Code Based Cryptography

Colloquium at Eastern Kentucky University

E. Martínez-Moro

imUVa Instituto de Investigación en Matemáticas

Universidad de Valladolid

Acknowledgements

Full papers: Two in Designs, Codes and Cryptography (also as preprints OWP 2012-01 at MFO) and one in Journal of Symbolic Computation. Coauthors: I. Márquez-Corbella, R. Pellikaan and D. Ruano.

The research reported in this paper was made possible by means of the "Research in Pairs" program of the MFO, the Mathematical Research Institute at Oberwolfach during the period January 24-February 5, 2011. We like to thank Stanislav Bulygin and Xin-Wen Wu for their valuable discussions on the topics of the papers.

Partially supported by Spanish MCINN under project MTM2007-64704. First author research is also supported by a FPU grant AP2008-01598 by Spanish MEC. Second author is also supported by Spanish MCINN under project MTM2010-21580-C02-02.

Outline

Acknowledgements

Introduction

Error-correcting codes

Cryptography
- McEliece's PKC
- Niederreiter PKC

Our attack

Projective systems and codes
- GRS codes and NRC
- AG codes

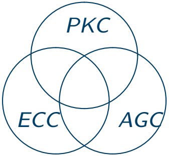
Sidelnikov-Shestakov I

AG, WAG and SAG codes

Retrieving the triple

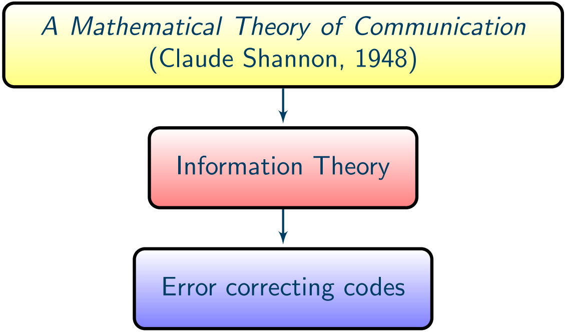
Curves defined by quadrics

Introduction



- ECC = Error-correcting codes
- AGC = Algebraic geometry curves
- PKC = Public-key cryptosystems

Error-correcting codes

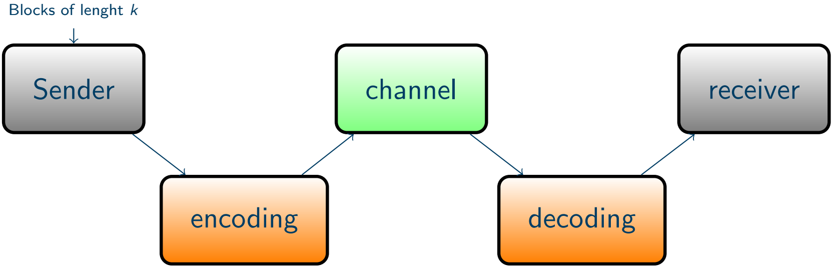


A Mathematical Theory of Communication
(Claude Shannon, 1948)

Information Theory

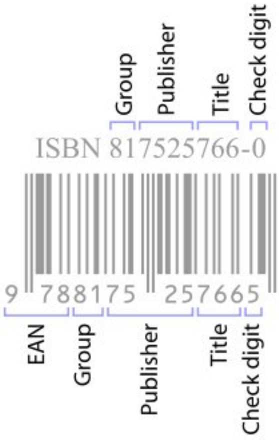
Error correcting codes

Error-correcting codes



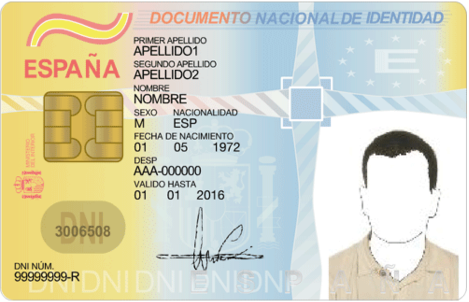
$$c: \quad \mathcal{A}^k \quad \longrightarrow \quad \mathcal{A}^n$$

Well known examples



$$(8{\cdot}1)+(1{\cdot}2)+(7{\cdot}3)+(5{\cdot}4)+(2{\cdot}5)+(7{\cdot}7)+(6{\cdot}8)+(6{\cdot}9)+(0{\cdot}10)=11{\cdot}\lambda$$

Well known examples



DOCUMENTO NACIONAL DE IDENTIDAD

ESPAÑA

PRIMER APELLIDO
APELLIDO1

SEGUNDO APELLIDO
APELLIDO2

NOMBRE
NOMBRE

SEXO M
NACIONALIDAD ESP

FECHA DE NACIMIENTO
01 05 1972

DESP
AAA-000000

VALIDO HASTA
01 01 2016

DNI
3006508

DNI NÚM.
99999999-R

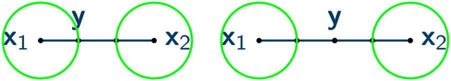
0	1	2	3	4	5	6	7	8	9	10	
T	R	W	A	G	M	Y	F	P	D	X	

11	12	13	14	15	16	17	18	19	20	21	22
B	N	J	Z	S	Q	V	H	L	C	K	E

Hamming distance

- **Hamming distance**: $\mathbf{x},\ \mathbf{y} \in \mathcal{A}^n$, $\mathrm{d}_H(\mathbf{x},\mathbf{y}) = |\{i \mid x_i \neq y_i\}|$.
- **Minimum distance of** $\mathcal{C} \subset \mathcal{A}^n$

$$d = \min\left\{\mathrm{d}_H(\mathbf{c}_1,\mathbf{c}_2) \mid \mathbf{c}_1,\ \mathbf{c}_2 \in \mathcal{C} \text{ and } \mathbf{c}_1 \neq \mathbf{c}_2\right\}.$$



$d = 3, 4$

Linear codes

$\mathcal{A} = \mathbb{F}_q$. A $[n, k]$ -linear code is just a $\mathbb{F}_q$-linear subspace of d $\mathbb{F}_q^n$ of dimension k. As usual, it can be given as a set of generators (the rows of a $k \times n$ generator matrix) or as the solutions of a system of homogeneous equations (the rows of a $(n-k) \times n$ parity check matrix).

