4F5: Advanced Communications and Coding

Coding Handout 1: Binary Linear Codes over the Erasure Channel

Jossy Sayir

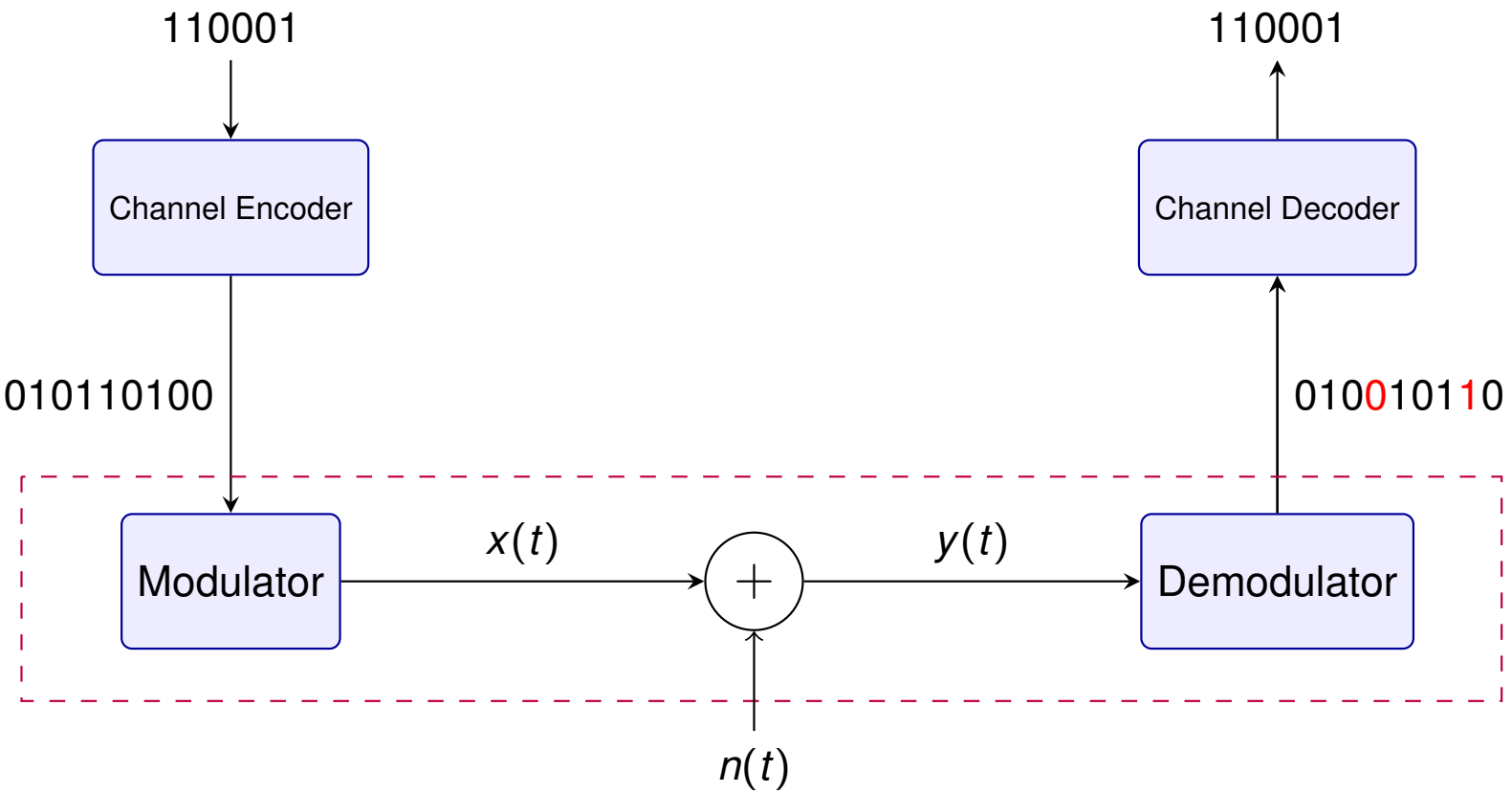
Signal Processing and Communications Lab
Department of Engineering
University of Cambridge
jossy.sayir@eng.cam.ac.uk

Michaelmas 2014

Outline of the Coding Part

1. Binary Linear Codes over the Binary Erasure Channel (BEC)
2. Binary Low-Density Parity-Check (LDPC) Codes
3. Mathematical Fundamentals of Algebraic Coding
4. Non-binary Iteratively Decodable Codes
5. Reed-Solomon Codes
6. (Trees, trellises, the Viterbi and BCJR Algorithms, Convolutional Codes)

The High-level Picture (repeat)



The Channel Coding Theorem (repeat)

Theorem

" For a DMC with capacity $\mathcal{C}$, all rates less than $\mathcal{C}$ are achievable."

