CURVES AND CODES

by

John R. Kerl

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Arts

ARIZONA STATE UNIVERSITY
April 2005

Overview

- Coding Theory
- Algebraic Geometry (key: Riemann-Roch)
- Construction and Encoding (Goppa)
- Decoding (Skorobogatov-Vlăduț)
- Further Directions
- References

Coding Theory

Originates in the engineering problem of digital communication over noisy channels.

Work over $\mathbb{F}_q$: low-degree extensions of $\mathbb{F}_2$, say, $q \leq 256$.

Definition. A *block code* is a subset of $\mathbb{F}_q^n$. A *linear block code* is a subspace of $\mathbb{F}_q^n$.

Encode k-tuples (blocks) by embedding $\mathbb{F}_q^k$ into a k-dimensional subspace C of $\mathbb{F}_q^n$.

Encoding, Transmission, Decoding

- Message word $\boldsymbol{m} \in \mathbb{F}_q^k$.
- Code word $\boldsymbol{u} \in \mathbb{F}_q^n$: $\boldsymbol{u} = \boldsymbol{m}G$ (encoding).
- Error word $\boldsymbol{e} \in \mathbb{F}_q^n$ (transmission).
- Received word $\boldsymbol{v} \in \mathbb{F}_q^n$: $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{e}$.
- Estimated error word $\widehat{\boldsymbol{e}}$ (decoding).
- Estimated received word $\widehat{\boldsymbol{u}} = \boldsymbol{v} - \widehat{\boldsymbol{e}}$.
- Estimated message word $\widehat{\boldsymbol{m}}$: solve linear system $\widehat{\boldsymbol{m}}G = \widehat{\boldsymbol{u}}$.

The matrix G is called a *generator matrix*. There is a corresponding *parity-check matrix* H such that the following sequence is exact:

$$0 \quad \longrightarrow \quad \mathbb{F}_q^k \quad \stackrel{\cdot G}{\longrightarrow} \quad \mathbb{F}_q^n \quad \stackrel{H\cdot}{\longrightarrow} \quad \mathbb{F}_q^{n-k} \quad \longrightarrow \quad 0$$

Thus, $C = \mathrm{im}(G) = \ker(H)$. Compute rows of H from a kernel basis for G.

Perpendicular space:

$$C^\perp = \{\boldsymbol{v} \in \mathbb{F}_q^n : \boldsymbol{v} \cdot \boldsymbol{u} = 0 \text{ for all } \boldsymbol{u} \in C\}.$$

Dot product is *not* positive definite. Example: $(1, 0, 1)$ is self-perpendicular in $\mathbb{F}_2^3$.

The G, H for C are the same as the H, G for $C^\perp$.

Hamming weight: $\mathsf{wt} : \mathbb{F}_q^n \to \mathbb{Z}$ by

$$\mathsf{wt}(\boldsymbol{u}) = \#\{u_i : u_i \neq 0\}.$$

This is a vector-space norm.

Hamming distance: $\mathsf{dist} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{Z}$ by

$$\mathsf{dist}(\boldsymbol{u}, \boldsymbol{v}) = \mathsf{wt}(\boldsymbol{u} - \boldsymbol{v}).$$

Minimum distance:

$$d(C) = \min\{\mathsf{dist}(\boldsymbol{u}, \boldsymbol{v}) : \boldsymbol{u}, \boldsymbol{v} \in C; \boldsymbol{u} \neq \boldsymbol{v}\}$$

For a linear code, all differences are in the subspace, so

$$d(C) = \min\{\mathsf{wt}(\boldsymbol{u}) : \boldsymbol{u} \in C; \boldsymbol{u} \neq \boldsymbol{0}\}$$

Code parameters: length n, dimension k, minimum distance d, alphabet size q. A linear block code is described as an $[n, k, d]_q$ code. Example: $[7, 3, 4]_2$.

One may think of k of the n symbols in each block as payload, and the remaining $n-k$ symbols as redundancy. Data rate: $R = k/n$.

The basic engineering problem: correct many errors at low transmission redudancy.

Maximum correctable errors per block: $\lfloor \frac{d-1}{2} \rfloor$.

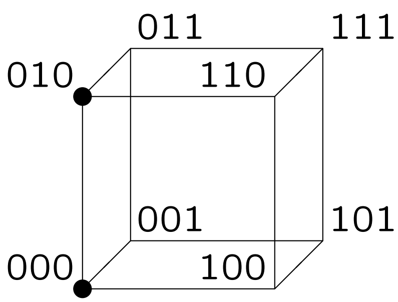
Mathematical problem statement for linear block codes: construct subspaces maximizing d, maximizing k, and/or minimizing n.

