Hardness of Approximation meets Parameterized Complexity

Karthik C. S.

New York University

December 26, 2020

Karthik C. S. (NYU)

Parameterized Inapproximability

< ∃ > December 26, 2020 1/22

Image: A match a ma

Э

DQC

- Day 1: The Setting
- Day 2: Gap Creation
- Day 3: Applications

- 2

590

イロト イボト イヨト イヨト

#### Part 1: Hardness of Approximation

- Hardness of Approximation in NP
- Hardness of Approximation in Parameterized Complexity

3

イロト イボト イヨト イヨト

#### Part 1: Hardness of Approximation

- Hardness of Approximation in NP
- Hardness of Approximation in Parameterized Complexity

#### Part 2: Key Problems in Parameterized Inapproximability

- MaxCover
- One-Sided Biclique

3

イロト イヨト イヨト

#### Part 1: Hardness of Approximation

- Hardness of Approximation in NP
- Hardness of Approximation in Parameterized Complexity

#### Part 2: Key Problems in Parameterized Inapproximability

- MaxCover
- One-Sided Biclique
- Part 3: Coding Theory
  - Definition and Geometric Intuition
  - Random Codes
  - Algebraic Codes

# Part 1 Hardness of Approximation

Karthik C. S. (NYU)

Parameterized Inapproximability

Many important optimization problems are not tractable.

イロト イヨト イヨト

э

Many important optimization problems are not tractable. A typical way to cope with the intractability of optimization problems is to design algorithms that find solutions whose cost or value is close to the optimum.

イロト イボト イヨト イヨト

Many important optimization problems are not tractable. A typical way to cope with the intractability of optimization problems is to design algorithms that find solutions whose cost or value is close to the optimum. In several interesting cases, it is possible to prove that even finding good approximate solutions is as hard as finding optimal solutions.

イロト イヨト イヨト

Many important optimization problems are not tractable. A typical way to cope with the intractability of optimization problems is to design algorithms that find solutions whose cost or value is close to the optimum. In several interesting cases, it is possible to prove that even finding good approximate solutions is as hard as finding optimal solutions. The area which studies such inapproximability results is called hardness of approximation.

Image: A matrix and a matrix

PCP Theorem: Bedrock of NP-Hardness of Approximation

イロト イヨト イヨト

э

590



PCP Theorem: Bedrock of NP-Hardness of Approximation

$$\pi_{i,j} \subseteq \Sigma_U \times \Sigma_W$$

< □ > < 同 >

Karthik C. S. (NYU)

Э

DQC



PCP Theorem: Bedrock of NP-Hardness of Approximation

 $\pi_{i,j} \subseteq \Sigma_U \times \Sigma_W$ 

 $\sigma_U: U \to \Sigma_U \text{ is a labeling of } U$  $\sigma_W: W \to \Sigma_W \text{ is a labeling of } W$ 

э

Sac



PCP Theorem: Bedrock of NP-Hardness of Approximation

 $\pi_{i,j} \subseteq \Sigma_U \times \Sigma_W$ 

 $\sigma_U: U \to \Sigma_U \text{ is a labeling of } U$  $\sigma_W: W \to \Sigma_W \text{ is a labeling of } W$ 

 $\begin{array}{l} (u_i, w_j) \in E \text{ is satisfied by } (\sigma_U, \sigma_W) \\ \text{if } (\sigma_U(u_i), \sigma_W(w_j)) \in \pi_{i,j} \end{array}$ 



PCP Theorem: Bedrock of NP-Hardness of Approximation

 $\pi_{i,j} \subseteq \Sigma_U \times \Sigma_W$ 

 $\sigma_U: U \to \Sigma_U \text{ is a labeling of } U$  $\sigma_W: W \to \Sigma_W \text{ is a labeling of } W$ 

 $\begin{array}{l} (u_i, w_j) \in E \text{ is satisfied by } (\sigma_U, \sigma_W) \\ \text{if } (\sigma_U(u_i), \sigma_W(w_j)) \in \pi_{i,j} \end{array}$ 