It can be (easily) proven that $k \leq n - d + 1$ (Singleton bound). If equality holds the code is called MDS (maximum distance separable code).

Example : Reed-Solomon Codes. Let $a_1, \ldots, a_q$ all the elements in $\mathbb{F}_q$ and $f(X) \in \mathbb{F}_q[X]$. We can define a linear space as the image of a linear mapping $f(x) \mapsto (f(a_1), \ldots, f(a_q))$.

$$\{\ (f(a_1), \ldots, f(a_q)) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k\ \}$$

Linear codes

$\mathcal{A} = \mathbb{F}_q$. A $[n, k]$ -linear code is just a $\mathbb{F}_q$-linear subspace of d $\mathbb{F}_q^n$ of dimension k. As usual, it can be given as a set of generators (the rows of a $k \times n$ generator matrix) or as the solutions of a system of homogeneous equations (the rows of a $(n-k) \times n$ parity check matrix).

It can be (easily) proven that $k \leq n - d + 1$ (Singleton bound). If equality holds the code is called MDS (maximum distance separable code).

Example : Reed-Solomon Codes. Let $a_1, \ldots, a_q$ all the elements in $\mathbb{F}_q$ and $f(X) \in \mathbb{F}_q[X]$. We can define a linear space as the image of a linear mapping $f(x) \mapsto (f(a_1), \ldots, f(a_q))$.

$$\{ \ (f(a_1), \ldots, f(a_q)) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \ \}$$

Linear codes

$\mathcal{A} = \mathbb{F}_q$. A $[n, k]$ -linear code is just a $\mathbb{F}_q$-linear subspace of d $\mathbb{F}_q^n$ of dimension k. As usual, it can be given as a set of generators (the rows of a $k \times n$ generator matrix) or as the solutions of a system of homogeneous equations (the rows of a $(n-k) \times n$ parity check matrix).

It can be (easily) proven that $k \leq n - d + 1$ (Singleton bound). If equality holds the code is called MDS (maximum distance separable code).

Example : Reed-Solomon Codes. Let $a_1, \ldots, a_q$ all the elements in $\mathbb{F}_q$ and $f(X) \in \mathbb{F}_q[X]$. We can define a linear space as the image of a linear mapping $f(x) \mapsto (f(a_1), \ldots, f(a_q))$.

$$\{ \ (f(a_1), \ldots, f(a_q)) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \ \}$$

Decoding linear codes

Decoding problem

Input: $(G, \mathbf{y})$
where G is a $k \times n$ a matrix G over $\mathbb{F}_q$ of rank k, and $\mathbf{y}$ in $\mathbb{F}_q^n$

Output: A closest codeword $\mathbf{c}$
so $\mathrm{d}_H(\mathbf{c}, \mathbf{y})$ is minimal for all $\mathbf{c}$ in the code C with generator matrix G

This problem is NP-hard
Berlekamp-McEliece-Van Tilborg

Decoding up to $\frac{1}{2}d$

Decoding arbitrary linear codes

Exponential complexity $\approx q^{e(R)n}$

Decoding special classes of codes

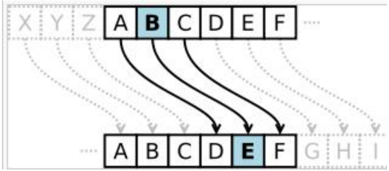
Efficient decoding algorithms up to half the minimum distance for:

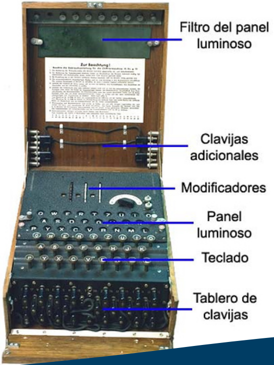
- Generalized Reed-Solomon codes
- Goppa codes
- Algebraic geometry codes

Polynomial complexity $\mathcal{O}(n^3)$

- Peterson, Arimoto 1960
- Berlekamp-Massey 1963
- Justesen-Larsen-Havemose-Jensen-Hoeholdt 1989
- Skorobogatov-Vladut 1990
- Sakata 1990
- Feng-Rao, Duursma 1993
- Sudan, Guruswami 1997

Kriptos + Graphos





Filtro del panel luminoso

Clavijas adicionales

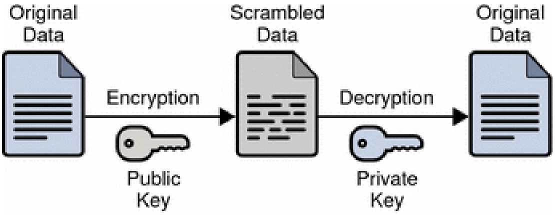
Modificadores

Panel luminoso

Teclado

Tablero de clavijas

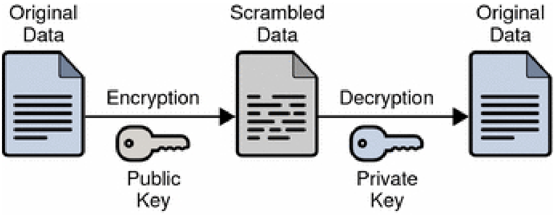
Public Key Cryptography



Bad news!!! Quantum computers could break RSA, DSA, ECDSA, ECC, ... in polynomial time due to **Shor's Algorithm**!

Good news!!! P-Q PK Cryptography: Hash-based cryptography, Code-based cryptography, Lattice-based cryptography, Multivariate-quadratic-equation cryptography.

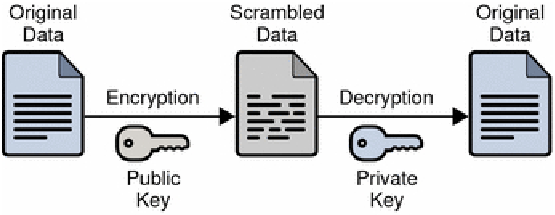
Public Key Cryptography



Bad news!!! Quantum computers could break RSA, DSA, ECDSA, ECC, ... in polynomial time due to **Shor's Algorithm**!

Good news!!! P-Q PK Cryptography: Hash-based cryptography, Code-based cryptography, Lattice-based cryptography, Multivariate-quadratic-equation cryptography.