Subspace packings:

$\mathbb{F}_2$

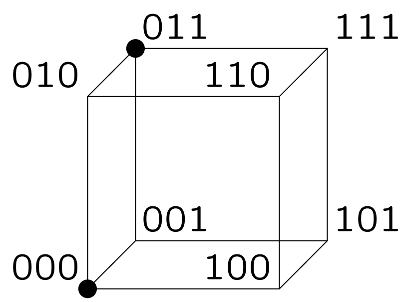
$\mathbb{F}_2$ inside $\mathbb{F}_2^3$

$d = 1$



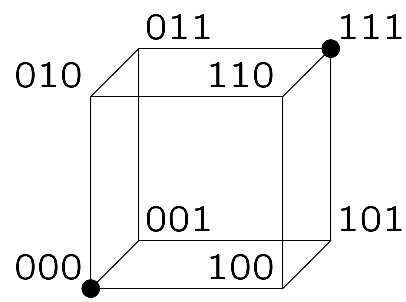
$\mathbb{F}_2$ inside $\mathbb{F}_2^3$

$d = 2$

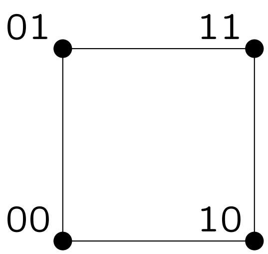


$\mathbb{F}_2$ inside $\mathbb{F}_2^3$

$d = 3$

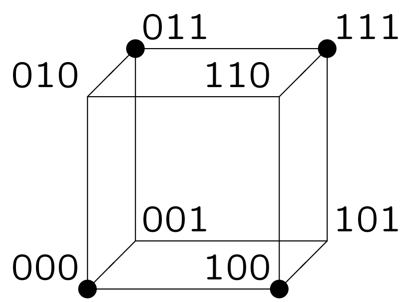


$\mathbb{F}_2^2$



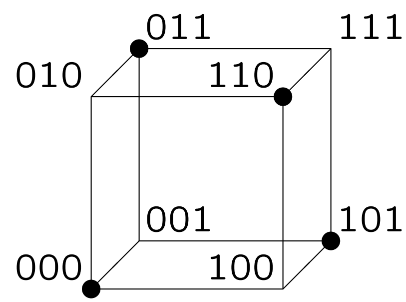
$\mathbb{F}_2^2$ inside $\mathbb{F}_2^3$

$d = 1$



$\mathbb{F}_2^2$ inside $\mathbb{F}_2^3$

$d = 2$



Algebraic Geometry

Consider *projective plane curves* V: points of $\mathbb{P}^2(\mathbb{F}_q)$ which are zeroes of a single homogeneous equation $\phi(X, Y, Z) \in K[X, Y, Z]$.

Restrict attention to *smooth curves*, i.e. ϕ and its partials simultaneously vanish nowhere.

Result: V smooth implies ϕ is absolutely irreducible.

Plücker formula for genus g: for smooth plane curves, with $d = \deg(\phi)$,

$$g = \frac{(d-1)(d-2)}{2}.$$

Let $I(V/K) = \langle\phi\rangle \in K[X, Y, Z]$. Coordinate ring:

$$K[V] = \frac{K[X, Y, Z]}{I(V/K)}.$$

Function field $K(V)$: quotient field of $K[V]$.

Divisor group: free abelian group on points of V, e.g. $D = \sum_{P\in V} n_P P$. *Support* of D: P such that $n_P \neq 0$. A divisor D is *effective*, written $D \succcurlyeq 0$, if $n_P \geq 0$ for all $P \in V$.

Intersection divisor of F:

$$\text{div}(F) = \sum n_P P - \sum n_Q Q$$

where P's are zeroes of F, Q's are poles of F, n_P's are zero multiplicities, n_Q's are pole orders.

Vector space associated to a divisor:

$$\mathcal{L}(D) = \{F \in K(V) : \mathrm{div}(F) + D \succcurlyeq 0\} \cup \{0\}.$$

Dimension over K: $\ell(D)$.

Key property of $\mathcal{L}(D)$: for all $F \in \mathcal{L}(D)$, poles are confined to the point(s) of D.

