CS3200: Computer Networks

Lecture 8

IIT Palakkad

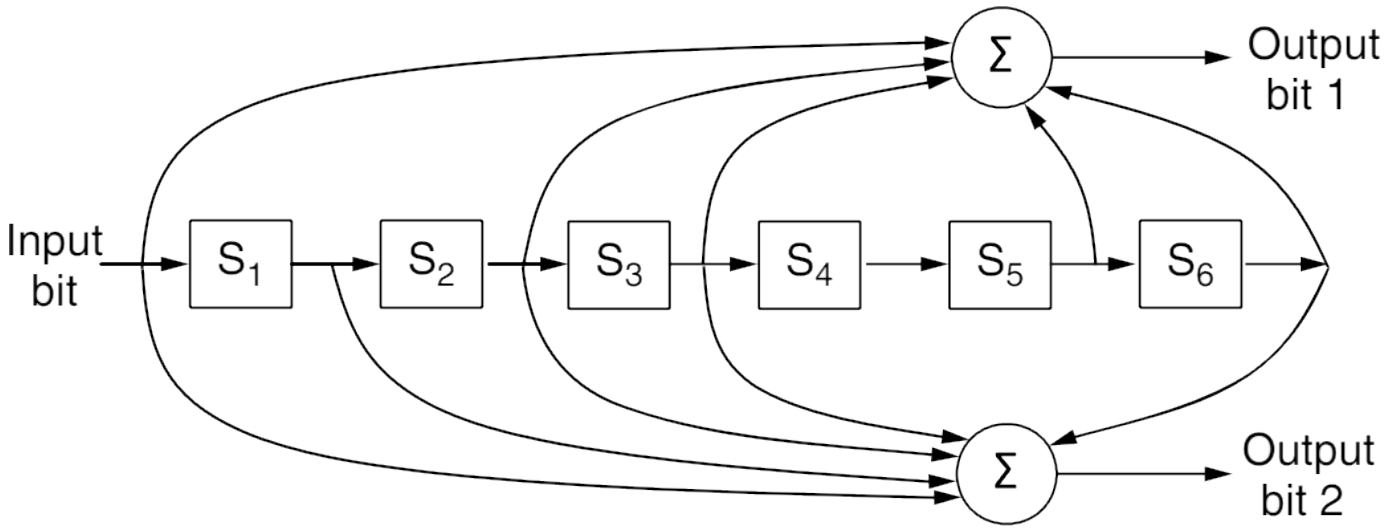
13 Aug, 2019

Convolution Codes

- An encoder processes a sequence of input bits and generates a sequence of output bits.
- No natural message size or encoding boundary as in a block code.
- Output is a function of current and previous input bits.
- Number of previous bits on which the output depends is called the **constraint length** of the code.
- Convolutional codes are specified in terms of their rate and constraint length.

Convolution Codes

A very popular convolution code known as the NASA convolutional code of $r = 1/2$ and $k = 7$, since it was first used for the Voyager space missions starting in 1977.



Convolution Codes

- For small values of k, convolution codes can be decoded with the widely used algorithm developed by Viterbi.

- Convolutional codes have been popular in practice because it is easy to factor the uncertainty of a bit being a 0 or a 1 into the decoding. For example, suppose -1V is the logical 0 level and +1V is the logical 1 level, we might receive 0.9V and -0.1V for 2 bits. Instead of mapping these signals to 1 and 0 right away, we would like to treat 0.9V as "very likely a 1" and -0.1V as "maybe a 0" and correct the sequence as a whole.

Reed-Solomon Code

- Unlike Hamming codes, which operate on individual bits, Reed-Solomon codes operate on m bit symbols.
- Key idea — every n degree polynomial is uniquely determined by $n + 1$ points.
- Imagine that we have two data points that represent a line and we send those two data points plus two check points chosen to lie on the same line.
- If one of the points is received in error, we can still recover the data points by fitting a line to the received points. Three of the points will lie on the line, and one point, the one in error, will not. By finding the line we have corrected the error.

Reed-Solomon Code

- Actually defined as polynomials that operate over finite fields.
- For m bit symbols, the codewords are $2^m - 1$ symbols long.
- A popular choice is to make $m = 8$ so that symbols are bytes. A codeword is then 255 bytes long. The (255, 223) code is widely used; it adds 32 redundant symbols to 223 data symbols.
- Decoding with error correction is done with an algorithm developed by Berlekamp and Massey that can efficiently perform the fitting task for moderate-length codes.
- Reed-Solomon codes are widely used in practice because of their strong error-correction properties, particularly for burst errors.