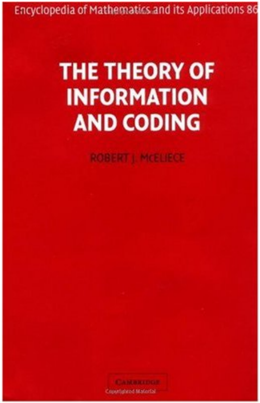
Public Key Cryptography



Bad news!!! Quantum computers could break RSA, DSA, ECDSA, ECC, ... in polynomial time due to **Shor's Algorithm**!

Good news!!! P-Q PK Cryptography: Hash-based cryptography, Code-based cryptography, Lattice-based cryptography, Multivariate-quadratic-equation cryptography.

Robert J. McEliece



Encyclopedia of Mathematics and its Applications 86

THE THEORY OF INFORMATION AND CODING

ROBERT J. MCELIECE

CAMBRIDGE

Copyrighted Material

Robert J. McEliece, California Institute of Technology and NASA Jet Propulsion Laboratory, Pasadena.

McEliece's PKC

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

Key generation

1. Let $\mathcal{C}$ be an $[n, k, d]$-linear code $\mathbb{F}_q$.
   $G \in \mathbb{F}_q^{k \times n}$ a generator matrix.
   $S \in \mathbb{F}_q^{k \times k}$ a non-singular matrix.
   $P \in \mathbb{F}_q^{n \times n}$ a permutation matrix.
2. Public key: $(G' = SGP, t)$.
3. Secret key: (G, S, P)

Encode

$\mathbf{m} \in \mathbb{F}_q^k$ $\mathbf{y}' = \mathbf{m}G' + \mathbf{e}'$ where $\mathbf{e}' = \mathbf{e}P$ in $\mathbb{F}_q^n$ of weight t.

Decode

1. Compute $\mathbf{y} = \mathbf{y}'P^{-1} = \mathbf{m}G'P^{-1} + \mathbf{e}'P^{-1} = \mathbf{m}SG + \mathbf{e}$.
2. Decode in $\mathcal{C}$ to recover $\mathbf{m}S$. $\mathbf{m} = \mathbf{m}SS^{-1}$.

McEliece's PKC

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

Key generation

1. Let $\mathcal{C}$ be an $[n, k, d]$-linear code $\mathbb{F}_q$.
   $G \in \mathbb{F}_q^{k\times n}$ a generator matrix.
   $S \in \mathbb{F}_q^{k\times k}$ a non-singular matrix.
   $P \in \mathbb{F}_q^{n\times n}$ a permutation matrix.
2. Public key: $(G' = SGP, t)$.
3. Secret key: (G, S, P)

Encode

$\mathbf{m} \in \mathbb{F}_q^k$ $\mathbf{y}' = \mathbf{m}G' + \mathbf{e}'$ where $\mathbf{e}' = \mathbf{e}P$ in $\mathbb{F}_q^n$ of weight t.

Decode

1. Compute $\mathbf{y} = \mathbf{y}'P^{-1} = \mathbf{m}G'P^{-1} + \mathbf{e}'P^{-1} = \mathbf{m}SG + \mathbf{e}$.
2. Decode in $\mathcal{C}$ to recover $\mathbf{m}S$. $\mathbf{m} = \mathbf{m}SS^{-1}$.

McEliece's PKC

R. J. McEliece.
A public-key cryptosystem based on algebraic coding theory.
DSN Progress Report, 42-44:114-116, 1978.

Key generation

1. Let $\mathcal{C}$ be an $[n, k, d]$-linear code $\mathbb{F}_q$.
   $G \in \mathbb{F}_q^{k\times n}$ a generator matrix.
   $S \in \mathbb{F}_q^{k\times k}$ a non-singular matrix.
   $P \in \mathbb{F}_q^{n\times n}$ a permutation matrix.
2. Public key: $(G' = SGP, t)$.
3. Secret key: (G, S, P)

Encode

$\mathbf{m} \in \mathbb{F}_q^k$ $\mathbf{y}' = \mathbf{m}G' + \mathbf{e}'$ where $\mathbf{e}' = \mathbf{e}P$ in $\mathbb{F}_q^n$ of weight t.

Decode

1. Compute $\mathbf{y} = \mathbf{y}'P^{-1} = \mathbf{m}G'P^{-1} + \mathbf{e}'P^{-1} = \mathbf{m}SG + \mathbf{e}$.
2. Decode in $\mathcal{C}$ to recover $\mathbf{m}S$. $\mathbf{m} = \mathbf{m}SS^{-1}$.

Atacks

Mainly Information Set Decoding.

A. Canteaut and H. Chabanne.
A further improvement of the work factor in an attempt at breaking McEliece's cryptosystem.
EUROCODE 94, 1994.

A. Canteaut and F. Chabaud.
A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511.
IEEE Transaction on Information Theory.

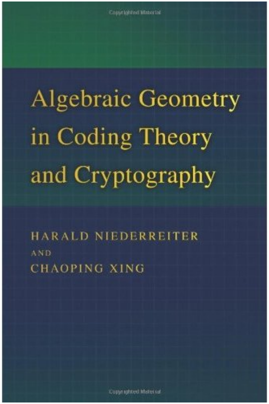
A. Canteaut and N. Sendrier.
Crytanalysis of the original McEliece cryptosystem.
Advances in cryptology - ASIACRYPT'98.

P. J. Lee and E. F. Brickell.
An observation on the security of McEliece's public-key cryptosystem.
Advances in cryptology - EUROCRYPT'98.

J. van Tilburg.
On the McEliece public-key cryptosystem.
Advances in cryptology - CRYPTO'88.

D. J. Bernstein, T. Lange, C. Peters.
Attacking and defending the McEliece cryptosystem.
Post-Quantum Cryptography

Harald Niederreiter



Algebraic Geometry in Coding Theory and Cryptography

HARALD NIEDERREITER AND CHAOPING XING

Harald Niederreiter, Johann Radon Institute for Computational and Applied Mathematics (RICAM)

Niederreiter's PKC

H. Niederreiter.
Knapsack-type crypto system and algebraic coding theory.
Problems of Control and Information Theory, 1986.

Key generation

1. Let $\mathcal{C}$ be an $[n, k, d]$-linear code. $H \in \mathbb{F}_q^{(n-k)\times n}$ a parity check m. $S \in \mathbb{F}_q^{(n-k)\times(n-k)}$ non-singular.
2. $P \in \mathbb{F}_q^{n\times n}$ a permutation m.
3. Public key: $(H' = SHP, t)$.
4. Secret key: (H, S, P).

