Reed-Solomon Error-correcting Codes

The Deep Hole Problem

Matt Keti
(Advisor: Professor Daqing Wan)

Department of Mathematics
University of California, Irvine

November 8, 2012

Preview of Topics

The Basic Problem

The Basic Problem

The Basic Problem

The Basic Problem

Repetition Codes

Fix the number N to be the number of times a symbol is to be repeated.

Input: A message symbol B.
Output: The string $\underbrace{BBB\ldots B}_{N \text{ times}}$, to be transmitted.

If the message is damaged during transit, the receiver can recover the original message by taking the most popular symbol.

Richard Hamming (1915-1998)

Hamming $(7, 4)$ Encoding

Input: The message vector $m = (m_1, m_2, m_3, m_4)^T$, where the m_i are elements of $\mathbb{F}_2$.
Output: The codeword vector $c = Gm$, to be transmitted, where

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Hamming $(7, 4)$ Decoding

Input: A received message vector $r = (r_1, r_2, r_3, r_4, r_5, r_6, r_7)^T$.

Computation:

Calculate the syndrome vector Hr, where

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

If the syndrome vector is not zero, treat it as a binary number.

In the received message, flip the bit in the position corresponding to that number.

Output: The message vector $(r_3, r_5, r_6, r_7)^T$.

Properties of a Code

In an error-correcting code, let k be the message length and $n > k$ be the block length.

Properties of a Code

In an error-correcting code, let k be the message length and $n > k$ be the block length.

Hamming distance: the number of coordinates in which two words differ, denoted $d(\cdot, \cdot)$

Properties of a Code

In an error-correcting code, let k be the message length and $n > k$ be the block length.

Hamming distance: the number of coordinates in which two words differ, denoted $d(\cdot, \cdot)$

Minimum distance: the smallest distance between any two distinct codewords

Properties of a Code

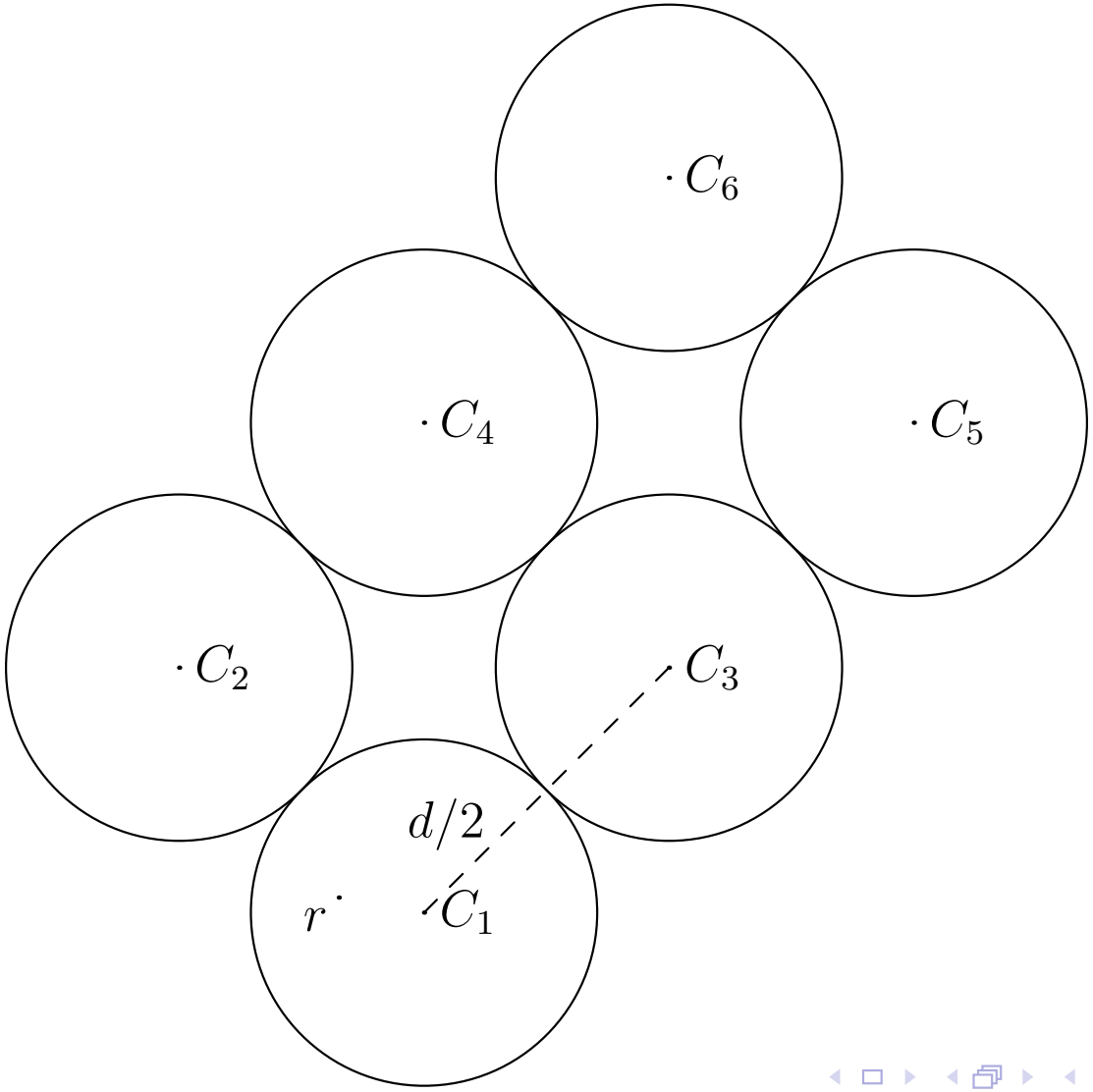
In an error-correcting code, let k be the message length and $n > k$ be the block length.

Hamming distance: the number of coordinates in which two words differ, denoted $d(\cdot, \cdot)$

Minimum distance: the smallest distance between any two distinct codewords

Information rate: the measure of the amount of data versus redundant information, given by k/n

Properties of a Code



Properties of Repetition Codes

In a three-time repetition code, $k = 1$ and $n = 3$.

Minimum distance: 3

Correctable errors: 1

Information rate: $1/3$

Properties of Repetition Codes

In a three-time repetition code, $k = 1$ and $n = 3$.

- Minimum distance: 3
- Correctable errors: 1
- Information rate: $1/3$

In an odd N-time repetition code, $k = 1$ and $n = N$.

- Minimum distance: N
- Correctable errors: $\lfloor N/2 \rfloor$
- Information rate: $1/N$

Properties of Hamming $(7, 4)$

In Hamming $(7, 4)$, $k = 4$ and $n = 7$.

- Minimum distance: 3
- Correctable errors: 1
- Information rate: $4/7$

Goal for Error-correcting Codes

Goal: To find codes that have a high information rate as well as a strong error-correcting capability.

Preview of Topics

2. Reed-Solomon Codes
   - Encoding and Decoding
   - Code Properties
   - Applications in Technology

Irving Reed (1923-2012) and Gustave Solomon (1930-1996)

Reed-Solomon Encoding (Original Formulation)

Idea: A polynomial of degree $k-1$ is determined by k of its points. If we have $n > k$ of its points, we can still potentially recover the polynomial even if some of those points are mixed-up.

Reed-Solomon Encoding (Original Formulation)

Fix a finite field $\mathbb{F}_q$, a message block size k, and a subset $D = \{x_1, x_2, \ldots, x_n\} \subseteq \mathbb{F}_q$ so that $n > k$.

