

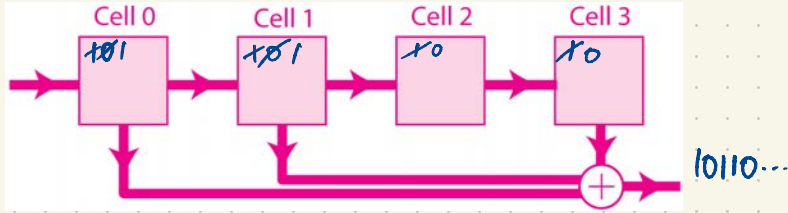
A 3D perspective view of a grid of cubes. Most cubes are grey, but one cube in the center-left area is a bright, reflective gold color. The lighting creates shadows and highlights on the surfaces of the cubes, giving them a three-dimensional appearance.

# Information Theory

Book II

eg. an infinite stream of bits  $a_0, a_1, a_2, a_3, a_4, \dots$  ( $a_i \in F$ ) can be encoded eg. represent the plaintext bitstream as a  $a_0 + a_1x + a_2x^2 + a_3x^3 + \dots \in \mathbb{F}_2[[x]]$

$\mathbb{F}[[x]]$  = ring of <sup>(formal)</sup> power series in  $x$  with coefficients in  $F$ .

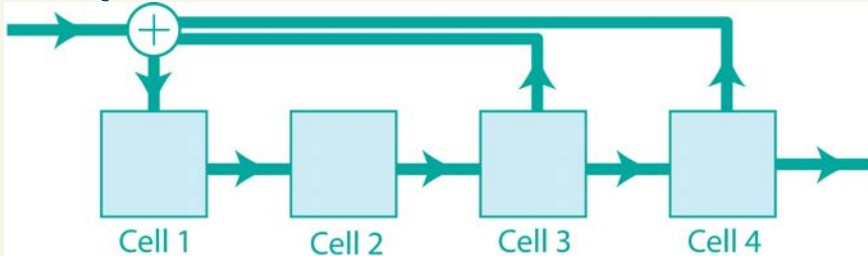


eg. consider an input bitstream ~~11001~~  $1100111110010\dots$  which is encoded by the shift register above to obtain the output bitstream  $101100101\dots$

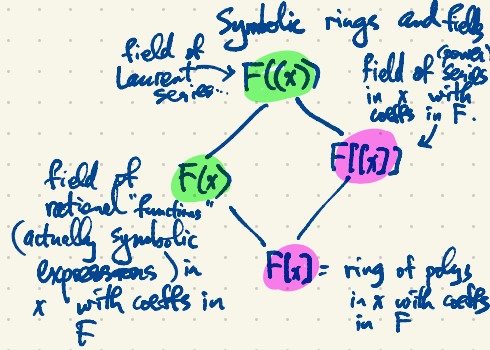
Compare: this is equivalent to multiplication by  $1+x+x^3$ :

$$(1+x+x^3)(1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+\dots) = 1+x^2+x^3+x^6+x^8+\dots$$

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



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



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.

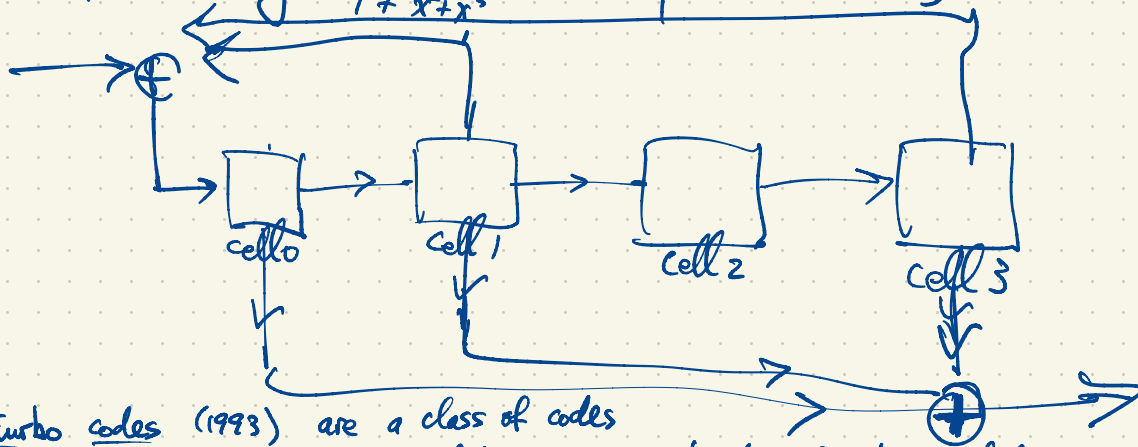
$g(x) = 2+2x \in \mathbb{F}_3[x]$  is a polynomial of degree 1.