Specifically,

1. *Fix $R < \mathcal{C}$ and pick any $\epsilon > 0$. Then, for all sufficiently large n there exists an $(2^{nR}, n)$ code with maximal probability of error less than ϵ.*
2. *Conversely, any sequence of $(2^{nR}, n)$ codes with maximal probability of error $P_e^{(n)} \to 0$ as $n \to \infty$ must have $R \leq \mathcal{C}$.*

The Channel Coding Theorem (repeat)

Theorem

" For a DMC with capacity $\mathcal{C}$, all rates less than $\mathcal{C}$ are achievable."

Specifically,

1. *Fix $R < \mathcal{C}$ and pick any $\epsilon > 0$. Then, for all sufficiently large n there exists an $(2^{nR}, n)$ code with maximal probability of error less than ϵ.*
2. *Conversely, any sequence of $(2^{nR}, n)$ codes with maximal probability of error $P_e^{(n)} \to 0$ as $n \to \infty$ must have $R \leq \mathcal{C}$.*

Binary (mod 2) matrix multiplication

$$\boldsymbol{c} = [0,1,0,0,1] \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

- if $\mathbb{B} = \{0,1\}$, this is linear algebra over $\mathbb{B}^n$
- concepts of rank, determinant, dimension, orthogonal spaces, carry over gracefully from linear algebra over $\mathbb{R}^n$
- difference: all sets here have a finite number of elements

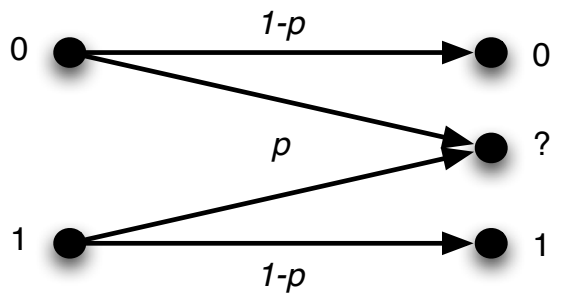
Binary Linear Codes

- $K \times N$ encoder (generator) matrix $\boldsymbol{G}$ with indpendent rows defines a code
- Code $\mathcal{C}$ is set of all vectors $\boldsymbol{c}$ obtained by multiplying any binary vector $\boldsymbol{u}$ of length K by $\boldsymbol{G}$, i.e., $\boldsymbol{c} = \boldsymbol{u}\boldsymbol{G}$.
- Replacing rows of $\boldsymbol{G}$ by sums of rows leaves the code invariant (Gaussian elimination!)
- Rate of the code: $R = K/N$
- Parity-check matrix is a matrix of $(N - K)$ independent row vectors orthogonal to rows of $\boldsymbol{G}$. For any $\boldsymbol{c} \in \mathcal{C}$, $\boldsymbol{c}\boldsymbol{H}^T = 0$, and any vector $\boldsymbol{c} \in \mathbb{B}^N$ such that $\boldsymbol{c}\boldsymbol{H}^T = 0$ is in $\mathcal{C}$
- if $\boldsymbol{G} = [\boldsymbol{I}_K, \boldsymbol{P}]$, then the corresponding $\boldsymbol{H} = [\boldsymbol{P}^T, \boldsymbol{I}_{N-K}]$ ($\boldsymbol{G} = [\boldsymbol{I}_K, \boldsymbol{P}]$ is called the systematic encoder matrix of $\mathcal{C}$ and always exists)