Input: The message $m = (m_0, m_1, m_2, \ldots, m_{k-1})$, represented by the polynomial

$$m(x) = m_0 + m_1 x + m_2 x^2 + \ldots + m_{k-1} x^{k-1}$$

where the m_i are elements of $\mathbb{F}_q$.
Output: The codeword $(m(x_1), m(x_2), \ldots, m(x_n))$, to be transmitted.

Reed-Solomon Encoding (Original Formulation)

Take the finite field $\mathbb{F}_{2^2}$, α a root of $x^2 + x + 1 \in \mathbb{F}_2[x]$, the message block length 2, and $D = \mathbb{F}_{2^2}$. Suppose $m = (10, 11)$. Then,

$$m(x) = 10 + 11x = \alpha + (\alpha + 1)x$$

and the transmitted codeword will be

$$(m(00), m(01), m(10), m(11)) = (10, 01, 11, 00)$$

Reed-Solomon Encoding (Original Formulation)

In summary, we have

Message	1011
Codeword	10011100

Reed-Solomon Decoding (Original Formulation)

Input: A received message $r = (r_1, r_2, \ldots, r_n)$.

Computation:

Find the interpolated polynomials of all combinations of k points from $(x_1, r_1), (x_2, r_2), \ldots, (x_n, r_n)$.

Output: The most popular polynomial.

Reed-Solomon Decoding (Original Formulation)

Suppose there are t coordinate errors. This means that the correct polynomial appears $\binom{n-t}{k}$ times, and any one incorrect polynomial appears at most $\binom{t+k-1}{k}$ times. In order for the procedure to output the original message, we must have

$$\binom{t+k-1}{k} < \binom{n-t}{k}$$

which implies the error-correcting capacity

$$t < \left\lfloor \frac{n-k+1}{2} \right\rfloor$$

Reed-Solomon Decoding (Original Formulation)

Suppose the message $r = 10101100$ is received. Up to $\lfloor (4-2+1)/2 \rfloor = 1$ error can be corrected. $\binom{4}{2} = 6$ pairs of points must be examined. The frequencies are

# of occurrences	Polynomial
2	$10 + 11x$
1	$11 + 11x$
1	$11 + 01x$
1	$00 + 10x$
1	$10 + 00x$

The most popular polynomial is $10 + 11x$, so the decoded message is $m = 1011$.

Reed-Solomon Encoding (BCH Formulation)

Idea: Suppose $g(x)$ is a polynomial with roots $\{x_1, x_2, \ldots, x_n\}$. Let $m(x)$ be some other polynomial. Then take $c(x) = m(x)g(x)$. If we make no mistake about $c(x)$, then

$$c(x_1) = c(x_2) = \ldots = c(x_n) = 0$$

If any of the terms is not zero, then some of the coefficients of $c(x)$ were mixed-up, and we can use those values to try to recover $c(x)$.

Reed-Solomon Encoding (BCH Formulation)

Fix a finite field $\mathbb{F}_q$, a generator α of $\mathbb{F}_q^*$, and an error tolerance t. Set

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{2t})$$

Input: The message $m = (m_0, m_1, m_2, \ldots, m_{k-1})$, represented by the polynomial

$$m(x) = m_0 + m_1 x + m_2 x^2 + \ldots + m_{k-1} x^{k-1}$$

where the m_i are elements of $\mathbb{F}_q$ and $k = q - 2t - 1$.
Output: The codeword formed by the coefficients of $m(x)g(x)$, to be transmitted.

Reed-Solomon Decoding (BCH Formulation)

Input: A received message $r = (r_0, r_1, r_2, \ldots, r_{n-1})$, represented by

$$r(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1} x^{n-1}$$

Computation:

Calculate the syndromes

$$S_j = r(\alpha^j) = \sum_{k=1}^{t} e_{i_k} (\alpha^j)^{i_k}$$

for $j = 1, 2 \ldots, n-k$, where e_i is the error value in the i-th component of r, and t is the number of errors.

Find the error positions α^{i_k} and error values e_{i_k}, and make the appropriate corrections in $r(x)$.

Reed-Solomon Decoding (BCH Formulation)

Output: The polynomial $r(x)/g(x)$.

Note: The computational step can be handled by reformulating the unknowns in the S_j as a system of linear equations (Peterson) and then applying the famous Berlekamp-Massey algorithm, which can uniquely decode with up to $\lfloor (n-k+1)/2 \rfloor$ errors in polynomial time.

Properties of Reed-Solomon Codes

In a common $(255, 223)$ Reed-Solomon code (over $\mathbb{F}_{2^8}^*$),

- Minimum Distance: 33
- Correctable Errors: 16
- Information Rate: 223/255

Properties of Reed-Solomon Codes

In a common $(255, 223)$ Reed-Solomon code (over $\mathbb{F}_{2^8}^*$),

- Minimum Distance: 33
- Correctable Errors: 16
- Information Rate: $223/255$

In a general (n, k) Reed-Solomon code,

- Minimum Distance: $n - k + 1$
- Correctable Errors: $\lfloor (n - k + 1)/2 \rfloor$
- Information Rate: k/n

Properties of Reed-Solomon Codes

Theorem (Singleton)

Given an (n, k) q-symbol code with minimum distance d, we must have

$$d \leq n - k + 1$$

Properties of Reed-Solomon Codes

Theorem (Singleton)

Given an (n, k) q-symbol code with minimum distance d, we must have

$$d \leq n - k + 1$$

Reed-Solomon codes match the Singleton bound, meaning that they have the best possible minimum distance given their size.

Properties of Reed-Solomon Codes

Reed-Solomon codes are particularly effective against burst errors. In the example, the two red bits were flipped.

Transmitted	10011100
Received	10101100

Since the two bits correspond to the same symbol, this only counts as a single error. This effect is more dramatic when there are more bits per symbol. (For example, in a code over $\mathbb{F}_{2^8}$.)

Compact Discs

Compact Discs

CDs make use of two cross-interleaved Reed-Solomon codes (CIRC), the first is a $(32, 28)$ code C_1 and the second is a $(28, 24)$ code C_2, both over $\mathbb{F}_{2^8}$.

Compact Discs

CDs make use of two cross-interleaved Reed-Solomon codes (CIRC), the first is a $(32, 28)$ code C_1 and the second is a $(28, 24)$ code C_2, both over $\mathbb{F}_{2^8}$.

Interleaving of data symbols prevents burst errors from overwhelming any one block.

Compact Discs

CDs make use of two cross-interleaved Reed-Solomon codes (CIRC), the first is a $(32, 28)$ code C_1 and the second is a $(28, 24)$ code C_2, both over $\mathbb{F}_{2^8}$.

Interleaving of data symbols prevents burst errors from overwhelming any one block.

If the C_1 or C_2 decoders fail to correct the errors in a block, the symbols in the block are flagged as erasures so that the hardware can attempt to conceal the corruption.

Compact Discs

The CIRC setup can correct a burst error lasting about 4000 bits, or 2.5mm in track length.

If the errors are too overwhelming, data blocks can be interpolated or concealed for errors spanning around 12300 bits, or 7.7mm in track length.

QR Codes

QR codes were invented by the Toyota subsidiary Denso Wave in 1994 and are freely available for use.

QR Codes

QR codes were invented by the Toyota subsidiary Denso Wave in 1994 and are freely available for use.

A 21×21 QR code ('Version 1') contains 26 bytes of information.

QR Codes

QR codes were invented by the Toyota subsidiary Denso Wave in 1994 and are freely available for use.

A 21×21 QR code ('Version 1') contains 26 bytes of information.

There are four levels of error-correction:

Level	Check Symbols	Data Bytes
L	7	19
M	10	16
Q	13	13
H	17	9

where the coding is done over $\mathbb{F}_{2^8}$.

QR Codes

A 21×21 QR code with level M encoding uses the generator polynomial

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{10})$$

where α is a multiplicative generator of $\mathbb{F}_{2^8}^*$.