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

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

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

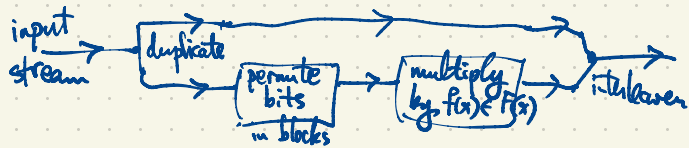
Multiplication by any rational function can be implemented using a single shift register e.g. multiplication by  $\frac{1+x+x^3}{1+x^2+x^3}$  is implemented using the shift register



Turbo codes (1993) are a class of codes used for encoding streams of data using combinator 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

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

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

$\swarrow a_1=1 \quad \swarrow a_2=0 \quad \swarrow a_3=1 \quad \swarrow a_4=0 \quad \swarrow a_5=1$

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

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

$$(a+b)^3 = a^3 + b^3$$

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

$$\begin{aligned} \frac{1+x^2+x^5}{1+(x+x^3)} &= (1+x^2+x^5) \left( 1 + (x+x^3) + (x+x^3)^2 + (x+x^3)^3 + (x+x^3)^4 + (x+x^3)^5 + \dots \right) \\ &= (1+x^2+x^5) \left( 1 + (x+x^3) + (x^2+x^6) + (x^3+x^5+\dots) + (x^4+\dots) + (x^5+\dots) + \dots \right) \\ &\quad (x^3+3x^5+3x^7+x^9) \\ &= (1+x^2+x^5)(1+x+x^2+x^4+\dots) \\ &= 1+x+x^2+x^5+\dots \end{aligned}$$

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



$F = \mathbb{F}_2 = \{0, 1\}$  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	$x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$

primitive

not primitive

$x^2, x^2+1, x^2+x, x^2+x+1$  all poly's of degree 2.  
 $x \cdot x \quad (x+1)(x+1) \quad x(x+1)$   
 $x^4+x^2+1 = (x^2+x+1)^2$

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  $(a_0, a_1, a_2, a_3, a_4, a_5, a_6) \mapsto (a_6, a_0, a_1, \dots, a_5)$   $a_i \in F$

eg.  $\{(0000000)\}$

$\{0000000, 1111111\}$

$F^7 \leftarrow g(x)=1, h(x)=x^3-1$

$\{\text{words in } F^7 \text{ of even weight}\} = \langle 1100000, 1010000, 1001000, 1000100, 1000010, 1000001 \rangle$

Hamming  $[7, 4, 3]_2$  code  $\mathcal{H} = \langle 1101000, 0110100, \dots, 1010001 \rangle$  (all cyclic shifts of 1101000 span this code)

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

7 7 7 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

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

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

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

$\begin{matrix} 110100 \\ 010100 \\ \hline 101100 \end{matrix}$

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

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

$$x^{q-1} \stackrel{\leftarrow n = \text{length}}{\in} F[x]$$

$$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + 1) = (x-1) \underbrace{(x^3 + x + 1)}_{\substack{\text{i.e. } x+1 \\ (x-\alpha)(x-\alpha^2)(x-\alpha^4)}} (x^3 + x^2 + 1) = (x-\beta)(x-\beta^2)(x-\beta^4)$$

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

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

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

i.e.  $x^q - 1$  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  $\mathbb{F}_8$ .

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

If  $f(x) \in \mathbb{F}_p[x]$  is irreducible of degree  $d$ , then  $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^d} = \mathbb{F}_p[\beta]$  where  $\beta$  is a root of  $f(x)$ .

$$= \{a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{d-1}\beta^{d-1} : a_i \in \mathbb{F}_p\}$$

( $\beta$  generates  $\mathbb{F}_{p^d} \supset \mathbb{F}_p$  as an algebra)

If in fact  $\mathbb{F}_{p^d} = \{0, 1, \beta, \beta^2, \beta^3, \dots, \beta^{d-2}\}$  then we say  $\beta$  is a primitive element and we say  $f(x)$  is a primitive polynomial.

