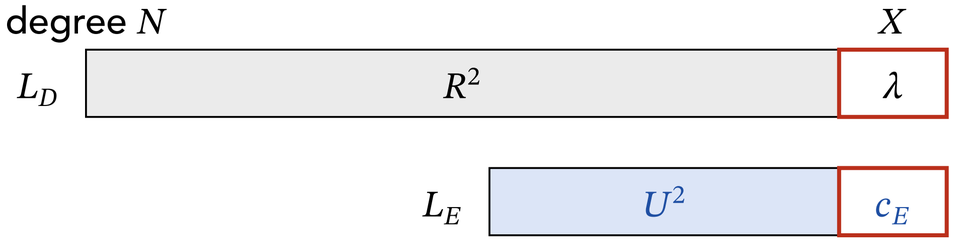
Hyperplanes: L_W is linearized, so $L'_W = c_W$ is constant.

$L' = c$ constant $\iff$ $L = U^2 + cX$

In characteristic two, X^k has derivative zero for every even k.

The domain is a subspace too: $L_D = R^2 + \lambda X$, $\deg R = N/2$.

Look for other sets $E \subseteq D$ with $L'_E = c_E$ constant:



Adding them cancels the linear terms

$$\left(R + \sqrt{\lambda/c_E}\ U\right)^2 = L_D + \frac{\lambda}{c_E} L_E$$

L_D and L_E vanish on E, hence so does the left side.

FOR EACH SUCH SET E

$$P_E = R + C_E \qquad C_E = \sqrt{\lambda/c_E}\ U$$

P_E vanishes on E, $\deg C_E = |E|/2$

$|E| < N/2$: then $\deg C_E < K = N/4$, and all such E form one family, with one pair (f, g).

Hyperplanes: the boundary case $|E| = N/2$.

Needed: superpolynomially many such sets E, with $|E|$ just below $N/2$

Gold Construction

2. Where to find such sets: level sets of quadratic functions

A test: the indicator of E has least degree

H: degree below N, 1 on E, 0 on $D \setminus E$.
It has $N - |E|$ roots, hence $\deg H \geq N - |E|$.

Equality: $L_D = \mu H L_E$, and then $L'_E = \lambda/\mu$.

The degree of H is read from H'

$$H^2 + H = \frac{L_D}{\lambda} H' \qquad \deg H = \frac{N + \deg H'}{2}$$

Why: $H^2 + H$ vanishes on D, so it equals $L_D Q$.
Differentiate: $H' = \lambda Q + L_D Q'$, and degrees force $Q' = 0$.

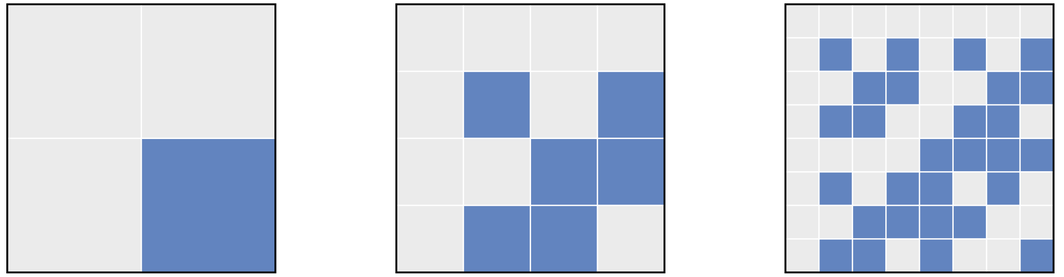
Least degree $\deg H = N - |E|$ needs $\deg H' \leq N - 2|E|$.

Linear: H' is constant: the hyperplanes, $\deg H = N/2$.

Quadratic: $H' = J +$ constant, with J linearized.

Quadratic ψ of rank $2t$

$\psi = x_1 x_2 + \cdots + x_{2t-1} x_{2t} + \kappa$ in suitable coordinates
Radical: the other $d - 2t$ directions, which ψ ignores.