Random Linear Coding for the BEC

Coding and Decoding for the Binary Erasure Channel

- For the BEC, linear codes can be decoded by matrix inversion:
  - eliminate the columns of $\boldsymbol{G}$ corresponding to erased positions in the codeword $\longrightarrow \boldsymbol{G}'$
  - invert $\boldsymbol{G}'$
  - recover the information bits $\boldsymbol{b} = \boldsymbol{c}'\boldsymbol{G}'^{-1}$ where $\boldsymbol{c}'$ is the vector containing only the non-erased bits of the received sequence
- A similar decoder can be constructed based on the parity-check matrix $\boldsymbol{H}$, where decoding is achieved via triangulation of the portion of $\boldsymbol{H}$ corresponding to the erased bits
- The complexity of matrix inversion or triangulation decoding is the complexity of Gauss elimination over GF(2), i.e. on the order N^2 if N is the codeword length
- What is the probability of success of matrix inversion decoding if the generator matrix $\boldsymbol{G}$ has been selected at random? (random coding)



Binary Erasure Channel (BEC)

Random Linear Coding for the BEC

Probability of Inverting a Random Matrix

- The matrix inversion decoder will be successful if the matrix $\boldsymbol{G}'$ with erased columns has rank $K = NR$, i.e., if $\boldsymbol{G}'$ has full rank
- Let $\boldsymbol{A}$ be a random binary $k \times n$ matrix chosen uniformly at random, with $k \leq n$. How probable is it that $\boldsymbol{A}$ has rank k?
- There are $2^{k \times n}$ binary $k \times n$ matrices and $\prod_{i=0}^{k-1}(2^n - 2^i)$ of them have rank k (for each row, choose any sequence of length n except any linear (binary) combination of previous rows)
- The resulting probability of full rank is

$$P(\text{rank}(\boldsymbol{A}) = k) = \frac{\prod_{i=0}^{k-1}(2^n - 2^i)}{2^{k \times n}} = \prod_{i=n-k+1}^{n}(1 - 2^{-i})$$

- For $n = k$, we have

$$P(\text{rank}(\boldsymbol{A}) = k) = \frac{1}{2}\frac{3}{4}\frac{7}{8}\frac{15}{16}\ldots(1 - 2^{-n})$$

  whose limit as n goes to infinity is 0.288788
- For $n > k$, the product omits the first and smallest terms ($1/2, 3/4$, etc.), so the limit gets larger and closer to 1 as $n - k$ grows

Random Linear Coding for the BEC

Rate and Chebyshev's inequality

- Remember that the capacity of a BEC with erasure probability p is $C = 1 - p$ and we know from the converse to the coding theorem that we cannot hope to achieve arbitrary reliability for $R \geq C$ with any type of coding, so all the more so now that we restrict ourselves to linear coding
- Therefore, let the rate be $R = 1 - p - \varepsilon$ for any arbitrarily small $\varepsilon > 0$
- Let W be the number of erased bits in our block of length N. W follows a binomial distribution

$$P_W(w) = \binom{N}{w} p^w (1-p)^{n-w},$$

  and we have $\mathrm{E}[W] = Np$ and $\mathrm{var}(W) = Np(1-p)$
- We use Chebyshev's inequality

$$P(|W - pN| \geq \alpha) \leq \frac{Np(1-p)}{\alpha^2},$$

  which, by setting $\alpha = \delta N$, gives us

$$P(|W - pN| \leq \delta N) \geq 1 - \frac{p(1-p)}{N\delta^2}.$$

Random Linear Coding for the BEC

Probability of success for random coding

- Let us denote $D = |W - pN|$. We can now write the probability of successful decoding P_s as

$$\begin{aligned} P_s &= P_{s|D\leq\delta N} P(D \leq \delta N) + P_{s|D>\delta N} P(D > \delta N) \\ &\geq P_{s|D\leq\delta N} P(D \leq \delta N) && \text{(dropping a positive term)} \\ &\geq P_{s|W=pN+\delta N} \left(1 - \frac{p(1-p)}{N\delta^2}\right) && \text{(Chebyshev's inequality)} \end{aligned}$$

  where we have also used the fact that the probability of success over the interval $|W - pn| \leq \delta n$ is smallest[a] for $W = pn + \delta n$

- We now use the expression we computed for the probability of successfully inverting a random matrix, whose dimensions are $NR = N(1 - p - \varepsilon)$ rows and $N - (pN + \delta N) = N(1 - p - \delta)$ columns, to get

$$P_s \geq \left(1 - \frac{p(1-p)}{N\delta^2}\right) \prod_{i=N(\varepsilon-\delta)+1}^{N(1-p-\delta)} (1 - 2^{-i})$$

[a] we brush over all integer constraints on the number of erasures and the matrix sizes. The proof can be made precise by appropriate use of floor or ceiling integer rounding functions.