 $VAL(\Gamma, \sigma_U, \sigma_W) = Fraction of edges satisfied by (\sigma_U, \sigma_W)$ 

4 E b



PCP Theorem: Bedrock of NP-Hardness of Approximation

 $\pi_{i,j} \subseteq \Sigma_U \times \Sigma_W$ 

 $\sigma_U: U \to \Sigma_U \text{ is a labeling of } U$  $\sigma_W: W \to \Sigma_W \text{ is a labeling of } W$ 

 $\begin{array}{l} (u_i, w_j) \in E \text{ is satisfied by } (\sigma_U, \sigma_W) \\ \text{if } (\sigma_U(u_i), \sigma_W(w_j)) \in \pi_{i,j} \end{array}$ 

 $VAL(\Gamma, \sigma_U, \sigma_W) = Fraction of edges satisfied by (\sigma_U, \sigma_W)$ 

 $\mathsf{VAL}(\Gamma) = \max_{\sigma_U, \sigma_W} \mathsf{VAL}(\Gamma, \sigma_U, \sigma_W)$ 

< ロト < 同ト < ヨト < ヨト



Determining if VAL( $\Gamma$ ) = 1 or if VAL( $\Gamma$ )  $\leq$  0.99 is NP-Hard

PCP Theorem: Bedrock of NP-Hardness of Approximation

 $\pi_{i,j} \subseteq \Sigma_U \times \Sigma_W$ 

 $\sigma_U: U \to \Sigma_U \text{ is a labeling of } U$  $\sigma_W: W \to \Sigma_W \text{ is a labeling of } W$ 

 $\begin{array}{l} (u_i, w_j) \in E \text{ is satisfied by } (\sigma_U, \sigma_W) \\ \text{if } (\sigma_U(u_i), \sigma_W(w_j)) \in \pi_{i,j} \end{array}$ 

 $VAL(\Gamma, \sigma_U, \sigma_W) = Fraction of edges satisfied by (\sigma_U, \sigma_W)$ 

 $\mathsf{VAL}(\Gamma) = \max_{\sigma_U, \sigma_W} \mathsf{VAL}(\Gamma, \sigma_U, \sigma_W)$ 

< ロ ト < 同 ト < 三 ト < 三 ト

3



Karthik C. S. (NYU)

E

◆□▶ ◆□▶ ◆三▶ ◆三▶

590



 $n \cdot |\Sigma_U| \text{ nodes in } U$  $m \cdot |\Sigma_W| \text{ nodes in } W$  $(u_i, \alpha), (w_j, \beta) \in E_{\text{ext}}$ iff  $(u_i, w_i) \in E \text{ and } (\alpha, \beta) \in \pi_{i,i}$ 

3

- 4 ⊒ →

< 4<sup>™</sup> ► <

DQC



 $n \cdot |\Sigma_U| \text{ nodes in } U$  $m \cdot |\Sigma_W| \text{ nodes in } W$  $(u_i, \alpha), (w_j, \beta) \in E_{\text{ext}}$ iff  $(u_i, w_i) \in E \text{ and } (\alpha, \beta) \in \pi_{i,i}$ 

 $S \subseteq W$  is a labeling of W if  $\forall i \in [k], |S \cap W_i| = 1$ 

 $T \subseteq U$  is a labeling of U if  $\forall i \in [k], |T \cap U_i| = 1$ 

3

- 4 ⊒ →



 $n \cdot |\Sigma_U| \text{ nodes in } U$  $m \cdot |\Sigma_W| \text{ nodes in } W$  $(u_i, \alpha), (w_j, \beta) \in E_{\text{ext}}$ iff  $(u_i, w_i) \in E \text{ and } (\alpha, \beta) \in \pi_{i,i}$ 

- $S \subseteq W$  is a labeling of W if  $\forall i \in [k], |S \cap W_i| = 1$
- $T \subseteq U$  is a labeling of U if  $\forall i \in [k], |T \cap U_i| = 1$

3

- 4 ⊒ →

• Many Optimization problems are NP-Hard

イロト イボト イヨト イヨト

Э

- Many Optimization problems are NP-Hard
- Coping mechanisms
  - Approximation Algorithms
  - Fixed Parameter Tractability

- Many Optimization problems are NP-Hard
- Coping mechanisms
  - Approximation Algorithms
  - Fixed Parameter Tractability
- Set Cover: Hard to cope!