$t = 1$: $N/4$ $\quad$ $t = 2$: $3N/8$ $\quad$ $t = 3$: $7N/16$

One cell per coset of the radical. Blue: $E = \{\psi = 1\}$.

$$|E| = T = \frac{N}{2} - \frac{N}{2^{t+1}}$$

Least degree needs $\deg J \leq N - 2T = N/2^t$.

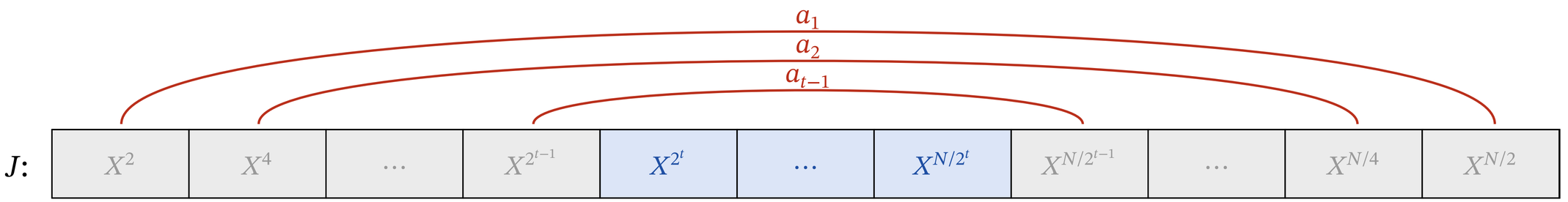
The rank alone does not give this: in general $\deg J = N/2$.

Gold Construction

3. Full field: the degree condition is $t-1$ linear conditions

$D = \mathbb{F}_N$, $N = 2^d$: $\psi = \mathrm{Tr}(a_1 x^3) + \mathrm{Tr}(a_2 x^5) + \cdots$ + linear + constant

$H' = J +$ constant, and J is linearized: its possible terms are



The term $\mathrm{Tr}(a_i\, x^{2^i+1})$ adds $a_i X^{2^i} + a_i^{2^{d-i}} X^{N/2^i}$ to J: one term at each end.

$\deg J \le N/2^t$ exactly when $a_i = 0$ for every $i < t$: only the exponents $2^i + 1$ with $i \ge t$ remain [Gold 1968]

Top end: $\deg J \le N/2^t$, the least degree $\deg H = N - T$ that the level sets need

Bottom end: $J = J_0^{2^t}$, and J_0 vanishes on the radical: every nonzero solution has rank $\ge 2t$

Each condition clears one term at each end, linearly in ψ. The same holds on any additive D.

Gold Construction

4. Any additive domain: the Gold moments, and many solutions

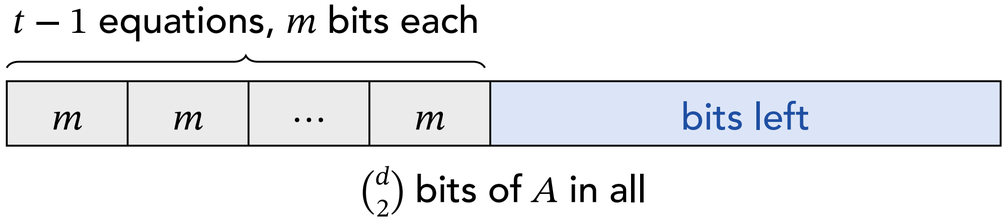
Any additive $D \subseteq \mathbb{B} = \mathbb{F}_{2^m}$, $|D| = 2^d$: the same conditions in coordinates

$$M_k(A) = \sum_{i<j} A_{ij}\left(\omega_i \omega_j^{2^k} + \omega_j \omega_i^{2^k}\right) = 0, \qquad k = 1, \ldots, t-1$$

A: the matrix of the cross terms $x_i x_j$ of ψ. $\omega_i^2 = \ell_i'$, where ℓ_i is the linearized polynomial of x_i.

Together these clear both ends of J, as on the full field.