QR Codes

A 21×21 QR code with level M encoding uses the generator polynomial

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{10})$$

where α is a multiplicative generator of $\mathbb{F}_{2^8}^*$.

It will be able to correct up to five errors.

QR Codes

Error correction in QR codes allows them to be read even if they are damaged or obstructed.

Some use this property for artistic purposes:

Voyager Probes

Reed-Solomon codes were first used for space exploration in the Voyager missions (1977).

Voyager Probes

Reed-Solomon codes were first used for space exploration in the Voyager missions (1977).

The Voyager spacecraft were to transmit full-colour 800×800 images at 8 bits per pixel.

Voyager Probes

Reed-Solomon codes were first used for space exploration in the Voyager missions (1977).

The Voyager spacecraft were to transmit full-colour 800×800 images at 8 bits per pixel.

Compressing the colour images made them vulnerable to bit errors, so engineers employed a Reed-Solomon code composed with a convolutional code to compensate.

Voyager Probes

Voyager uses a $(255, 223)$ code over $\mathbb{F}_{2^8}$, which is represented by the primitive polynomial $f(x) = x^8 + x^4 + x^3 + x^2 + 1$.

The generator polynomial is

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{32})$$

where α is a root of $f(x)$.

Preview of Topics

3 List Decoding
- The Problem
- A Breakthrough Algorithm

Improving Error Tolerances

Question: Can the error-correcting limit be improved in an efficient way?

Improving Error Tolerances

Question: Can the error-correcting limit be improved in an efficient way?

Given an (n, k) Reed-Solomon code with minimum distance $d = n - k + 1$, it is possible to efficiently decode a received message to a unique codeword as long as there are less than $\lfloor d/2 \rfloor$ errors. The situation could possibly be improved by dropping uniqueness, which motivates the following concept:

Improving Error Tolerances

Problem (List Decoding)

Given a received message r and an error tolerance t, to find all codewords c such that $d(c, r) \leq t$.

Note that if $t = \lfloor d/2 \rfloor$, this concept reduces to unique decoding. It was unknown for many years whether or not it was possible to do this efficiently for $t > \lfloor d/2 \rfloor$.

Madhu Sudan (1966)

Venkatesan Guruswami (1976)

Guruswami-Sudan List Decoding Algorithm (Sketch)

Input: A received message $r = (r_1, r_2, \ldots, r_n)$ and an error tolerance t.

Computation:

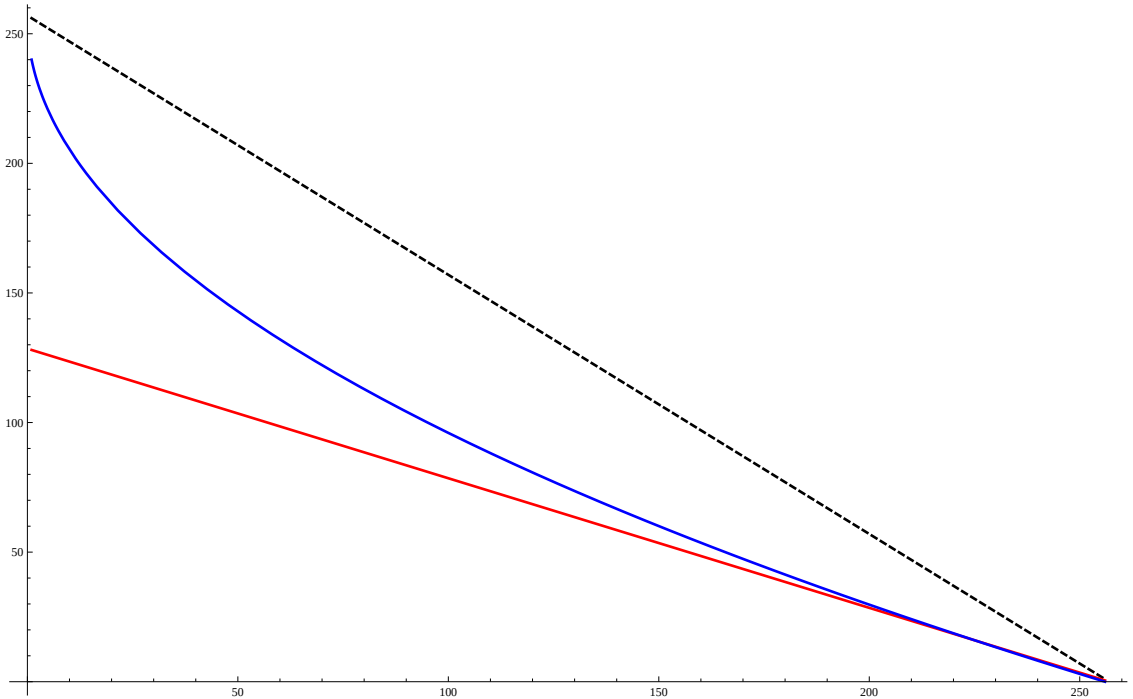
Find a two-variable polynomial $Q(x, y)$ with suitably high degree so that $Q(x_i, r_i) = 0$ for $1 \leq i \leq n$.

Find all factors of $Q(x, y)$ of the form $y - p(x)$, where $\deg p(x) < k$.

Output: Those polynomials $y = p(x)$ such that $r_i = p(x_i)$ for at least $n - t$ of the (x_i, r_i).

Guruswami-Sudan List Decoding Algorithm (Sketch)

The Guruswami-Sudan algorithm can correct up to $n - \sqrt{nk}$ errors in randomised polynomial time.



Preview of Topics

4. Attempting to Further Improve Error-Correction Limits
   - New Problems
   - Hardness Results
   - The Deep Hole Problem

Two Problems

Definition (Distance to a Code)

For an error-correcting code $\mathcal{C}$ and a word r, denote $d(r, \mathcal{C})$ to be the shortest distance between r and each codeword from $\mathcal{C}$.

Two Problems

Problem (Maximum-Likelihood Decoding)

Given a received word r, to find an explict codeword c such that $d(r, c) = d(r, \mathcal{C})$.

Two Problems

Problem (Maximum-Likelihood Decoding)

Given a received word r, to find an explict codeword c such that $d(r, c) = d(r, \mathcal{C})$.

Problem (Bounded Distance Decoding)

Given a received word r and a bound B, to find just one codeword c such that $d(r, c) \leq B$.

Results by Guruswami-Vardy

Theorem (Guruswami-Vardy, 2005)

For an integer $t \geq 1$, let $m = 3t$, $k = t^3 - t - 1$, and $n = t^3$. There is a class of (n, k) Reed-Solomon codes over $\mathbb{F}_{2^m}$ with evaluation set of size $|D| = n$ such that maximum-likelihood decoding is NP-complete.

Results by Guruswami-Vardy

Theorem (Guruswami-Vardy, 2005)

For an integer $t \geq 1$, let $m = 3t$, $k = t^3 - t - 1$, and $n = t^3$. There is a class of (n, k) Reed-Solomon codes over $\mathbb{F}_{2^m}$ with evaluation set of size $|D| = n$ such that maximum-likelihood decoding is NP-complete.

The proof gives a polynomial-time reduction of the maximum-likelihood decoding problem to the three-dimenisonal matching problem, which has been shown to be NP-complete.

Results by Guruswami-Vardy

Note here that the evaluation set D is a tremendously small set compared to $\mathbb{F}_q$ (i.e. t^3 versus 2^{3t}). Guruswami and Vardy suggested that the maximum-likelihood decoding might be easier if D is much larger or has some algebraic structure.