Theorem (Riemann-Roch). *If* $\deg(D) > 2g - 2$, *then*

$$\ell(D) = \deg(D) - g + 1.$$

Always:

$$\ell(D) \geq \deg(D) - g + 1.$$

Definition. If $\ell(rP) = \ell((r-1)P)$, r is a *Weierstrass gap* of P.

Results: A non-negative integer r is a non-gap of P iff there is an $F \in K(V)$ with a pole of order r in P, and poles at no other point of V. The number of gaps is g. By Riemann-Roch, gaps are at or below $2g-2$.

Proposition. *Let* $(\gamma_i : i \in \mathbb{Z}_+)$ *be an enumeration of the non-gaps of* P*, with* $0 = \gamma_1 < \gamma_2 < \ldots$*. Let* $F_i \in \mathcal{L}(\gamma_i P)$ *be such that* $\nu_P(F) = -\gamma_i$*. Then* $\{F_1 \ldots, F_r\}$ *is a basis for* $\mathcal{L}(\gamma_r P)$*.*

Find non-gaps by finding $g-1$ functions with distinct pole orders at rP, $0 \leq r \leq 2g-2$.

Klein quartic example: $X^3Y + Y^3Z + Z^3X = 0$. Label some points $P_1 = [1,0,0]$, $P_2 = [0,1,0]$, $P_3 = [0,0,1]$. Intersection divisors:

$$\begin{aligned}
\mathrm{div}(X) &= 3P_3 + P_2 \\
\mathrm{div}(Y) &= 3P_1 + P_3 \\
\mathrm{div}(Z) &= 3P_2 + P_1 \\
\mathrm{div}\left(\frac{X^iY^j}{Z^{i+j}}\right) &= (-i+2j)P_1 + (-2i-3j)P_2 + (3i+j)P_3.
\end{aligned}$$

Let $D = rP_2$. With $-i + 2j \geq 0$, poles are confined to P_2, and X^iY^j/Z^{i+j} span $\mathcal{L}(D)$.

The Klein quartic has degree 4, hence genus 3. There are 3 gaps, between 0 and $2g-2=4$.

r	i	j	$i+j$	F	$-i+2j$	$-2i-3j$	$3i+j$
0,1,2	0	0	0	1	0	0	0
3,4	0	1	1	Y/Z	2	-3	1
5	1	1	2	XY/Z^2	1	-5	4
6	0	2	2	Y^2/Z^2	4	-6	2
7	2	1	3	X^2Y/Z^3	0	-7	7
8	1	2	3	XY^2/Z^3	3	-8	5
9	0	3	3	Y^3/Z^3	6	-9	3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Since $g-1=2$ functions have been found with pole order between 0 and 4, namely, 0 and 3, gaps for the Klein quartic are at 1, 2, and 4.

Code Construction

Let V be a smooth projective plane curve defined over $\mathbb{F}_q$. Let $\boldsymbol{P} = (P_1, \ldots, P_n)$ be a vector of distinct $\mathbb{F}_q$-rational points of V. Let D be a divisor on V, with $0 < \deg(D) < n$, with support disjoint from $\boldsymbol{P}$. Thus all F in $\mathcal{L}(D)$ are pole-free on $\boldsymbol{P}$. Here, D is always a one-point divisor; $\boldsymbol{P}$ is most or all of the other points.

Definition. The *Goppa primary code* for $V, \boldsymbol{P}, D$ is

$$C_p(V, \boldsymbol{P}, D) = \{\boldsymbol{v} \in \mathbb{F}_q^n : F(\boldsymbol{P}) \cdot \boldsymbol{v} = 0 \text{ for all } F \in \mathcal{L}(D)\}.$$

Definition. The *Goppa dual code* for $V, \boldsymbol{P}, D$ is

$$C_d(V, \boldsymbol{P}, D) = \{F(\boldsymbol{P}) : F \in \mathcal{L}(D)\} = \varepsilon(\mathcal{L}(D))$$

where ε is the evaluation map $\varepsilon : F \mapsto F(\boldsymbol{P})$. Thus,

$$C_p = \{\boldsymbol{v} \in \mathbb{F}_q^n : \boldsymbol{u} \cdot \boldsymbol{v} = 0 \text{ for all } \boldsymbol{u} \in C_d\} = C_d^{\perp}.$$

Lemma. *If* $\deg(D) < 0$, *then* $\mathcal{L}(D) = \{0\}$.

