

# CS70 - Lecture 12 Notes

Name: Felix Su    SID: 25794773

Spring 2016    GSI: Gerald Zhang

## Berklecamp-Welsh Algorithm

### Existence:

- Exists because packets constructed using  $P(x)$

### Unique:

- Proved assuming  $\frac{Q'(x)}{E(x)} = \frac{Q(x)}{E'(x)} = P(x)$
- $E(x)$  and  $E'(x)$  have at most  $k$  roots each
- Cross multiply assumption at  $n$  valid points, so claim is true for  $n$  points, which make  $P(x)$  a unique  $< n$  degree polynomial
- **Fact:**  $Q'(x)E(x) = Q(x)E'(x)$  on  $n + 2k$  values of  $x$ 
  - Holds when  $E(x)$  or  $E'(x)$  are 0
  - Use above method of cross multiplication when not zero

### Encoding/Decoding Polynomial Summary:

#### Summary: polynomials.

Set of  $d + 1$  points determines degree  $d$  polynomial.

Encode secret using degree  $k - 1$  polynomial:

Can share with  $n$  people. Any  $k$  can recover!

Encode message using degree  $n - 1$  polynomial:

$n$  packets of information.

Send  $n + k$  packets (point values).

Can recover from  $k$  losses: Still have  $n$  points!

Send  $n + 2k$  packets (point values).

Can recover from  $k$  corruptionss.

Only one polynomial contains  $n + k$

Efficiency.

Magic!!!!

Error Locator Polynomial.

Relations:

Linear code.

Almost any coding matrix works.

Vandermonde matrix (the one for Reed-Solomon)..

allows for efficiency. Magic of polynomials.

## Counting

- Counting Numbers:  $0, 1, 2, \dots$  all Natural Numbers  $\mathbb{N}$
- **Countable if there is a bijection between  $S$  and some subset of  $\mathbb{N}$**
- if subset of  $\mathbb{N}$  = finite,  $S$  has finite **cardinality**
- if subset of  $\mathbb{N}$  = infinite,  $S$  is **countably infinite**
  - Evens are countably infinite
  - Integers are countably infinite
  - Pairs of Natural Numbers are countably infinite
  - Rationals are countably infinite (subset of pairs of natural numbers with gcd of 1)
  - Reals are uncountable
- All countably infinite sets have the same cardinality

## Isomorphism Principle:

- If there is  $f : D \rightarrow R$  that is one to one and onto, (bijective) then  $|D| = |R|$

## Listing:

- A bijection with a subset of natural numbers
- The  $n$ th item in the list is a mapping  $n \in \mathbb{N} \rightarrow f(n)$
- If you can list a set you can show a bijection
- Finite List: Bijection with subset of  $\mathbb{N}\{0, \dots, |S| - 1\}$
- Infinite List: Bijection with  $\mathbb{N}$

## Enumerating $\equiv$ Countability = Listing:

- Enumerating a set  $\implies$  countability
- Corollary: Any subset  $T$  of a countable set  $S$  is also countable
- Each element of  $x \in S$  has a specific, finite position in a list (ex.  $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ )
- Fails for integers if you list positive integers before negative integers
  - $\mathbb{Z} = \{\{0, 1, 2, \dots\} \text{ and then } \{-1, -2, \dots\}\}$
  - -1s position is not finite, because there are  $\infty$  positive integers
  - So.. you must **interweave**

## Diagonalization:

- **Diagonal Number** Number that is not in the list of  $f(n)$
- Ex. Method to create diagonal number for Reals: Digit  $i$  is 7 if number  $i$ 's  $i$ th digit is not 7, 6 otherwise. For every  $n$ th position on the list, at least the  $n$ th digit will be different than the diagonal number's  $n$ th digit. Contradiction because the diagonal number is real.
- Check if this creates contradiction. If diagonal number is in the questionable set, the list could not have existed and thus it is not countable.