Encode

$\mathbf{m} \in \mathbb{F}_q^k$ como $\mathbf{y}' = \mathbf{m}H'^T$.

Decode

1. Compute the syndrome of $\mathbf{y}'$: $\mathbf{y} = \mathbf{y}' = (S^{-1})^T = \mathbf{m}P^T H^T = \mathbf{m}' H^T$.
2. Decode within $\mathcal{C}$, i.e. we find $\mathbf{m}' = \mathbf{m}P^T$, thus $\mathbf{m}$.

Y. Xing Li, R. H. Deng and X. Mei Wang.
On the equivalence of McEliece's and Niederreiter public-key cryptosystems.
IEEE Transaction on Information Theory, 1994.

Niederreiter's PKC

H. Niederreiter.
Knapsack-type crypto system and algebraic coding theory.
Problems of Control and Information Theory, 1986.

Key generation

1. Let $\mathcal{C}$ be an $[n, k, d]$-linear code.
   $H \in \mathbb{F}_q^{(n-k)\times n}$ a parity check m.
   $S \in \mathbb{F}_q^{(n-k)\times(n-k)}$ non-singular.
2. $P \in \mathbb{F}_q^{n\times n}$ a permutation m.
3. Public key: $(H' = SHP, t)$.
4. Secret key: (H, S, P).

Encode

$\mathbf{m} \in \mathbb{F}_q^k$ como $\mathbf{y}' = \mathbf{m}H'^T$.

Decode

1. Compute the syndrome of $\mathbf{y}'$: $\mathbf{y} = \mathbf{y}' = (S^{-1})^T = \mathbf{m}P^TH^T = \mathbf{m}'H^T$.
2. Decode within $\mathcal{C}$, i.e. we find $\mathbf{m}' = \mathbf{m}P^T$, thus $\mathbf{m}$.

Y. Xing Li, R. H. Deng and X. Mei Wang.
On the equivalence of McEliece's and Niederreiter public-key cryptosystems.
IEEE Transaction on Information Theory, 1994.

Niederreiter's PKC

H. Niederreiter.
Knapsack-type crypto system and algebraic coding theory.
Problems of Control and Information Theory, 1986.

Key generation

1. Let $\mathcal{C}$ be an $[n, k, d]$-linear code. $H \in \mathbb{F}_q^{(n-k)\times n}$ a parity check m. $S \in \mathbb{F}_q^{(n-k)\times(n-k)}$ non-singular.
2. $P \in \mathbb{F}_q^{n\times n}$ a permutation m.
3. Public key: $(H' = SHP, t)$.
4. Secret key: (H, S, P).

Encode

$\mathbf{m} \in \mathbb{F}_q^k$ como $\mathbf{y}' = \mathbf{m}H'^T$.

Decode

1. Compute the syndrome of $\mathbf{y}'$: $\mathbf{y} = \mathbf{y}' = (S^{-1})^T = \mathbf{m}P^T H^T = \mathbf{m}'H^T$.
2. Decode within $\mathcal{C}$, i.e. we find $\mathbf{m}' = \mathbf{m}P^T$, thus $\mathbf{m}$.

Y. Xing Li, R. H. Deng and X. Mei Wang.
On the equivalence of McEliece's and Niederreiter public-key cryptosystems.
IEEE Transaction on Information Theory, 1994.

Niederreiter's PKC

H. Niederreiter.
Knapsack-type crypto system and algebraic coding theory.
Problems of Control and Information Theory, 1986.

Key generation

1. Let $\mathcal{C}$ be an $[n,k,d]$-linear code. $H \in \mathbb{F}_q^{(n-k)\times n}$ a parity check m. $S \in \mathbb{F}_q^{(n-k)\times(n-k)}$ non-singular.
2. $P \in \mathbb{F}_q^{n\times n}$ a permutation m.
3. Public key: $(H' = SHP, t)$.
4. Secret key: (H, S, P).

Encode

$\mathbf{m} \in \mathbb{F}_q^k$ como $\mathbf{y}' = \mathbf{m}H'^T$.

Decode

1. Compute the syndrome of $\mathbf{y}'$: $\mathbf{y} = \mathbf{y}' = (S^{-1})^T = \mathbf{m}P^T H^T = \mathbf{m}' H^T$.
2. Decode within $\mathcal{C}$, i.e. we find $\mathbf{m}' = \mathbf{m}P^T$, thus $\mathbf{m}$.

Y. Xing Li, R. H. Deng and X. Mei Wang.
On the equivalence of McEliece's and Niederreiter public-key cryptosystems.
IEEE Transaction on Information Theory, 1994.

Atacks

V. M. Sidelnikov and S. O. Shestakov.
On insecurity of cryptosystems based on generalized Reed-Solomon codes.
Discrete mathematics and Applications.

C. Faure and L. Minder.
Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes.
Proceedings 11th Int. Workshop on Algebraic and Combinatorial Coding Theory, 2008.

imUVa
Instituto de Matemáticas

Modifications

T. Berger and P. Loidreau.
How to mask the structure of codes for a cryptographic use.
Designs, Codes and Cryptography, 35: 63–79, 2005.

C. Wieschebrink.
An attack on the modified Niederreiter encryption scheme.
In PKC 2006, Lecture Notes in Computer Science, volume 3958, 14–26, Berlin, 2006. Springer.

C. Wieschebrink.
Cryptoanalysis of the Niederreiter public key scheme based on GRS subcodes.
In Post-Quantum Cryptography, Lecture Notes in Computer Science, volume 6061, 6–72, Berlin, 2010. Springer.

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.
The non-gap sequence of a subcode of a generalized Reed-Solomon code.
Designs,Codes and Cryptography Jan. 2013

More modifications and attacks

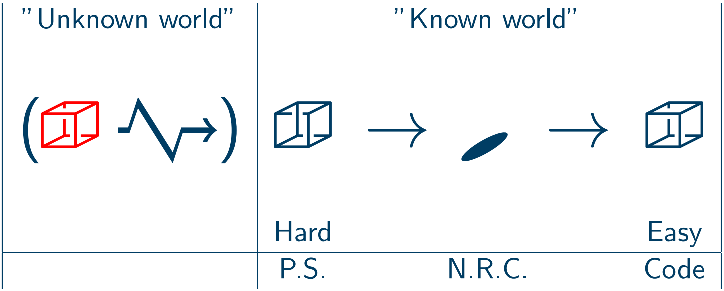
H. Janwa and O. Moreno.
McEliece public crypto system using algebraic-geometric codes.
Designs, Codes and Cryptography, 8:293-307, 1996.

