CS229r. Lecture 19

4/4/17

0) LRCs

Today: 1) High-Rate LDCs

1.1) Multiplicity Codes

1.2) Alternates: Lifted Codes, Expander Codes } $n^{o(1)}$ locality

1.3) ~~LG~~ - Alon-Luby Tranform + Mult. } $n^{o(1)}$ locality

---

Part 0) LRCs : See notes for lecture 18

1.1 Multiplicity Codes:

Recall Reed-Muller Codes:

m-variate over $\mathbb{F}_q$; deg. $d \rightsquigarrow q$ $(d<q)$

coefficients $(m = O(1);\ q \to \infty)$: $\approx \frac{q^m}{m!} = \frac{n}{m!}$

locality: $q = n^{1/m}$

locality $n^\epsilon \Rightarrow$ Rate $= \frac{1}{(\frac{1}{\epsilon})!} \approx (\epsilon)^{1/\epsilon}$.

Q: Can we get $R = \Omega(1)$ with locality n^ϵ $(\epsilon \to 0)$?

Multiplicity Codes

Key Idea: Derivatives of polynomial give extra information about polynomial;

Information is "local".

Example:

for $f \in \mathbb{F}_q[X,Y]$ $\quad f_X$ = derivative wrt. X

f_Y = " Y.

Let $d = (2-\epsilon)\cdot q$;

- Encoding(f) = $\langle f(\alpha,\beta), f_X(\alpha,\beta), f_Y(\alpha,\beta) \rangle_{\alpha,\beta \in \mathbb{F}_q}$
- Maps $(\epsilon \to 0)$: $\mathbb{F}_q^{2q^2} \longrightarrow \mathbb{F}_q^{3\cdot q^2}$

(Rate approaching $2/3$)

- Decoding:
  - Note that $f|_{\ell : Y = a_2 X + b_2}$ (X) = poly of deg $\le d = (2-\epsilon)\cdot q$
  - $f(\alpha,\beta)\Big|_{\beta = a\cdot\alpha + b}$ gives q pieces of info. about $f|_\ell$
  - Can we compute $(f|_\ell)^{(k)}(\alpha,\beta)$? ← derivative of $(f|_\ell)$ wrt Z.

Calculus: $(f|_\ell)_2 = a_1 \cdot f_x + a_2 \cdot f_y$

Conclusion: can obtain: $\langle f|_\ell^{(\ell(t))}, (f|_\ell)_2^{(\ell(t))} \rangle_{(\ell(t) \mid t \in \mathbb{F}_q)}$

$\Rightarrow$ $2q$ "info" about $f|_\ell$

more than degree $d = (2-\epsilon)q$.

$\Rightarrow$ can recover coefficients of $f|_\ell$.

$\Rightarrow$ can compute $f(\alpha,\beta)$ $\forall$ $(\alpha,\beta) \in \ell$.

locality $= O(q)$; But not yet a locally correctible code.

(1) Need also to compute $f_x(\alpha,\beta)$; $f_y(\alpha,\beta)$

(2) ~~How~~ Need to correct ~~ϵ~~ $\epsilon' > 0$ fraction errors.

(2): Hermite decoding Problem:

given $g, h : \mathbb{F}_q \to \mathbb{F}_q$ s.t. $\exists f \in \mathbb{F}_q[X]$ $\deg f \le d = (2-\epsilon)q$

$$\text{s.t. } \left| \{ a \mid (f(a), f_x(a)) \neq (g(a), h(a)) \} \right| \le \epsilon' \cdot q.$$

find f; Exercise: Abstract Decoding

Solving (1): Decode two independent lines passing through (α, β); Yields $(f_{\ell_1})_2(\alpha,\beta)$; $(f_{\ell_2})_2(\alpha,\beta)$

$$\Rightarrow \quad a_1 f|_x + a_2 f|_y$$

$$b_1 f|_x + b_2 f|_y$$

Solve linear system to get $f_x(\alpha,\beta)$

$f_y(\alpha,\beta)$.

Conclusion.. Can get locality $\sqrt{n}$ with Rate $> \frac{1}{2}$

More derivatives $\Rightarrow$ Rate $\to 1$.

Clarification:

Hasse derivative: Right definition of derivative over finite fields.

for m-var. polynomials: let X^d denote $x_1^{d_1} \cdots x_m^{d_m}$

for $e = e_1 .. e_m$, $\partial_e f(x) =$ coefficient of Z^e in $f(x+Z) = \sum_{e'} Z^{e'} f_{e'}(x)$

Hasse derivative Properties:

① linear, polynomial ...

even over finite fields { ② $\forall e$ s.t $\Sigma e_i \le t$ $f_e(a) = 0 \Rightarrow a$ is a zero of multiplicity $(t+1)$ of f.

③ $\partial_{e_1} \partial_{e_2} f \neq \binom{e_1+e_2}{e_1} \partial_{e_1+e_2} f$

However $\partial_{e_1+e_2} f(a) = 0 \Rightarrow \partial_{e_1}(\partial_{e_2} f)(a) = 0$.

④ Otherwise behaves like usual derivatives.

