# E2 205 Error-Control Coding
# Lecture 19

Scribe - Vikram Verma

October 16, 2019

## 1 Belief Propagation (via the Generalised Distribution Law)

Consider the computation

$$a(b+c) = ab + ac \tag{1}$$

$$\alpha(x,w) = \sum_{x,z} f(x,y,z)g(x,z) \tag{2}$$

$$\beta(y) = \sum_{x,w,z} f(x,y,w)g(x,z) \tag{3}$$

Assume that $w, x, y, z$ take on values from a common alphabet $\mathscr{A}$ of size $|\mathscr{A}| = q$

### 1.1 GDL Approach to Computation

$$\beta(y) = \sum_{x,w,z} f(x,y,w)g(x,z)$$

$$= \sum_{x,w} \Big[ \sum_{z} f(x,y,w)g(x,z) \Big]$$

$$= \sum_{x,w} f(x,y,w) \sum_{z} g(x,z)$$

$$= \sum_{x,w} f(x,y,w)h(x)$$

$$= \sum_{x} h(x) \sum_{w} f(x,y,z)$$

$$= \sum_{x} h(x)p(x,y)$$

Total number of computation

$$= q(q-1) + q^2(q-1) + q(2q-1)$$

$$= q^3 + 2q^2 - 2q$$

## 1.2 Marginalize The Complex Function Problem

$\{\mathbb{R}, +, .\}$ field

$\{[0, \infty), +, .\}$
Under 'Addition',it is Closure, Associative, Identity Element $\{0\}$ and Commutative but No Inverse exist.
Under 'Multiplication',it is closure, associative, identity element $\{1\}$, commutative and inverse exist.
This is "Sum-Product Semiring".

$\{[0, \infty), max, .\}$ field
Under '$max$'(it is like Addition),it is closure, associative, identity element $\{0\}$ and commutative but No inverse exist.
Under 'Multiplication',it is closure, associative, identity element $\{1\}$, commutative and inverse exist.
This is "Max-Product Semiring".

$\{[-\infty, \infty), min, sum\}$
Under $min$, it is closure, associative, identity element $\{\infty\}$ and commutative but No inverse exist.
Under $sum$, it is closure, associative, identity element $\{0\}$, commutative and No inverse exist.
This is "Min-Sum Semiring".

Note- $a.(b+c) = a.b + a.c$
$a.(max\{b,c\}) = max\{a.b, a.c\}$ under $\{[0,\infty), max, .\}$
$a + min\{b,c\} = min a + b, a + c$ under $\{[-\infty,\infty), min, sum\}$

**Definition 1** *A commutative semiring is a set R,together with two binary operation called " + " and "." such that:*
*S1. Under + we have closure, associative, identity element, commutative*
*S2. Under . we have closure, associative, identity element, commutative*
*S3. The distribution law holds*
$a.(b+c) = a.b + a.c$, *where* $a, b, c \in R$

{{0,1},OR,AND}
Under 'OR', it is closure, associative, identity element {0} and commutative but No inverse exist.
Under 'AND', it is closure, associative, identity element {1}, commutative and No inverse exist.

## 1.3 The MPF Problem

(Marginalize a Product Function)

Setting: A Set $S$ = {1,2, ...n }, collection of index
A set of $n$ variable $x_1, x_2 \ldots x_n$
$x_S = \{\ x_1, x_2 \ldots x_n\ \}$
A set of $M$ subsets of $S, S_j \subseteq S$
$S_j = \{i_1, i_2, \ldots i_{|S_j|}\}$
$\implies x_{S_j} \triangleq \{x_{i_1}, x_{i_2} \ldots x_{i_{|S_j|}}\}$
$x_i \in A_i$ the alphabet of $x_i$
$|A_i| = q_i$
$A_{S_j}$ = alphabet of $x_{S_j}$
$|A_{S_j}| = q_{S_j}$

## 1.4 Local Kernals

$\alpha_j : x_{S_j} \to R$ semiring, $1 \leq j \leq M$

$$\beta(x_{S_j}) = \sum_{x_{S\setminus S_j}} \prod_{i=1}^{M} \alpha_i(x_{S_i})$$

**Example 2** *Walsh-Hadamard Transform*

$$F(x_4x_5x_6) = \sum_{x_1x_2x_3} (-1)^{(x_1x_4+x_2x_5+x_3x_6)} f(x_1x_2x_3)$$

$f(x_1x_2x_3) : F_2^3 \to \mathbb{F}_2$
$S = \{1, 2, \ldots, 6\}$
*Kernals are-*
$S_1 = \{1, 2, 3\}, \alpha_1(x_{s_1}) = \alpha_1(x_1x_2x_3) = f(x_1x_2x_3)$
$S_2 = \{1, 4\}, \alpha_2(x_{s_2}) = (-1)^{(x_1x_4)}$
$S_3 = \{2, 5\}, \alpha_3(x_{s_3}) = (-1)^{(x_2x_5)}$
$S_4 = \{3, 6\}, \alpha_4(x_{s_4}) = (-1)^{(x_3x_6)}$
$S_5 = \{4, 5, 6\}, \alpha_5(x_{s_5}) = 1$

**Example 3** *Maximum Likelihood Codeword Decoding of a block code (binary [7,4,2]).*
*Assume transmission over BSC.*

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

$s = 1, d_{min} = s + 1 = 2$
*Let*

$$F_i(x_i) = \max_{\underline{x} \in \mathbb{C}, \sim x_i} p(\underline{y}/\underline{x})$$

*max over* $\sim x_i$ *means all variables other than* $x_i$*.*

$$\hat{x}_i = \arg\max_{a_i} F_i(a_i)$$

| | *x=0* | *x=1* |
|---|---|---|
| $F_1(x_1)$ | *2* | *8* |
| $F_2(x_2)$ | *1* | *8* |
| $F_3(x_3)$ | *8* | *6* |
| $F_4(x_4)$ | *2* | *8* |
| $F_5(x_5)$ | *-1* | *8* |
| $F_6(x_6)$ | *8* | *4* |
| $F_7(x_7)$ | *6* | *8* |

$$\underline{\hat{x}} = 1101101$$

$$\chi(x_1x_2x_4) = 1 \ \textit{if} \ x_1 + x_2 + x_4 = 0(mod2).$$

$$F_i(x_i) = \max_{\sim x_i} p(\underline{y}/\underline{x})\chi(x_1x_2x_4)\chi(x_3x_4x_6)\chi(x_4x_5x_7)$$

$$F_i(x_i) = \max_{\sim x_i} \prod_{i=1}^{7} p(y_i/x_i)\chi(x_1x_2x_4)\chi(x_3x_4x_6)\chi(x_4x_5x_7)$$

$S = \{1, 2, \ldots, 7\}$
$x_{S_i} = x_i, 1 \leq i \leq 7$
$x_{S_8} = x_1x_2x_4$
$x_{S_9} = x_3x_4x_6$
$x_{S_{10}} = x_4x_5x_7$

*(This is an MPF problem in 'Max-product Semiring)*