Results by Cheng-Wan

Problem (Discrete Logarithm)

Given a finite field $\mathbb{F}_q$, a generator g of $\mathbb{F}_q^*$, and a nonzero element a, to find an integer i such that

$$g^i = a$$

The value of i is denoted $\log_g a$.

Results by Cheng-Wan

Problem (Discrete Logarithm)

Given a finite field $\mathbb{F}_q$, a generator g of $\mathbb{F}_q^*$, and a nonzero element a, to find an integer i such that

$$g^i = a$$

The value of i is denoted $\log_g a$.

This problem occurs in many cryptographic systems. Although no general hardness results have been proved, it is still believed to be very difficult.

Results by Cheng-Wan

Cheng and Wan proved a variety of conditional hardness results by converting Reed-Solomon decoding problems into discrete logarithm problems and applying the index calculus algorithm.

Results by Cheng-Wan

In an (n, k) Reed-Solomon code over $\mathbb{F}_q$, let $\hat{g}(n, k, q)$ be the smallest positive integer g such that $\binom{n}{g}/q^{g-k}$ is less than 1.

Theorem (Cheng-Wan, 2004)

If there exists an algorithm solving the list decoding problem of radius $n - \hat{g}$ in time $q^{O(1)}$, then discrete logarithm over the finite field $\mathbb{F}_{q^{\hat{g}-k}}$ can be computed in random time $q^{O(1)}$.

Results by Cheng-Wan

Theorem (Cheng-Wan, 2004)

Let h be a positive integer satisfying

$$q \geq \max(g^2, (h-1)^{2+\varepsilon}) \quad \text{and} \quad g \geq (4/\varepsilon + 2)(h+1)$$

for a constant $\varepsilon > 0$. If the bounded distance decoding problem of radius $B = q - g$ for the $(q, g-h)$ Reed-Solomon code can be solved in time $q^{O(1)}$, the discrete logarithm problem over $\mathbb{F}_{q^h}$ can be solved in random time $q^{O(1)}$.

Results by Cheng-Wan

Theorem (Cheng-Wan, 2010)

Let $\delta > 0$ be a constant and $m > 1$ be an integer. Suppose h and k are integers satisfying

$$h \leq \frac{q^{\frac{1}{2+\delta}}}{m} + \frac{1}{m}\ ,\ h \leq \frac{\sqrt{q}}{m(4/\delta + 2)} - \frac{1}{m}\ ,\ q \leq k \leq q^m - q$$

The discrete logarithm in $\mathbb{F}^*_{q^{mh}}$ can be solved in randomized time $(q^m)^{O(1)}$ with oracle access to a maximum-likelihood decoder for a (q^m, k) Reed-Solomon code over $\mathbb{F}_{q^m}$.

Results by Cheng-Wan

Theorem (Cheng-Wan, 2010)

Let ε be a positive constant less than $1/3$ and $g = \frac{2+3\varepsilon}{1-3\varepsilon}(h+1)$. In an $(q, q-g-h)$ Reed-Solomon code over $\mathbb{F}_q$ for sufficiently large q, there does not exist a randomized polynomial time bounded distance decoder at distance $(2/3+\varepsilon)d$, where d is the minimum distance, unless the discrete logarithm problem over $\mathbb{F}_{q^h}$ can be solved in randomized time $q^{O(1)}$ for any $h \leq q^{0.8\varepsilon}$.

Applications to the Discrete Logarithm Problem

Augot and Morain (2012) built on the work by Cheng and Wan by making the conversion to discrete logarithms effective.

Applications to the Discrete Logarithm Problem

Augot and Morain (2012) built on the work by Cheng and Wan by making the conversion to discrete logarithms effective.

The conversion can be set up in this way:

Let $F = \mathbb{F}_{q^h}$ and $K = \mathbb{F}_q$. Take a fixed monic $Q(X)$ from $K[X]$, with deg $Q(X) = h$, and a set $S \subset F$ with size n so that $Q(a) \neq 0$ for all $a \in S$. Let $1 \leq \mu \leq n$.

Applications to the Discrete Logarithm Problem

Theorem (Augot-Morain, 2012)

For any $f(X)$ in $K[X]$ with $\deg f(X) < \mu$, there exists $A \subset S$ where $|A| = \mu$ such that

$$\prod_{a \in A}(X - a) \equiv f(X) \pmod{Q(x)}$$

if and only if the word represented by the polynomial

$$y(X) = -f(X)/Q(X) - X^k$$

is exactly distance $n - \mu$ from the Reed-Solomon code with $k = \mu - h$ and evaluation set $D = S$. All such sets A can be found by decoding the word $y(X)$ up to radius $n - \mu$.

Applications to the Discrete Logarithm Problem

Discrete logarithms can be computed using a procedure similar to index calculus. If $Q(X)$ is a primitive polynomial, take $f(X) = X^u$ for random u. After finding all relations of the form

$$\prod_{a \in A} (X - a) \equiv f(X) \pmod{Q(x)}$$

using Reed-Solomon decoding, we can try to set up a linear system to solve for the values of $\log(X - a)$ for all $a \in S$.

Applications to the Discrete Logarithm Problem

Augot and Morain showed that computing discrete logarithms in $\mathbb{F}_{q^h}$ using their implementation takes $\tilde{O}(h!\ q^2)$ operations over $\mathbb{F}_q$.

The Deep Hole Problem

For an (n, k) Reed-Solomon code, it can be shown that for any received word r, we always have $d(r, \mathcal{C}) \leq n - k$. This number is the so-called covering radius, the maximum value of $d(r, \mathcal{C})$ over all possible words r.

The Deep Hole Problem

For an (n, k) Reed-Solomon code, it can be shown that for any received word r, we always have $d(r, \mathcal{C}) \leq n - k$. This number is the so-called covering radius, the maximum value of $d(r, \mathcal{C})$ over all possible words r.

For r satisfying $d(r, \mathcal{C}) = n - k$, Guruswami and Vardy called this a deep hole. They observed that as a consequence of their results in their family of codes, determining whether or not r is a deep hole is actually NP-hard.

The Deep Hole Problem

For an (n, k) Reed-Solomon code, it can be shown that for any received word r, we always have $d(r, \mathcal{C}) \leq n - k$. This number is the so-called covering radius, the maximum value of $d(r, \mathcal{C})$ over all possible words r.

For r satisfying $d(r, \mathcal{C}) = n - k$, Guruswami and Vardy called this a deep hole. They observed that as a consequence of their results in their family of codes, determining whether or not r is a deep hole is actually NP-hard.

As before, the situation might be different for codes with evaluation sets of larger size or some algebraic structure.

The Deep Hole Problem

Take an (n, k) Reed-Solomon code over $\mathbb{F}_q$ with some evaluation set D (preferably with some algebraic structure, as in $D = \mathbb{F}_q$ or $D = \mathbb{F}_q^*$).

Problem (Determining Deep Holes)

Given a received message r, to determine whether or not r is a deep hole.

Preview of Topics

5 Previous Results on Deep Holes

- Results when $D = \mathbb{F}_q$
- Results when $D = (\mathbb{F}_q)^*$

Some Simple Bounds

Let $u = (u_1, u_2, \ldots, u_n)$ be a received message. Use Lagrange Interpolation to find the associated polynomial $u(x)$. If $\deg u(x) \leq k - 1$, then u is a codeword. Otherwise, a short argument shows that

$$n - \deg u(x) \leq d(u, \mathcal{C}) \leq n - k$$

Note that if $\deg u(x) = k$, then u is automatically a deep hole.

5 Previous Results on Deep Holes

- Results when $D = \mathbb{F}_q$
- Results when $D = (\mathbb{F}_q)^*$

Results by Cheng-Murray

Cheng and Murray considered the deep hole problem for codes over $\mathbb{F}_q$ with evaluation set $D = \mathbb{F}_q$. They came up with the following conjecture:

Conjecture (Cheng-Murray, 2007)

The only deep holes are those words u such that $\deg u(x) = k$.

