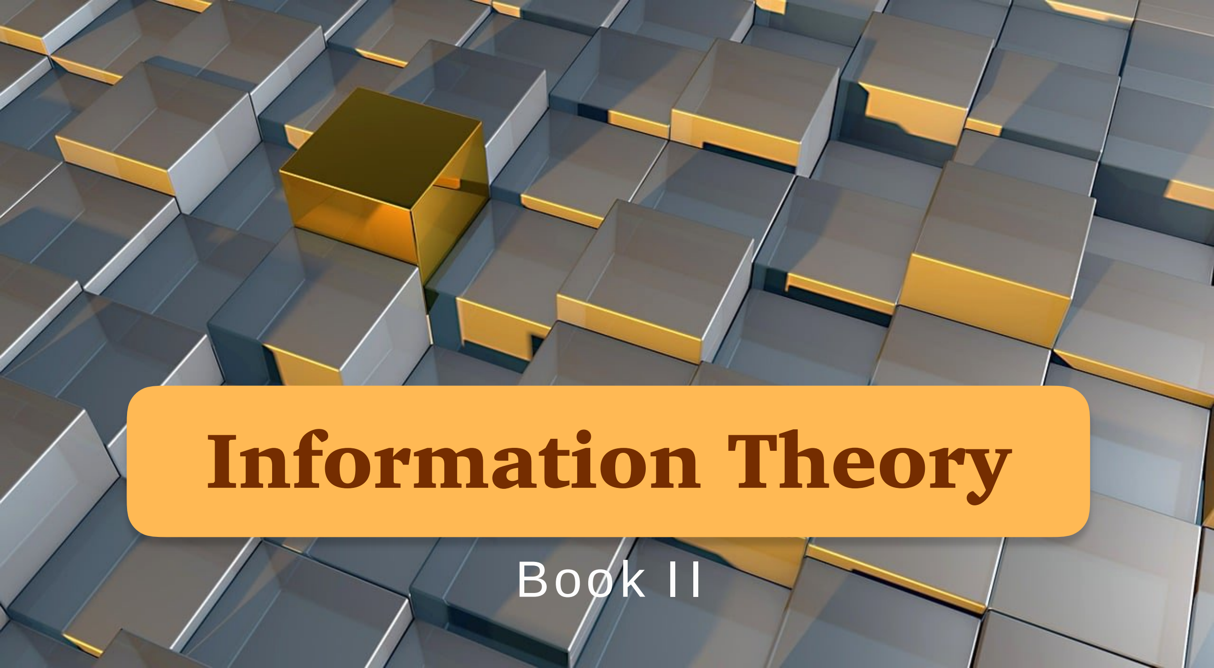
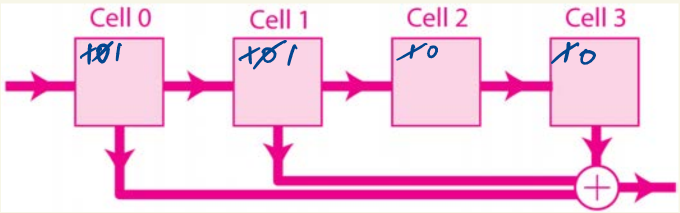


Information Theory

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.

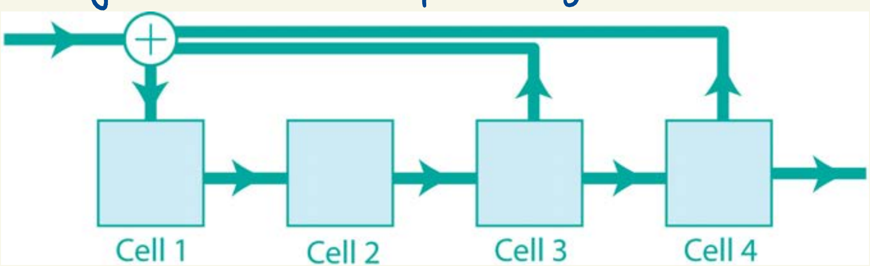


Eg. consider an input bitstream 1100110111110010... which is encoded by the shift register above to obtain the output bitstream 101100101...

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

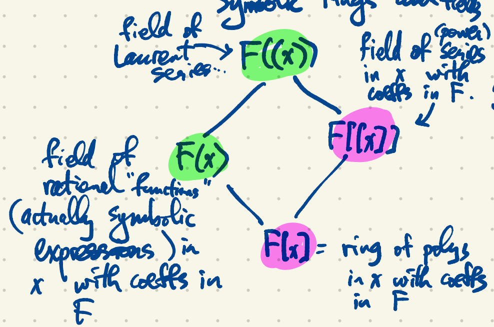
$(1+x+x^3)(1+x+x^4+x^5+x^7+x^8+x^9+x^{10}+x^{13}+\cdots) = 1 + x^2 + x^3 + x^6 + x^8 + \cdots$

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



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.