If  $f(x) = x^4 + x^3 + x^2 + x + 1$  and  $\beta \in \mathbb{F}_{16} = \mathbb{F}_2$  is a root of  $f(x)$  then  $\beta^5 = 1$  since  $\beta$  is a root of  $f(x)$

$$\beta^5 - 1 = (\beta-1)(\beta^4 + \beta^3 + \beta^2 + \beta + 1) = 0$$

$0, 1, \beta, \beta^2, \beta^3, \beta^4, 1, \beta, \beta^2, \dots$  doesn't give all of  $\mathbb{F}_{16}$ .

There are eight ways to factor  $x^7 - 1 = g(x)h(x)$  in  $\mathbb{F}_2[x]$ . In each case  $g(x)$  is a generator poly. and  $h(x)$  is a parity check poly. for a cyclic code of length 7 over  $\mathbb{F}_2 = \{0, 1\} = F$ . Cyclic (linear) codes  $\leftrightarrow$  ideals in  $\mathbb{F}_2[x]/(x^7 - 1)$

$g(x) = 1, h(x) = x^7 - 1$  gives  $F^7$

$g(x) = x^7 - 1, h(x) = 1$  gives  $\{0000000\}$

$g(x) = x + 1, h(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$  gives all words of <sup>even</sup> weight i.e.  $\langle 1100000, 1010000, \dots, 1000001 \rangle$

$g(x) = x^6 + x^5 + \dots + 1, h(x) = x + 1$  gives  $\langle 1111111 \rangle = \{0000000, 1111111\}$

$g(x) = 1 + x + x^3, h(x) = 1 + x^2 + x^3 + x^4$  gives  $\mathcal{H}$   $[7, 4, 3]_2$  code

BCH bound : a lower bound for performance of a cyclic code.

Consider a cyclic code of length  $n$  over  $F$ , i.e. an ideal in  $\mathbb{F}_q[x]/(x^n - 1)$  with gen. poly.  $g(x)$ , parity check poly.  $h(x)$ ,  $x^n - 1 = g(x)h(x)$ ,  $g(x)$  primitive,  $\beta$  root of  $g(x)$  in  $\mathbb{F}_{q^r}$ ,  $r = \deg g(x)$ , and  $\beta, \beta^2, \dots, \beta^{s-1}$  are roots of  $g(x)$ , then the code has min. distance  $\geq s$ .

For Hamming  $[7, 4, 3]_2$  code  $\beta$  root of  $g(x) = 1 + x + x^3 \in F[x]$ ,  $\beta \in \mathbb{F}_8 = \mathbb{F}_2[\beta]$   
 Also  $\beta^2$  ... by Freshman's Dream

$1 + \beta + \beta^3 = 0$   
 $(1 + \beta + \beta^3)^2 = 1 + \beta^2 + \beta^6 = 0 = 1 + \beta^2 + (\beta^2)^3 \Rightarrow \mathcal{H}$  has min. dist.  $\geq 3$ .



BCH : R.C. Bose  
 Dijen Ray-Chandhuri  
 Hocquengham

The Gilbert-Varshamov Bound (GV-bound): a lower bound for existence of good codes  
 $A_2(n, d) = \max |C|$  s.t.  $C \subseteq A^n$ ,  $|C| = q$  with min. distance  $\geq d$  i.e.  $d(w, w') \geq d$  for all  $w \neq w'$  in  $C$ .

Ball of radius  $r$  in  $A^n$  centered at  $0 \in A^n$   
 has cardinality  $|B_r(0)| = \sum_{k=0}^r \binom{n}{k} (q-1)^k$

$e = \lfloor \frac{d-1}{2} \rfloor =$  error-correcting capability.

Hamming bound:  $A_2(n, d) \leq \frac{q^n}{|B_e|}$  : balls of radius  $e$  centered at codewords  $w \in C$  are required to be disjoint

$$\bigsqcup_{w \in C} B_e(w) \subseteq A^n \Rightarrow |C| \cdot |B_e(w)| \leq q^n$$

$$\Rightarrow |C| \leq \frac{q^n}{|B_e(w)|}$$

In the other direction the GV-bound

$$A_2(n, d) \geq \frac{q^n}{|B_{d-1}(0)|} \quad \text{so} \quad \frac{q^n}{|B_{d-1}(0)|} \leq A_2(n, d) \leq \frac{q^n}{|B_e(0)|}$$

Proof: Let  $C \subseteq A^n$  be any  $q$ -ary code with  $|C| = A_2(n, d)$ . We claim

$$\bigcup_{w \in C} B_{d-1}(w) \supseteq A^n$$

Codes satisfying this condition by greedy construction.  
 But such codes are usually not practical because membership & decoding are not efficient.

