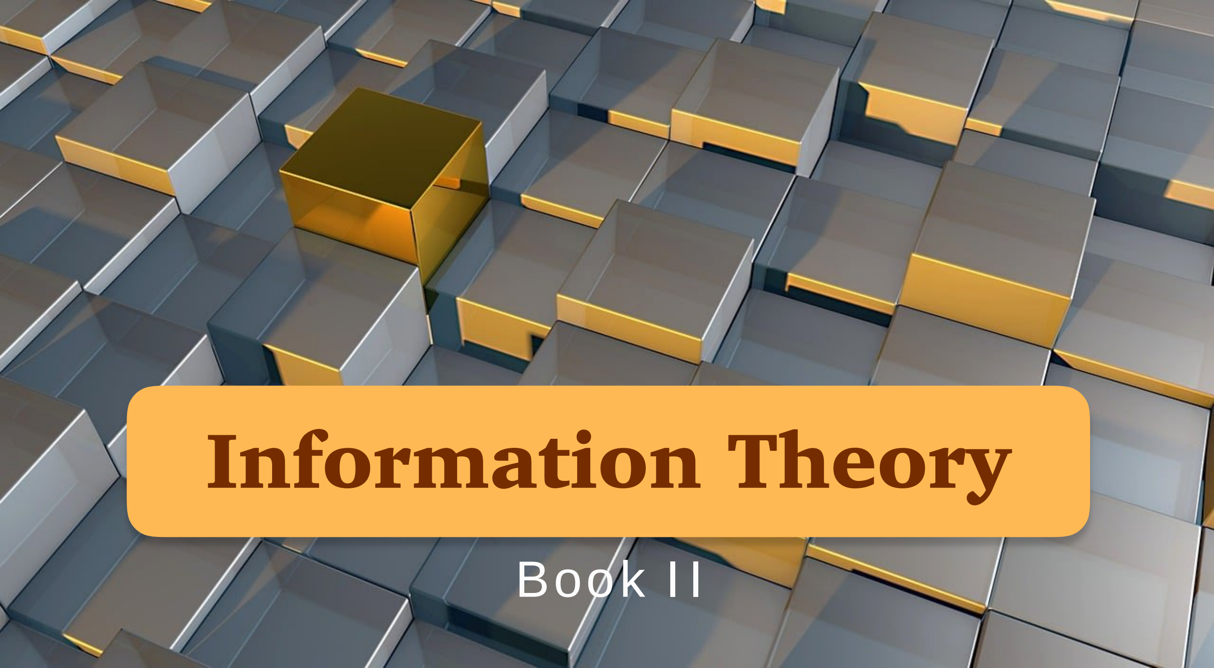
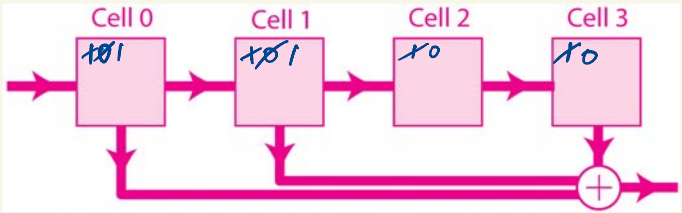


Information Theory

Book II

Eg. an infinite stream of bits $a_0 a_1 a_2 a_3 a_4 \cdots$ $(a_i \in F)$ can be encoded eg. represent the plaintext bitstream as a $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots \in \mathbb{F}_2[[x]]$

$F[[x]]$ = ring of (formal) power series in x with coefficients in F.



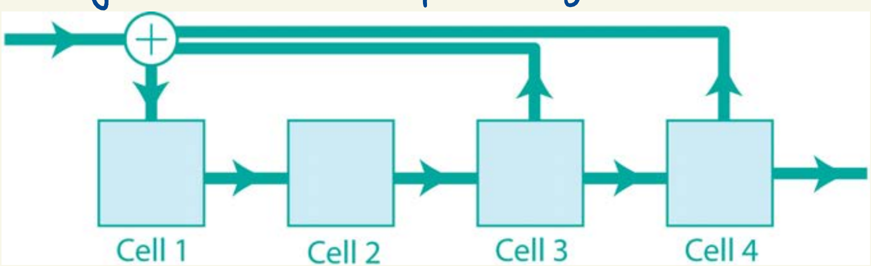
10110...

Eg. consider an input bitstream 1100110011110010... which is encoded by the shift register above to obtain the output bitstream 101100101...

Compare: this is equivalent to multiplication by $1+x+x^3$:

$(1+x+x^3)(1+x+x^4+x^5+x^7+x^8+x^9+x^{10}+x^{13}+\cdots) = 1 + x^2 + x^3 + x^6 + x^8 + \cdots$

Decoding of this data is accomplished using backward shift registers eg.



which performs division by $1+x+x^3$ in $\mathbb{F}_2((x))$

Symbolic rings and fields

$$\begin{tikzcd}
 & F((x)) \arrow[dl, dash] \arrow[dr, dash] & \\
F(x) \arrow[dr, dash] & & F[[x]] \arrow[dl, dash] \\
 & F[x] &
\end{tikzcd}$$

field of Laurent series $\to F((x))$

field of (power) series in x with coeffs in F. $\to F[[x]]$

field of rational "functions" (actually symbolic expressions) in x with coeffs in F: $F(x)$

$F[x]$ = ring of polys in x with coeffs in F

polynomials vs. polynomial functions

eg. $\mathbb{F}_3 = \{0,1,2\} = \mathbb{Z}/3\mathbb{Z}$

eg. $f(x) = 2 + x + x^3 \in \mathbb{F}_3[x]$ is a polynomial of degree 3.