Linear over $\mathbb{F}_2$: many solutions

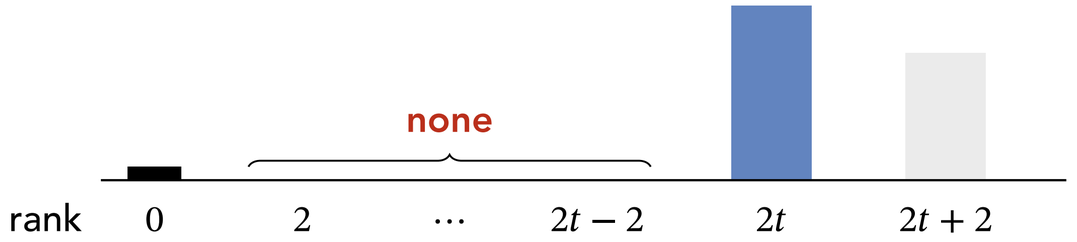


$\mathscr{A}$: the space of solutions $\quad |\mathscr{A}| \;\geq\; 2^{\binom{d}{2} - m(t-1)}$

Each matrix of rank $2t$ gives 2^{2t} level sets E of size T.

Many of rank exactly $2t$

Every nonzero solution has rank $\geq 2t$ (bottom end).



Delsarte–Goethals: if $\Delta = m - t\,(m - d + \iota) \geq 1$,

$$\#\{\text{rank } 2t\} \geq (2^\Delta - 1) \begin{bmatrix} n \\ t \end{bmatrix}_4$$

$n = \lfloor d/2 \rfloor$, $\iota = 1$ if d is even, $\iota = 0$ if d is odd

Gold Construction

5. From the count to exceptional challenges

The count needs a dense domain

$\Delta = m - t\,(m - d + \iota) \geq 1$: raising t by one costs $m - d + \iota$

DOMAIN OF SIZE 2^d IN $\mathbb{F}_{2^m}$

$m \geq 2d$	$\Delta < 1$ for $t \geq 2$: hyperplanes only
$m - d$ fixed	$t = \Theta(\log N)$: $N^{\Omega(\log N)}$ sets
$m \leq d + 3$	$N^{(1/8 - o(1))\log_2 N}$ sets, $T = N/2 - \Theta(N^{3/4})$
Binius64	$d = 27$, $m = 32$: $t = 6$

Distinct challenges $z_E = C_E(\beta)$

Two members $P, \tilde{P}$ give the same challenge when $P(\beta) = \tilde{P}(\beta)$: in general at up to $K = N/4$ poles.

Here every member satisfies

$$P'\left(P^2 + L_D\right) = \lambda P$$

Hence $P(\beta)$ determines $P'(\beta)$, and two members have equal derivatives at no more than $N/2^{2t}$ poles.

Some pole β then gives at least half of $\min\{L,\ (q - N)\,2^{2t}/N\}$ distinct challenges.

BINIUS64: COMMON AGREEMENT	AGREEMENT OF $f + z\,g$	PROBABILITY OVER $\mathbb{F}_{2^{128}}$
$N/4$, exactly	$T/N \approx 0.494$	above $2^{-29.889}$

Gold Construction

6. Generalization to every characteristic: $\mathbb{B} = \mathbb{F}_{b^{2n}}$, rate $1/b^2$

Any prime power b: the word $R = X^{N/b}$, degree below $K = N/b^2$

Proposition 5.21

- **Agreement sets:** zeros of $\sum_{i \geq t} \mathrm{Tr}(a_i\, x^{b^i+1})$ of rank $2t$ and elliptic type [Schmidt]
- **Size:** exactly $T = N/b - (b-1)\, N/b^{t+1}$ zeros each, just below N/b

Squares become bth powers

proof of Theorem 5.22

$$Q^b - Q = (X^N - X)\, Q'$$

- **Why:** Q takes values in $\mathbb{F}_b$ on D, so $Q^b - Q$ vanishes on D
- **Divide** by F, the bth root of Q': $P = Q/F$ has degree N/b and the same T roots
- **Codeword:** $C = P - R$ has $C^b = Q/F^b - X$, so $\deg C = T/b < K$

Theorem 5.22, Corollary 5.23

Lists: $N^{\Omega_b(\log N)}$ codewords at agreement $1/b - \Theta_b(N^{-1/4})$; **pairs:** many distinct challenges