If not, there exists  $w' \in A^n$ ,  $w' \notin \bigcup_{w \in C} B_{d-1}(w)$  so  $d(w', w) > d-1$  for all  $w \in C$ .

But then  $C \cup \{w'\}$  has min. distance  $\geq d$ . This contradicts the maximality of  $C$  among all  $q$ -ary codes of length  $n$  having min. distance  $d$ .

$$\text{So } |C| |B_{d-1}(0)| \geq |A^n| = q^n$$



We regard the GV bound as an existence proof only.

Recommended viewing:  
 YouTube videos on coding & info. theory (including alg. geom. codes) by Mary Whatters

Asymptotic version of GV-bound due to Shannon:

Fix  $0 < \delta < 1$ .  $|B_{S_n}(0)| \approx |A^n|^{h_2(\delta)} = q^{nh_2(\delta)}$ ,  $0 \leq h_2(\delta) \leq 1$ .

$$\log_2 |B_{S_n}(0)| \approx nh_2(\delta)$$

This is a true asymptotic formula: for fixed  $q$  and  $\delta \in (0, 1)$ ,

$$\frac{\log_2 |B_{S_n}(0)|}{nh_2(\delta)} \rightarrow 1 \quad \text{as } n \rightarrow \infty.$$

$$\log_2 |B_{S_n}(0)| \sim nh_2(\delta).$$

More precisely,

$$nh_2(\delta) - o(n) \leq \log_2 |B_{S_n}(0)| \leq nh_2(\delta)$$

The  $q$ -ary entropy function

binary entropy function

$$h_2(q) = -\delta \log_2 \delta - (1-\delta) \log_2 (1-\delta) = \delta \log_2 \frac{1}{\delta} + (1-\delta) \log_2 \frac{1}{1-\delta}$$

Ex. consider a random stream of information coming from letters in  $A$ ,  $|A|=q$ ,  $A = \{x_1, \dots, x_q\}$

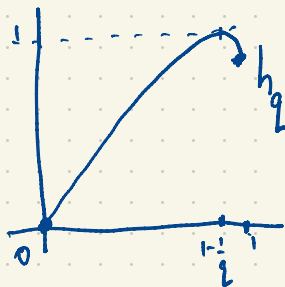
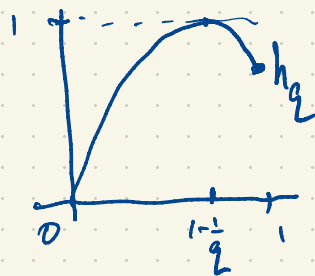
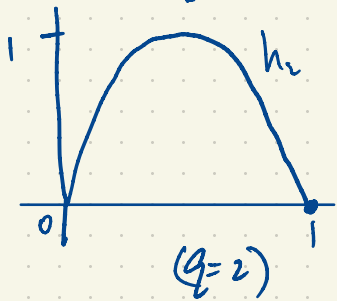
with letter  $x_i$  having frequency  $\frac{p_i}{q}$

$$(2 \leq i \leq q) \quad \delta (1-p) + \frac{p}{q} + \frac{p}{q} + \dots + \frac{p}{q} = 1.$$

single char. form

$$H(\text{this stream}) = \sum p \log \frac{1}{p} = -\sum p \log p = -(1-p) \log (1-p) - \left(\frac{p}{q}\right) \log \frac{p}{q} = p \log (q-1) - p \log p - (1-p) \log (1-p)$$

$$h_2(\delta) = \delta \log_2(q-1) - \delta \log_2 \delta - (1-\delta) \log_2(1-\delta)$$



increasing  $q$

$$h_q(x) = x \log_2(q-1) + \frac{\log_2 q}{\log_2 q} h_2(x) \quad \text{Let } x \rightarrow 1^-$$

$$h_q(x) \rightarrow \log_2(q-1) \text{ as } x \rightarrow 1^-$$

For long codes ( $n \gg 0$ ) over a fixed alphabet  $|A|=q$ , we consider the information rate  $R = \frac{\log_2 |C|}{n} = \frac{k}{n}$  in the case of an  $[n, k]_q$ -code

$$\text{relative distance } \delta = \frac{d}{n}$$

$$\text{relative error-correcting capability } \frac{e}{n} = \frac{d}{2n} = \frac{\delta}{2}$$

For  $q \geq 49$  (1982) we have a new lower bound for asymptotically good explicit codes using algebraic geometry (Tsfasman, Vlăduț, Zink)

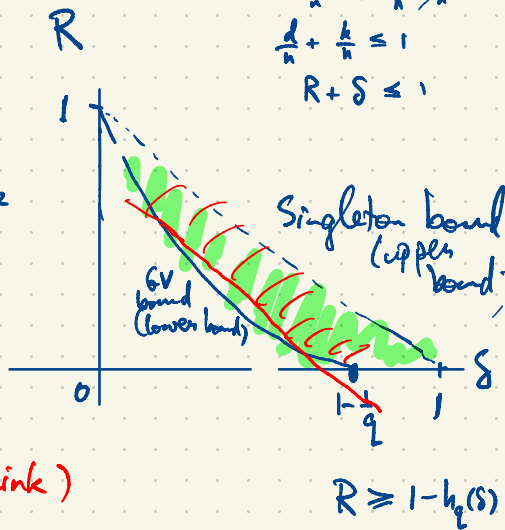
Singleton bound:

$$d \leq n - k + 1$$

$$\frac{d}{n} \leq 1 - \frac{k}{n} + \frac{1}{n}$$

$$\frac{d}{n} + \frac{k}{n} \leq 1$$

$$R + \delta \leq 1$$



The 1982 theorem literally says: There exists a family  $X_i$  of algebraic curves over  $\mathbb{F}_q$  ( $i=1,2,3,\dots$ ) such that  $X_i$  has  $n_i+1$  (rational) points over  $\mathbb{F}_q$ , genus  $g_i$  with

$$\frac{g_i}{n_i} \rightarrow \frac{1}{q-1} \text{ as } i \rightarrow \infty.$$

The Reed-Solomon codes come from the simplest curve of all, the projective line  $P^1F = F \cup \{\infty\}$  ( $F$ : field) of genus 0.



$S^2$

$g=0$



$T^2 = S^1 \times S^1$

$g=1$



$g=2$



$g=3$

On a curve  $X$ ,  $\Omega_X = \{\text{smooth global differential 1-forms}\}$  is a vector space of dimension  $\dim \Omega_X = g$ .  
 The number of  $\mathbb{F}_q$  points on the curve (if it's defined over  $\mathbb{F}_q$ ),  $N_q$ , satisfies  $|N_q - (q+1)| \leq 2g\sqrt{q}$   
 Hasse-Weil bound.

Ex.  $P^1F$  has  $N = q+1$  points,  $g=0$

irreducible  
 For a plane curve of degree  $d$  (defined by a poly. equation of degree  $d$ ) has genus  $g \leq \binom{d-1}{2} = \frac{(d-1)(d-2)}{2}$   
 (equality for smooth curve;  $g = \binom{d-1}{2} - \sum \binom{\nu_i}{2}$ )

$y^2 = x^2 \iff y = \pm x$   has  $2q+1$  points singular points

$y^2 - x^2 = (y+x)(y-x) = 0$

Irreducible conic:  
 $y^2 = x^2 + (t, t^2) \quad t \in F$  genus  $g=0$   
 plus one point at infinity  
 $q+1$  points

Smooth curve of degree  $d=3$  has genus  $g = \binom{3-1}{2} = 1$  is topologically a torus.  
(elliptic curve)

eg.  $y^2 = \text{cubic in } x \text{ with no repeated roots}$  is an elliptic curve.

$$y^2 = x^3 - x = x(x+1)(x-1)$$

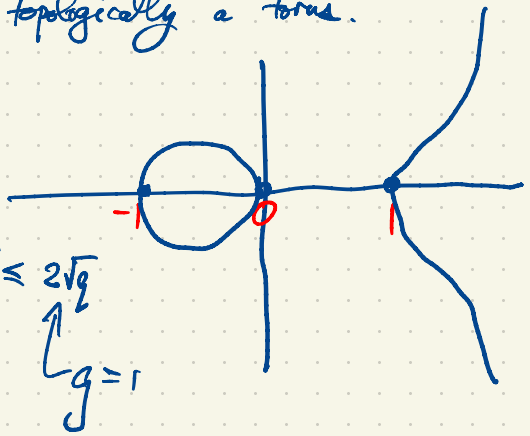
$g=1$  (torus)

H.W bound: over  $\mathbb{F}_q$  the number of points satisfies  $|N - (q+1)| \leq 2\sqrt{q}$

$q > 3$   $q = \text{prime } p \geq 5$

$N = q+1$  if  $q = \text{prime } p \equiv 3 \pmod{4}$   
 $q+1 \pm 2$  if  $q = \text{prime } p \equiv 1 \pmod{4}$

$$|E| \leq 2\sqrt{q}$$



Projective line  $P^1 \mathbb{F} = \mathbb{F} \cup \{\infty\} = X$

We consider rational functions  $f(x) \in \mathbb{F}(X)$  defined on a curve  $X$  (eg.  $X = P^1 \mathbb{F}$ )

eg.  $\mathbb{F} = \mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$   $\frac{1 \quad B \quad C \quad D \quad E \quad F \quad G \quad \infty}{0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6} = X$

Formal integers - linear combinations of points  $A, B, C, D, E, F, G, \infty$  on  $X$  are called divisors as a book keeping device for keeping track of zeroes and poles of functions on  $X$ .

eg.  $f(x) = (x-1)(x-2)(x-5) = x^3 + 3x^2 - x - 3 = x^3 + 3x^2 + 6x + 4$  has simple zeroes at  $B, C, F$  and a triple pole at  $\infty$

Near  $\infty$ ,  $z = \frac{1}{x}$ ;  $f(x) = f(\frac{1}{z}) = \frac{1}{z^3} + \frac{3}{z^2} + \frac{6}{z} + 4 = \frac{1+3z+6z^2+4z^3}{z^3}$  so  $f$  has a triple pole at  $z=0$  (i.e. at  $x = \infty$ ).

The divisor of  $f(x)$  is  $B+C+F-3\infty =: \text{Div}(f)$  (Sometimes abbreviated  $(f)$ ).



More complicated:  $f(x) = \frac{(x-1)^2(x+3)^4(x+5)}{(x+2)(x+1)^3}$

$\text{Div}(f) = 2B + 4E + C - F - 3G - 3\infty$



$z = \frac{1}{x}$

$f(x) = f\left(\frac{1}{z}\right) = \frac{\left(\frac{1}{z}-1\right)^2\left(\frac{1}{z}+3\right)^4\left(\frac{1}{z}+5\right)}{\left(\frac{1}{z}+2\right)\left(\frac{1}{z}+1\right)^3} \cdot \frac{z^7}{z^7} = \frac{(1-z)^2(1+3z)^4(1+5z)}{(1+2z)(1+z)^3 \cdot z^3}$

triple pole at  $z=0$  (ie. at  $x=\infty$ )

The degree of  $D = \sum_i m_i P_i$  is  $\deg D = \sum_i m_i$ , ( $m_i \in \mathbb{Z}$ )

For any  $f(x) \in F(x)$ ,  $\deg(\text{Div } f) = 0$ . (equally many poles as zeroes)

Given a divisor  $D = \sum_i m_i P_i - \sum_j n_j Q_j$  ( $m_i, n_j \geq 1$ ),

we consider the vector space  $\mathcal{L}(D) = \{f(x) \in F(x) : f \text{ has a zero of multiplicity at least } m_i \text{ at } P_i, f \text{ has a pole of order at most } n_j \text{ at } Q_j, \text{ and possibly other zeroes but no other poles}\}$

In the case of  $P \cdot F = F \cup \{\infty\}$ , consider  $D = k \cdot \infty$ ,  $\deg D = k$ .

$\mathcal{L}(k \cdot \infty) = \{f(x) \in F(x) : f \text{ has a pole of order at most } k \text{ at } \infty; \text{ no other poles}\}$

$\dim \mathcal{L}(k \cdot \infty) = k+1$ .  $\mathcal{L}(D) = \{f : \text{Div } f + D \geq 0\}$  (there can be as many zeroes as you like)

$\mathcal{L}(-k \cdot \infty) = \{\text{polynomials in } x \text{ of degree at most } k\} = \{a_0 + a_1 x + a_2 x^2 + \dots + a_k x^k : a_i \in F\}$

has basis  $\{1, x, x^2, \dots, x^k\}$ .

The Riemann-Roch theorem gives a relation for determining  $l(D) = \dim \mathcal{L}(D)$ .

$l(D) - l(K-D) = \deg D - g + 1$  where  $K$  is a "canonical divisor"

non-negative integers

$l(D) \geq \deg D - g + 1$  is Riemann's bound

The genus of a smooth curve  $X$  is the dimension  $g = \dim \Omega_X$  where  $\Omega_X$  is the vector space of <sup>(globally smooth)</sup> differential 1-forms on  $X$ .

eg.  $X =$  projective line  $P^1 F$  over  $F$ ,  $P^1 F = F \cup \{\infty\}$

A 1-form has the <sup>(shape)</sup> form  $\omega = f(x) dx = f(\frac{x}{y}) d(\frac{x}{y}) = -\frac{f(\frac{x}{y}) dy}{y^2}$ .

$$y = \frac{1}{x}, \quad x = \frac{1}{y}$$

$$\frac{d(\frac{1}{y})}{dy} = -\frac{1}{y^2}$$

$$d(\frac{1}{y}) = -\frac{dy}{y^2}$$

On  $P^1 F$  there is no (nonzero) global 1-form

If  $f(x)$  is a poly of degree  $k$  in  $x$  then it has a pole of order  $k$  at  $\infty$  (and  $k$  zeroes in  $F$ ).

So  $\omega = f(x) dx$  has a pole of order  $k+2$  at  $\infty$ .

$\frac{1}{x^2} dx$  has no pole at  $\infty$  but it has a double pole at the origin.

$$= -y^2 \frac{dy}{y^2} = -dy$$

$\text{Div } \omega = \sum (\text{zeros of } \omega) - \sum (\text{poles of } \omega)$  the divisor of  $\omega$

For  $\omega$  a 1-form on  $P^1 F$ ,  $\deg(\omega) = -2$  (2 more poles than divisors, counting multiplicity).

$$\Omega_{P^1 F} = \{0\}, \quad g = \dim \Omega_{P^1 F} = 0.$$

For an elliptic curve e.g. the curve  $X: y^2 = x^3 - x$  has  $\Omega_X = \text{span}\{\omega\}$

$$g = \dim \Omega_X = 1.$$

First, why is  $X$  a smooth cubic curve?

$$X: f = y^2 - x^3 + x = 0$$

$$Df = (1-3x^2, 2y)$$

$$\begin{matrix} \uparrow \\ \text{P}^1 F \end{matrix} \quad \begin{matrix} \text{P} \\ \text{f} = 0 \end{matrix}$$

$$\begin{cases} 1-3x^2 = 0 \\ 2y = 0 \\ y^2 - x^3 + x = 0 \end{cases}$$

has no solutions.

( $\omega$  is a global smooth 1-form)

$y^2 = x^3$  is singular at  $(0,0)$

$$f(x,y) = y^2 - x^3$$

$$Df = \left( \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right) = (-3x^2, 2y)$$

$y^2 = x^3 - x$  points  $(x, y, 1)$  of a cubic curve with  $z \neq 0$ .

$y^2 z = x^3 - x z^2$  points  $(x, y, z)$  in homogeneous coords

If  $z=0$ :  $x=0$ ,  $y=1$

Near this point,  $y \neq 0$ , divide by  $y$  to get  $z = x^3$ .

$$f = y^2 x^3 + x = 0$$

$$y^2 = x^3 - x$$

$$dy^2 = d(x^3 - x)$$

$$2y dy = (3x^2 - 1) dx$$

$$\omega = \frac{dy}{3x^2 - 1} = \frac{dx}{2y}$$

This equation  $\frac{dy}{3x^2 - 1} = \frac{dx}{2y}$  is preserved under scalar multiples  $(x, y) \mapsto (\lambda x, \lambda y)$  ( $\lambda \neq 0$ )

$$(x, y, z) \mapsto \left(\frac{x}{y}, 1, \frac{z}{y}\right)$$

$$\frac{y^2 z}{y^3} = \frac{x^3 - x z^2}{y^3}$$

$$z' = (x')^3 - x'(z')^2$$

$y = x^2 - xy^2$   
 $(0, 0)$  is a smooth point.