Reed-Solomon Error Correction

Andreas Boulios and Nakul Khambhati

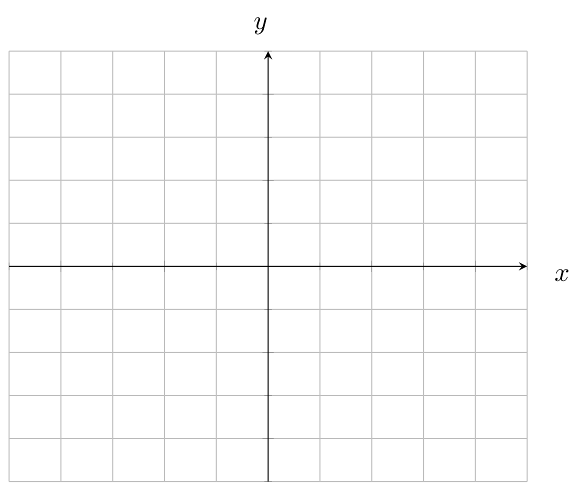
December 8, 2023

1 Introduction to Reed-Solomon

Suppose you want to send a message consisting of 2 numbers to a friend of yours. As per usual during transmission **one of the numbers** that you send will be altered / corrupted. You want find a way for your friend to retrieve your original intended message from the corrupted version they received.
Message: $\{y_0, y_1\}$.
The sender of the message will send a 4 number message according to the following procedure:

1. Draw the line passing through the points $(0, y_0)$, $(1, y_1)$.
2. Let y_2, y_3 be the y-values of the line at $x = 2$, and $x = 3$ respectively.
3. Send the message $\{y_0, y_1, y_2, y_3\}$.

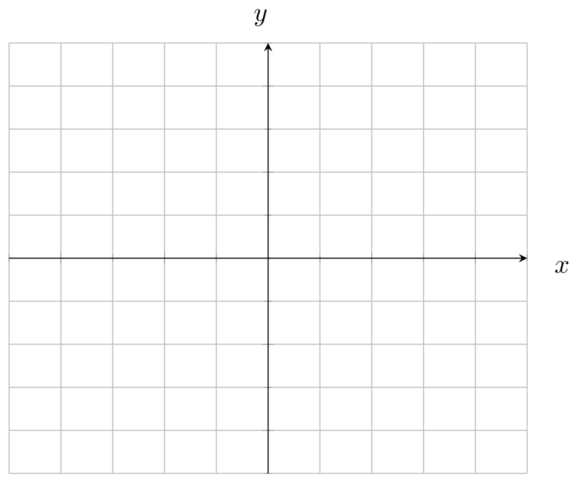
Problem 1.1.
Do this for $y_0 = 1$, and $y_1 = 2$. What is the 4 number message that you are going to send?



Notice that the points you drew above should all lie on the same line!

Problem 1.2.
Imagine that you received the following message from someone using the procedure above.
Received: $\{0, 1, 1, 1.5\}$.

1. Draw the points whose y-values are the numbers you received and x-values corresponding to the position they have in the list, starting at 0. (i.e. $\{(0, 0), (1, 1), (2, 1), (3, 1.5)\}$).
2. Looking at these points, which one was altered during transmission?
3. What was the original intended message.



Of course the strategy above only works for a message of length 2, and uses the fact that given two points there is a unique line passing through them. This strategy is a simple case of the Reed-Solomon error correcting method, which works for messages of any length.
But first, polynomials.

2 Polynomials and Basic Arithmetic

A polynomial in one variable is an expression of the following form:
$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

The values of a_i are called the coefficients. The degree of the polynomial, or $\deg(p(x))$ is equal to the highest power of x that appears in the polynomial. So, above if $a_n \neq 0$, then $\deg(p(x)) = n$. Degree 1 polynomials are lines (or "linear"), degree 2 are called quadratic, and degree 3 are called cubic.

We can "evaluate the polynomial" at a given number by replacing all instances of x with that number and compute the resulting expression, e.g.

Let $p(x) = 4x^3 + 3x - 2$, then $p(x)$ evaluated at 2.5 is:
$$p(2.5) = 4(2.5)^3 + 3(2.5) - 2 = 68$$

Let p, and q be polynomials of degree n:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$
$$q(x) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$$
Then: $p(x) \pm q(x) = (a_n \pm b_n)x^n + (a_{n-1} \pm b_{n-1})x^{n-1} + \cdots + (a_1 \pm b_1)x + a_0 \pm b_0$

To multiply two polynomials multiply every pair of terms and take their sum, e.g. :

$$(a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0)$$
$$= (a_2b_2)x^4 + (a_2b_1 + a_1b_2)x^3 + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0$$

Generally, notice, the i_{th} coefficient of the product is: $a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i$

2.1 Warm-up

Problem 2.1.
Let $p(x) = x^2 - 3x + 2$. Evaluate $p(x)$ at 0, 1, 2, and 3. Proceed to show that for any value of k, $p(3/2 - k) = p(3/2 + k)$.