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan.
On the unique representation of very strong algebraic geometry codes.
Designs, Codes and Cryptography,Online first, to appear 2013.

I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan, D. Ruano.
Computing the representation of VSAG codes.
Journal of Symbolic Computation, Submitted Dec. 2012.

Our attack

Main objective:



"Unknown world"	"Known world"		
	Hard		Easy
	P.S.	N.R.C.	Code

such that

Projective systems and codes

Katsman-Tsfasman-Vladut:

Let $\mathbb{F}$ be a field.
A projective system $\mathcal{P} = (P_1, \ldots, P_n)$ in $\mathbb{P}^r(\mathbb{F})$ is an n-tuple of points P_j in the projective space such that not all these points lie in a hyperplane.

Let $P_j = (p_{0j} : p_{1j} : \ldots : p_{rj})$ and let $G_{\mathcal{P}}$ be the $(r+1) \times n$ matrix with $(p_{0j}, p_{1j}, \ldots, p_{rj})^T$ as j-th column. Then $G_{\mathcal{P}}$ has rank $r+1$, since not all points lie in a hyperplane.

Code of a curve in projective space

If $\mathbb{F}$ is a finite field, then $G_{\mathcal{P}}$ is the generator matrix of a nondegenerate $[n, r+1, d]$ code over $\mathbb{F}$ where $n-d$ is the maximal number of points of $\mathcal{P}$ that lie in a hyperplane of $\mathbb{P}^{k-1}(\mathbb{F})$.

Example

Let $\mathcal{X}$ be an irreducible projective curve over $\mathbb{F}_q$ of degree m in $\mathbb{P}^{k-1}$ Let $\mathcal{P}$ be an enumeration of n points of $\mathcal{X}(\mathbb{F}_q)$ Then $G_{\mathcal{P}}$ is the generator matrix of a code with parameters $[n, k, d]$

$$d \geq n - m.$$

Codes and projective systems

Conversely:
Let G be a generator matrix of a nondegenerate $[n, k, d]$ code over $\mathbb{F}_q$. Then G has no zero columns, take the columns of G as homogeneous coordinates of points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$. This gives the projective system $\mathcal{P}_G$ over $\mathbb{F}_q$ of G.

One-to-one correspondence between:
generalized equivalence classes of nondegenerate $[n, k]$ codes over $\mathbb{F}_q$ and equivalence classes of projective systems of n points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

Generalized Reed-Solomon codes

$\mathbf{a} = (a_1, \ldots, a_n)$ an n-tuple of mutually distinct elements of $\mathbb{F}_q$
$\mathbf{b} = (b_1, \ldots, b_n)$ an n-tuple of nonzero elements of $\mathbb{F}_q$

$GRS_k(\mathbf{a}, \mathbf{b}) =$

$$\{ \ (f(a_1)b_1, \ldots, f(a_n)b_n) \mid f(X) \in \mathbb{F}_q[X], \deg(f(X)) < k \ \}$$

Parameters: $[n, k, n-k+1]$ if $k \leq n$.
Generator matrix:

$$G_k(\mathbf{a}, \mathbf{b}) = \begin{pmatrix} b_1 & \cdots & b_j & \cdots & b_n \\ a_1 b_1 & \cdots & a_j b_j & \cdots & a_n b_n \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ a_1^{k-1} b_1 & \cdots & a_j^{k-1} b_j & \cdots & a_n^{k-1} b_n \end{pmatrix}$$

Normal rational curves and GRS codes

The projective system of the the code $GRS_k(\mathbf{a}, \mathbf{b})$ with generator matrix $G_k(\mathbf{a}, \mathbf{b})$ is

$$\mathcal{P}_k(\mathbf{a}) = ((1 : a_j : \cdots : a_j^i : \cdots : a_j^{k-1}) \mid j = 1, \ldots, n)$$

Consider the embedding $\mathbb{P}^1 \to \mathbb{P}^r$ by the degree r map given by

$$(y_0 : y_1) \mapsto (y_0^r : y_0^{r-1} y_1 : \cdots : y_0^{r-i} y_1^i : \cdots : y_0 y_1^{r-1} : y_1^r)$$

The image of this map in $\mathbb{P}^r$ is the NRC (normal rational curve) $\mathcal{X}_r$. Every hyperplane intersects $\mathcal{X}_r$ in at most r points and

$$\mathcal{P}_k(\mathbf{a}) \subseteq \mathcal{X}_{k-1}(\mathbb{F}_q).$$

Vanishing ideal of rational normal curve

The vanishing ideal $I(\mathcal{X}_r)$ of $\mathcal{X}_r$ is generated by the quadratic polynomials:

$$X_i X_{r-i} - X_j X_{r-j}, \quad \text{for } 0 \leq i < j \leq r$$

that is the determinantal ideal of the 2×2 minors of the $2 \times r$ matrix

$$\begin{pmatrix} X_0 & X_1 & \cdots & X_i & \cdots & X_{r-1} \\ X_1 & X_2 & \cdots & X_{i+1} & \cdots & X_r \end{pmatrix}$$

since the rows of the matrix

$$\begin{pmatrix} 1 & y & \cdots & y^i & \cdots & y^{r-1} \\ y & y^2 & \cdots & y^{i+1} & \cdots & y^r \end{pmatrix}$$

are dependent for all y.

Algebraic geometry codes

Let $\mathcal{X}$ be an algebraic variety over $\mathbb{F}_q$ with a subset $\mathcal{P}$ of $\mathcal{X}(\mathbb{F}_q)$ enumerated by $P_1, \ldots, P_n$.
Suppose that we have a vector space L over $\mathbb{F}_q$ of functions on $\mathcal{X}$ with values in $\mathbb{F}_q$ So $f(P_i) \in \mathbb{F}_q$ for all i and $f \in L$. In this way we have an evaluation map

$$ev_{\mathcal{P}} : L \longrightarrow \mathbb{F}_q^n$$

defined by $ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$

This evaluation map is linear, so its image is a linear code.

