Mathematical Methods in Coding Theory: Tree Codes

Nikola Kovachki

California Institute of Technology

nkovachki@caltech.edu

October 17, 2015

A Distributed Control Problem

- System controller needs to apply input in real time, and delay can cause instability or or loss in performance.
- The measurement and control subsystems are not co-located as in most traditional control systems.
- Need to reliably transmit information in real time over a noisy channel.
- Examples: unmanned vehicles/drones, satalite communication, unmanned chemical plants, intelligent highways, the smart grid, etc.

The Solution: Tree Codes

- Classical coding theory is concerned with encoding blocks of data and sending them over noisy channels with no cosideration for time reliability.
- A tree code is an encoding scheme that works on a continous stream of data and guratees a better probability of correct decoding of earlier bits as we move further in time.
- Tree codes were first introduced in the early 1990s by Caltech Professor Leonard Schulman who proved they exist with a small probability (from a random coding point of view).
- More recently they were shown to exist with a high probability as adjacency matrices of certain expander graphs.

Casual Linear Codes

Casual Linear Codes

A casual linear code of rate $R = \frac{k}{n}$ is represented by a sequence of linear maps $f_\tau : \mathbb{F}_2^{k\tau} \to \mathbb{F}_2^n$.

LDPC Matrix Reformation

We can represent the above definition by a parity-check matrix

$$H_{n,R} = \begin{pmatrix} H_{11} & 0 & \cdots & \cdots & \cdots \\ H_{21} & H_{22} & 0 & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ H_{\tau 1} & H_{\tau 2} & \cdots & H_{\tau\tau} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

where $H_{ij} \in \mathbb{F}_2^{\bar{n} \times n}$ with $\bar{n} = n(1 - R)$.

Tree Codes

The Anytime-Reliability Condition

Consider a causal linear code C with rate $R = \frac{k}{n}$ which maps a sequence of k-dimensional binary vectors $\{b_\tau\}_{\tau=0}^{\infty}$ to a sequence of n-dimensional binary vectors $\{c_\tau\}_{\tau=0}^{\infty}$. Let $\hat{b}_{\tau|t}$ be the decoder's estimate of b_τ for some $\tau < t$ at time t. Then for some fixed distance d_0, independent of t, C is called a tree code (or an anytime-reliable causal linear code) with parameters (η, β, d_0) if

$$\mathbb{P}[\hat{b}_{t-d|t} \neq b_{t-d}] \leq \eta 2^{-\beta n d} \quad \forall t, d \geq d_0$$

Intuatively, the probability of making a decoding error decays exponentially in time.

Anytime-Reliability in Terms of Weight Enumerators

- It was recently proven by Sukhavasi and Hassibi that the anytime-reliability condition can be re-stated in terms of the weight enumerator of the code.
- Let $H_{n,R}^t$ be the $\bar{n}t \times nt$ leading principal minor of $H_{n,R}$.
- $C_t = \{c \in \mathbb{F}_2^{nt} : H_{n,R}^t c = 0\}$.
- $C_{t,d} = \{c \in C_t : c_{\tau<t-d+1} = 0, c_{t-d+1} \neq 0\}$.
- $N_{w,d}^t = |\{c \in C_{t,d} : ||c|| = w\}|$ where by $||\cdot||$ we denote the Hamming weight of c.
- Then assuming the all zero codeword is transmitted, uder ML-decoding, a code is anytime-reliable if $N_{w,d}^t \leq 2^{\theta w}$ and $\text{argmin}_w(N_{w,d}^t \neq 0) \geq \alpha nd$, $\forall t, d \geq d_0$ where α and θ are constants depending on the Bhattacharyya parameter of our channel.

The Goal

- Our goal is to contruct a code that satisfies the previously stated weight enumerator conditions.
- In this talk, I'll focus on how we can actually count $N^t_{w,d}$ for a specific construction, and, time permitting, I'll briefly touch on the second condition.

A Possible Construction

- In a 2015 paper, an Swedish lab group showed through empirical testing and exit chart analysis that they have found a parity-check matrix which defines an anytime-reliable code.
- They defined the parity-check matrix for a code of rate $\frac{1}{2}$ as follows

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

- They however give no rigorous proof that the code defined by H is anytime-reliable.