Problem 2.2.
Compute the coefficients and degree of $q(x) = (x - 1)(x - 2)(x - 3)$.

Problem 2.3.
Let $p(x) = a_n x_n + \cdots + a_1 x + a_0$. If $p(1) = 0$, compute $S = a_n + a_{n-1} + \cdots + a_1 + a_0$.

Problem 2.4.
Let f be a quadratic polynomial with $f(-1) = 1$, $f(0) = 2$, and $f(2) = 3$. Find f.

Problem 2.5.
Let $\deg(p(x)) = a$ and $\deg(p(x)) = b$, what can you say about the degrees of:

1. $p(x) + q(x)$
2. $p(x)q(x)$

We say a polynomial p has a zero at x_0 if p$(x_0) = 0$.

Problem 2.6.
Let $p(x)$ have n zeroes, and $q(x)$ have m zeroes (not necessarily different). What can you say about the number of zeroes for:

1. $p(x) + q(x)$
2. $p(x)q(x)$

Problem 2.7.
Assume that for $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, we know that $p(1) = p(0)$. What is the value of $a_n + a_{n-1} + \cdots + a_1$

Problem 2.8.
What is the sum of the coefficients of $(x + 2y - 1)^6$ when expanded completely.

Problem 2.9.
Challenge: Suppose $p(x)$ has only positive integer coefficients. If $p(1) = 3103$, and $p(10000) = 101000000023000$. Find $p(x)$.

3 Roots and factorization

In this section we will prove the following: Given n points (i.e. (x,y) pairs) there is a unique polynomial of degree less than n, passing through those points. Before we start with the proof we need the following:

The fundamental theorem of algebra states that a non-zero polynomial of degree n can have at most n roots. Further, if it has exactly n roots then it can be written in the following form:
$p(x) = a(x - r_1)(x - r_2)\cdots(x - r_n)$, where r_i are its roots. Generally, if $p(r) = 0$, then $(x - r)$ is a factor of $p(x)$. In other words, $p(x) = (x - r)q(x)$, for some polynomial $q(x)$.

Problem 3.1.
Find the polynomial p if:

1. $p(x)$ is linear with $p(1) = 0$, and p$(2) = 1$.
2. If $\deg(p(x)) = 2$, $p(1) = 0$, $p(2) = 0$, $p(3) = 1$

Problem 3.2.
Find a degree $n-1$ polynomial, $p(x)$, with roots at $1, 2, \cdots, n-1$. Then use it to construct the degree $n-1$ polynomial, with the same roots, but with $p(n) = 1$.

Problem 3.3.
Given $x_1, \cdots, x_n$ for each value of i find $g_i(x)$ with $\deg((g_i(x)) = n-1$,$g_i(x_i) = 1$, and $g_i(x_j) = 0$ for $i \neq j$.

Problem 3.4.
For the g_is from the previous problem what is the value of $p(x) = y_1 g_1(x) + y_2 g_2(x) + \cdots + y_n g_n(x)$ at each x_i. What is the degree of $p(x)$?

We say the polynomial $p(x)$ passes through the point (a, b) if $p(a) = b$.

Problem 3.5.
Using the previous problems find a formula for the polynomial of degree at most $n-1$ that passes through the points: $(x_1, y_1), \cdots, (x_n, y_n)$.

Problem 3.6.
Suppose we have two polynomials $q(x), p(x)$ both of degree less than n, and both passing through $(x_1, y_1), \cdots, (x_n, y_n)$. Consider $f(x) = p(x) - q(x)$.

- What is the maximum degree of $f(x)$?
- What is the minimum number of roots of $f(x)$?
- Use the fundamental theorem of algebra to show $f(x) = 0$.
- Conclude that the polynomial of degree less than n, passing through n points is unique.

3.1 Meaning of Uniqueness

Problem 3.7. 1. Use the method above to find a polynomial, $p(x)$, of degree less than 3, passing through $(-2, 0), (-1, 0), (0, 2)$.

2. What is $p(1)$
3. Find the polynomial ,$q(x)$, of degree less than 3 passing through $(-1, 0), (0, 2), (1, p(1))$.
4. Compare $p(x)$ and $q(x)$ and explain.