Agreement is b times the degree $\Longrightarrow$ Johnson only at rate $1/b^2$

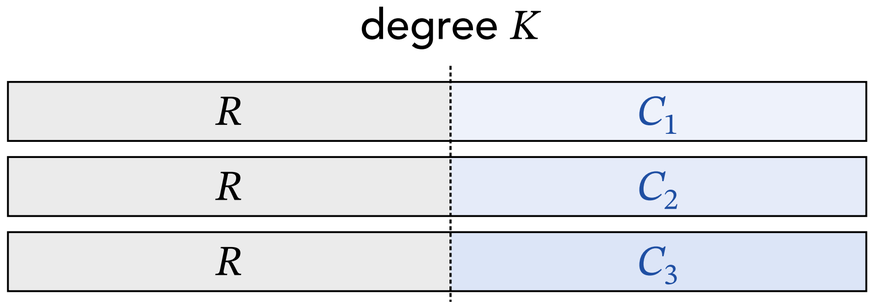
Comparison with Concurrent Work

Similarities and Differences in Techniques & Results

Every list bound comes from one recipe

- (i) many sets of T points in D
- (ii) their polynomials share every coefficient above K

[BKR]; the two properties as in [AGG26, Section 2]



Shared

rate $1/b^2$: $Q^b - Q = (X^N - X)\,Q'$ for quadratic forms Q, then division by the bth root of Q' on different families of forms

[AGG26] Thm 1.1; our Thm 5.22

Zhu: BCH supports, Schmidt's count, the word $x^{N/2}$

Differences

Zhu: the domain $\mathscr{E}_W(\mathbb{F}_{2^h})$, W found by double counting

ours: Gold equations on every prescribed additive D

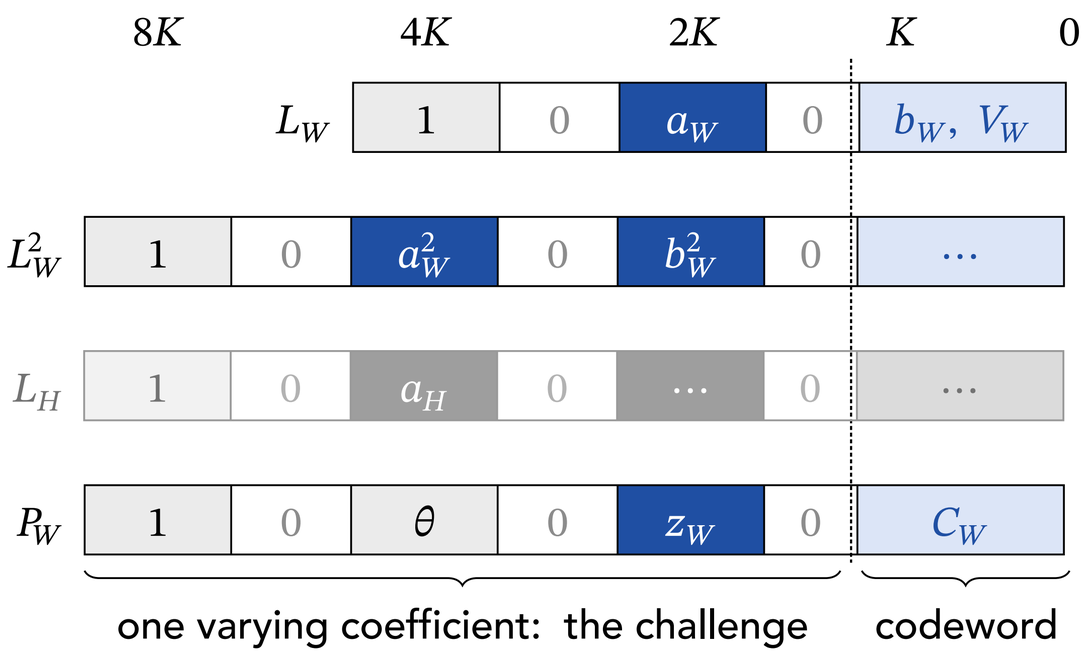
[AGG26], prime fields: a multiplicative subgroup, moved by low-degree maps