Codes on the affine line

The classical example: Generalized Reed-Solomon codes

The geometric object $\mathcal{X}$ is the affine line over $\mathbb{F}_q$, the points are n distinct elements of $\mathbb{F}_q$, L is the vector space of polynomials of degree at most $k-1$ with coefficients in $\mathbb{F}_q$.
This vector space has dimension k. Such polynomials have at most $k-1$ zeros so nonzero codewords have at least $n-k+1$ nonzeros.
I.e. the code has parameters $[n,k,n-k+1]$ if $k \leq n$.

Codes on curves-function fields

Let $\mathcal{X}$ be an algebraic curve over $\mathbb{F}_q$ of genus g (that is to say the curve is nonsingular, absolutely irreducible and projective). $\mathbb{F}_q(\mathcal{X})$ is the function field of the curve $\mathcal{X}$ with field of constants $\mathbb{F}_q$

Let f be a nonzero rational function on the curve. The divisor of zeros and poles of f is denoted by (f).

Let E be a divisor of $\mathcal{X}$ of degree m. Then

$$L(E) = \{\ f \in \mathbb{F}_q(\mathcal{X}) \mid f = 0 \text{ or } (f) \geq -E\ \}.$$

The dimension of the space $L(E)$ is denoted by $l(E)$ and $l(E) \geq m + 1 - g$ and equality holds if $m > 2g - 2$ by the Theorem of Riemann-Roch.

Codes on curves

Let $\mathcal{P} = (P_1, \ldots, P_n)$ an n-tuple of mutual distinct points of $\mathcal{X}(\mathbb{F}_q)$ with divisor $D = P_1 + \cdots + P_n$

If the support of E is disjoint from D, then the evaluation map

$$\mathrm{ev}_{\mathcal{P}} : L(E) \to \mathbb{F}_q^n$$

where $\mathrm{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$, is well defined.

The algebraic geometry code $C_L(\mathcal{X}, \mathcal{P}, E)$ is the image of $L(E)$ under the evaluation map $\mathrm{ev}_{\mathcal{P}}$.
If $m < n$, then $C_L(\mathcal{X}, \mathcal{P}, E)$ is an $[n, k, d]$ code with

$$k \geq m + 1 - g \quad \text{and} \quad d \geq n - m.$$

Dual codes on curves

Let ω be a differential form with a simple pole at P_j with residue 1 for all $j = 1, \ldots, n$.
Let K be the canonical divisor of ω and let m be the degree of the divisor E on $\mathcal{X}$ with disjoint support from $\mathcal{P}$.

Let $E^{\perp} = D - E + K$ and $m^{\perp} = \deg(E^{\perp})$. Then $m^{\perp} = 2g - 2 - m + n$ and

$$C_L(\mathcal{X}, \mathcal{P}, E)^{\perp} = C_L(\mathcal{X}, \mathcal{P}, E^{\perp})$$

Codes on curves

Embedding of $\mathcal{X}$ in linear system of E of degree m. Let $f_1, f_2, \dots, f_k$ be a basis of $L(E)$

$$\varphi : \mathcal{X} \longrightarrow \mathbb{P}^{k-1}$$

$$P \mapsto (f_1(P), f_2(P), \dots, f_k(P))$$

$\mathcal{Y} = \varphi(\mathcal{X})$ is a curve of degree m in $\mathbb{P}^{k-1}$ and $\mathcal{Q} = (\varphi(P_1), \dots, \varphi(P_n))$ is a projective system.

$$G_{\mathcal{Q}} = \begin{pmatrix} f_1(P_1) & \cdots & f_1(P_j) & \cdots & f_1(P_n) \\ f_2(P_1) & \cdots & f_2(P_j) & \cdots & f_2(P_n) \\ \vdots & \dots & \vdots & \dots & \vdots \\ f_k(P_1) & \cdots & f_k(P_j) & \cdots & f_k(P_n) \end{pmatrix}$$ generator matrix.

minimum distance $\geq n - m$.

Sidelnikov-Shestakov I

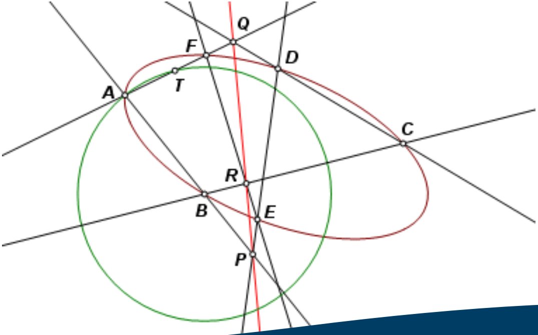
Suppose $\mathcal{C}$ is the class of Generalized Reed-Solomon codes. A GRS code of length n and dimension $k = r + 1$ gives a projective system of n points in general position on a NRC of degree r in projective space of dimension r.

Special case: $k = 3$ and $r = 2$:
a NRC of degree 2 in the projective plane is a conic. 5 points in general position determine this conic

Steiner: parametrization of this conic in the plane given these 5 points.
Algorithm of Sidelnikov-Shestakov for arbitrary k
Complexity: linear algebra $\mathcal{O}(n^3)$

Conic determined by 5 points

Pascal's theorem. When a hexagon is inscribed in a conic, the three pairs of opposite sides define three points of intersection. These three points are collinear. In this case five of the hexagon vertices are given, A, B, C, D, E. The conic section is the locus of the sixth vertex F, which must satisfy the property of collinearity.

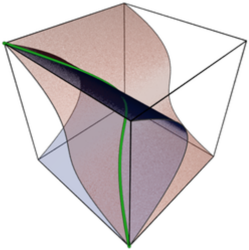


NRC of degree r ($r + 2$ points)

Veronese 1882, Bordiga 1885, Castelnuovo 1885:

Let $\mathcal{P}$ be a collection of $r + 3$ points in general position in $\mathbb{P}^r$. Then there is a unique NRC of degree r passing through the points of $\mathcal{P}$.

Twisted cubic, r=3: The zero locus of three smooth quadrics $F_0 = XZ - Y^2$, $F_1 = YW - Z^2$, $F_2 = XW - YZ$.



