“Polynomial Codes over Certain Finite Fields”

A paper by:
Irving Reed and Gustave Solomon

presented by Kim Hamilton
March 31, 2000

Significance of this paper:

- Introduced ideas that form the core of current commonly-used error-correcting techniques.

R-S codes used for:

- Data Storage. Ex: Compact Discs. Encoding/Decoding system allows scratched CDs to sound perfect.
- Data Transmission. Ex: Allowed high quality pictures to be sent back from Voyager II. Data transmitted over tens of millions of miles.

Irving S. Reed

- 1923: Born in Seattle, WA
- 1944: B.S. Mathematics, Cal Tech
- 1949: Ph.D. Mathematics, Cal Tech
- 1949-50: Northrop Aircraft Company
- 1950-51: Computer Research Corp.
- **1951-1960: M.I.T. Lincoln Labs; paper published in 1960**
- 1960-63: Rand Corporation
- 1963-present: Professor of E.E. and C.S. at University of Southern California

* Helped design one of the world’s first digital computers

Gustave Solomon

- 1931: Born in Brooklyn, NY
- B.S. Mathematics, Yeshiva University
- 1956: Ph.D. Mathematics, M.I.T.
- late 1950's: taught math at Boston and Johns Hopkins Universities
- **1957-61: M.I.T. Lincoln Labs**
- after 1960: Jet Propulsion Laboratory and TRW Systems; visiting/adjunct professorships at U.C. Berkeley, UCLA, Cal Tech
- Jan. 31, 1996: died at his home in Beverly Hills, CA

* Spent free time composing popular songs and folks songs!

Irving S. Reed and Gustave Solomon

Coding Theory Introduction

Main problem of information and coding theory:

A stream of source data, in the form of 0’s and 1’s, is being transmitted over a communications channel, such as a telephone line. Occasionally, disruptions can occur in the channel, causing 0’s to turn into 1’s and vice versa.

Question: How can we tell when the original data has been changed, and when it has, how can we recover the original data?

Coding Theory Introduction (cont'd)

Easy things to try:

- Do nothing. If a channel error occurs with probability p, then the probability of making a decision error is p.
- Send each bit 3 times in succession. The bit that occurs the majority of the time gets picked. (E.g. 010 => 0) If errors occur independently, then the probability of making a decision error is $3*p^2 - 2*p^3$, which is less than p for p<1/2.
- Generalize above: Send each bit n times, choose majority bit. In this way, we can make the probability of making a decision error arbitrarily small, but inefficient in terms of transmission rate.

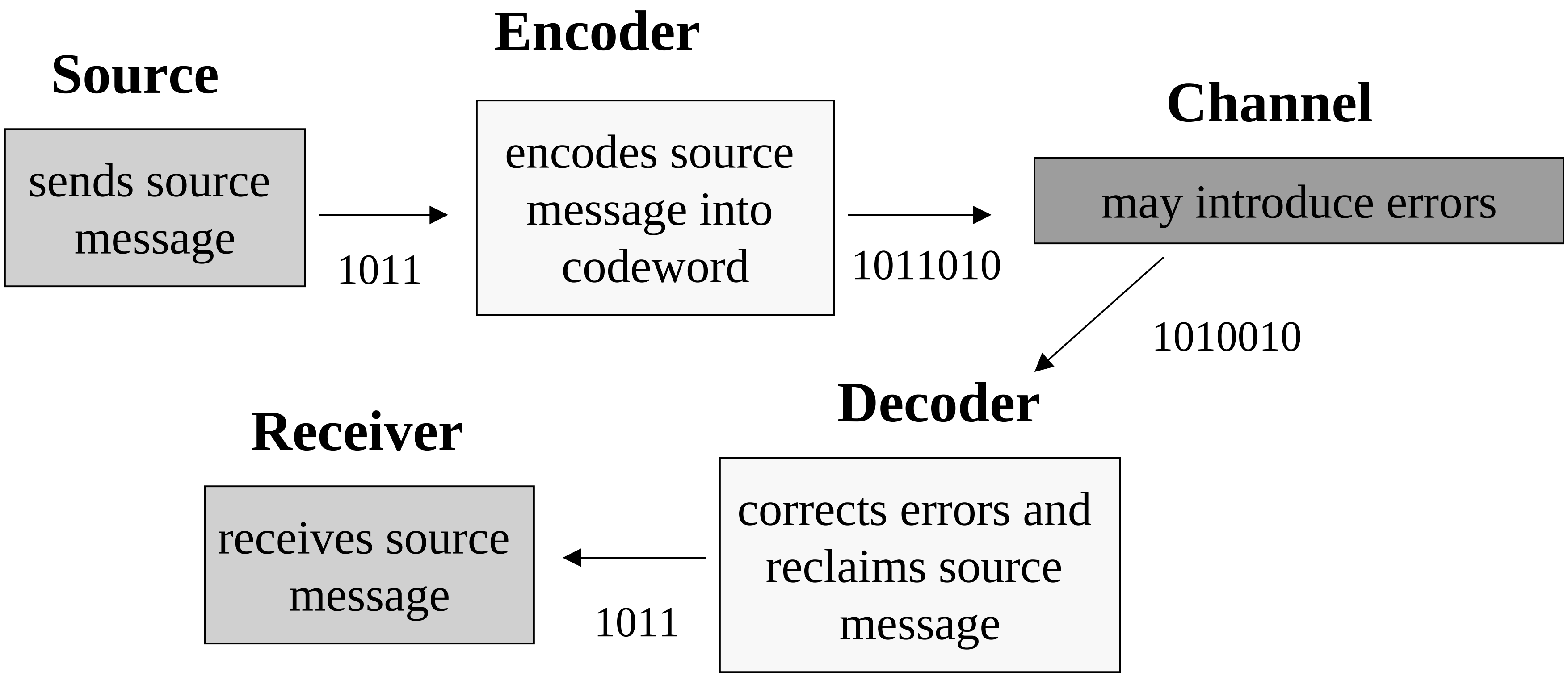
Coding Theory Introduction (cont'd)

From the previous suggestions, we see the basic elements of an encoding of data:

Encode source information, by adding additional information, sometimes referred to as *redundancy*, that can be used to detect, and perhaps correct, errors in transmission.

