Multiplicity Codes

Note Title 11/28/2011

Motivational Spiel

- Have heard of Locally decodable codes.
- Seem like a very useful notion.
- But all applications have been negative (PCPs, hardness of approx., average-case hardness, etc.)
- Why?

My take

- Rate matters in practice.
- Practioners used to rates of 80%, 90%;
- LDCs don't work in this regime!

Fix Notation

Codes : k - letter messages
$\downarrow$
n - letter codewords.

Recall Definition

- (ℓ, ϵ, δ) - LDC
  - C_n maps $\Sigma^k \to \Sigma^n$
  - $\ell(n)$ - locality (# queries)
  - Corrects $\epsilon(n)$ fraction errors w.p. $1 - \delta(n)$

- ℓ - LDC

  $\exists\ \epsilon, \delta > 0$ s.t. $\forall n$,

  C_n is $(\ell(n), \epsilon, \delta)$ - LDC

Known results

Positive Results

- Multivariate Polynomials

$$\left.\begin{aligned} \ell(n) &= n^{\epsilon} \\ \text{Rate} &= \epsilon^{\Theta(\frac{1}{\epsilon})} \end{aligned}\right\} \text{high rate}$$

$$\left.\begin{aligned} \ell(n) &= \ell = O(1) \\ n &= 2^{k^{1/\ell}} \end{aligned}\right\} \text{low rate}$$

- [YEKHANIN, RAGHAVENDRA, EFREMENKO]

$$\ell(n) = O(1)$$

$$n = \exp\left(\exp\left((\log k)^{1/\log \ell}\right)\right)$$

Negative Results

[KATZ-TREVISAN], [KERENIDIS, de WOLF]

- Binary LDC with $\ell(n) = \ell = O(1)$ must satisfy $n \geq k^{1+\Omega(\frac{1}{\ell})}$
- $\ell = 3 \Rightarrow n = \Omega(k^2)$.
- Say nothing if $\ell = \omega(\log n)$.
- Also nothing if $|\Sigma| \to \infty$?
  [Check...]

In Practice?

- Anything with $\ell = o(k)$ interesting
- Best such setting $\ell = \Theta(\sqrt{k})$
  $R \to 1/2$

Rate 1/2? Bivariate Polynomials

Messages : $Q(x,y)$: $\deg Q \leq d$

Encoding : Evaluations over $\mathbb{F}_q \times \mathbb{F}_q$

Parameters:

$$n = q^2$$

$$k = \binom{d+2}{2} \qquad d \leq q-1$$

$$= q^2 - \binom{2q-d}{2} \qquad d > q-1$$

Rel. distance $= 1 - \frac{d}{q}$ if $d \leq q$

$= 1 - O\left(\frac{1}{q}\right)$ o.w.

(Locality) $\ell = O(q)$ if $d \leq q$

- To correct ϵ fraction errors, distance $= 2\epsilon$.

$$d = (1-2\epsilon)q$$

$$\text{Rate} = \binom{d+2}{2} \Big/ q^2 \approx \frac{(1-2\epsilon)^2}{2} \to \frac{1}{2}$$

as $\epsilon \to 0$

- In general m variables with pos. dist.

$$\Rightarrow \text{Rate} \leq \frac{1}{m!}$$

- Locality $\ell \approx q^{1/m}$ $\Rightarrow$ Need $m \geq 2$.

Multiplicity Codes [Kopparty, Saraf, Yekhanin]

Main Idea:

Messages: $Q(x,y)$ $\deg Q \leq d$

Encoding: Evaluations of $\left(Q, \frac{\partial Q}{\partial x}, \frac{\partial Q}{\partial y}\right)$

(polynomial & its derivatives)

Why does this help?

- Let $(a,b) \in \mathbb{F}_q^2$ be zero of Q of **multiplicity 2** if

$$Q(a,b) = \frac{\partial Q}{\partial x}(a,b) = \frac{\partial Q}{\partial y}(a,b) = 0$$

- **Multiplicity Schwartz-Zippel:**
  if $Q \not\equiv 0$, $\deg Q \leq d$ then

$$\mathbb{E}_{(a,b)}\left[\text{mult}(Q; a,b)\right] \leq \frac{d}{q}.$$

- Corollary: Viewed as a code over $\Sigma = \mathbb{F}_q^3$ multiplicity code above has distance $1 - \frac{d}{2q}$

- Can use $d = 2(1-2\epsilon)q \to 2q$

- $k = \frac{\binom{d+2}{2}}{3} = \frac{2}{3} n$

- Locality = ?