Only ours: pole reduction, one pair with one challenge per codeword, kept distinct by the collision bound

Both concurrent papers bound **list sizes only**: neither gives proximity gap or MCA counterexamples

Codimension Two Construction

Additive domain $D \subseteq \mathbb{B}$, $|D| = N = 16K$, and arbitrary $\theta \in \mathbb{F}\backslash\mathbb{B}$



Locator $L_W = (X - w_1)\cdots(X - w_{N/4})$ of $W \leq D$

Coefficients (a_W, b_W) determine W; only a_W lies above K

$a_W \in \mathbb{B}$ alone gives at most $|\mathbb{B}|$ distinct challenges

Squaring doubles every degree: b_W^2 moves above K

but a_W^2 now varies at degree $4K$

Hyperplane $H = W \cup (W + v)$, $v \in D\backslash W$

$L_H = L_W(L_W + c)$ with $c = L_W(v)$: $a_H = a_W^2 + c$ varies

Choose $c = a_W^2 + \theta$ instead: degree $4K$ holds θ

$$P_W = L_W(L_W + a_W^2 + \theta) \qquad z_W = a_W^3 + b_W^2 + \theta\, a_W$$

Roots of P_W **in** D: exactly W, as $L_W + c$ is never 0 on D: $L_W + a_W^2 \in \mathbb{B}$ and $\theta \notin \mathbb{B}$

Distinct challenges: 1 and θ are independent over $\mathbb{B}$, so z_W determines (a_W, b_W), hence W

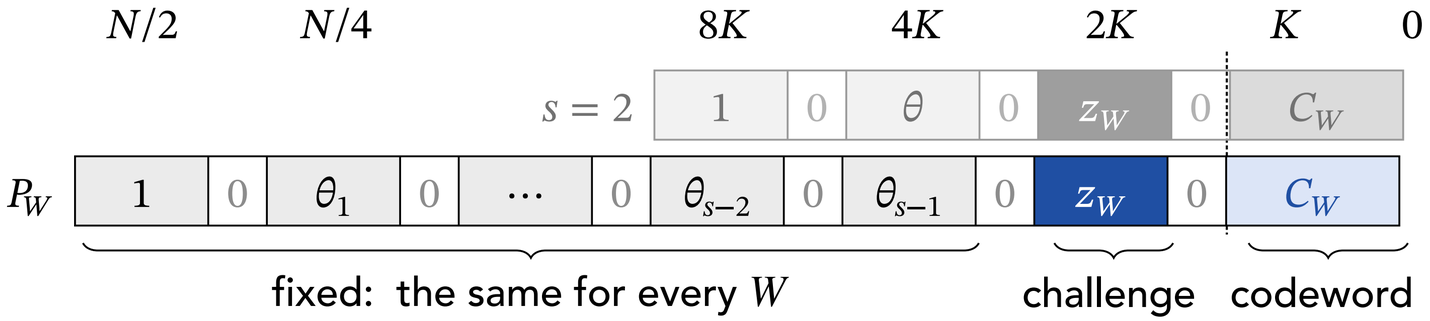
Inputs: $f = X^{8K-1} + \theta X^{4K-1}$, $g = X^{2K-1}$ **Codeword:** C_W/X, of degree below K ($0 \in W$, so X divides C_W)

$$f + z_W\, g - C_W/X = P_W/X = 0 \quad \text{on } W\backslash\{0\}$$

$(N-1)(N-2)/6$ distinct challenges at agreement $N/4 - 1$, rate $1/16$, just above Johnson

Every Challenge, at Every Rate

Additive domain D of size N, challenge field $\mathbb{F}$ of size $q \le N^a$ for a fixed a