The more redundancy we add, the more reliably we can detect and correct errors, but the less efficient we become at transmitting the source data.

Components in Communications Process



Source

sends source message

1011

Encoder

encodes source message into codeword

1011010

Channel

may introduce errors

1010010

Decoder

corrects errors and reclaims source message

1011

Receiver

receives source message

Shannon’s Theorem

Noisy Coding Theorem due to Shannon (1948)

Roughly: Consider channel with capacity C. If we are willing to settle for a rate of transmission that is strictly below C, then there is an encoding scheme for the source data that will reduce the probability of a decision error to any desired level.

Problem: Proof not constructive! To this day, no one has found a way to construct the coding schemes promised by Shannon’s theorem.

Additional concerns:

- Is the coding scheme easy to implement, both in encoding and decoding?
- May require extremely long codes.

“Polynomial Codes Over Certain Finite Fields”

Code = mapping from vector space of dimension m over a finite field K (denote $V_m(K)$) into a vector space of higher dimension n>m over the same field ($V_n(K)$).

Let K = $Z_2(\alpha)$, α is root of primitive irreducible polynomial over Z_2 . Can represent elements of K as $0, \beta, \beta^2, \ldots, \beta^{2\wedge n-1} = 1$, where β is the generator of the multiplicative cyclic group.

If the code we want to send is $(a_0, a_1, \ldots, a_{m-1})$, where $a_i \in Z_2$, define $P(x) = a_0 + a_1x + a_2x^2 + \ldots a_{m-1}x^{m-1}$

Code maps:

$(a_0, a_1, \ldots, a_{m-1}) \rightarrow (P(0), P(\beta), P(\beta^2), \ldots, P(1))$

Receiving End

Receive the message $(P(0), P(\beta), P(\beta^2), \ldots, P(1))$. If no transmission errors, we could solve for the original message by solving simultaneously any m of the following 2^n equations:

$P(0) = a_0$

$P(\beta) = a_0 + a_1 \beta + a_2 \beta^2 + \ldots + a_{m-1} \beta^{m-1}$

$P(\beta^2) = a_0 + a_1 \beta^2 + a_2 \beta^4 + \ldots + a_{m-1} \beta^{2m-2}$

…..

$P(1) = a_0 + a_1 + a_2 + \ldots + a_{m-1}$

Any m of these are linearly independent, so we get a unique solution.

Transmission Errors

But, what if errors occur during transmission?

Lemma (p. 302): For s errors, we can get at most (s+m-1)-choose-m determinations for a single wrong m-tuple.

Proof: Since the equations are independent, any m of them have exactly one solution vector *a*. To obtain more than one vote, *a* must be the solution of more than m equations. An incorrect *a* can be the solution of at most s+m-1 equations, consisting of s incorrect equations and m-1 correct equations. Therefore, an incorrect *a* can be the solution to at most (s+m-1)-choose-m sets of m equations.

Transmission Errors (cont’d)

Thus, we have:

Correct solution: $a = (a_0, a_1, \ldots, a_{m-1})$

* gets at least (2^n-s)-choose-m votes.

Incorrect solutions: b_1 , b_2, …, b_t, *(all m-tuples),*

where t <= *(*2^n-choose-m) - ((2^n-s)-choose-m)

* each get at most (s+m-1)-choose-m votes.

Transmission Errors (cont’d)

Thus, if we have:

(2^n-s)-choose-m > (s+m-1)-choose-m

In other words:

s < (2^n-m+1)/2

Then by taking the majority vote, we will determine the correct m-tuple (the original message).

The code will then correct errors of order less than $(2^n-m+1)/2$

Features of Reed-Solomon Codes:

- Maximum Distance Separable
- Burst Errors

  * Current implementations in CD technology can deal with error bursts as long as 4000 consecutive bits
- Erasures
- Redundancy occurs naturally

Some Notes on Decoding

One decoding scheme is mentioned in the paper:

Majority vote:

- Take all 2^n choose m combinations of equations.
- Solve for coefficients.
- The set of coefficients that gets the most votes wins.

Obvious Problem:

- Intractable; need more efficient

Some Notes on Decoding (cont'd)

More efficient decoding attempts:

- 1960 - Peterson provided first explicit description of a decoding algorithm for binary BCH codes. Complexity increases with square of number of errors corrected.
- 1967 - Berlekamp introduced first truly efficient algorithm for both binary and nonbinary BCH codes. Complexity increases linearly with number of errors.
- 1975 - Sugiyama, et al. Showed that Euclid's algorithm can be used to decode BCH and R-S codes.

Discussion Questions

- Complexity Issues in decoding
- Why didn’t they incorporate notion of *distance*?
- Any other major applications that I didn’t mention?
- Guilty pleasures: Any Solomon stories?

  - singing opera at parties

  - Feldenkreis

  - didn’t believe in doctors, died of a stroke