  - Can recover $Q(a,b)$ for any (a,b) by picking random line through (a,b). $\ell = O(\sqrt{n})$

  - But not done: also need to recover $\frac{\partial Q}{\partial x}$

- Natural idea: $\frac{\partial Q}{\partial x}$ is a degree $d-1$ polynomial.
  - ☐ Recover from lines?
  - ☐ Doesn't work; don't have $\frac{\partial^2 Q}{\partial x^2}$, $\frac{\partial^2 Q}{\partial x \partial y}$!

- Better idea: When we recover $Q(a,b)$, we actually recover $Q|_\ell$ for some line ℓ through (a,b)

  actually gives "$\frac{\partial Q}{\partial \ell}$" also

  [if $\ell = \alpha x + \beta y + \gamma$, then we get
  $$\alpha \frac{\partial Q}{\partial x} + \beta \frac{\partial Q}{\partial y}$$]

- two linearly ind. lines through (a,b) give $\frac{\partial Q}{\partial x}(a,b)$, $\frac{\partial Q}{\partial y}(a,b)$

Summary

- 2-variate polynomials with multiplicity 2 yield $\ell = O(\sqrt{n})$

  Rate $\longrightarrow$ $2/3$

  Breaks Rate $\leq \frac{1}{2}$ barrier !

- To get further
  - higher multiplicities $\longrightarrow$ Rate $\to 1$
  - more variables $\longrightarrow$ $\ell = O(n^{\gamma})$

    $\gamma \to 0$.

Formalities:

Derivative =?

Higher multiplicity = ?

(Will do everything in bivariate setting; higher derivatives follow)

Univariate setting: f has zero of multiplicity m at α if

$$(x-\alpha)^m \text{ divides } f(x)$$

$$\Leftrightarrow \quad x^m \text{ divides } f(x+\alpha)$$

$\Leftrightarrow$ if $f(x+y) = \sum_i c_i(y) \cdot x^i$

then $c_i(y) = 0 \quad \forall i \in \{0, \dots m-1\}$

Bivariate Setting = ?

- $Q(x,y)$ has zero of multiplicity <u>one</u> at (a,b) if $Q(a,b)=0$

  $\Longleftrightarrow$ $Q \in$ Ideal generated by $(x-a)$ and $(y-b)$

  $$\left[Q = A(x,y)\cdot(x-a) + B(x,y)\cdot(y-b) \right]$$

- Q has zero of mult. m at (a,b) if $Q \in I^m$

  where
  - $I = \langle x-a, y-b \rangle$
  - $I \cdot J = \text{span}\left\{ p \cdot q \;\middle|\; \begin{array}{l} p \in I \\ q \in J \end{array} \right\}$
  - $I^m = \underbrace{I \cdot I \cdots I}_{m \text{ times}}$

- Equivalenty if $\bar{x} = (x_1, x_2)$, $\bar{z} = (z_1, z_2)$

$$Q(\bar{x}+\bar{z}) = \sum_{i,j} C_{ij}(\bar{z})\, x_1^i x_2^j$$

then $C_{ij}(a,b) = 0$ for all $i+j < m$.

- $C_{ij}(\bar{z}) \triangleq (i,j)^{th}$ (Hasse) Derivative of Q.

  order of $C_{ij} \triangleq i+j$; will denote Q_{ij}

- $\mathrm{Mult}(Q; a,b)$ = largest m s.t. all Hasse derivatives of order smaller than m vanish at (a,b).

- With definitions above can prove mult. Schwartz-Zippel lemma.

Other Properties

- Linearity: $(A+B)_{ij} = A_{ij} + B_{ij}$
- $\deg Q_{ij} \leq \deg Q - i - j$
- $\left(Q_{i_1,j_1}\right)_{i_2,j_2} \neq Q_{i_1+i_2,\, j_1+j_2}$
- $Q_{i_1+i_2,\, j_1+j_2}(a,b) = 0$

  $\rightarrow \left(Q_{i_1,j_1}\right)_{i_2,j_2}(a,b) = 0.$
- $Q_{i,j}$ not (locally) computable from Q