Results by Cheng-Murray

They were unable to prove their conjecture completely, but they reduced the problem to finding a rational point on an algebraic hypersurface and were able to derive the following result only for $q = p$:

Theorem (Cheng-Murray, 2007)

Let p be a prime and $1 < k < p^{1/4-\varepsilon}$ be a positive integer. Let u be a received word and $u(x)$ be its interpolated polynomial. If the degree of $u(x)$ satisfies

$$k < \deg u(x) < k + p^{3/13-\varepsilon}$$

then u is not a deep hole.

Results by Cheng-Murray

As an example, choose $p = 929$. Then in the $(929, k)$ Reed-Solomon code (for $1 < k < 5.25$), if the degree of $u(x)$ satisfies

$$k < \deg u(x) < k + 4.84$$

then u is not a deep hole.

Results by Li-Wan

Li and Wan studied the problem in terms of solving polynomial congruences, using character sums combined with Weil's character sum bounds to count solutions. They were able to give some exact distance measurements under the right conditions.

Theorem (Li-Wan, 2010)

Let u be a received word and $u(x)$ be its interpolated polynomial. Suppose $1 \leq d := \deg u(x) - k \leq q - 1 - k$. If

$$q > \max((k+1)^2, d^{2+\varepsilon}) \text{ and } k > \left(\frac{2}{\varepsilon} + 1\right) d + \frac{8}{\varepsilon} + 2$$

for some constant $\varepsilon > 0$, then $d(u, \mathcal{C}) < q - k$. In other words, u is not a deep hole. *Continued...*

Results by Li-Wan

Theorem, continued...

Furthermore, if

$$q > \max((k+1)^2, (d-1)^{2+\varepsilon}) \text{ and } k > \left(\frac{4}{\varepsilon} + 1\right) d + \frac{4}{\varepsilon} + 2$$

for some constant $\varepsilon > 0$, then $d(u, \mathcal{C}) = q - (k + d)$.

Several other authors followed these techniques to get new bounds.

Results by Liao

Theorem (Liao, 2011)

Let $r \geq 1$ be an integer. Let u be a received word and $u(x)$ be the interpolated polynomial of degree m. If $m \geq k + r$,

$$q > \max\left\{2\binom{k+r}{2} + (m-k), (m-k)^{2+\varepsilon}\right\}$$

and

$$k > \frac{1}{1+\varepsilon}\left(r + (2+\varepsilon)\left(\frac{m}{2} + 1\right)\right)$$

for some constant $\varepsilon > 0$, then $d(u, \mathcal{C}) \leq q - k - r$.

Results by Cafure-Matera-Privitelli

Using some techniques from algebraic geometry, Cafure, Matera, and Privitelli slightly improved on one of Li-Wan's previous results with

Theorem (Cafure-Matera-Privitelli, 2012)

Let u be a received word and $u(x)$ be is interpolated polynomial with $1 \leq d := \deg(u(x)) - k \leq q - 1 - k$. Assume that

$$q > \max((k+1)^2, 14d^{2+\varepsilon}) \text{ and } k > d\left(\frac{2}{\varepsilon} + 1\right)$$

for some constant $\varepsilon > 0$. Then u is not a deep hole.

Results by Zhu-Wan

In the previous results, many of the conditions required $u(x)$ to be a polynomial with degree only slightly larger than k. Zhu and Wan improved upon this by observing that some high degree polynomials can also be represented by low-degree rational functions. They came up with the following:

Results by Zhu-Wan

Theorem (Zhu-Wan, 2012)

Let $r \geq 1$ be an integer. Suppose we can write

$$\left(\frac{w(x_1)}{h(x_1)}, \frac{w(x_2)}{h(x_2)}, \ldots, \frac{w(x_q)}{h(x_q)} \right) = u$$

for some $h(x) \in \mathbb{F}_q[x]$, with $\gcd(h(x), x^q - x) = 1$, and $\deg h(x) + k \leq \deg w(x) \leq q - 1$. Let m be the smallest such degree of $w(x)$, and set $r \leq d := m - k \leq q - 1 - k$. *Continued...*

Results by Zhu-Wan

Theorem, continued...

There are positive constants c_1 and c_2 such that if

$$d < c_1 q^{1/2} \ , \ \left(\frac{d+r}{2} + 1\right) \log_2 q < k < c_2 q$$

then $d(u, \mathcal{C}) \leq q - k - r$.

5 Previous Results on Deep Holes

- Results when $D = \mathbb{F}_q$
- Results when $D = (\mathbb{F}_q)^*$

Results by Wu-Hong

Wu and Hong studied the deep hole problem when $D = \mathbb{F}_q^*$. Using this evaluation set allowed them to use the BCH formulation of Reed-Solomon codes.

Theorem (Wu-Hong, 2011)

Take a Reed-Solomon code over $\mathbb{F}_q$ with $q \geq 4$ and $2 \leq k \leq q-2$. Then polynomials of the form $u(x) = ax^{q-2} + v(x)$ with $a \neq 0$, where $\deg v(x) \leq k-1$, represent deep holes.

Results by Wu-Hong

This work shows that the Cheng-Murray conjecture is false when $D = \mathbb{F}_q^*$. Wu and Hong attempted to modify the conjecture to include certain polynomials of degree $q - 2$. This would later be disproved by Zhang, Fu, and Liao.

Results by Zhang-Fu-Liao

Zhang, Fu, and Liao proved an extension of Wu-Hong that allows D to be any evaluation set except $\mathbb{F}_q$.

Theorem (Zhang-Fu-Liao, 2012)

Take a Reed-Solomon code over $\mathbb{F}_q$ with evaluation set $D \neq \mathbb{F}_q$. Then for any $a \neq 0$, $b \notin D$, polynomials of the form

$$u(x) = a(x - b)^{q-2} + v(x)$$

where $\deg v(x) \leq k - 1$, represent deep holes.

Results by Zhang-Fu-Liao

They also adapted work from Li-Wan to find more deep holes for a specific message length k.

Theorem (Zhang-Fu-Liao, 2012)

For $q > 4$, take a Reed-Solomon code over $\mathbb{F}_q$ with evaluation set $D = \mathbb{F}_q^*$ or $D = \mathbb{F}_q^*/\{1\}$ and $k = q - 4$. If $a \neq 0$, then polynomials of the form

$$u(x) = ax^{q-3} + v(x)$$

where $\deg v(x) \leq k - 1$, represent deep holes.

Results by Zhang-Fu-Liao

Finally, they found a class of received words that are not deep holes.

Theorem (Zhang-Fu-Liao, 2012)

Take a Reed-Solomon code over $\mathbb{F}_q$ for $q > 5$, $2 \leq k \leq q-3$, and $D = \mathbb{F}_q^*$. Polynomials of the form

$$u(x) = ax^{k+2} + bx^{k+1} + cx^k + v(x)$$

where $a \in \mathbb{F}_q^*$, $b, c \in \mathbb{F}_q$, and $\deg v(x) \leq k-1$, do not represent deep holes.

Preview of Topics

6 Our Results on Deep Holes
- Extensions to Zhu-Wan
- Prerequisites for a Proof
- A (Very Rough) Sketch of the Proof
- Summary and Further Work

6 Our Results on Deep Holes

- Extensions to Zhu-Wan
- Prerequisites for a Proof
- A (Very Rough) Sketch of the Proof
- Summary and Further Work

Zhu and Wan's original work applied for Reed-Solomon codes over $\mathbb{F}_q$ with evaluation set $D = \mathbb{F}_q$.

In new work with Zhu and Wan, we were able to produce new statements for codes with slightly smaller evaluation sets.