Proof. Let F be non-zero in $K(V)$. From the zeroes-and-poles proposition, $\deg \operatorname{div}(F) = 0$. Thus

$$\begin{aligned} & \deg \operatorname{div}(F) + \deg(D) = \deg(\operatorname{div}(F) + D) < 0 \\ \Longrightarrow \quad & \operatorname{div}(F) + D \not\geq 0 \\ \Longrightarrow \quad & F \notin \mathcal{L}(D). \end{aligned}$$

$\square$

Theorem. *If* $\deg(D) > 2g-2$*, the dimension of* C_p *is* $n - \deg(D) + g - 1$.

Proof. Let $k = \dim(C_p)$. Then $\dim(C_p^\perp) = \dim(C_d) = n-k$. Prove that the latter is $\deg(D) - g + 1$. By Riemann-Roch, $\ell(D) = \deg D - g + 1$. Show ε is 1-1 since $C_d = \varepsilon(\mathcal{L}(D))$. Let $\varepsilon(F) = 0$ for some $F \in \mathcal{L}(D)$. Then all $F(P_j) = 0$, so all $n_{P_j} > 0$ in $\operatorname{div}(F)$. Since all $P_j \notin \operatorname{supp}(D)$, $\operatorname{div}(F) + D - P_1 - \ldots - P_n \succcurlyeq 0$. Since $\deg(D) < n$, $\deg(D - P_1 - \ldots - P_n) < 0$. By the lemma, $\mathcal{L}(D - P_1 - \ldots - P_n) = \{0\}$. $\square$

Theorem. *If* $\deg(D) > 2g-2$*, then* $d(C_p) \geq \deg(D) - 2g + 2$*.*

Proof. Show minimum weight since C_p is linear. Let $\boldsymbol{u}$ be of minimum weight $w > 0$. WLOG renumber P_j's and u_j's such that the first w of the u_j's are non-zero. Seeking a contradiction, suppose $w < \deg(D) - 2g + 2$. Let $D_w = D - P_1 - \ldots - P_w$ and $D_{w-1} = D - P_1 - \ldots - P_{w-1}$. Since $w < \deg(D) - 2g + 2$, $\deg(D) - w = \deg(D_w) > 2g - 2$ and thus $\deg(D_{w-1}) > 2g - 2$ as well. By Riemann-Roch, $\ell(D_w) = \deg(D) - w - g + 1$ and $\ell(D_{w-1}) = \deg(D) - w - g + 2$. Thus $\exists\ F \in \mathcal{L}(D_{w-1})$, $F \notin \mathcal{L}(D_w)$. This implies $F(P_j) = 0$ for $1 \leq j < w$, and $F(P_w) \neq 0$. Since $D_{w-1} \preccurlyeq D$, $F \in \mathcal{L}(D)$ and $F(\boldsymbol{P}) \cdot \boldsymbol{u} = F(P_w)u_w \neq 0$, contradicting $\boldsymbol{u} \in C_p$. $\square$

Encoding

Let $k = n - \ell(D)$. Let $\{F_1, \ldots, F_{n-k}\}$ be a basis for $\mathcal{L}(D)$. A G for C_d, hence an H for C_p, is $F_i(P_j)$.

Compute a kernel basis to get a G for C_p. Encode $\boldsymbol{m}G = \boldsymbol{u}$.

Decoding

Received word is $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{e}$. *Error location*: P_j such that $e_j \neq 0$. *Error locator*: $\lambda \in K(V)$ such that $\lambda(P_j) = 0$ for all error locations of $\boldsymbol{e}$, and pole-free on $\boldsymbol{P}$. *Minimum correctable error weight*: t.

Proposition. *Let A be a divisor on V with support disjoint from $\boldsymbol{P}$ such that $\ell(A) > t$. Then an error locator exists in $\mathcal{L}(A)$. (Here, $A \preccurlyeq D$, i.e. one-point divisor on the same point.)*

Proposition. *Let R be a divisor on V with support disjoint from $\boldsymbol{P}$ such that* $\deg(R) > t + 2g - 1$. *Then $\lambda \in K(V)$, pole-free on $\boldsymbol{P}$, locates $\boldsymbol{e}$ iff $(\rho\lambda)(\boldsymbol{P}) \cdot \boldsymbol{e} = 0$ for all $\rho \in \mathcal{L}(R)$.*

Proposition. *Let the* $\ell(R) \times \ell(A)$ *matrix* S *be given by* $S_{ij} = (\rho_i \lambda_j)(\boldsymbol{P}) \cdot \boldsymbol{e}$. *Then* $\lambda = \sum_{j=1}^{\ell(A)} c_j \lambda_j \in \mathcal{L}(A)$ *locates* $\boldsymbol{e}$ *iff* $\boldsymbol{c}$ *solves* $S\boldsymbol{c} = \mathbf{0}$.