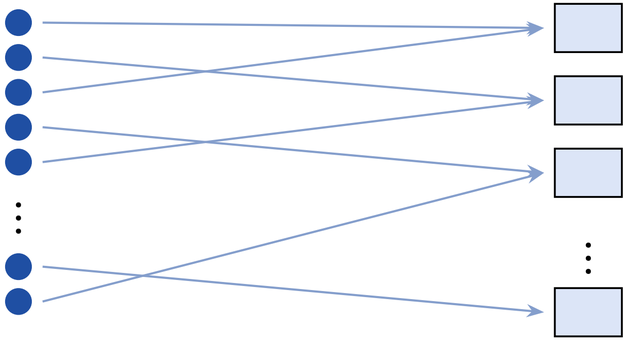
Codimension 2: previous slide

Codimension s: $P_W = A_W(L_W)$

$\deg A_W = 2^{s-1}$, $|W| = 4K = N/2^s$

Theorem. For each $\rho \in (0,1)$ there is a constant $\alpha \in (\rho, \sqrt{\rho})$, depending only on ρ and a, such that for large N some pair f, g has $\mathrm{CA}(f,g) = \lfloor \rho N \rfloor$ at message length $\lfloor \rho N \rfloor$, yet every $f + z\,g$, $z \in \mathbb{F}$, agrees with a codeword on αN points

subspaces W $\quad W \mapsto z_W$ $\quad$ **elements of $\mathbb{F}$**



1. Every element of $\mathbb{F}$ is a challenge

Take $s > 2a$: then $M = \Theta(N^s) > (q-1)^2$ subspaces,

and some $\theta_1, \ldots, \theta_{s-1}$ give $qM/(q+M-1) > q-1$ distinct z_W

2. Any rate ρ, with a gap of $\Theta(N)$

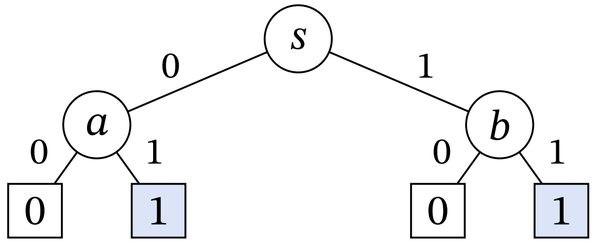
Build the pair on $D_0 \le D$, $|D_0| = \mu N$, message length $K_0 = \mu N/2^{s+2}$

Multiply by the locator of $\lfloor \rho N \rfloor - 2K_0 + 1$ points outside D_0

Each point is a new agreement: $\lfloor \rho N \rfloor + 2K_0$ for every challenge

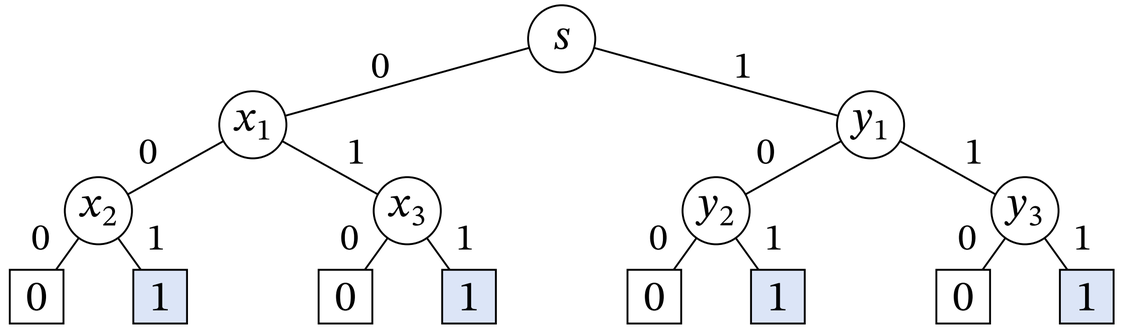
Decision Trees Construction

A tree of linear tests on D selects the set A of points that reach a leaf 1



height 2: 3 functionals, 2 tests on each path

$A = \{s = 0,\ a = 1\} \cup \{s = 1,\ b = 1\}$



height 3: 7 functionals, 3 tests on each path

Tree functions of height h

- $2^h - 1$ independent functionals, $d \geq 2^h - 1$
- support $A = \{\varphi = 1\}$: 2^{h-1} disjoint flats F_j
- each flat has size $m = N/2^h$, and $|A| = N/2$
- $\Theta_h(N^{2^h-1})$ distinct A: $\approx N^{2^h-1}$ spans of functionals