Defn: Multiplicity Codes

Mult (m, d, q, s)

m, d, q: usual; s: new: multiplicity

- Encode polynomials f by evaluating $\{\langle f_e(a) \mid wt(e) \le s \rangle\}_a$

Parameters {

- $d = (1-\delta) s \cdot q \Rightarrow$ distance $= \delta$

Alphabet $= \mathbb{F}_q^{\binom{m+s}{m}}$;

Dimension $= \binom{m+d}{m}$; $n = q^m$

Locality $=$ poly$(s) \cdot q = O(q) = O(n^{1/m})$

(6)

$$\text{Rate} = \frac{\binom{m+d}{m}}{\binom{m+s}{m}\cdot q^m} \approx \frac{d^m \cdot m!}{m!\, s^m \cdot q^m} \approx \left(\frac{d}{sq}\right)^m$$

$s \gg m$
$s \approx m^2$

Locality ~~$\cdots$~~ : n^{ϵ} as $\epsilon \to 0$ [By letting $m = \frac{1}{\epsilon}$]

Rate $= 1 - \epsilon T$ by letting $s = \frac{1}{\epsilon^2}$

& $d = \left(1 - \frac{\epsilon}{m}\right) \cdot sq \approx$ ~~$(1-\epsilon^2)sq$~~

$\approx (1 - \epsilon T) sq$

so relative dist $\approx \epsilon T$.

Conclusion: Can get arbitrarily ~~good~~ small $\epsilon > 0$, $T > 0$

& have locality n^{ϵ} & Rate $1 - T$.

[Pay price in distance].

Can we get $\epsilon = o(1)$? .... Wail.

Other Codes

Reed-Solomon

Lifted Codes: ~~Given~~ $\mathcal{L}(m,d,q)$ [Guo, Kopparty, S.]

- $\mathcal{L}(m,d,q) = \{ f : \mathbb{F}_q^m \to \mathbb{F}_q \mid \forall \text{ lines } \ell \ \deg(f|_\ell) \le d \}$

- if $d < q(1-\frac{1}{p})$ & $q = p^t$ for prime p;

  then $\mathcal{L}(m,d,q) = RM(m,d,q)$

  else NOT;

  Furthermore as we fix m, p & let $t \to \infty$

  & $d \to q$

  Rate $\to 1$.

- local Decoding? Same as RM codes

Expander (Tanner Codes): [Hemenway, Ostrovsky, Wootters]

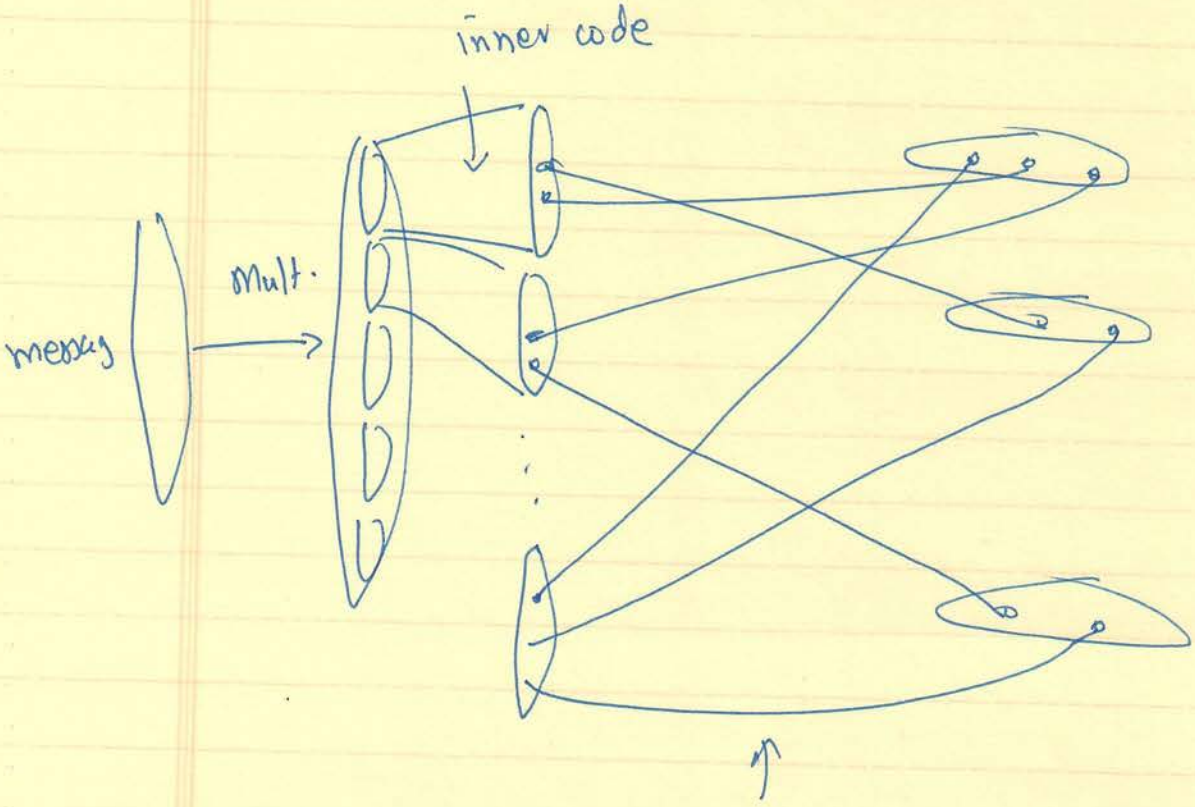
Expander codes where inner codes are (weak) LCCs.

...

$n^{o(1)}$ locality with $R = 1 - \delta - \epsilon$ ...

Key Idea: - Use Multiplicity codes of $n^{o(1)}$ locality with distance $= o(1)$. [Rate $= 1 - o(1)$]

- Use Alon-Luby Transform to improve distance!



Both steps Local.

Achieves: $R = 1 - \delta - \epsilon$

Corrects: $\frac{\delta}{2}$ fraction errors locally!!