Generalized Reed-Solomon Codes

John McCall

Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

April 13, 2014

Overview

- Data transmission has become vital in today's society.
- Transmission methods are not perfect.
- Error correcting codes help to alleviate the burden of transmission.

Outline

Outline

Introducing $\mathbb{F}_{64}$

The finite field of 64 elements.
[Insert picture of ASCII table showing the elements]

Representation of our Elements

- Each element is encoded as a 6-bit binary string.
- We can represent that string as a polynomial in $\mathbb{F}_2[x]$.

For example:

- $\# \to 000011 \to x + 1$

Addition in $\mathbb{F}_{64}$

- Regular polynomial addition, but the coefficients are added modulo 2.
- $(x^4 + x^2 + x + 1) + (x^3 + x + 1) = x^4 + x^3 + x^2$.

Multiplication in $\mathbb{F}_{64}$

- Similar to regular multiplication, except the result cannot be larger than degree 5.
- We have to use an irreducible polynomial to mod out terms that are of too high a degree.
- The polynomial: $x^6 + x + 1 \rightarrow x^6 = x + 1$.

Multiplication Example

- $(x^5 + x^2 + x + 1)(x^4 + x)$
- $= x^9 + x^6 + x^6 + x^5 + x^4 + x^3 + x^2 + x$
- $= x^9 + x^5 + x^4 + x^3 + x^2 + x$
- $= (x^6)(x^3) + x^5 + x^4 + x^3 + x^2 + x$
- $= (x + 1)(x^3) + x^5 + x^4 + x^3 + x^2 + x$
- $= x^4 + x^3 + x^5 + x^4 + x^3 + x^2 + x$
- $= x^5 + x^2 + x$

Multiplication Table

[Insert Multiplication Table Here]

Outline

Introduction to Codes

A *code* is a rule for converting information from one representation into another.

- $A \to 0$
- $B \to 1$
- $\vdots$
- $Z \to 25$

Encoding

Encoding is the act of conversion, following the rules of the code.

- HELLO $\rightarrow$ 8 5 12 12 15

Errors

Random errors are a type of error that corrupts individual symbols during transmission.

- 8 5 1**2** 12 15 → 8 5 1**9** 12 15

Burst errors are errors that corrupt a large chunk of symbols.

- 8 5 **12 12 1**5 → 8 5 **19 24** 5

Error Correction

Error detecting codes are a type of code that can detect when these errors occur.
Error correcting codes are a type of code that can correct these errors.

Introduction to CRC

- Used to detect accidental changes in data.
- Appends a check value to the message prior to transmission.
- After transmission the check value is recomputed and compared to the original value.

Application and Integrity

- CRC is good at detecting random errors and burst errors.
- It is not suitable for detecting intentional modifications to the data.

Example

To compute a binary CRC with a 3-bit check value:

- Start with our message encoded in binary: 11010011101100
- Find a irreducible polynomial of degree 3: $x^3 + x + 1 \rightarrow 1011$

Coming soon:

The remainder of the CRC example.

Outline

History

- Introduced in 1960 by I.S. Reed and G. Solomon.
- Useful in practical applications and mathematically interesting.
- Used CD players and deep-space communications.

The Code

- Reed-Solomon (RS) codes are a liner, error correcting code.
- A RS-code is capable of correcting $\frac{n-k}{2}$ symbol errors. Where n is the total number of symbols, and k is the number of data symbols.
- Great at correcting burst errors.

Representation

A message encoded using an RS-code is a polynomial with the message symbols embedded in the coefficients.
For our example, the polynomial would be in in $\mathbb{F}_{64}[x]$ and is our codeword.

- $\mathrm{H} + \mathrm{E}x + \mathrm{L}x^2 + \mathrm{L}x^3 + \mathrm{O}x^4$.

Generalized Reed-Solomon Codes

- There is an alternate representation, known as Generalized Reed-Solomon (GRS) Codes.
- In this representation the message polynomial is evaluated at n distinct points and multiplied by a scalar.
- The result is a n-dimensional vector, which is used as the codeword.
- This is the representation that will be used for the remainder of the presentation.