Problem 3.8.
Suppose $p(x)$ is the unique polynomial of degree less than n, passing though $(x_1, y_1), \cdots, (x_n, y_n)$. Further, let $p(x_{n+1}) = y_{n+1}$

1. Let S be a collection of n points from $(x_1, y_1), \cdots, (x_{n+1}, y_{n+1})$. Use the uniqueness of $p(x)$ to show that $p(x)$ is the polynomial passing through S, regardless of the choice of S.
2. Suppose someone changes the value of y_1 into y_1'. Does the unique polynomial passing through $(x_2, y_2), \cdots, (x_{n+1}, y_{n+1})$, also pass through (x_1, y_1')?
3. Does the unique polynomial of degree less than n, passing through $(x_1, y_1'), (x_2, y_2), \cdots, (x_n, y_n)$ also go through (x_{n+1}, y_{n+1})? *Hint: Assume it does and reach a contradiction using the previous question.*

4 Reed-Solomon Codes

We are now ready to put this all together and finish the Reed-Solomon error correcting method. We have the usual setup:
A message in this case will be a list of real numbers. We want to send a message to a friend of ours. However, the medium we are using for transmission is imperfect. Each time we send a message one of the numbers send will be corrupted/altered. For example,

Message sent: $\{1.1, 3, 7\}$
Message received: $\{1.1, 4, 7\}$

We shall start simple. Imagine we want to send a message consisting of 3 numbers.
Message: $\{y_0\ , y_1, y_2\}$.

- **Step 1:** Find polynomial (of degree less than 3) passing through $(0, y_0), (1, y_1)$ and $(2, y_2)$
- **Step 2:** Evaluate the polynomial at x = 3, and x = 4, let y_3, and y_4 be these values respectively.
- **Step 3:** Send $\{y_0\ , y_1, y_2\ ,y_3, y_4\}$.

Problem 4.1.
Suppose $y_0 = 1$, $y_1 = 3$,$y_2 = 7$, (i.e. the message you want to send is $\{1, 3, 7\}$). Using the method above, which 5 numbers should you send?

Notice that the points $\{(0,y_0)$, $(1,y_1)$, $(2,y_2)$,$(3,y_3)$, $(4,y_4)\}$, should all lie on a polynomial of degree at most 2.

Let's look at the receiver's perspective.
Message received: $\{y_0$, y_1, y_2 ,y_3, $y_4\}$
The receiver starts by drawing the points: $\{(0,y_0)$, $(1,y_1)$, $(2,y_2)$,$(3,y_3)$, $(4,y_4)\}$. Now since during the transmission only one of the y-values was altered, we know that 4 of these points lie on the same polynomial (of degree at most 2).

Receiver's goal: Then the receiver has to identify which one of these points doesn't lie in the same degree 2 polynomial as the others. The receiver does that by ignoring 2 points at a time and considering the unique polynomial of degree 2 or less passing through the other 3.

For the following problems suppose that during transmission y_2 was altered. (i.e. the remaining points corresponding to y_0, y_1, y_3, y_4 go through the same degree 2 polynomial).

When the receiver ignores the erroneous point:

Problem 4.2.
Suppose the receiver first ignores the points $(2,y_2)$, and $(4,y_4)$ Let $q(x)$ be the unique polynomial (degree 2 or less) passing through $\{(0,y_0)$, $(1,y_1)$, $(3,y_3)\}$.

1. Does $q(x)$ pass through $(4,y_4)$?
2. Does $q(x)$ pass through $(2,y_2)$
3. Can you then conclude that during transmission y_2 was altered?
4. Can you recover the original message?

When the receiver doesn't ignore the erroneous point:

Problem 4.3.
Suppose the receiver ignored the points $(0,y_0)$ and $(1,y_1)$. Let $q(x)$ be the unique degree 2 or less polynomial passing through $\{(2,y_2)$, $(3,y_3)$, $(4,y_4)\}$.

1. Does $q(x)$ pass through $(0,y_0)$?
2. Does $q(x)$ pass through $(1,y_1)$?
3. Having performed these checks, which of the y-values can he be certain were not altered during transmission?

As we can see the receiver's strategy then is the following: Message received: $\{y_0, y_1, y_2, \cdots, y_n\}$

- **Step 1:** Draw the points $\{(0,y_0)$, $(1,y_1)$, $(2,y_2), \cdots, (n,y_n)\}$.
- **Step 2:** Choose n-2 of those points and define the unique polynomial (degree less than n-2) passing through them.
- **Step 3:** Check whether this polynomial passes through the remaining two points.

  If it passes through both, there is no error.

  If it only passes through one, then the other one is the error.

  If it passes through neither then the error is in the collection of n-2 points we chose in step 2, so, we repeat step 2 for a different collection of points.

Problem 4.4.
Suppose you receive the following message: $4, 2, 2, 4, 7$. Which number was altered during transmission, and what is the original 3-number message?

Problem 4.5.
Suppose you receive the following message: $-3, -1, 1, 3, 4, 7$. Which number was altered during transmission, and what is the original 4-number message?