- Many Optimization problems are NP-Hard
- Coping mechanisms
  - Approximation Algorithms
  - Fixed Parameter Tractability
- Set Cover: Hard to cope!
- New direction: Fixed Parameter Approximability

Is there a  $F(k) \cdot poly(n)$  time algorithm that approximates to a factor T(k)?

< ロ ト < 同 ト < 三 ト < 三 ト

## Parameterized Inapproximability: Partial Summary

#### Parameterized Inapproximability: Recent Developments



イロト イヨト イヨト

## Part 2

#### Key Problems in Parameterized Inapproximability

Karthik C. S. (NYU)

Parameterized Inapproximability

December 26, 2020 10 / 22



Image: A matrix and a matrix

E

590



Each  $W_i$  is a Right Super Node Each  $U_i$  is a Left Super Node

Karthik C. S. (NYU)

э

DQC



Each  $W_i$  is a Right Super Node Each  $U_i$  is a Left Super Node

$$S \subseteq W$$
 is a labeling of  $W$  if  $\forall i \in [k], |S \cap W_i| = 1$ 

э

DQC



Each  $W_i$  is a Right Super Node Each  $U_i$  is a Left Super Node

 $S \subseteq W$  is a labeling of W if  $\forall i \in [k], |S \cap W_i| = 1$ 

 $S \text{ covers } U_i \text{ if } \\ \exists u \in U_i, \ \forall v \in S, (u, v) \in E \end{cases}$ 



Each  $W_i$  is a Right Super Node Each  $U_i$  is a Left Super Node

 $S \subseteq W$  is a labeling of W if  $\forall i \in [k], |S \cap W_i| = 1$ 

 $S \text{ covers } U_i \text{ if } \\ \exists u \in U_i, \ \forall v \in S, (u, v) \in E \end{cases}$ 

 $MaxCover(\Gamma, S) = Fraction of$  $U_i's covered by S$ 



Each  $W_i$  is a Right Super Node Each  $U_i$  is a Left Super Node

 $S \subseteq W$  is a labeling of W if  $\forall i \in [k], |S \cap W_i| = 1$ 

 $S \text{ covers } U_i \text{ if } \\ \exists u \in U_i, \ \forall v \in S, (u, v) \in E \end{cases}$ 

 $MaxCover(\Gamma, S) = Fraction of$  $U_i's covered by S$ 

 $\mathsf{MaxCover}(\Gamma) = \max_{S} \mathsf{MaxCover}(\Gamma, S)$ 



Determine if MaxCover( $\Gamma$ ) = 1 or MaxCover( $\Gamma$ ) < s

Each  $W_i$  is a Right Super Node Each  $U_i$  is a Left Super Node

 $S \subseteq W$  is a labeling of W if  $\forall i \in [k], |S \cap W_i| = 1$ 

S covers  $U_i$  if  $\exists u \in U_i, \forall v \in S, (u, v) \in E$ 

 $MaxCover(\Gamma, S) = Fraction of$  $U_i$ 's covered by S

 $MaxCover(\Gamma) = \max_{c} MaxCover(\Gamma, S)$ 

< □ > < @ >

3

## *k*-Clique as MaxCover



王

900

◆□▶ ◆□▶ ◆三▶ ◆三▶

#### *k*-Clique as MaxCover



#### Input of *k*-Clique problem: $G([n], E_0)$

Karthik C. S. (NYU)

< □ > < 同 >

E

DQC
#### k-Clique as MaxCover



Input of *k*-Clique problem:  $G([n], E_0)$ 

Each  $W_i$  is a copy of  $E_0$ Each  $U_i$  is a copy of [n]

- 一司

DQC

#### k-Clique as MaxCover



Input of *k*-Clique problem:  $G([n], E_0)$ 

Each  $W_j$  is a copy of  $E_0$ Each  $U_i$  is a copy of [n]