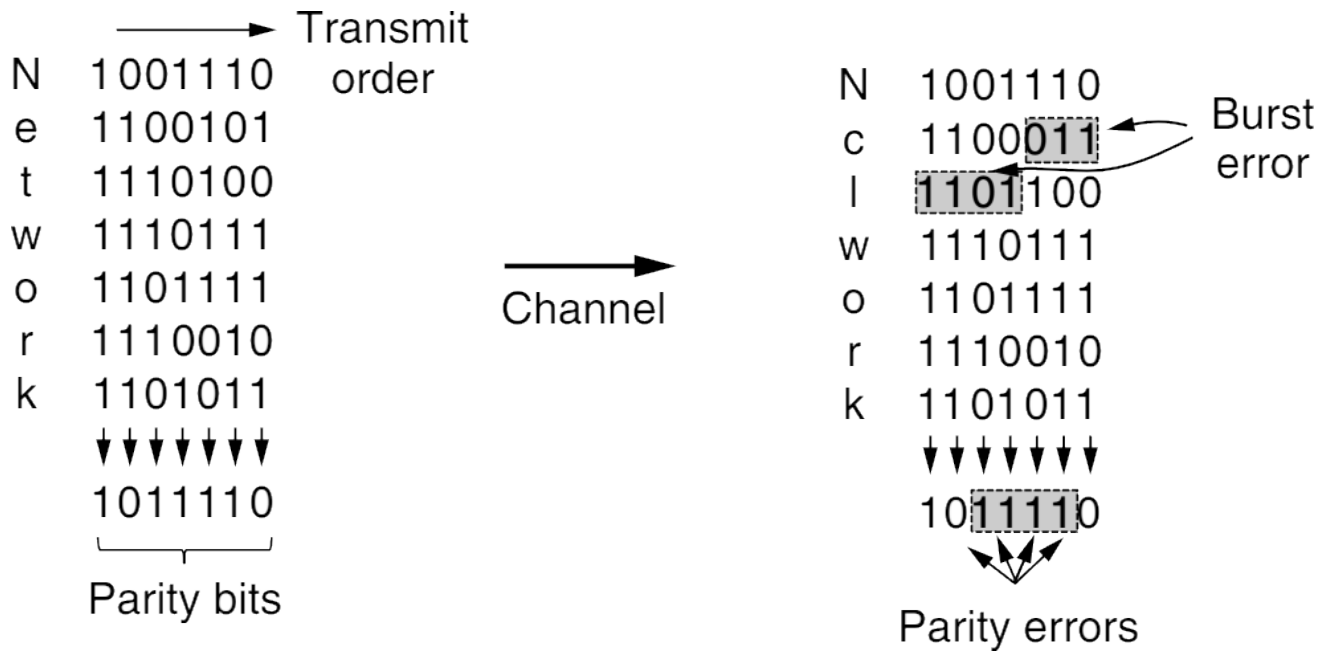
Error Detecting Codes

- Consider a case where a single parity bit is appended to the data.
- The parity bit is chosen so that the number of 1 bits in the codeword is even (or odd).
- For example, when 1011010 is sent in even parity, a bit is added to the end to make it 10110100. With odd parity 1011010 becomes 10110101.
- A code with a single parity bit has a distance of 2, since any single-bit error produces a codeword with the wrong parity. This means that it can detect single-bit errors.

Improving Parity Check

- Block to be sent is regarded as a rectangular matrix n bits wide and k bits high, and compute parity for each row.

- A more popular technique is **interleaving**.



Checksum

- "Checksum" is often used to mean a group of check bits associated with a message.
- The checksum is usually placed at the end of the message, as the complement of the sum function.
- Errors may be detected by summing the entire received codeword, both data bits and checksum.
- One example of a checksum is the 16-bit Internet checksum used on all Internet packets as part of the IP protocol.

Cyclic Redundancy Check (CRC)

- They are also known as **polynomial code**.
- A k-bit frame is regarded as the coefficient list for a polynomial with k terms, ranging from x^{k-1} to x^0.
- For example, 110001 has 6 bits and thus represents a six-term polynomial with coefficients 1, 1, 0, 0, 0, and 1: $1x^5 + 1x^4 + 0x^3 + 0x^2 + 0x^1 + 1x^0$.
- Polynomial arithmetic is done modulo 2, according to the rules of algebraic field theory

Cyclic Redundancy Check (CRC)

- Sender and receiver must agree upon a **generator polynomial**, $G(x)$, in advance.
- Both the high- and low-order bits of the generator must be 1.
- To compute the CRC for some frame with m bits corresponding to the polynomial $M(x)$, the frame must be longer than the generator polynomial.
- The idea is to append a CRC to the end of the frame in such a way that the polynomial represented by the checksummed frame is divisible by $G(x)$.

Cyclic Redundancy Check (CRC)

Algorithm for computing CRC

1. Let r be the degree of $G(x)$. Append r zero bits to the low-order end of the frame so it now contains $m + r$ bits and corresponds to the polynomial $x^r M(x)$.

2. Divide the bit string corresponding to $G(x)$ into the bit string corresponding to $x^r M(x)$, using modulo 2 division.

3. Subtract the remainder (which is always r or fewer bits) from the bit string corresponding to $x^r M(x)$ using modulo 2 subtraction. The result is the checksummed frame to be transmitted. Call its polynomial $T(x)$.

Let us calculate the checksummed frame for 1101011111 using the generator $G(x) = x^4 + x + 1$.