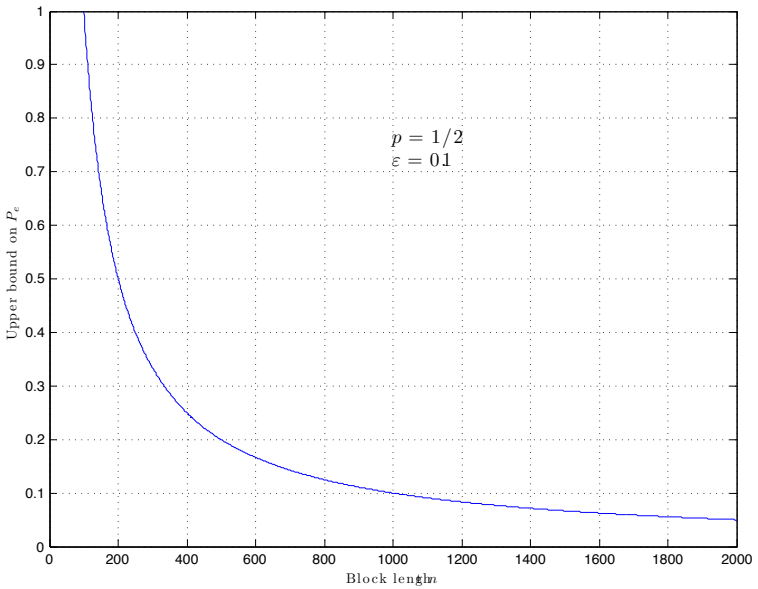
Random Linear Coding for the BEC

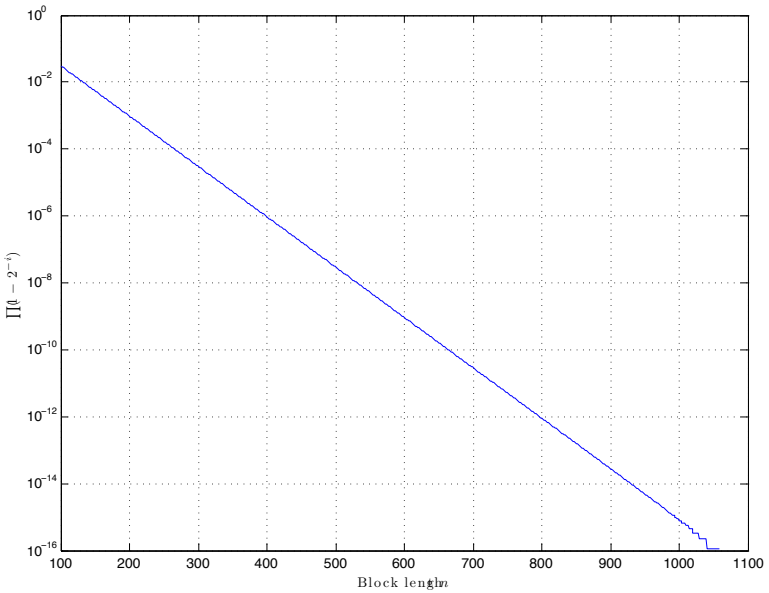
Probability of error for random coding

- We now get for the probability of error $P_e = 1 - P_s$, by choosing $\delta = \varepsilon/2$,

$$P_e \leq 1 - \left(1 - \frac{4p(1-p)}{N\varepsilon^2}\right) \prod_{i=N\varepsilon/2+1}^{N(1-p-\varepsilon/2)} (1 - 2^{-i})$$

which can be made arbitrarily small for any given ε by choosing N appropriately large





Upper bounds including the Chebyshev averaging - excluding averaging (i.e. assuming $W = Np$)

Random coding for the BEC

What we have learnt...

- For the BEC, linear codes achieve arbitrary reliability on average over all codes by choosing N large
- In fact, linear codes achieve capacity for any symmetric channel
- The "matrix inversion decoder" does not extend beyond the BEC
- We need more general decoding methods for other channels