For distinct i, j, j', introduce all edges between  $W_{i,j'}$  and  $U_i$ 

Sac

## k-Clique as MaxCover



Determine if  $MaxCover(\Gamma) = 1$ or  $MaxCover(\Gamma) \le 1 - \frac{1}{\binom{k}{2}}$  Input of *k*-Clique problem:  $G([n], E_0)$ 

Each  $W_j$  is a copy of  $E_0$ Each  $U_i$  is a copy of [n]

For distinct i, j, j', introduce all edges between  $W_{i,j'}$  and  $U_i$ 

< □ > < 同 >

• W[1]-Complete if there are F(k) left super nodes

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ - 三 - のへで

- W[1]-Complete if there are F(k) left super nodes
- 1 vs.  $k/n^{1/\sqrt{k}}$  is W[1]-Hard

▲□▶ ▲□▶ ▲ 三▶ ▲ 三▶ - 三 - のへで

- W[1]-Complete if there are F(k) left super nodes
- 1 vs.  $k/n^{1/\sqrt{k}}$  is W[1]-Hard
- Central problem to understand parameterized inapproximability of Set Cover and Clique



Karthik C. S. (NYU)

E

590

イロト イボト イヨト イヨト



Introduce all edges between:  $W_j$  and  $W_{j'}$  $U_i$  and  $U_{i'}$ 

3

DQC



Introduce all edges between:  $W_j$  and  $W_{j'}$  $U_j$  and  $U_{i'}$ 

There is a (r + k) sized clique iff MaxCover $(\Gamma) = 1$ 

Sac

э



Introduce all edges between:  $W_j$  and  $W_{j'}$  $U_j$  and  $U_{i'}$ 

There is a (r + k) sized clique iff MaxCover $(\Gamma) = 1$ 

MaxCover from ETH and SETH have r = F(k)

3

Sac

## **One-Sided Biclique**



- 2

900

<ロト <回ト < 回ト < 回ト

## **One-Sided Biclique**



Find k vertices in Wwith most common neighbors

Э

## **One-Sided Biclique**



Find k vertices in Wwith most common neighbors

Э

• Colored vs. Non-colored

イロト イヨト イヨト

э

- Colored vs. Non-colored
- Covering vs. Common neighbors

э

- Colored vs. Non-colored
- Covering vs. Common neighbors
- One-Sided Biclique reduces to MaxCover: Color Coding
  - What about the other direction?

Image: Image:

Ξ

- Hardness of Approximation meets Parameterized Complexity: New Exciting Area!
- MaxCover and One-Sided Biclique are key problems for which we have proved inapproximaiblity results.

# Part 3 Coding Theory

Karthik C. S. (NYU)

Parameterized Inapproximability

December 26, 2020 18 / 22

## Coding Theory: Geometric Motivation

• Consider all strings/points in  $\{0,1\}^n$ 

イロト 不得下 イヨト イヨト 二日

## Coding Theory: Geometric Motivation

- Consider all strings/points in  $\{0,1\}^n$
- Consider subset of  $\{0,1\}^n$  of even Hamming weight

- Consider all strings/points in  $\{0,1\}^n$
- Consider subset of  $\{0,1\}^n$  of even Hamming weight
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 3?

- Consider all strings/points in  $\{0,1\}^n$
- Consider subset of  $\{0,1\}^n$  of even Hamming weight
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 3?
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 0.9n?

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

- Consider all strings/points in  $\{0,1\}^n$
- Consider subset of  $\{0,1\}^n$  of even Hamming weight
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 3?
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 0.9n?
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 0.5n?

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

- Consider all strings/points in  $\{0,1\}^n$
- Consider subset of  $\{0,1\}^n$  of even Hamming weight
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 3?
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 0.9n?
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 0.5n?
- What is the largest subset of  $\{0,1\}^n$  whose all pairwise Hamming distances is at least 0.49n?