Combinatorial Approach

- Let H_n be the $n \times 2n$ leading princical minor of H.
- We are interested in counting the two-dimensional sequence $c(n,k) = |\{c \in \mathbb{F}_2^{2n} : H_n c = 0, ||c|| = k, c_1 \neq 0\}|$
- Mathematically, the most natural way of counting such a sequence is through a generating function. So we want to compute a closed form for the function,
$$C(x,y) = \sum_{n,k \geq 0} c(n,k) x^n y^k$$
- Before we can do this, however, we need to find some reccurence relations for $c(n,k)$. In fact, we will relate $c(n,k)$ to the sequences $a(n,k) = |\{c \in \mathbb{F}_2^{2n} : H_n c = 0, ||c|| = k\}|$ and $b(n,k) = |\{c \in \mathbb{F}_2^{2n} : H_n c = 1, ||c|| = k\}|$ where $1 = (1,1,...,1) \in \mathbb{F}_2^n$.

Reccurences

Theorem

The following reccurence relations hold

$$a(n+1,k+2) = a(n,k+2) + b(n,k)$$
$$b(n+1,k+1) = a(n,k) + b(n,k)$$
$$c(n+1,k+2) = b(n,k)$$

Proof.

Let $A_n = \{c \in \mathbb{F}_2^{2n} : H_n c = 0\}$ and $\bar{A}_n = \{c \in \mathbb{F}_2^{2n} : H_n c = 1\}$. If $c \in A_n$ then c is orthogonal to every row of H_n. Since H_n has all 1(s) in the first the for column then $\forall y \in \bar{A}_n \; \exists! x \in A_n$ s.t. $y = x + (1,0,0,...,0)$ where uniqueness comes from the fact that $A_n, \bar{A}_n$ are linear subspaces of $\mathbb{F}_2^{2n}$ as H_n is of full rank. Hence

$$\bar{A}_n = A_n \oplus (1,0,0,...,0) \tag{1}$$

Reccurences

Proof.

Notice,

$$H_{n+1} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & H_n & \\ 1 & 0 & & & \end{pmatrix}$$

so take $x \in \mathbb{F}_2^{2(n+1)}$ and write $x = (x_1, x_2, y)$ where $y \in \mathbb{F}_2^{2n}$. We want to know when $x \in A_{n+1}$. Clearly we need $x_1 = x_2$. If $x_1 = x_2 = 0$ then $y \in A_n$ because x_1 and x_2 do not contribute to the inner product. If $x_1 = x_2 = 1$ then $y \in \bar{A}_n$ because x_1 and x_2 contribute exactly 1 to the inner product. From this along with Eq. (1) we conclude

$$A_{n+1} = \{(0,0,y) : y \in A_n\} \cup \{(1,1,y) : y \in \bar{A}_n\}$$
$$\bar{A}_{n+1} = \{(1,0,y) : y \in A_n\} \cup \{(0,1,y) : y \in \bar{A}_n\}$$

Reccurences

Proof.

$$A_{n+1} = \{(0,0,y) : y \in A_n\} \cup \{(1,1,y) : y \in \bar{A}_n\}$$
$$\bar{A}_{n+1} = \{(1,0,y) : y \in A_n\} \cup \{(0,1,y) : y \in \bar{A}_n\}$$

These immediately imply

$$a(n+1,k) = a(n,k) + b(n,k-2)$$
$$b(n+1,k) = a(n,k-1) + b(n,k-1)$$
$$c(n+1,k) = b(n,k-2)$$

and thus our reccurences hold. □

- Note that the only things we used in this proof were the fact that H_n is Toeplitz and that there are all one and zeros along its first and second rows. This implies that this method of counting is applicable to other Toeplitz constructions.