AG, WAG and SAG codes

A code C over $\mathbb{F}$ is called weakly algebraic-geometric (WAG) if $C = C_L(\mathcal{X}, \mathcal{P}, E)$ for some triple $(\mathcal{X}, \mathcal{P}, E)$ where:

– $\mathcal{X}$ is an algebraic curve over $\mathbb{F}_q$
– $\mathcal{P}$ is an n-tuple of mutually distinct points of $\mathcal{X}(\mathbb{F}_q)$
– E is divisor of degree m on $\mathcal{X}$

Then $(\mathcal{X}, \mathcal{P}, E)$ is called a WAG representation of C. If $m < n$, then it is called AG. If $2g - 2 < m < n$, then it is called strongly algebraic-geometric (SAG).

Theorem[Pellikaan-Shen-van Wee]: Every code has a WAG representation

Equivalent representations

Two representations $(\mathcal{X}, \mathcal{P}, E)$ and $(\mathcal{Y}, \mathcal{Q}, F)$ are called equivalent or isomorphic if there is an isomorphism of curves $\varphi : \mathcal{X} \to \mathcal{Y}$ such that $\varphi(\mathcal{P}) = \mathcal{Q}$ and $\varphi(E) \equiv F$

They are called strict equivalent or strict isomorphic if moreover $\varphi(E) \equiv_{\mathcal{Q}} F$

Proposition

Let $(\mathcal{X}, \mathcal{P}, E)$ and $(\mathcal{Y}, \mathcal{Q}, F)$ be WAG representations of C and D, resp.

Then:

(1) If $(\mathcal{X}, \mathcal{P}, E)$ and $(\mathcal{Y}, \mathcal{Q}, F)$ are equivalent, then $C \equiv D$

(2) If $(\mathcal{X}, \mathcal{P}, E)$ and $(\mathcal{Y}, \mathcal{Q}, F)$ are strict equivalent, then $C = D$

Retrieving E from $(\mathcal{X}, \mathcal{P})$

Theorem[Munuera-Pellikaan]:

Let $\mathcal{X}$ be a curve of genus g and $D = P_1 + \cdots + P_n$ and let E and F be divisors of degree m with $2g - 1 < m < n - 1$.

Then

$$C_L(\mathcal{X}, \mathcal{P}, E) = C_L(\mathcal{X}, \mathcal{P}, F) \text{ if and only if } E \equiv_{\mathcal{P}} F.$$

Strict equivalent representations

Let $(\mathcal{X}, \mathcal{P}, E)$ be a *WAG* representation of C such that $m > 2g$ and let $r = l(E) - 1$ and $\{f_0, \ldots, f_r\}$ be a basis of $L(E)$. Consider the map $\varphi_E : \mathcal{X} \longrightarrow \mathbb{P}^r$ defined by $\varphi_E(P) = (f_0(P), \ldots, f_r(P))$.
If $m > 2g$, then $r = m - g$ and φ_E defines an embedding of the curve $\mathcal{X}$ in $\mathbb{P}^r$ of degree m with image $\mathcal{Y} = \varphi_E(\mathcal{X})$.

Let $Q_j = \varphi_E(P_j)$ and $\mathcal{Q} = (Q_1, \ldots, Q_n)$ then $\varphi_E(E) = \mathcal{X} \cdot H = F$ for some hyperplane H of $\mathbb{P}^r$ that is disjoint from $\mathcal{Q}$.

Furthermore $(\mathcal{Y}, \mathcal{Q}, F)$ is also a WAG representation of the code C that is strict isomorphic with $(\mathcal{X}, \mathcal{P}, E)$.

How to "decode" $(\mathcal{Y}, \mathcal{Q}, F)$ without knowing $(\mathcal{X}, \mathcal{P}, E)$?

Intervals

Theorem before implies, ☡ **provided we have an efficient procedure for decoding the VSAG representation**, that one should not use VSAG codes for the McEliece PKC system in the range

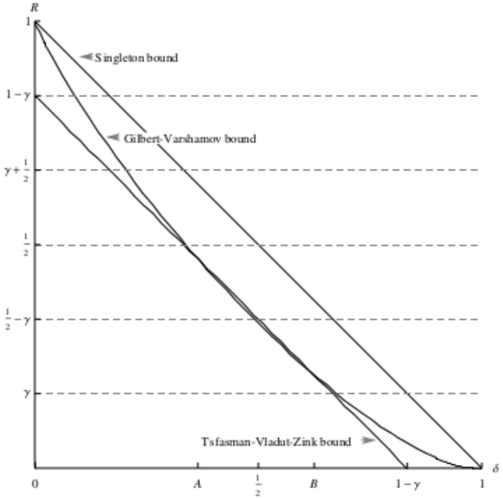
$$\gamma \leq R \leq \tfrac{1}{2} - \gamma \quad \text{or} \quad \tfrac{1}{2} + \gamma \leq R \leq 1 - \gamma,$$

By a shortening argument, we proved that also codes in the range

$$\tfrac{1}{2} - \gamma \leq R \leq 1 - 3\gamma \quad \text{or} \quad 3\gamma \leq R \leq \tfrac{1}{2} + \gamma,$$

should be excluded. $[\gamma, \frac{1}{2} - \gamma]$, $[\frac{1}{2} + \gamma, 1 - \gamma]$, $[\frac{1}{2} - \gamma, 1 - 3\gamma]$ and $[3\gamma, \frac{1}{2} + \gamma]$ are nonempty if and only if $\gamma \leq \frac{1}{4}$, and the union of these intervals cover the whole interval $[\gamma, 1 - \gamma]$ if and only if $\gamma \leq \frac{1}{6}$.

Intervals


R
1
1 − γ
γ + 1/2
1/2
1/2 − γ
γ
Singleton bound
Gilbert-Varshamov bound
Tsfasman-Vladut-Zink bound
0
A
1/2
B
1 − γ
1
δ

Curves defined by quadrics

Normal rational normal curve is defined by quadratic equations.

The canonical model of a non-hyperelliptic projective curve of genus at least three is the intersection of quadrics and cubics, and of quadrics only except in case of a trigonal curve and a plane quintic Enriques 1919, Petri 1923 and Babbage 1939.