Proposition. *Let* A *have support disjoint from* $\boldsymbol{P}$, $\ell(A) > t$, *and* $\deg(A) < \deg(D) - 2g + 2 - t$. *Let* $\lambda \in \mathcal{L}(A)$ *locate* $\boldsymbol{e}$. *Let* $\widehat{\boldsymbol{Z}}$, $\widehat{\boldsymbol{z}}$ *be* P_j*'s,* e_j*'s such that* $\lambda(P_j) = 0$. *Let* M *be a divisor of* V *with support disjoint from* $\boldsymbol{P}$ *such that* $\deg(M) > \deg(A) + 2g - 2$. *Let* $\mu_1, \ldots, \mu_{\ell(M)}$ *be a basis of* $\mathcal{L}(M)$. *Then* $\widehat{\boldsymbol{z}}$ *is uniquely determined by any error locator* $\lambda \in \mathcal{L}(A)$ *and the syndromes* $\mu(\boldsymbol{P}) \cdot \boldsymbol{v}$ *with respect to functions* $\mu \in \mathcal{L}(M)$. *Specifically,* $\widehat{\boldsymbol{z}}$ *is the unique solution of the system of equations*

$$\mu_i(\widehat{\boldsymbol{Z}}) \cdot \widehat{\boldsymbol{z}} = \mu_i(\boldsymbol{P}) \cdot \boldsymbol{v}$$

Remark. Take $R = D - A$, $M = D$.

Received word $\boldsymbol{v} = (*, *, *, *, *, *, *)$.

Solve homogeneous system $S\boldsymbol{c} = \mathbf{0}$ to get $\lambda = \sum c_j \lambda_j$.

Apply λ to $\boldsymbol{P}$: $(*, *, 0, *, 0, 0, *)$.

Error locations: $3, 5, 6$.

Solve inhomogenous system:

$$\begin{bmatrix} \mu_1(P_3) & \mu_1(P_5) & \mu_1(P_6) \\ \mu_2(P_3) & \mu_2(P_5) & \mu_2(P_6) \\ \mu_3(P_3) & \mu_3(P_5) & \mu_3(P_6) \\ \mu_4(P_3) & \mu_4(P_5) & \mu_4(P_6) \end{bmatrix} \begin{bmatrix} \widehat{z}_3 \\ \widehat{z}_5 \\ \widehat{z}_6 \end{bmatrix} = \begin{bmatrix} \mu_1(\boldsymbol{P}) \cdot \boldsymbol{v} \\ \mu_2(\boldsymbol{P}) \cdot \boldsymbol{v} \\ \mu_3(\boldsymbol{P}) \cdot \boldsymbol{v} \\ \mu_4(\boldsymbol{P}) \cdot \boldsymbol{v} \end{bmatrix}.$$

Error word: $(0, 0, \widehat{z}_3, 0, \widehat{z}_5, \widehat{z}_6, 0)$.

Further Directions

- Non-smooth curves, computation of genus.
- Error processing up to $\lfloor \frac{d-1}{2} \rfloor$ (Duursma).
- Higher-dimensional projective spaces are needed for high-quality codes.
- More efficient decoding algorithms.

References

MacWilliams, F.J. and Sloane, N.J.A. The Theory of Error-Correcting Codes. Elsevier Science B.V., 1997.

Silverman, J. The Arithmetic of Elliptic Curves. Springer-Verlag, 1986.

Goppa, V.D. (1977). *Codes associated with divisors*. Probl. Inform. Transmission, vol. 13, 22-26.

Skorobogatov, A.N. and Vlăduţ, S.G. *On the decoding of algebraic-geometric codes*. IEEE Trans. Inform. Theory, vol. 36, pp. 1051-1060, Nov. 1990.

Pretzel, O. Codes and Algebraic Curves. Oxford University Press, 1998.

Walker, J.L. Codes and Curves. American Mathematical Society, 2000.

Høholdt, T., van Lint, J.H., and Pellikaan, R. *Algebraic Geometry Codes*. Handbook of Coding Theory, vol. 1, pp. 871-961 (Pless, V.S., Huffman, W.C. and Brualdi, R.A. Eds.). Elsevier, Amsterdam, 1998.