The Generating Function

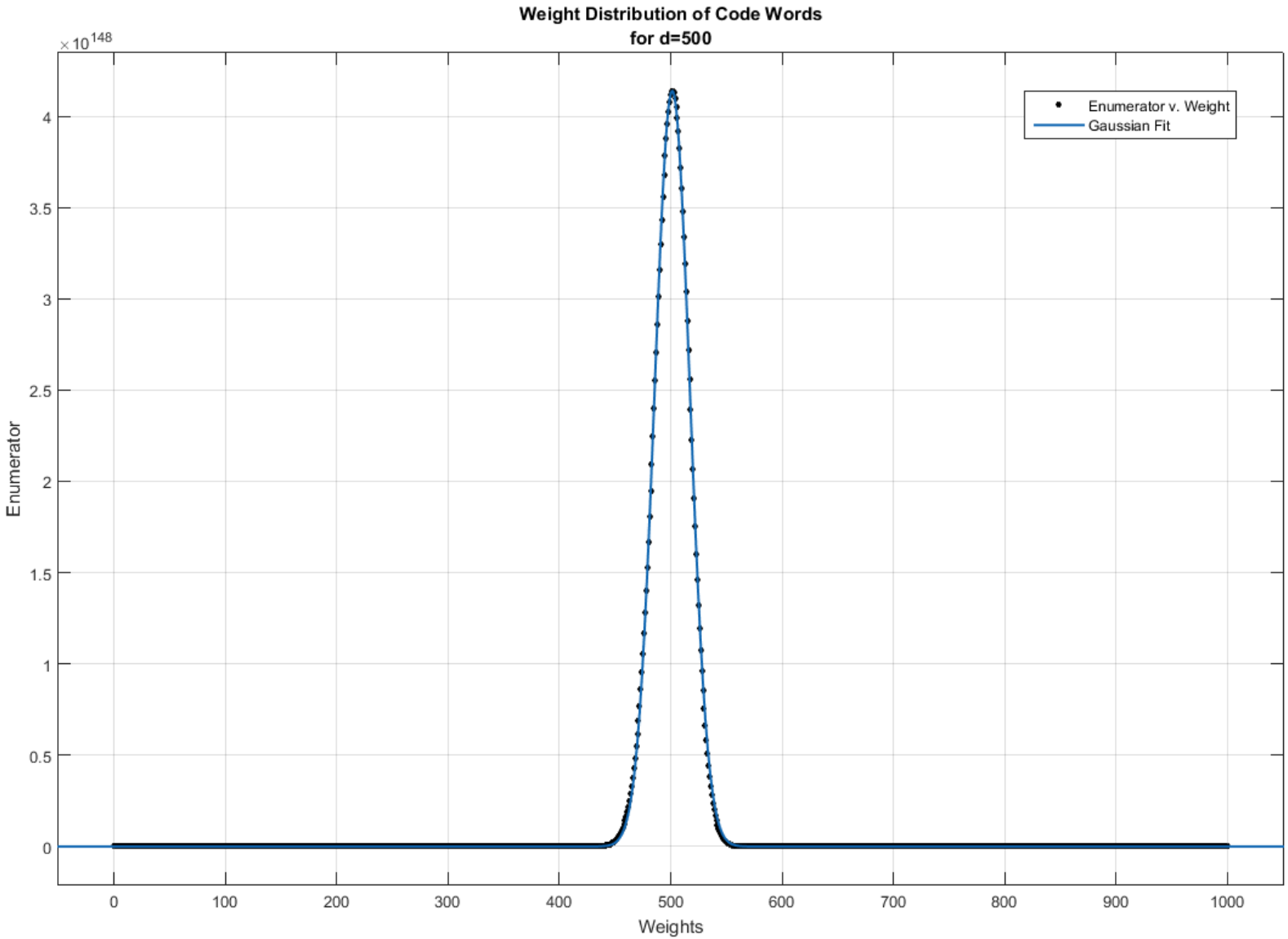
- Now that we have reccurences, we can assume the initial conditions $a(0,0) = b(0,0) = c(0,0) = 0$ and, after a bit of algebra, we conclude that our sum converges in $\{(x,y) \in \mathbb{C}^2 : x \in \mathbb{D}, y \in \mathbb{C}\}$ to

$$C(x,y) = \frac{(x-1)(1+x(y^2-y))}{(y^3x - xy + y + 1)x - 1}$$

- The Taylor series of such a function around $x = 0$ is

$$\sum_{n=0}^{\infty} \left(\sum_{k=0}^{2n} c(n,k) y^k \right) x^n$$

- So if are able to compute sufficient derrivaties of $C(x,y)$ we would have a closed form for $c(n,k)$. However such a task is intractable and the following heuristic explains why.


Weight Distribution of Code Words
for d=500
×10^148
Enumerator v. Weight
Gaussian Fit
Enumerator
Weights
0
0.5
1
1.5
2
2.5
3
3.5
4
0
100
200
300
400
500
600
700
800
900
1000

Asymptotics

- Since asking for a closed from of $c(n,k)$ may be too much, we can at least ask for an asymptotic. That a relatively nice closed form function $f(n,k)$ such that

$$\frac{f(n,k)}{c(n,k)} \to 1 \quad \text{as} \quad (n,k) \to \infty$$

- In the one-dimensional case, this problem is easily solved by the Cauchy Integral Formula. However there is no multi-dimensional analog.
- Need to use algebraic geometry, mainly calculating the ideal generated by the variety $V = \{(x,y) \in \mathbb{C}^2 : (y^3x - xy + y + 1)x - 1 = 0\}$.

Asymptotics

- We currently don't have a good way to perform such a calculation, however, we can calculate an asymptotic for the diagonal, that is

$$c(n, n) \sim \frac{2^n}{\sqrt{\pi n}}$$

- For details on the algebraic geometry needed to perform such a calculation, see Pemantle's paper: https://www.math.upenn.edu/ pemantle/papers/twenty.pdf.