Input to pole reduction

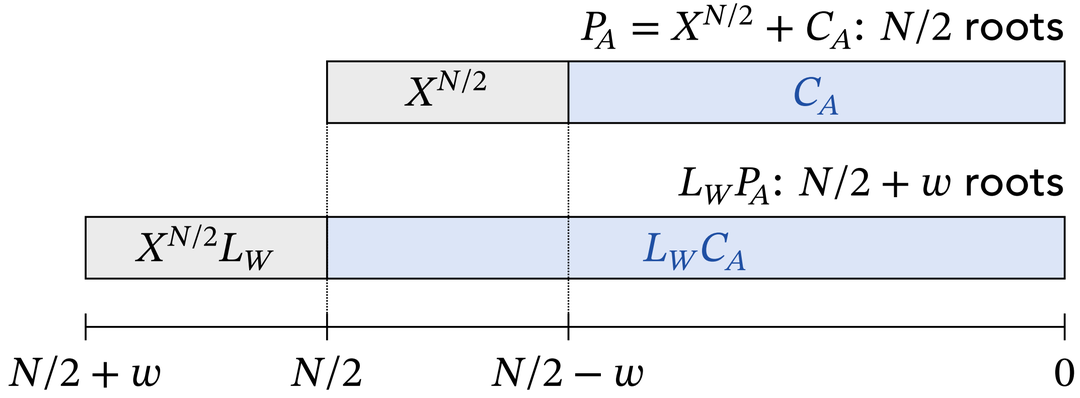
- a flat F of size m: $L_F = X^m + G_F$, $\deg G_F \leq m/2$
- $L_A = L_{F_1} \cdots L_{F_{2^{h-1}}} = X^{N/2} + C_A$
- $\deg C_A \leq N/2 - m/2 = N/2 - N/2^{h+1}$
- common part $R = X^{N/2}$, $T = N/2$, $K = N/2 - N/2^{h+1}$

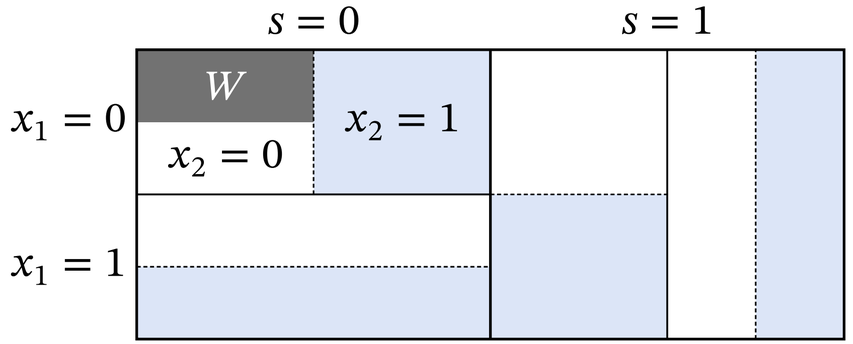
Rate $1/2 - 2^{-h-1}$: a pair with $\mathrm{CA}_K(f, g) = K$, and $\Omega_h(\min\{N^{2^h-1},\ q/N\})$ challenges at agreement $1/2$

$\Longrightarrow$ **height** 2, **rate** $3/8$: $\Omega(\min\{N^3,\ q/N\})$ challenges at agreement $1/2$, cubic in N when $q \geq N^4$

Decision Trees at Rate One Half

Padding by a subspace W: rate exactly $1/2 + 2^{-h-1}$





L_W raises T and K together

$L_W P_A$ vanishes on $A \cup W$, which gives $T = N/2 + w$.

$R = X^{N/2} L_W$ and $\deg(L_W C_A) \le N/2$: thus $K = N/2$.

$\Longrightarrow$ $T - K = w$ as before, now at rate exactly $1/2$.

This requires $A \cap W = \varnothing$ for every set A.