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

#### • $C \subseteq \{0,1\}^L$

999

イロト イロト イヨト イヨト 二日

- $C \subseteq \{0,1\}^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

999

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

- $C \subseteq \{0,1\}^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

A good code: for  $\rho, \delta > 0$ ,  $|C| = 2^{\rho L}$ ,  $\Delta(C) = \delta L$ .

Karthik C. S. (NYU)

▲ロト ▲母 ト ▲ヨト ▲ヨト ヨー ショウ

For some small  $\rho > 0$ , if we pick  $2^{\rho L}$  random strings uniformly and independently then they form a code with distance at least 1/4 (whp).

イロト 不得下 イヨト イヨト 二日

For some small  $\rho > 0$ , if we pick  $2^{\rho L}$  random strings uniformly and independently then they form a code with distance at least 1/4 (whp).

- $\mathbb{E}[\|x-y\|_0] = L/2$
- Chernoff:  $\Pr[||x y||_0 \le L/4] = e^{-L/100}$

For some small  $\rho > 0$ , if we pick  $2^{\rho L}$  random strings uniformly and independently then they form a code with distance at least 1/4 (whp).

- $\mathbb{E}[||x-y||_0] = L/2$
- Chernoff:  $\Pr[||x y||_0 \le L/4] = e^{-L/100}$
- Union Bound:

$$\Pr[\min_{x,y\in C}\{\|x-y\|_0\} \le L/4] = 2^{2\rho L} e^{-L/100} < 0.001$$

For some small  $\rho > 0$ , if we pick  $2^{\rho L}$  random strings uniformly and independently then they form a code with distance at least 1/4 (whp).

- $\mathbb{E}[||x-y||_0] = L/2$
- Chernoff:  $\Pr[||x y||_0 \le L/4] = e^{-L/100}$
- Union Bound:

$$\Pr[\min_{x,y\in C}\{\|x-y\|_0\} \le L/4] = 2^{2\rho L} e^{-L/100} < 0.001$$

#### Many Efficient Deterministic Good Codes Exist!

Karthik C. S. (NYU)

•  $C \subseteq [q]^L$ 

- $C \subseteq [q]^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

999

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

- $C \subseteq [q]^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

• Singleton Bound:  $|C| \leq q^{L-\Delta(C)+1}$ 

▲ロト ▲母 ト ▲ヨト ▲ヨト ヨー ショウ

- $C \subseteq [q]^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

- Singleton Bound:  $|C| \leq q^{L-\Delta(C)+1}$
- Reed Solomon Codes: All degree d univariate polynomials over  $\mathbb{F}_q$

イロト (四) (三) (三) (二) (つ)

- $C \subseteq [q]^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

- Singleton Bound:  $|C| \leq q^{L-\Delta(C)+1}$
- Reed Solomon Codes: All degree d univariate polynomials over  $\mathbb{F}_q$
- $|RS| = q^{d+1}$
## Coding Theory: Reed Solomon Codes

- $C \subseteq [q]^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

- Singleton Bound:  $|C| \leq q^{L-\Delta(C)+1}$
- Reed Solomon Codes: All degree d univariate polynomials over  $\mathbb{F}_q$
- $|\mathsf{RS}| = q^{d+1}$
- Δ(RS) = q d (because any degree d univariate polynomial can have at most d roots)

<ロ > < 同 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < 回 > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ >

## Coding Theory: Reed Solomon Codes

- $C \subseteq [q]^L$
- Distance of C:

$$\Delta(C) := \min_{x,y\in C} \|x-y\|_0$$

- Singleton Bound:  $|C| \leq q^{L-\Delta(C)+1}$
- Reed Solomon Codes: All degree d univariate polynomials over  $\mathbb{F}_q$
- $|\mathsf{RS}| = q^{d+1}$
- Δ(RS) = q d (because any degree d univariate polynomial can have at most d roots)
- Reed Solomon Codes meet the Singleton bound!

▲□▶ ▲□▶ ▲三▶ ▲三▶ 三三 つのべ

- MaxCover: Gap Creation by using Codes
- One-Sided Biclique: Gap creation by using Random Graphs/Polynomials

イロト 不得下 イヨト イヨト 二日