Our Results

Theorem

Let $\mathcal{C}$ be a Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set D with $|D| > q/2$. Let u be a received word. Suppose we can write

$$\left(\frac{w(x_1)}{h(x_1)}, \frac{w(x_2)}{h(x_2)}, \ldots, \frac{w(x_{|D|})}{h(x_{|D|})}\right) = u$$

for some $h(x) \in \mathbb{F}_q[x]$, with no roots in D, and $\deg h(x) + k \leq \deg w(x) \leq |D| - 1$. Let m be the smallest such degree of $w(x)$. Let $1 \leq r \leq d := m - k \leq |D| - k - 1$.

Continued...

Our Results

Theorem, continued...

If the bound

$$\left|\sum_{a\in D}\chi(1-ax)\right| \leq Kq^{1/2}$$

is true over all nontrivial characters $\chi : (\mathbb{F}[x]/(\bar{h}(x)))^* \to \mathbb{C}$ with $\chi(\mathbb{F}_q^*) = 1$ for some $K \geq d$ and $\bar{h}(x) = x^{m-k+1}h(1/x)$, there are positive constants c_1 and c_2 such that if

$$d \leq K < c_1 q^{1/2}\ ,\ \frac{(\frac{d+r}{2}+1)\log_2 q}{\log_2|D|+1-\log_2 q} < k < c_2 q$$

then $d(u,\mathcal{C}) \leq |D| - k - r$.

Our Results

We have a more familiar setting by taking $D = \mathbb{F}_q^*$ and $h(x) = 1$.

Corollary

Take a Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set $D = \mathbb{F}_q^*$. Let $r \geq 1$ be an integer and u a received word with interpolated polynomial $u(x)$ such that $r \leq d := \deg(u(x)) - k \leq q - 2 - k$. There are positive constants c_1 and c_2 such that if

$$d < c_1 q^{1/2} \ , \ \frac{(\frac{d+r}{2} + 1)\log_2 q}{\log_2(q-1) + 1 - \log_2 q} < k < c_2 q$$

then $d(u, \mathcal{C}) \leq q - 1 - k - r$.

Examples

Take a Reed-Solomon code over $\mathbb{F}_{2^8}$ with evaluation set $D = \mathbb{F}_{2^8}^*$.

Examples

Take a Reed-Solomon code over $\mathbb{F}_{2^8}$ with evaluation set $D = \mathbb{F}_{2^8}^*$.

If $r \geq 1$, and u is a codeword with $r \leq d \leq 254 - k$, then we can find c_1 and c_2 such that if

$$d < 16c_1 \quad \text{and} \quad 8.045\left(\frac{d+r}{2} + 1\right) < k < 256c_2$$

then $d(u, \mathcal{C}) \leq 255 - k - r$.

Examples

Take a Reed-Solomon code over $\mathbb{F}_{2^8}$ with evaluation set $D = \mathbb{F}_{2^8}^*$.

If $r \geq 1$, and u is a codeword with $r \leq d \leq 254 - k$, then we can find c_1 and c_2 such that if

$$d < 16c_1 \quad \text{and} \quad 8.045\left(\frac{d+r}{2} + 1\right) < k < 256c_2$$

then $d(u, \mathcal{C}) \leq 255 - k - r$.

Consider $d = r = 1$. In other words, we want to classify codewords whose polynomial (or rational) interpolations are degree $k + 1$ (in the numerator).

Examples

From the proof of the theorem, we can explicitly compute c_1 and c_2 using the formulas

$$1 < 16c_1 \ , \ c_1 + c_2 = 255 \cdot 256^{-\frac{k+2}{k+1}} - \frac{1}{2}$$

Examples

From the proof of the theorem, we can explicitly compute c_1 and c_2 using the formulas

$$1 < 16c_1 \ , \ c_1 + c_2 = 255 \cdot 256^{-\frac{k+2}{k+1}} - \frac{1}{2}$$

To obtain a wide range of k, fix $c_1 = .0626$. Then we have the condition

$$16.09 < k < 256 \left(255 \cdot 256^{-\frac{k+2}{k+1}} - \frac{1}{2} - .0626 \right)$$

Examples

The inequality is satisfied when $17 \leq k \leq 96$.

Examples

The inequality is satisfied when $17 \leq k \leq 96$.

Therefore, for codes using this range of message lengths, received words u represented by a polynomial (or rational function) of degree $k+1$ (in the numerator) are not deep holes.

Examples

The inequality is satisfied when $17 \leq k \leq 96$.

Therefore, for codes using this range of message lengths, received words u represented by a polynomial (or rational function) of degree $k+1$ (in the numerator) are not deep holes.

More specifically, we can give the estimate $d(u, \mathcal{C}) \leq 254 - k$.

Examples

Similarly, for $r = 1$ and $d = 2$, polynomials (or rational functions) of degree $k + 2$ (in the numerator) do not represent deep holes when the message length satisfies $30 \leq k \leq 59$.

Such words u satisfy the estimate $d(u, \mathcal{C}) \leq 254 - k$.

Examples

Here is a table with a few examples of words covered by our bounds. We will denote α to be a multiplicative generator for $\mathbb{F}_{2^8}^*$.

Examples

Here is a table with a few examples of words covered by our bounds. We will denote α to be a multiplicative generator for $\mathbb{F}_{2^8}^*$.

d	k	Polynomial Interpolation
1	17	$x^{18} + 3x^2 + 1$
1	17	$x^{254} + x^{17} + 1$
2	30	$x^{254} + x^{253} + x^{30}$
2	30	$(\alpha^4 + 1)x^{254} + \ldots + (\alpha^6 + \alpha^3 + \alpha^2 + 1)$

Examples

Here is a table with a few examples of words covered by our bounds. We will denote α to be a multiplicative generator for $\mathbb{F}_{2^8}^*$.

d	k	Polynomial Interpolation
1	17	$x^{18} + 3x^2 + 1$
1	17	$x^{254} + x^{17} + 1$
2	30	$x^{254} + x^{253} + x^{30}$
2	30	$(\alpha^4 + 1)x^{254} + \ldots + (\alpha^6 + \alpha^3 + \alpha^2 + 1)$
		Rational Interpolation
1	17	N/A
1	17	$(x^{18} + x + 1)/x$
2	30	$(x^{32} + x + 1)/x^2$
2	30	$(x^{32} + x^2 + \alpha)/(x^2 - \alpha^2 x + \alpha + 1)$

Multiplicative Characters

Definition (Multiplicative Character)

Let $h(x)$ be a polynomial from $\mathbb{F}_q[x]$. We say that a homomorphism $\chi : (\mathbb{F}_q[x]/(h(x)))^* \to \mathbb{C}$ is a multiplicative character of $(\mathbb{F}_q[x]/(h(x)))^*$.

It can be extended to the entire group $\mathbb{F}_q[x]/(h(x))$ by setting $\chi(f(x)) = 0$ if $\gcd(f(x), h(x)) \neq 1$.