One W for all sets costs a factor N^h

Since $R = X^{N/2} L_W$ is common to all A, W is fixed first.

Each test on the all-zero path must vanish on W.

$\Longrightarrow$ W lies in that path's leaf 0, outside every A.

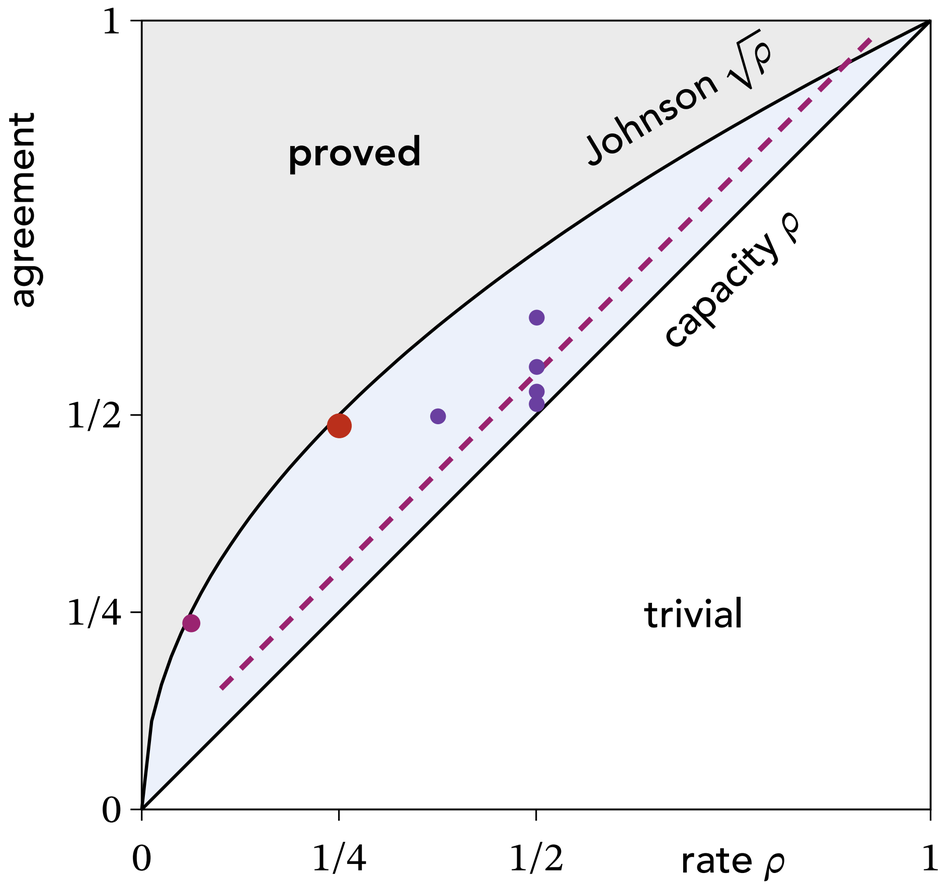
This leaves $\Theta_h(N^{2^h - h - 1})$ of the $\Theta_h(N^{2^h - 1})$ supports.

Fixed $h \ge 3$, any additive domain: $\Omega_h(\min\{N^{2^h - h - 1}, q/N\})$ challenges at agreement $1/2 + 2^{-h-1}$

$\Longrightarrow$ **LeanVM ($N = 2^{22}$, $\mathbb{F}_{2^{192}}$), $h = 4$:** exceptional probability $\ge 2^{-20}$ at agreement 0.53125

Summary & Open Questions

One mechanism: a family $P_i = R + C_i$ with a long shared top gives one pair (f, g) for the whole family



Gold construction

$N^{\Omega(\log N)}$ at rate $1/4$, approaching Johnson

Subspace locators

$\Theta(N^2)$ just above Johnson; every z, every rate

Decision trees

rate $1/2$, agreement $1/2 + 2^{-h-1}$

Every result is verified in Lean.

Open questions

Lower bounds: better counterexamples, filling in more of the map

Upper bounds: MCA beyond Johnson on domains with fast encoding, which SNARK provers need

Thank you!