The Code

Let F be a field. Choose nonzero elements $\hat{v} = v_1, v_2 ..., v_n \in F$ and distinct elements $\hat{\alpha} = \alpha_1, \alpha_2 ..., \alpha_n \in F$.

$C = \text{GRS}_{\ n,k}(\hat{\alpha}, \hat{v}) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), ..., v_n f(\alpha_n) | f(x) \in F[x]_k\}$

- $F = \mathbb{F}_{64}$.
- $\hat{v} = (!, !, ..., !)$.
- $\hat{\alpha} = (A, B, ..., W)$.
- $f(x)$ is our *message polynomial*.

Message Polynomial

- The message: "THIS IS MAJOR TOM".
- $f(x) = \mathrm{T} + \mathrm{H}x + \mathrm{I}x^2 + \mathrm{S}x^3 + \ x^4 + \mathrm{I}x^5 + \mathrm{S}x^6 + \ x^7 + \mathrm{M}x^8 + \mathrm{A}x^9 + \mathrm{J}x^{10} + \mathrm{O}x^{11} + \mathrm{R}x^{12} + \ x^{13} + \mathrm{T}x^{14} + \mathrm{O}x^{15} + \mathrm{M}x^{16}$
- $\hat{c} = \hat{p} + \hat{e}$

The Codeword

The codeword, $\hat{c} = (v_1 f(\alpha_1), v_2 f(\alpha_2), ..., v_n f(\alpha_n))$

- $\hat{c} = (!f(\mathrm{A}), !f(\mathrm{B}), ..., !f(\mathrm{W}))$
- $\hat{c} = \{\mathrm{T}, (, \mathrm{U}, 8, \mathrm{P}, \mathrm{K}, \mathrm{G}, \mathrm{N}, \mathrm{W}, \mathrm{P}, 4, \mathrm{K}, ', \_, \mathrm{N}, (, \mathrm{M}, \mathrm{H}, \mathrm{K}, 1, '', <, \mathrm{K}\}$

The Received Message

- $\hat{c} = \{\mathrm{T}, (, \mathrm{U}, 8, \mathrm{P}, \mathrm{K}, \mathbf{G}, \mathrm{N}, \mathrm{W}, \mathrm{P}, \mathbf{4}, \mathrm{K}, ', \_, \mathrm{N}, (, \mathrm{M}, \mathrm{H}, \mathrm{K}, 1, '', <, \mathrm{K}\}$
- $\hat{p} = \{\mathrm{T}, (, \mathrm{U}, 8, \mathrm{P}, \mathrm{K}, \mathbf{P}, \mathrm{N}, \mathrm{W}, \mathrm{P}, \boldsymbol{\&}, \mathrm{K}, ', \_, \mathrm{N}, (, \mathrm{M}, \mathrm{H}, \mathrm{K}, 1, '', \mathbf{R}, \mathrm{K}\}$

Finding the Dual Code

- Want to find $\hat{u}$ such that $C^{\perp} = \text{GRS}_{n,k}(\hat{\alpha}, \hat{u})$
- $L(x) = (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$
- $L_i(x) = \frac{L(x)}{(x - \alpha_i)}$

Finding the Dual Code

- $\hat{u} = (L_1(\alpha_1), L_2(\alpha_2), \ldots L_n(\alpha_n),)$
- $\hat{u} = (L_1(A), L_2(B), \ldots L_{23}(W))$
- $\hat{u} = \{2, \mathrm{D}, \mathrm{V}, +, 9, \mathrm{O},], \mathrm{G}, *, \wedge, 3, 5, \mathrm{X}, ,, \mathrm{A}, \mathrm{A}, >, <, \mathrm{C}, 8, \mathrm{G}, \mathrm{E}, :\}$

Finding the Syndrome Polynomial

-

Outline

Final Thoughts

Questions