Weil's Character Sum Bound

Theorem (Weil)

Let $h(x)$ be a polynomial of positive degree in the ring $\mathbb{F}_q[x]$, and let $\chi : (\mathbb{F}[x]/(h(x)))^* \to \mathbb{C}$ be a multiplicative character. If χ is not trivial, then

$$\left| \sum_{a \in \mathbb{F}_q} \chi(x - a) \right| \leq (\deg h(x) - 1) q^{1/2}$$

Furthermore, if χ is not trivial but $\chi(\mathbb{F}_q^*) = 1$, then

$$\left| 1 + \sum_{a \in \mathbb{F}_q} \chi(x - a) \right| \leq (\deg h(x) - 2) q^{1/2}$$

Weil's Character Sum Bound, modified

Lemma

Let $h_1(x)$ be a polynomial from $\mathbb{F}_q[x]$ not divisible by x, $h(x) = x^k h_1(x)$ for $k \geq 1$, and $\chi : (\mathbb{F}[x]/(h_1(x)))^* \to \mathbb{C}^*$ with χ nontrivial and $\chi(\mathbb{F}_q^*) = 1$. For a subgroup $(\mathbb{F}_q^*)^{\frac{q-1}{\ell}}$ of $\mathbb{F}_q^*$, we have

$$\left| \sum_{a \in (\mathbb{F}_q^*)^{\frac{q-1}{\ell}}} \chi(x-a) \right| \leq (\deg h(x) - 1) q^{1/2}$$

Li-Wan's New Sieve

Let D be a finite set and let X be a subset of D^k. Denote

$$\bar{X} = \{(x_1, x_2, \ldots, x_k) \in X \mid x_i \neq x_j, i \neq j\}$$

Let $f(x_1, x_2, \ldots, x_k)$ be a complex-valued function defined over X. Denote

$$F = \sum_{x \in \bar{X}} f(x_1, x_2, \ldots, x_k)$$

Li-Wan's New Sieve

Let S_k be the symmetric group on $\{1, 2, \ldots, k\}$. Each permutation $\tau \in S_k$ can be uniquely factorised as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. Namely,

$$\tau = (i_1 i_2 \ldots i_{a_1})(j_1 j_2 \ldots j_{a_2}) \cdots (l_1 l_2 \ldots l_{a_s})$$

with $a_i \geq 1$ and $1 \leq i \leq s$. Define

$$X_\tau = \{(x_1, x_2, \ldots, x_k) \mid x_{i_1} = \ldots = x_{i_{a_1}}, \cdots, x_{l_1} = \ldots = x_{l_{a_s}}\}$$

Similarly define

$$F_\tau = \sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k)$$

Li-Wan's New Sieve

We say that τ is of the type $(c_1, c_2, \ldots, c_k)$ if it has exactly c_i cycles of length i. Let $N(c_1, c_2, \ldots, c_k)$ be the number of permutations of type $(c_1, c_2, \ldots, c_k)$. Define

$$C_k(t_1, t_2, \ldots, t_k) = \sum_{\sum ic_i = k} N(c_1, c_2, \ldots, c_k) t_1^{c_1} t_2^{c_2} \cdots t_k^{c_k}$$

Li-Wan's New Sieve

Now we have the following combinatorial result:

Suppose $q \geq d$. If $t_i = q$ for $d|i$ and $t_i = s$ for $d \nmid i$, then we have

$$C_k(s, \ldots s, q, s, \ldots, x, q, \ldots) = k! \sum_{i=0}^{\lfloor k/d \rfloor} \binom{\frac{q-s}{d} + i - 1}{i} \binom{s + k - di - 1}{k - di}$$
$$\leq \left(s + k + \frac{q-s}{d} - 1 \right)_k$$

where $(x)_k = x(x-1)(x-2)\cdots(x-k+1)$.

Li-Wan's New Sieve

Furthermore, we say that X is symmetric if for any $x \in X$ and any $g \in S_k$, we have $g \circ x \in X$. Also, if a complex-valued function f is defined on X, we say that it is normal on X if X is symmetric and for any two conjugate elements in S_k, τ and τ', we have

$$\sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k) = \sum_{x \in X_{\tau'}} f(x_1, x_2, \ldots, x_k)$$

Then, we have the result:

If f is normal on X, then

$$F = \sum_{\sum ic_i = k} (-1)^{k - \sum c_i} N(c_1, c_2, \ldots, c_k) F_\tau$$

Rephrasing Error Distance

Lemma

Let $\mathcal{C}$ be a Reed-Solomon code over $\mathbb{F}_q$ using the evaluation set D. Let u be a received word and $u(x)$ its interpolated polynomial with $\deg u(x) = k + d$, where $k + 1 \leq k + d \leq q - 1$. The error distance $d(u, \mathcal{C}) \leq |D| - k - r$ for some $1 \leq r \leq d$ if and only if there exists a subset $\{x_{i_1}, x_{i_2}, \ldots, x_{i_{k+r}}\} \subset D$ and a polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $d - r$ such that

$$u(x) - v(x) = (x - x_{i_1})(x - x_{i_2}) \cdots (x - x_{i_{k+r}})g(x)$$

for some $v(x)$ with $\deg v(x) \leq k - 1$.

6 Our Results on Deep Holes

- Extensions to Zhu-Wan
- Prerequisites for a Proof
- A (Very Rough) Sketch of the Proof
- Summary and Further Work

The Basic Idea

Our idea is to phrase the problem in terms of finding solutions to a polynomial congruence. In particular, our results will be proved if we can guarantee that there is at least one solution to our congruence.

To do this, we will use a character sum argument combined with estimations from Li-Wan's new sieve.

Sketch of Proof

Suppose we are given a received word u. We have assumed that u can be interpolated by a rational function $w(x)/h(x)$, where $\deg w(x) = m$, $\deg h(x) \leq m - k$, and $h(x)$ has no roots in D.

Sketch of Proof

Suppose we are given a received word u. We have assumed that u can be interpolated by a rational function $w(x)/h(x)$, where $\deg w(x) = m$, $\deg h(x) \leq m - k$, and $h(x)$ has no roots in D.

We may assume that $w(0) = 1$ by shifting by a constant codeword and rescaling if necessary.

Sketch of Proof

Suppose we are given a received word u. We have assumed that u can be interpolated by a rational function $w(x)/h(x)$, where $\deg w(x) = m$, $\deg h(x) \leq m - k$, and $h(x)$ has no roots in D.

We may assume that $w(0) = 1$ by shifting by a constant codeword and rescaling if necessary.

Let $\bar{h}(x) = x^{m-k+1}h(1/x)$. This is a polynomial of degree $m - k + 1 = d + 1$ and divisible by x since $h(0) \neq 0$ and $\deg(h(x)) \leq m - k$.

Sketch of Proof

Suppose we are given a received word u. We have assumed that u can be interpolated by a rational function $w(x)/h(x)$, where $\deg w(x) = m$, $\deg h(x) \leq m - k$, and $h(x)$ has no roots in D.

We may assume that $w(0) = 1$ by shifting by a constant codeword and rescaling if necessary.

Let $\bar{h}(x) = x^{m-k+1}h(1/x)$. This is a polynomial of degree $m - k + 1 = d + 1$ and divisible by x since $h(0) \neq 0$ and $\deg(h(x)) \leq m - k$.

Let $A = (\mathbb{F}_q[x]/(\bar{h}(x)))^*$ and $\hat{A}$ denote the group of all characters of A. Let $\hat{B}$ be the set of characters χ in $\hat{A}$ with $\chi(\mathbb{F}_q^*) = 1$.

Sketch of Proof

Now $d(u, \mathcal{C}) \leq |D| - k - r$ if and only if there is some polynomial $f(x) \in \mathbb{F}_q[x]$ with $\deg f(x) \leq k - 1$ such that

$$\frac{w(x)}{h(x)} + f(x) = \frac{w(x) + f(x)h(x)}{h(x)}$$

has at least $k + r$ distinct roots in D.

Sketch of Proof

Now $d(u, \mathcal{C}) \leq |D| - k - r$ if and only if there is some polynomial $f(x) \in \mathbb{F}_q[x]$ with $\deg f(x) \leq k - 1$ such that

$$\frac{w(x)}{h(x)} + f(x) = \frac{w(x) + f(x)h(x)}{h(x)}$$

has at least $k + r$ distinct roots in D. In other words, there are points $\{x_1, x_2, \ldots, x_{k+r}\} \subset D$ where

$$w(x) + f(x)h(x) = (x - x_1)(x - x_2) \cdots (x - x_{k+r})v(x)$$

for some polynomial $v(x)$ with $\deg v(x) = m - (k + r)$.

