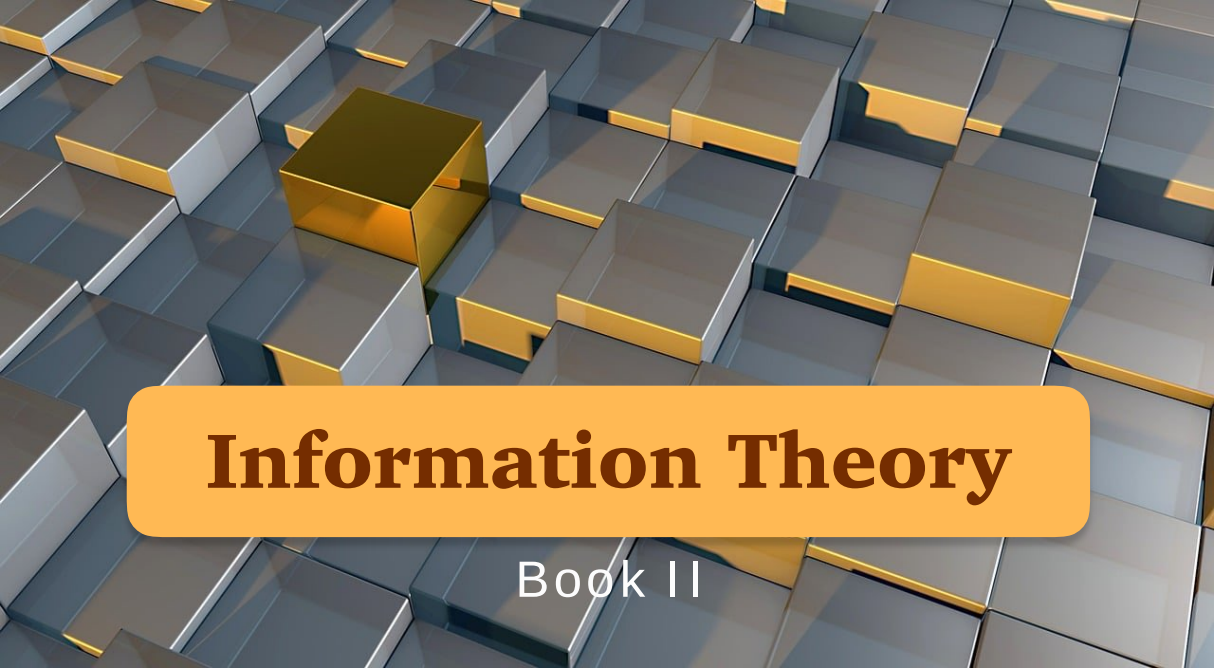
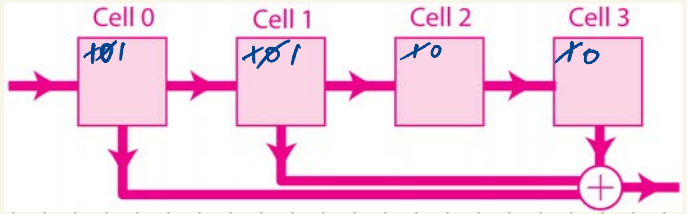


Information Theory

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.



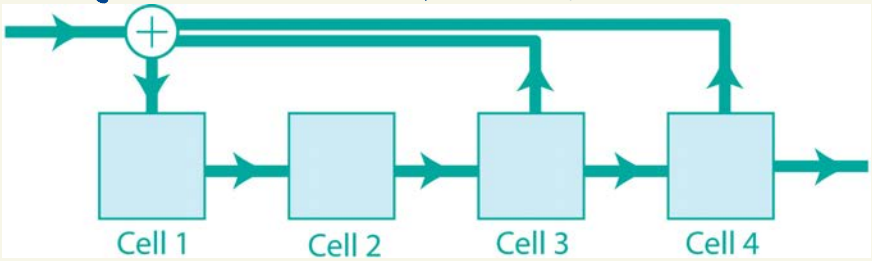
10110...

Eg. consider an input bitstream 11001101111 0010...
which is encoded by the shift register above to obtain the output bitstream 10110010 1...

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

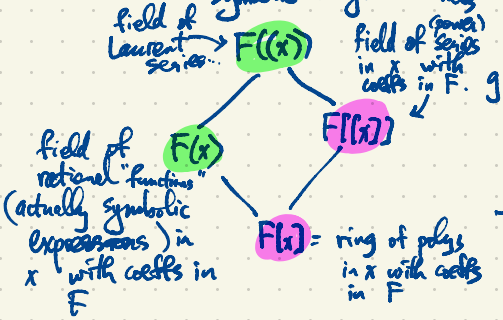
$(1+x+x^3)(1+x+x^4+x^5+x^7+x^8+x^9+x^{10}+x^{12}+\cdots) = 1 + x^2 + x^3 + x^6 + x^8 + \cdots$

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



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.

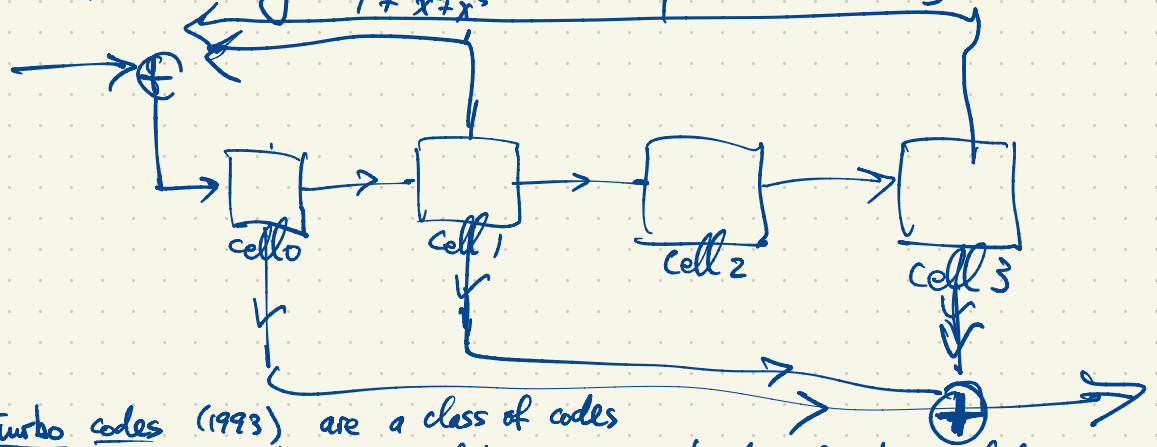
$g(x) = 2 + 2x \in \mathbb{F}_3[x]$ is a polynomial of degree 1.

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

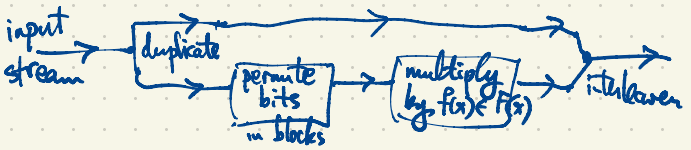
Multiplication by any rational function can be implemented using a single shift register eg.
multiplication by $\frac{1+x+x^3}{1+x^2+x^3}$ is implemented using the shift register



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.


input
stream
duplicate
permute
bits
in blocks
multiply
by f(x) (f(x))
interleaver