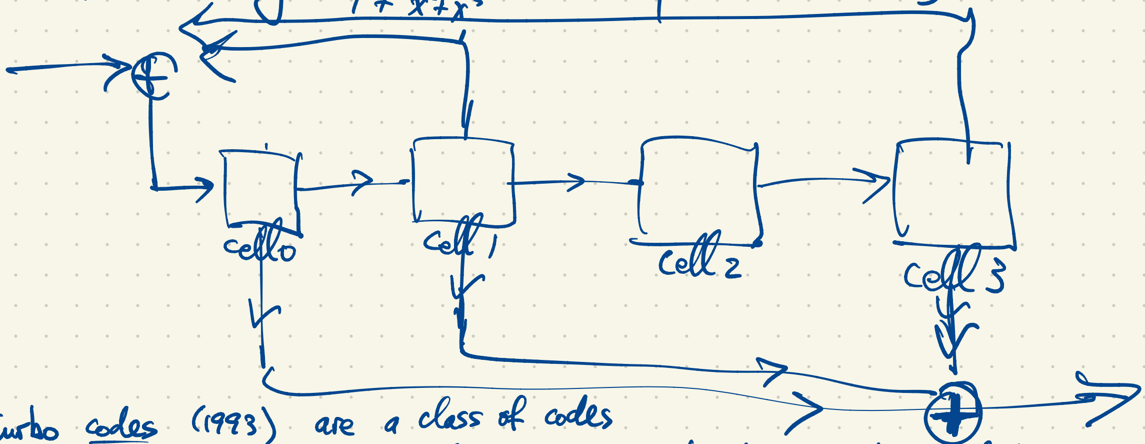
$g(x) = 2 + 2x \in \mathbb{F}_3[x]$ is a polynomial of degree 1.

a	$f(a)$	$g(a)$
0	2	2
1	1	1
2	0	0

$f(x), g(x)$ are distinct poly's but they represent the same function $\mathbb{F}_3 \to \mathbb{F}_3$.

eg. $f(x) = \dfrac{1+x+x^3}{x+x^2} \in \mathbb{F}_2(x)$

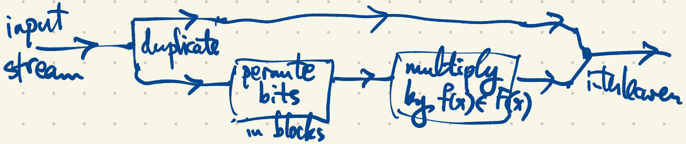
Multiplication by any rational function can be implemented using a single shift register e.g. multiplication by $\frac{1+x+x^3}{1+x^2+x^3}$ is implemented using the shift register



Turbo codes (1993) are a class of codes used for encoding streams of data using combinations of gates including

- multiplication by a rational function in $F(x)$
- splitters & interleavers
- permutations
- puncturing

eg.



$F(x) \subset F((x))$ eg. for $F = \mathbb{F}_2 = \{0,1\}$

First method

$$f(x) = \frac{1+x^2+x^5}{x+x^2+x^4} = \frac{1+x^2+x^5}{x(1+x+x^3)} = \frac{1}{x}\left[\frac{1+x^2+x^5}{1+x+x^3}\right] = \frac{1}{x}\left[1+x+x^3+x^5+\cdots\right] = \frac{1}{x}+1+x^2+x^4+\cdots$$

$(a+b)^2 = a^2+b^2$

$(a+b)^4 = a^4+b^4$

$$\frac{1+x^2+x^5}{1+x+x^3} = 1 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + \cdots$$

$a_1=1$, $a_2=0$, $a_3=1$, $a_4=0$, $a_5=1$

$$1+x^2+x^5 = (1+x+x^3)(1+x+x^3+x^5+\cdots)$$

Second method Geometric series $\frac{1}{1-u} = 1+u+u^2+u^3+u^4+\cdots$

$$\frac{1+x^2+x^5}{1+(x+x^3)} = (1+x^2+x^5)\left(1+(x+x^3)+(x+x^3)^2+(x+x^3)^3+(x+x^3)^4+(x+x^3)^5+\cdots\right)$$

$$= (1+x^2+x^5)\left(1+(x+x^3)+(x^2+x^6)+(x^3+x^5+\cdots)+(x^4+\cdots)+(x^5+\cdots)+\cdots\right)$$

$(x^3+3x^5+3x^7+x^9)$

$$= (1+x^2+x^5)(1+x+x^2+x^4+\cdots)$$

$$= 1+x+x^3+x^5+\cdots$$

$$f(x) = \frac{1}{x}(1+x+x^3+x^5+\cdots) = \frac{1}{x}+1+x^2+x^4+\cdots$$

$F = \mathbb{F}_2 = \{0,1\}$ for the time being

The irreducible (monic) polynomials in $F[x]$:

degree	irred. polys
1	x, $x+1$
2	x^2+x+1
3	x^3+x+1, x^3+x^2+1
4	x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$
....	....

$\underset{x\cdot x}{\underset{\parallel}{x^2}}$, $\underset{(x+1)(x+1)}{\underset{\parallel}{x^2+1}}$, $\underset{x(x+1)}{\underset{\parallel}{x^2+x}}$, x^2+x+1 all poly's of degree 2.

$x^4+x^2+1 = (x^2+x+1)^2$

See MacWilliams & Sloane, The Theory of Error-Correcting Codes for more extensive lists of irreducible polynomials.