Sketch of Proof

Then replacing x with $1/x$ and multiplying through by x^m, it is enough to find such a subset for the equation

$$\tilde{w}(x) + \tilde{f}(x)\bar{h}(x) = (1 - x_1x)(1 - x_2x)\cdots(1 - x_{k+r}x)\tilde{v}(x)$$

where $\tilde{w}(x) = x^m w(1/x)$, $\tilde{f}(x) = x^{k-1} f(1/x)$, and $\tilde{v}(x) = x^{m-(k+r)} v(1/x)$.

Sketch of Proof

Then replacing x with $1/x$ and multiplying through by x^m, it is enough to find such a subset for the equation

$$\tilde{w}(x) + \tilde{f}(x)\bar{h}(x) = (1 - x_1x)(1 - x_2x)\cdots(1 - x_{k+r}x)\tilde{v}(x)$$

where $\tilde{w}(x) = x^m w(1/x)$, $\tilde{f}(x) = x^{k-1} f(1/x)$, and $\tilde{v}(x) = x^{m-(k+r)} v(1/x)$.
Then this equation is equivalent to

$$\frac{(1 - x_1x)(1 - x_2x)\cdots(1 - x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)} \equiv 1 \pmod{\bar{h}(x)}$$

Sketch of Proof

Let the number of solutions to this equation be denoted by N_u, noting that the $x_i \in D$ are distinct, $\tilde{v}(0) = 1$ (since $\tilde{w}(0) = 1$), and $\deg \tilde{v}(x) = m - (k + r) = d - r$.

Sketch of Proof

Let the number of solutions to this equation be denoted by N_u, noting that the $x_i \in D$ are distinct, $\tilde{v}(0) = 1$ (since $\tilde{w}(0) = 1$), and $\deg \tilde{v}(x) = m - (k + r) = d - r$.

In our terms, N_u gives the number of codewords f in $\mathcal{C}$ where $d(u, f) \leq |D| - k - r$. If N_u is positive, then $d(u, \mathcal{C}) \leq |D| - k - r$.

Sketch of Proof

By taking character sums of both sides of our congruence and then counting, we have

$$N_u = \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x) = d-r}} \sum_{\chi \in \hat{B}} S_\chi(x_1, x_2, \ldots, x_{k+r}, x)$$

where, for ease of notation, we define

$$S_\chi(x_1, x_2, \ldots, x_{k+r}, x) = \chi\left(\frac{(1-x_1x)(1-x_2x)\cdots(1-x_{k+r}x)\tilde{v}(x)}{\tilde{w}(x)}\right)$$

Sketch of Proof

For the case where $r < d$, we can instead consider a weighted version

$$N = \frac{1}{|\hat{B}|} \sum_{\substack{x_i \in D \\ \text{distinct}}} \sum_{\substack{\tilde{v}(x), \tilde{v}(0)=1 \\ \deg \tilde{v}(x) = d-r}} \Lambda(\tilde{v}) \sum_{\chi \in \hat{B}} S_\chi(x_1, x_2, \ldots, x_{k+r}, x),$$

where Λ denotes the von Mangoldt function.

Note that if $N > 0$, then $N_u > 0$.

Sketch of Proof

Rearranging and evaluating parts of the previous expression gives us

$$\left| N - \frac{1}{|\hat{B}|}(|D|)_{k+r}(q^{d-r}-1) \right|$$

$$= \left| \frac{1}{|\hat{B}|} \sum_{\substack{\tilde{v}(x),\tilde{v}(0)=1 \\ \deg \tilde{v}(x)=d-r}} \Lambda(\tilde{v}) \sum_{\substack{\chi \in \hat{B} \\ \chi \neq 1}} \sum_{\substack{x_i \in D \\ \text{distinct}}} S_\chi(x_1, x_2, \ldots, x_{k+r}, x) \right|$$

Sketch of Proof

We can estimate the right hand side using Li-Wan's new sieve as well as the Weil bound. If we do this, we have

$$\left| N - \frac{1}{|\hat{B}|}(|D|)_{k+r}(q^{d-r}-1) \right| \leq \frac{1}{|\hat{B}|} d q^{\frac{3d-r}{2}} \left(K q^{1/2} + k + \frac{q}{2} \right)_{k+r}$$

where we recall that $(x)_k = x(x-1)(x-2)\cdots(x-k+1)$.

Sketch of Proof

Therefore, it is sufficient to prove that

$$(|D|)_{k+r}(q^{d-r}-1) > dq^{\frac{3d-r}{2}}\left(Kq^{1/2}+k+\frac{q}{2}\right)_{k+r}$$

Sketch of Proof

Therefore, it is sufficient to prove that

$$(|D|)_{k+r}(q^{d-r}-1) > dq^{\frac{3d-r}{2}}\left(Kq^{1/2}+k+\frac{q}{2}\right)_{k+r}$$

Solving the inequality for k gives the condition

$$k > \frac{\log_2 d + (\frac{d+r+1}{2})\log_2 q - r\,(\log_2 |D| + 1 - \log_2 q)}{\log_2 |D| + 1 - \log_2 q}$$

Here we require that $|D| > q/2$ in order for the term $\log_2 |D| + 1 - \log_2 q$ to be positive and preserve the inequality.

Sketch of Proof

Since $r \leq d \leq K < q^{1/2}$, we can just replace the term

$$\log_2 d - r\left(\log_2 |D| + 1 - \log_2 q\right)$$

with $\frac{1}{2}\log_2 q$ to receive a simpler condition:

$$k > \frac{\left(\frac{d+r}{2} + 1\right)\log_2 q}{\log_2 |D| + 1 - \log_2 q}$$

Our theorem is proved.

6 Our Results on Deep Holes

- Extensions to Zhu-Wan
- Prerequisites for a Proof
- A (Very Rough) Sketch of the Proof
- Summary and Further Work

Summary

In certain Reed-Solomon codes with large evaluation sets satisfying certain character sum bounds, we have found families of received words that are not deep holes.

We can apply these results specifically for $D = \mathbb{F}_q$ or $D = \mathbb{F}_q^*$.

Further Work (Short Term)

These results raise a few questions:

Further Work (Short Term)

These results raise a few questions:

Our techniques only work when $|D| > q/2$, which prevents us from making any statements when D is relatively small. Can we come up with better estimates to allow for small D, particularly when D is a subgroup of $\mathbb{F}_q^*$?

Further Work (Short Term)

These results raise a few questions:

- Our techniques only work when $|D| > q/2$, which prevents us from making any statements when D is relatively small. Can we come up with better estimates to allow for small D, particularly when D is a subgroup of $\mathbb{F}_q^*$?
- We were also required to assume $d < c_1 q^{1/2}$. If it were possible to relax the condition to $d < c_1 q^{1/2+\varepsilon}$, we would be able to choose much smaller values of c_1 to get better information rates on our codes. Is it possible to do this?

Further Work (Long Term)

Researchers have approached the deep hole problem from two ways:

- Find families of words that are not deep holes
- Find families of words that are deep holes

Further Work (Long Term)

Researchers have approached the deep hole problem from two ways:

- Find families of words that are not deep holes
- Find families of words that are deep holes

Most current results only apply to families of very low degree (slightly higher than k) or very high degree (slightly less than q). Our goal is to try to fill up the gap and complete the classification of deep holes.

Reed-Solomon Error-correcting Codes

The Deep Hole Problem

Matt Keti
(Advisor: Professor Daqing Wan)

Department of Mathematics
University of California, Irvine

November 8, 2012