Expander Codes

M. Sipser and D. A. Spielman
Presented by Sophia Sun. CSE 254 fall 2018

outline

- Intro to coding theory (10 min)
- Expander graphs and expander codes (15 min)
- why do we care??? (5 min)
Self-correcting codes

The $[7,4]$ Hamming code

$x_1, x_2, x_3, x_4 | x_5, x_6, x_7$. Where:

$x_5 = x_2 + x_3 + x_4$; $x_6 = x_1 + x_3 + x_4$; $x_7 = x_1 + x_2 + x_4$

Generator Matrix:

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

Parity-check Matrix:

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

Error detection & correcting:

$H \cdot [1,1,1,1,1,1,1]^T = [0,0,0]$  
$H \cdot [1,0,1,1,1,1,1]^T = [0,1,0]$
Linear Codes! (definitions)

Definition 2 (Error correcting code) An code $C$ of length $n$ over a finite alphabet $\Sigma$ is a subset of $\Sigma^n$. The elements of $C$ are called the codewords in $C$. Let $|\Sigma| = q$, we say that $C$ is a $q$-ary code. When $q = 2$, we say that $C$ is a binary code.

Definition 3 (Minimum distance) The minimum distance, or simply distance, of a code $C$, denoted $\Delta(C)$, is defined to be the minimum Hamming distance between any two distinct codewords of $C$. i.e. $\Delta(C) = \min_{c_1, c_2 \in C} \Delta(c_1, c_2)$, Where $\Delta(x, y) = |\{i | x_i \neq y_i\}|$.

Definition 4 (Rate) The rate of a code $C \subseteq \Sigma^n$, denoted $R(C)$, is defined by

$$R(C) = \frac{\log|C|}{n \log|\Sigma|}$$

Thus, $R(C)$ is the amount of non-redundant information per bit in codewords of $C$. A $q$-ary code of dimension $l$ has $q^l$ codewords.

Linear Codes (definitions continued)

Definition 5 (Linear Code) If $\Sigma$ is a field and $C \subseteq \Sigma^n$ is a subspace of $\Sigma^n$, then $C$ is said to be a linear code.

As $C$ is a subspace, there exists a basis $c_1, c_2, ..., c_k$ where $k$ is the dimension of the subspace. Any codeword can be expressed as the linear combination of these basis vectors. We can write these vectors in matrix form as the columns of a $n \times k$ matrix. Such a matrix is called a generator matrix.

Notation: A $q$-ary linear code of block length $n$ and dimension $k$ will be referred to as an $[n, k]_q$ code.

Definition 6 (Generator Matrix) The generator matrix $G$ provides a way to encode a message $x \in F_q^k$ (thought of as a column vector) as the codeword $Gx \in C \subseteq F_q^n$.

Definition 7 (Parity check matrix) For all $[n, k]$ code $C$, there is a matrix $H \in F_q^{(n-k) \times n}$ of full row rank such that $C = \{c \in F_q^n | Hc = 0\}$. 
Expander graphs

A graph has good (vertex) expansion when: every ‘small’ subset of vertices is connected to a significantly ‘large’ neighbourhood in the graph.

Good expansion:

Minimal expansion:

very cool facts:

1. A randomly chosen d-regular graph will have good expansion with high probability. (David Ellis’s proof)
   a. In fact, we can take $\alpha \geq 0.18D$ for all $D \geq 3$, and $\alpha \rightarrow D/2$ as $D \rightarrow \infty$.

2. We can explicitly construct arbitrarily good expanders. (Trevisan’s notes)
   a. $\forall \epsilon > 0$, $m \leq n$, $\exists \gamma > 0$ and $D \geq 1$ such that a $(n, m, D, \gamma, D(1 - \epsilon))$ expander exists.

Definition 1 (Bipartite Expander Graph) A $(n, m, D, \gamma, \alpha)$ bipartite expander is a $D$-left-regular bipartite graph $G(L \cup R, E)$ where $|L| = n$ and $|R| = m$ such that $\forall S \subseteq L$ with $|S| \leq \gamma n$, $N(S) \geq \alpha|S|$. Here, $\alpha$ is called the expansion factor.
Expander Codes

... are linear codes whose factor graphs are bipartite expander graphs.

Properties:

Let $G$ be a $(n, m, D, \gamma, D(1 - \epsilon))$ expander, and let $C(G)$ be its corresponding expander code. Then:

Rate: The rate of a code is its dimension divided by its block length. Since the parity check matrix has size $m \times n$, then $C$ has rate $(n-m)/n = 1 - m/n$

Distance: $\Delta(C(G)) \geq \gamma n$ by pigeonhole principle.

In fact, $\Delta C(G) \geq 2\gamma(1 - \epsilon)n$.

Decoding of expander codes

**Simple Sequential Decoding Algorithm:**

- If there is a variable that is in more unsatisfied than satisfied constraints, then flip the value of that variable.
- Repeat until no such variable remains.

**Complexity:** $O(n)$

Proof of correctness (sketch):

1. If the $1< \gamma n$ (i.e. is an expander subset), there exists a digit in the left partition adjacent to more than $D/2$ unsatisfied checks. *(by pigeonhole)*
2. Given a word with less than $\gamma n(1-2\epsilon)$ errors, the number of errors will never increase in any interim step. *(by loop invariant)*
3. Note that the distance of the code is $> \gamma n$. So by 1 and 2, the algorithm will converge to the closest codeword.
Parallel Decoding of expander codes

Simple Parallel Decoding Algorithm:

- In parallel, flip each variable that is in more unsatisfied than satisfied constraints.
- Repeat until no such variable remains.

Complexity is closer to $O(n)$ with hardware implementation. (Sipser & Spielman)

Usefulness?

- Robustness
- Prevalence
  - Simplicity to construct - Expansion is a common property in higher dimensions
- Optimality
  - Can encode exponentially many states using codeword of length $n$ and can correct a fraction of errors
- Scalability and simplicity to decode, even in an associative network
The end. Thank you!

References:


