Codes from Polynomials over Finite Fields

Nathan Kaplan

University of California, Irvine
Joint Mathematics Meetings 2021

January 7, 2021

I. What is Coding Theory All About?

MAA Invited Paper Session on Coding Theory and Geometry

- **Friday January 8, 2021, 1:00 p.m.-3:50 p.m.**
  MAA Invited Paper Session on Coding Theory and Geometry
  Organizers:
  Nathan Kaplan, University of California Irvine nckaplan@math.uci.edu
  - 1:00 p.m.
    Applications of finite geometries in coding theory.
    Christine A Kelley*, University of Nebraska-Lincoln
    Michelle Haver, University of Nebraska-Lincoln
    (1163-AI-1443)
  - 1:30 p.m.
    Locally Recoverable Codes with Many Recovery Sets from Number Theory and Geometry.
    Beth Malmskog*, Colorado College
    Kathryn Haymaker, Villanova University
    Gretchen Matthews, Virginia Tech
    (1163-AI-1084)
  - 2:00 p.m.
    Locally Correctable Codes and the Sylvester-Gallai theorem.
    Zeev Dvir*, Princeton University
    (1163-AI-928)
  - 2:30 p.m.
    Some recent results on high rate local codes.
    Shubhangi Saraf*, Rutgers University
    (1163-AI-1672)
  - 3:00 p.m.
    Equiangular lines and spectral graph theory.
    Zilin Jiang, MIT
    Jonathan Tidor, MIT
    Yuan Yao, MIT
    Shengtong Zhang, MIT
    Yufei Zhao*, MIT
    (1163-AI-290)
  - 3:30 p.m.
    Toward classifying multipoint codes.
    Gretchen Matthews*, Virginia Tech
    (1163-AI-1177)

Communication over a Noisy Channel

Suppose we want to communicate over a noisy channel.

I will send you a message: 0 or a 1.

- If I send 0, there is a 90% chance you receive 0.
- If I send 1, there is a 90% chance you receive 1.

Idea: Instead of sending 0 or 1, I will send 000 or 111.

◦ If you receive 010, you 'decode' as 000 because it is likelier that I sent 000 and that there was 1 error than it is that I sent 111 and there were 2 errors.

- If I send 0 or 1, there is a 90% chance you receive the correct message.
- If I send 000 or 111, you receive the correct message with probability

$$(.9)^3 + \binom{3}{1}(.9)^2(.1) = .972.$$

There is a cost for this increased reliability– have to send 3 bits instead of 1.

Major Question

How do we efficiently build redundancy into our set of messages so that we can identify and correct errors?

Coding Theory Basics I

Let $\mathbb{F}_q$ be a finite field of size q.

Definition

- *A code over $\mathbb{F}_q$ of length n is a subset $C \subseteq \mathbb{F}_q^n$.*
- *C is a linear code if it is a linear subspace of $\mathbb{F}_q^n$.*
  That is, if $c_1, c_2 \in C$ then $c_1 + c_2 \in C$ and $\alpha c_1 \in C$ for any $\alpha \in \mathbb{F}_q$.
- *For $\substack{x=(x_1,\ldots,x_n) \\ y=(y_1,\ldots,y_n)} \in \mathbb{F}_q^n$, the Hamming distance between x and y is*

$$d(x, y) = \#\{i \mid x_i \neq y_i\}.$$

- *The Hamming weight of x is $\mathrm{wt}(x) = d(x, \mathbf{0}) = \#\{i \mid x_i \neq 0\}$.*

Example

$\{(0,0,0),(1,1,1)\} \subset \mathbb{F}_2^3$ is a 1-dimensional linear code.

$$d((0,0,0),(1,1,1)) = 3.$$

Coding Theory Basics II

Definition

The *minimum distance* *of a code* C *is*

$$d(C) = \min_{\substack{x,y \in C \\ x \neq y}} d(x,y).$$

○ If C is linear, $d(C)$ is the minimum weight of a nonzero $c \in C$.

$$d(x,y) = d(x-y, y-y) = \mathrm{wt}(x-y)$$

○ In a code with minimum distance d, can correct up to $t = \lfloor \frac{d-1}{2} \rfloor$ errors.

Example

$C = \{(0,0,0),(1,1,1)\} \subset \mathbb{F}_2^3$ has $d(C) = 3$.
You can correct up to $t = \lfloor \frac{3-1}{2} \rfloor = 1$ error.

Main Problem in Combinatorial Coding Theory

We want codes $C \subseteq \mathbb{F}_q^n$ of **large size** and **large minimum distance**.

Definition

Let $A_q(n, d)$ be the maximum size of a code $C \subseteq \mathbb{F}_q^n$ that has minimum distance at least d.

Main Problem in Combinatorial Coding Theory:
Compute values of $A_q(n, d)$.

On the Size of Optimal Three-Error-Correcting Binary Codes of Length 16

Patric R. J. Östergård

***Abstract*—Let $A(n, d)$ denote the maximum size of a binary code with length n and minimum distance d. It has been known for decades that $A(16, 7) = A(17, 8) = 36$ or 37, that is, that the size of optimal 3-error-correcting binary codes of length 16 is either 36 or 37. By a recursive classification via subcodes and a clique search in the final stage, it is shown that the size of optimal such codes is 36.**

attaining the lower bound have been constructed in [13], [14] (see also [10, pp. 57,58]) and the upper bound is from [3]. The problem of determining this particular value is also mentioned in [8, Research Problem 7.18]. The main result of this work is that the best known lower bound is the exact value: $A(17, 8) = 36$.

Tables for $A_2(n, d)$

[Östergård, 2011]: $A_2(17, 8) = 36$.

	d=4	d=6	d=8	d=10	d=12	d=14	d=16
6	4	2	1	1	1	1	1
7	8	2	1	1	1	1	1
8	16	2	2	1	1	1	1
9	20	4	2	1	1	1	1
10	40	6	2	2	1	1	1
11	72	12	2	2	1	1	1
12	144	24	4	2	2	1	1
13	256	32	4	2	2	1	1
14	512	64	8	2	2	2	1
15	1024	128	16	4	2	2	1
16	2048	256	32	4	2	2	2
17	2816-3276	258-340	36	6	2	2	2
18	5632-6552	512-673	64	10	4	2	2
19	10496-13104	1024-1237	128	20	4	2	2
20	20480-26168	2048-2279	256	40	6	2	2
21	40960-43688	2560-4096	512	42-47	8	4	2
22	81920-87333	4096-6941	1024	64-84	12	4	2
23	163840-172361	8192-13674	2048	80-150	24	4	2
24	327680-344308	16384-24106	4096	136-268	48	6	4
25	2^{19}-599184	17920-47538	4096-5421	192-466	52-55	8	4
26	2^{20}-1198368	32768-84260	4104-9275	384-836	64-96	14	4
27	2^{21}-2396736	65536-157285	8192-17099	512-1585	128-169	28	6
28	2^{22}-4792950	131072-291269	16384-32151	1024-2817	178-288	56	8

Figure: Brouwer's tables of upper and lower bounds for $A_2(n, d)$

What is $A_2(17, 6)$?

Bounds on the minimum distance of linear codes over GF(2)

length:	$1 \le n \le 256$
dimension:	$1 \le k \le 256$
Constructions for marked entries are missing	

n/k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1															
2	2	1														
3	3	2	1													
4	4	2	2	1												
5	5	3	2	2	1											
6	6	4	3	2	2	1										
7	7	4	4	3	2	2	1									
8	8	5	4	4	2	2	2	1								
9	9	6	4	4	3	2	2	2	1							
10	10	6	5	4	4	3	2	2	2	1						
n/k	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
11	11	7	6	5	4	4	3	2	2	2	1					
12	12	8	6	6	4	4	4	3	2	2	2	1				
13	13	8	7	6	5	4	4	4	3	2	2	2	1			
14	14	9	8	7	6	5	4	4	4	3	2	2	2	1		
15	15	10	8	8	7	6	5	4	4	4	3	2	2	2	1	
16	16	10	8	8	8	6	6	5	4	4	4	2	2	2	2	1
17	17	11	9	8	8	7	6	6	5	4	4	3	2	2	2	2
18	18	12	10	8	8	8	7	6	6	4	4	4	3	2	2	2
19	19	12	10	9	8	8	8	7	6	5	4	4	4	3	2	2
20	20	13	11	10	9	8	8	8	7	6	5	4	4	4	3	2
n/k	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
21	21	14	12	10	10	8	8	8	8	7	6	5	4	4	4	3
22	22	14	12	11	10	9	8	8	8	8	7	6	5	4	4	4
23	23	15	12	12	11	10	9	8	8	8	8	7	6	5	4	4
24	24	16	13	12	12	10	10	8	8	8	8	8	6	6	4	4
25	25	16	14	12	12	11	10	9	8	8	8	8	6	6	5	4
26	26	17	14	13	12	12	11	10	9	8	8	8	7	6	6	5
27	27	18	15	14	13	12	12	10	10	9	8	8	8	7	6	6
28	28	18	16	14	14	12	12	11	10	10	8	8	8	8	6	6
29	29	19	16	15	14	13	12	12	11	10	9	8	8	8	7	6
30	30	20	16	16	15	14	12	12	12	11	10	9	8	8	8	7
n/k	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
31	31	20	17	16	16	15	13	12	12	12	11	10	9	8	8	8
32	32	21	18	16	16	16	14	13	12	12	12	10	10	8-9	8	8
33	33	22	18	16	16	16	14	14	12	12	12	11	10	9-10	8-9	8
34	34	22	19	17	16	16	15	14	13	12	12	12	10	10	9-10	8-9
35	35	23	20	18	16	16	16	15	14	12-13	12	12	11	10	10	9-10
36	36	24	20	18	17	16	16	16	14	13-14	12-13	12	12	11	10	10

II. Reed-Solomon Codes

MDS Codes

Proposition (Singleton Bound)

$$A_q(n,d) \leq q^{n-(d-1)}$$

Proof.

1. Let $C \subseteq \mathbb{F}_q^n$ have $|C| = A_q(n,d)$ and $d(C) \geq d$.
2. Write down all the $A_q(n,d)$ codewords.
3. Choose any $d-1$ coordinates and erase them.
4. Get $A_q(n,d)$ **distinct** elements of $\mathbb{F}_q^{n-(d-1)}$.

□

Definition

A code for which equality holds, $|C| = q^{n-(d-1)}$ is called Maximum Distance Separable or MDS.

Reed-Solomon Codes

Let $p_1, p_2, \ldots, p_q$ be an ordering of the elements of $\mathbb{F}_q$.
Let V_d be the vector space of polynomials in $\mathbb{F}_q[x]$ of degree at most d.

Definition

The evaluation map is defined by

$$\begin{aligned} \mathrm{ev}\colon \quad V_d &\mapsto \mathbb{F}_q^q \\ \mathrm{ev}(f) &= (f(p_1), \ldots, f(p_q)) \in \mathbb{F}_q^q. \end{aligned}$$

- $\mathrm{ev}(f+g) = \mathrm{ev}(f) + \mathrm{ev}(g)$ and $\mathrm{ev}(\alpha f) = \alpha\, \mathrm{ev}(f)$.
  The image $\mathrm{ev}(V_d) \subseteq \mathbb{F}_q^q$ is a linear code.

  It is the Reed-Solomon code of length q and order d, $\mathrm{RS}(q, d)$.
- As long as there is no nonzero polynomial vanishing at every element of $\mathbb{F}_q$, this map is injective, and $\dim(\mathrm{RS}(q,d)) = \dim(V_d) = d + 1$.

  $x^q - x$ vanishes at every element of $\mathbb{F}_q$, so suppose $q > d$.

Reed-Solomon Codes are MDS

Proposition

Let F be a field.
A nonzero $f \in F[x]$ with $\deg(f) = d$ has at most d distinct roots in F.

- Suppose $f, g \in \mathbb{F}_q[x]$ each have degree at most d.
  Then $f - g$ is either 0 or has at most d roots in $\mathbb{F}_q$.
- Conclude that $d(\mathrm{RS}(q,d)) = q - d$.
- $|\mathrm{RS}(q,d)| = q^{d+1} = q^{q-(d(\mathrm{RS}(q,d))-1)}$.
- Therefore, RS(q,d) is an MDS code.

Main Conjecture for MDS Codes

Definition

Let $M(k,q)$ be the maximum n such that a k-dimensional linear MDS code $C \subseteq \mathbb{F}_q^n$ exists.

Conjecture (Main Conjecture for MDS Codes)

1. *If $q \leq k$, $M(k,q) = k+1$. (Easy: Suppose now that $q > k$.)*
2. *If q is even and $k = 3$ or $k = q-1$, then $M(k,q) = q+2$.*
3. *Otherwise, $M(k,q) = q+1$.*

Reed-Solomon Example: For $q > d$, $M(d+1,q) \geq q$.

Reed-Solomon Code: Example

- Let $q = 5$, $d = 2$. Consider $\mathrm{RS}(5,2) \subseteq \mathbb{F}_5^5$.
- Choose a basis for polynomials in $\mathbb{F}_5[x]$ of degree at most 2: $1, x, x^2$.
- $\mathrm{RS}(5,2)$ is the row span of the generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \end{pmatrix}$$

- No nonzero linear combination of rows has 0s in 3 or more coordinates.
- No 3×3 submatrix has determinant 0.

Question

- *Can we add another column to to get a 3×6 matrix over $\mathbb{F}_5$ such that no 3×3 submatrix has determinant 0?*
- *Is there a 3-dimensional MDS code $C \subseteq \mathbb{F}_5^6$ that gives $\mathrm{RS}(5,2)$ if you puncture in the last coordinate?*

Doubly Extended (Projective) Reed-Solomon Codes

Let

$$f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$$

where each $a_i \in \mathbb{F}_q$.

Consider the map

$$\begin{aligned} \mathrm{ev}' : \quad V_d & \mapsto \mathbb{F}_q^{q+1} \\ \mathrm{ev}'(f) = & \ (f(p_1), \ldots, f(p_q), a_d) \,. \end{aligned}$$

- The image is a linear subspace of $\mathbb{F}_q^{q+1}$.
- If $q > d$ this map is injective and the dimension is $d+1$.
- The image is an MDS code.
  If f, g have the same x^d coefficient, then $\deg(f-g) \leq d-1$ and either $f - g = 0$ or $f - g$ has at most $d-1$ roots in $\mathbb{F}_q$.
- This is a Doubly Extended or Projective Reed-Solomon code.

Reed-Solomon Code: Example 2

- Let $q = 5, \; d = 2$. The doubly extended Reed-Solomon code is the row span of the generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 1 & 4 & 4 & 1 & 1 \end{pmatrix}$$

- No nonzero linear combination of rows has 0s in 3 or more coordinates.
- No 3×3 submatrix has determinant 0.
- This is a 3-dimensional MDS code $C \subset \mathbb{F}_5^6$.
- There is no 3-dimensional MDS code $C \subset \mathbb{F}_5^7$.
- $M(3, 5) = 6$.

1. A k-dimensional linear code $C \subseteq \mathbb{F}_q^n$ is the row span of a $k \times n$ generator matrix G.
2. C is an MDS code if and only if every nonzero linear combination of the rows of G has at most $k-1$ coordinates equal to 0.
3. Equivalently, no $k \times k$ submatrix of G has determinant 0.

- $M(k,q)$ is the maximum n such that a k-dimensional linear MDS code $C \subseteq \mathbb{F}_q^n$ exists.
- $M(k,q)$ is the maximum n for which there exists a $k \times n$ matrix with entries in $\mathbb{F}_q$ such that no $k \times k$ submatrix has determinant 0.

Main Conjecture for MDS Codes III

Definition

Let $M(k, q)$ be the maximum n such that a k-dimensional linear MDS code $C \subset \mathbb{F}_q^n$ exists.

Conjecture (Main Conjecture for MDS Codes)

1. *If $q \leq k$, $M(k, q) = k + 1$. (Easy: Suppose now that $q > k$.)*
2. *If q is even and $k = 3$ or $k = q - 1$, then $M(k, q) = q + 2$.*
3. *Otherwise, $M(k, q) = q + 1$.*

Doubly Extended Reed-Solomon codes give $M(d + 1, q) \geq q + 1$.
Ball: True for q prime.
Nathan's Favorite Matrix: 5-dimensional MDS code $C \subseteq \mathbb{F}_9^{10}$ that does not 'come from' a Reed-Solomon code [Glynn].

III. Projective Reed-Muller Codes

More Variables: Reed-Muller Codes

Definition

- *Choose an ordering of the points of* $\mathbb{F}_q^n : \; p_1, \ldots, p_{q^n}$.
- *Let* $V_{n,d}$ *be the* $\binom{n+d}{d}$*-dimensional vector space of polynomials in* $x_1, \ldots, x_n$ *of degree at most* d.
- *The evaluation map is defined by*

$$\begin{aligned} \mathrm{ev}: \quad V_{n,d} \quad &\mapsto \quad \mathbb{F}_q^{q^n} \\ \mathrm{ev}(f) = \quad &(f(p_1), \ldots, f(p_{q^n})) \in \mathbb{F}_q^{q^n} \end{aligned}$$

- *The image is a linear code.*
- *As long as there is no degree* d *polynomial vanishing at every element of* $\mathbb{F}_q^n$*, which is true for* $q > d$*, this map is injective and the image* $\mathrm{RM}_q(d, n)$ *had dimension* $\binom{n+d}{d}$.
- *Note that* $\mathrm{RM}_q(d, 1) = \mathrm{RS}(q, d)$.

Question

- *What is the minimum distance of* $\mathrm{RM}_q(d, n)$*?*
- *What is the maximum number of zeros of a polynomial of degree at most* d *in* $\mathbb{F}_q[x_1, \ldots, x_n]$*?*

- Let $\alpha_1, \ldots, \alpha_d$ be distinct elements of $\mathbb{F}_q$.

$$f(x_1, \ldots, x_n) = (x_1 - \alpha_1)(x_1 - \alpha_2) \cdots (x_1 - \alpha_d)$$

vanishes at $d \cdot q^{n-1}$ elements of $\mathbb{F}_q^n$.

- $d(\mathrm{RM}_q(d, n)) = q^n - dq^{n-1} = (q - d)q^{n-1}$.

For $n > 1$, these codes are very far from being MDS.

IV. Weight Enumerators of Reed-Muller Codes

The Hamming Weight Enumerator of a Code

Definition

The *Hamming weight enumerator* *of* $C \subseteq \mathbb{F}_q^n$ *is*

$$W_C(X, Y) = \sum_{c \in C} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i \cdot X^{n-i} Y^i,$$

where $A_i = \#\{c \in C \mid \mathrm{wt}(c) = i\}.$

Example

For $C = \{(0,0,0),(1,1,1)\} \subset \mathbb{F}_2^3$, $\quad W_C(X, Y) = X^3 + Y^3.$

Question

- *What is the weight enumerator of the Reed-Solomon code* $\mathrm{RS}(q, d)$*?*
- *How many* $f \in \mathbb{F}_q[x]$ *of degree at most* d *have exactly* m *distinct roots in* $\mathbb{F}_q$*?*

◦ **Fact**: The weight enumerator of a k-dimensional MDS code $C \subseteq \mathbb{F}_q^n$ is determined by its parameters.

- Computing the weight enumerator of $\mathrm{RM}_q(1, n)$ is easy.
- Computing the weight enumerator of $\mathrm{RM}_q(2, n)$ is a counting problem about quadratic forms over finite fields.

Proposition

We have that $W_{\mathrm{RM}_q(2,2)}(X, Y)$ *is equal to*

$$X^{q^2} + \frac{(q-1)(q^3-q+2)}{2} Y^{q^2} + \frac{(q-1)^2 q^3}{2} X Y^{q^2-1}$$
$$+ \frac{(q-1)^2 q^3 (q+1)}{2} X^{q-1} Y^{q^2-q+1} + (q^3-q)(q^2-q+2) X^q Y^{q^2-q}$$
$$+ \frac{(q-1)^3 q^3}{2} X^{q+1} Y^{q^2-q-1} + \frac{(q-1)(q+1)q^3}{2} X^{2q-1} Y^{q^2-2q+1}$$
$$+ \frac{q(q+1)(q-1)^2}{2} X^{2q} Y^{q^2-2q}.$$

Reed-Muller Codes from Cubic Curves

Question

1. *How many $f_3 \in \mathbb{F}_q[x, y]$ of degree at most 3 have exactly m zeros?*
2. *How many smooth cubic curves $\{f_3(x, y) = 0\}$ have exactly m $\mathbb{F}_q$-rational points?*

A smooth cubic curve with an $\mathbb{F}_q$-rational point defines an elliptic curve.

Question

1. *How many isomorphism classes of elliptic curves $E/\mathbb{F}_q$ have a given number of $\mathbb{F}_q$-points?*
2. *For how many $a, b \in \mathbb{F}_q$ does the equation $y^2 = x^3 + ax + b$ have exactly m solutions $(x, y) \in \mathbb{F}_q^2$?*

Deuring, Waterhouse: Answer involves class numbers of orders in imaginary quadratic fields.

Put this together and get $W_{\mathrm{RM}_q(3,2)}(X, Y)$.

Question

1. *How many* $f_4 \in \mathbb{F}_q[x, y]$ *of degree at most 4 have exactly m zeros?*
2. *How many smooth quartic curves* $\{f_4(x, y) = 0\}$ *have exactly m* $\mathbb{F}_q$*-rational points?*
3. *What is the maximum number of* $\mathbb{F}_q$*-points of a smooth quartic curve* $\{f_4(x, y) = 0\}$*?*

Question

Can we say statistical things about the coefficients of $W_{\mathrm{RM}_q(2,4)}(X, Y)$*?*

The coefficients of $W_{\mathrm{RM}_q(2,3)}(X, Y)$ have a symmetry that the coefficients of $W_{\mathrm{RM}_q(2,4)}(X, Y)$ no longer have...

Definition

Let $N_q(t)$ be the number of $\mathbb{F}_q$-isomorphism classes of smooth (projective) plane quartics with $\#C(\mathbb{F}_q) = q + 1 - t$, each class weighted by $\frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(C)}$.

For $0 \leq t \leq 6\sqrt{q}$, let

$$\mathcal{V}_q(t) := N_q(t) - N_q(-t).$$

Not true that $N_q(t)$ must equal $N_q(-t)$.

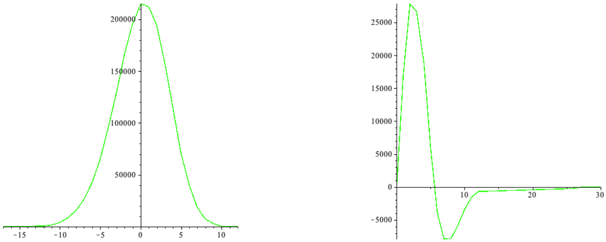


Figure: Graphs of $N_{11}(t)$ and $\mathcal{V}_{11}(t)$

See work of Lercier, Ritzenthaler, Rovetta, Sijsling, and Smith.

The Dual Code of a Linear Code

Definition

1. *For* $\substack{x=(x_1,\ldots,x_n)\\ y=(y_1,\ldots,y_n)} \in \mathbb{F}_q^n$ *let* $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$.
2. *For a linear code* $C \subseteq \mathbb{F}_q^n$*, the* *dual code* *is defined by*

$$C^{\perp} = \left\{ y \in \mathbb{F}_q^n \mid \langle x, y\rangle = 0 \ \forall x \in C \right\}.$$

Example

Let $C = \{(0,\ldots,0),(1,\ldots,1)\} \subset \mathbb{F}_2^n$.
Then $C^{\perp} = \{y \in \mathbb{F}_2^n \mid \text{wt}(y) \text{ is even}\}$.
We see that

$$W_C(X,Y) = X^n + Y^n,$$

and

$$W_{C^{\perp}}(X,Y) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} X^{n-2i} Y^{2i} = \frac{(X+Y)^n + (X-Y)^n}{2}.$$

Theorem (MacWilliams)

For a linear code $C \subseteq \mathbb{F}_q^n$

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C\left(X + (q-1)Y, X - Y\right).$$

◦ One way to prove this involves discrete Poisson summation.

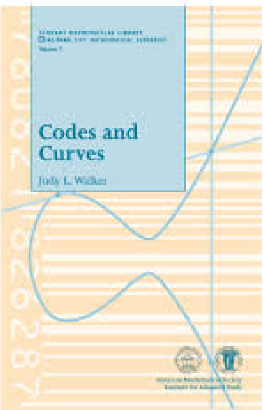
Idea: Study the weight enumerator of a code C by studying the weight enumerator of its dual code $C^\perp$.

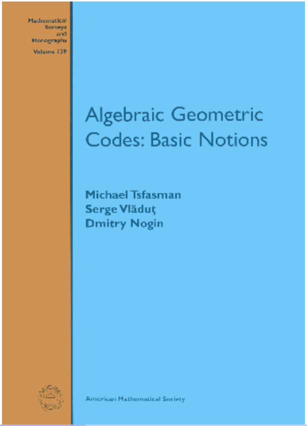
V. What else is there?

Algebraic Geometry Codes

Idea: Take a vector space of polynomials V. Get a code by evaluating elements of V at some subset of points of $\mathbb{F}_q^n$.

$\circ$ Number Theory $\rightarrow$ Coding Theory. Construct 'good codes' from Riemann-Roch spaces of divisors of algebraic curves with many $\mathbb{F}_q$-points.





Suppose you have a good code $C \subseteq \mathbb{F}_q^n$.

Question

How do you construct an ***efficient*** *encoding/decoding scheme?*

Question

I send you a message. You receive something that is not in the code. How do you find the codeword closest to it?