

Today [Yekhanin, Raghavendra, Efremenko]

Construction of LDC's.

~~—————φ—————~~

Recall from last lecture

Code  $E: \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$  given by

$$G = \begin{bmatrix} | & & & & | \\ v_1 & \dots & & & v_n \\ | & & & & | \end{bmatrix}$$

$\leftarrow n \rightarrow$

$$E: x \mapsto x \cdot G$$

~~—————φ—————~~

## Wish list

- For every  $i \in [k]$ , local "redundancy"

$$V_{i_1} + V_{i_2} + \dots + V_{i_\ell} = e_i$$

- Some symmetry in columns of  $G$ .



## [YRE] construction

### Ingredients

- $m \in \mathbb{Z}^+$

- $\mathbb{F}_q$  with  $q$  being primitive  $m^{\text{th}}$  root.  
( $m \mid q-1$ )

- $S \in \mathbb{Z}_m - \{0\}$

- ( $S$ -nice) matrix  $M \in \mathbb{Z}_m^{k \times n}$

- $G = g^M$  i.e.,  $G_{ij} = g^{M_{ij}}$

Defn:  $M$  is  $S$ -nice if

$$M = \left[ \begin{array}{c|c} M_1 & M_2 \end{array} \right]$$

$\xleftrightarrow{k} \quad \xleftrightarrow{n-k}$

- $(M_1)_{ii} = 0$ , •  $(M_2)_{ij} \in S$  if  $i \neq j$
- columns of  $M$  closed under addition.

~~—————~~

Theorem 1:  $M$  is  $S$ -nice  $\Rightarrow G$  is

$(|S|+1)$ -LDC

~~—————~~

Theorem 2: For infinitely many  $k \exists$

$\left( \mathbb{Z}_6^* \right)$ -nice matrices with

$$n \leq \exp(\exp(\sqrt{\log k}))$$

## Inward Theorem 1

Defn:  $S$  is  $t$ -sparse if  $\exists p \in \mathbb{F}_q[x]$

s.t.

①  $p(1) = 1$

②  $p(g^s) = 0 \quad \forall s \in S$

③  $p$  is  $t$ -sparse (has  $\leq t$  nonzero coeffs)

— x —

Lemma: if  $S$  is  $t$ -sparse &  $M$  is  $S$ -nice, then  $G = g^M$  is  $t$ -LDC

— x —

Proposition: Every  $S$  is  $(|S|+1)$  nice

(Lemma + Proposition  $\Rightarrow$  Theorem 1)

## Proof of Lemma

• Let  $p(x) = \sum c_d x^d$

• So  $p(g^{m_{ij}}) = 0$  if  $i \neq j$   
 $= 1$  if  $i = j$

•  $\sum c_d g^{m_{ij} \cdot d} = 0$  if  $i \neq j$   
 $= 1$  if  $i = j$

• Note  $(M_{ij})_j = v_i$

Furthermore exist  $i_2, i_3, \dots, i_{m-1}$  s.t.

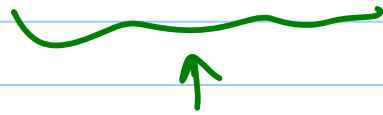
$$(d \cdot M_{ij})_j = v_{i_d}$$

•  $\sum c_d v_{i_d} = e_i$  !  $\leftarrow$   $t$ -local sum!

• Also have symmetry

$$\sum c_d \cdot g^{d \cdot M_{ij} + M_{ei}} = g^{M_{ei}} \quad \text{if } i=j$$

$$= 0 \quad \text{o.w.}$$



random column if  $l$  is random.



☒ Proof of Lemma & hence Theorem 1

## Towards Theorem 2

### First some negative results

Case 1:  $S = \{1\}$ ,  $m = \text{prime}$

$\Rightarrow n \geq m^{k-1} \Rightarrow n$  good for us.

Case 2:  $S = \mathbb{Z}_m^*$ ,  $m = \text{prime}$

$n \geq m^{\frac{k-1}{m-1}}$  (follows from above  
via tensor products)

Aside:

### Yekhanin's Construction

$m = \text{prime}$ ;  $q = m+1 = 2^t$

$S = \{1, 2, 4, 8, \dots, 2^{t-1}\}$

Lemma:  $\exists$  3-sparse  $p \in \mathbb{F}_2[x]$ ,  $p(q^{2^i}) = 0 \forall i$ .

Assuming  $\exists$  infinitely many such primes