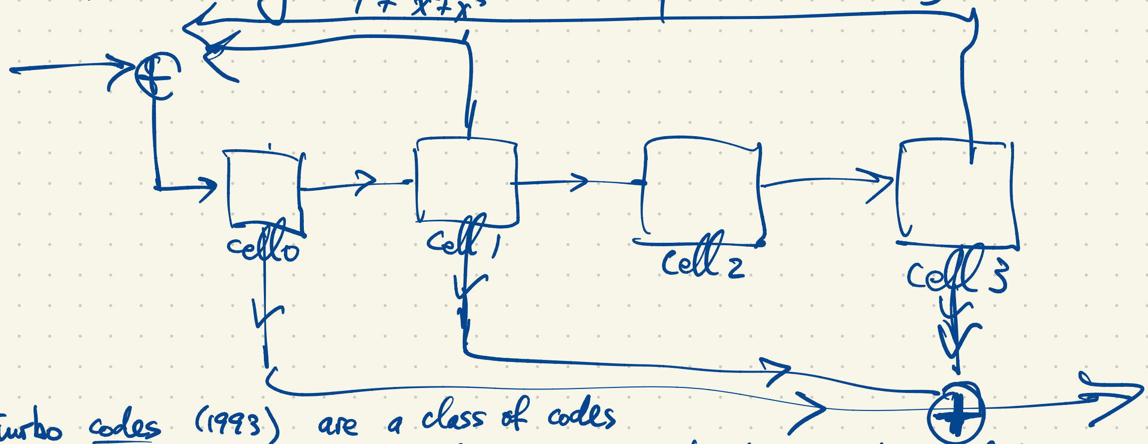
$g(x) = 2 + 2x \in \mathbb{F}_3[x]$ is a polynomial of degree 1.

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

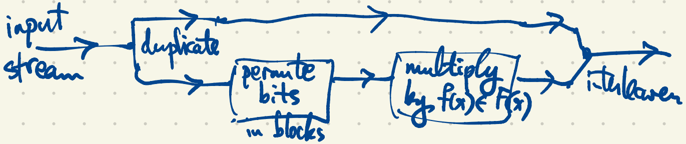
Multiplication by any rational function can be implemented using a single shift register e.g. multiplication by $\frac{1+x+x^3}{1+x^2+x^3}$ is implemented using the shift register



<u>Turbo codes</u> (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

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

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

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

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

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

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

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, $x^4+x^3+x^2+x+1$
....	....

x^2, x^2+1, x^2+x, x^2+x+1 all poly's of degree 2.
($x^2 = x\cdot x$, $x^2+1 = (x+1)(x+1)$, $x^2+x = x(x+1)$)

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

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

What are all the cyclic (linear) binary codes of length 7? There are exactly 8 of them. (why?)

- subspace of F^7, $F = \mathbb{F}_2 = \{0,1\}$
- invariant under cyclic shift $(a_0,a_1,a_2,a_3,a_4,a_5,a_6) \longmapsto (a_6,a_0,a_1,\dots,a_5)$ $a_i \in F$

A linear code $\mathcal{C} \subseteq F^n$ is cyclic iff its dual code $\mathcal{C}^\perp \subseteq F^n$ is also cyclic.

$\dim \mathcal{C} + \dim \mathcal{C}^\perp = n$.

eg. $\{(0000000)\}$
$\{0000000, 1111111\}$
F^7
$\{$words in F^7 of even weight$\}$ = ⟨1100000, 1010000, 1001000, 1000100, 1000010, 1000001⟩

```
 1110100
 0101000
 -------
 1011100
```

Hamming $[7,4,3]_2$ code $\mathcal{H}$: ⟨1101000, 0110100, ..., 1010001⟩ (all cyclic shifts of 1101000 span this code)

$\dim \mathcal{H} = 4$, $|\mathcal{H}| = 2^4 = 16$:
- 1 codeword of weight 0
- 7 3
- 7 4
- 1 7

Its dual $\mathcal{H}^\perp$, $\dim \mathcal{H}^\perp = 3$ is a $[7,3,4]_2$ - code.
$\mathcal{H}^\perp$ has 1 codeword of weight 0
7 4

$\mathcal{H}^\perp = \mathcal{H} \cap \langle 1111111 \rangle^\perp$

$\mathcal{H}' = \langle 1011000, 0101100, \dots, 0110001 \rangle$ also $[7,4,3]_2$

$\mathcal{H}'^\perp$ also $[7,3,4]_2$.

$x^7 - 1 \in F[x]$ ← n = length

actually $x^7 + 1$ $F = \mathbb{F}_2$

$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + 1) = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$

i.e. $x+1$

$(x-\alpha)(x-\alpha^2)(x-\alpha^4)$ $(x-\beta)(x-\beta^2)(x-\beta^4)$

If $E = \mathbb{F}_q$, $x^q - x = x(x-1)(x-a_2)(x-a_3)\cdots(x-a_q)$ ($x - 0$)

$a_0 = 0$, $a_1 = 1$, $a_2, a_3, \cdots, a_q$ are the field elements.

i.e. $x^{q-1} - 1$ has $q-1$ distinct roots which are the nonzero field elements.

If $\alpha \in \mathbb{F}_8$ is a root of $x^3 + x + 1$

$\mathbb{F}_8 = \mathbb{F}_2[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 : a_0, a_1, a_2 \in \mathbb{F}_2\}$

$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

Squaring is an automorphism of $\mathbb{F}_8$.

$(u+v)^2 = u^2 + v^2$

$(uv)^2 = u^2 v^2$