This result for the canonical divisor was generalized for arbitrary divisors E under certain constraints on the degree Mumford 1970, Saint-Donat 1972 and Arbarello 1978.

Curves defined by quadrics

Let $\mathcal{X}$ be an absolutely irreducible and nonsingular curve of genus g over the perfect field $\mathbb{F}$. Let E be a divisor on $\mathcal{X}$ of degree m.
If $m \geq 2g+2$ then $\mathcal{Y} = \varphi_E(\mathcal{X})$ is a normal curve in $\mathbb{P}^{m-g}$ which is the intersection of quadrics.

More precisely:
$I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$ the ideal generated by the homogeneous elements of degree two in $I(\mathcal{Y})$.

Retrieving $(\mathcal{X}, D, E)$ from the code

Let $\mathcal{Y}$ be a curve embedded in projective r-space of degree m, let $I(\mathcal{Y})$ be the vanishing ideal of $\mathcal{Y}$ and let $\mathcal{Q}$ be a subset of $\mathcal{Y}$ of n points. Then

$$I(\mathcal{Y}) \subseteq I(\mathcal{Q})$$

Let $I_2(\mathcal{Y})$ be the ideal generated by the homogeneous elements of degree two in $I(\mathcal{Y})$ and suppose $I_2(\mathcal{Y}) = I(\mathcal{Y})$

$$\text{If } n > 2m, \text{ then } I(\mathcal{Y}) = I_2(\mathcal{Q})$$

by Bézout.

ℹ Determination of $I_2(\mathcal{Q})$

Let $\mathcal{Q}$ be an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{Y}$ in $\mathbb{P}^r$ is given such that $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$.

Connsider the linear map

$$\sigma : \quad S^2(\mathcal{C}) \quad \longrightarrow \quad \mathcal{C}^{(2)},$$

where the element $x_i x_j$ is mapped to $\mathbf{g}_i * \mathbf{g}_j$. The kernel of this map will be denoted by $K^2(\mathcal{C})$.

Proposition : Let $\mathcal{Q}$ be an n-tuple of points in $\mathbb{P}^r(\mathbb{F}_q)$ not in a hyperplane, $k = r + 1$, $G_{\mathcal{Q}}$ be the $k \times n$ matrix associated to $\mathcal{Q}$ and $\mathcal{C}$ be the subspace of $\mathbb{F}_q^n$ generated by the rows of $G_{\mathcal{Q}}$. Then

$$I_2(\mathcal{Q}) = \{ \textstyle\sum_{1 \le i \le j \le k} a_{ij} X_i X_j \mid \sum_{1 \le i \le j \le k} a_{ij} x_i x_j \in K^2(\mathcal{C}) \}.$$

Computing $I_d(\mathcal{Q})$

In the general case we define the spaces $S^d(\mathcal{C})$, $\mathcal{C}^{(d)}$ and $K^d(\mathcal{C})$ for any positive integer d, then we have a similar result to the previous one relating $I_d(\mathcal{Q})$ and $K^d(\mathcal{C})$. Furthermore we have that $\mathcal{O}(n^2\binom{k+d-1}{d})$ is an upper bound on the complexity of the computation of $I_d(\mathcal{Q})$.

The problem of the efficient computation of the vanishing ideal of a finite set of points was introduced by Buchberger and Möller in 1982. Then several generalization have been proposed, for instance, to the case of points with multiplicity, Lakshman in 1991 and to the projective case, Cioffi in 1998. Lately, Abbott et al. came with a variant of the classical BM Algorithm where they tame the problem of coefficient growth.

ℹ Algorithm

Let $\mathbb{T}_2^{r+1}$ be the set of powers of degree two of the r variables $\{x_0, \ldots, x_r\}$, let σ be a term ordering in $\mathbb{T}_2^{r+1}$ and let $\mathcal{Q} = \{Q_1, \ldots, Q_n\}$ be an n-tuple of points in $\mathbb{P}^r(\mathbf{F}_q)$ where Q_j is given by the homogeneous coordinates $(q_{j0} : \ldots : q_{jr})$.

Initialization: Let:

- I1 L be the ordered list of the elements of $\mathbb{T}_2^{r+1}$ w.r.t. σ,
- I2 $G = []$ and $S = []$ be empty lists
- I3 and $M = (m_{ij})$ be an $0 \times n$ matrix over $\mathbb{F}_q$.

Algorithm (cont.)

```
Main loop: L1 IF $L$ is empty then go to the End
              ELSE choose the power product $t = \min_{\prec}(L)$ and
              remove it from $L$.
           L2 Compute the evaluation vector
              $(t(Q_1), \ldots, t(Q_n))$, and reduce it against the rows
              of the matrix $M$, to obtain $\mathbf{v} = (t(Q_1), \ldots, t(Q_n))$
              $-\sum_i a_i(m_{i1}, ..., m_{in})$ with $a_i \in \mathbb{F}_q$.
           L3 IF $\mathbf{v} = \mathbf{0}$ then add the polynomial $t - \sum_i a_i s_i$ to
              the list $G$, where $s_i$ is the $i$-th element of the list
              $S$. Goto L1.
              ELSE add $\mathbf{v}$ as a new row of $M$ and $t - \sum_i a_i s_i$
              as a new element to the list $S$. Goto L1.
End: Returns $G$, the reduced Gröbner b. of $I_2(\mathcal{Q})$ w.r.t. $\sigma$.
```

ℹ Computing $E = \mathcal{Y} \cdot H$

Let H be the hyperplane given by the linear equation $f(X) = 0$. We may assume without loss of generality after possibly extending the field of constants that $E = \mathcal{Y} \cdot H$ that there is a nonzero function $f \in \mathcal{L}(E)$ such that $(f)_\infty = E$, that means that the divisor of poles of f is equal to E. Let $\mathbf{g} = \mathrm{ev}_{\mathcal{P}}(f) \in \mathcal{C}_L(\mathcal{X}, \mathcal{P}, E) = \mathcal{C}$. Then $\mathbf{g} * C$ is a subspace of $\mathcal{C}^{(2)}$ and the coset $\mathcal{C}^{(2)}/\mathbf{g} * C$ has dimension $(2m+1-g)-(m+1-g) = m$. Therefore we have an explicitly given $\mathbb{F}_q$-linear map:

$$\mathbb{F}_q[X_1, \ldots, X_k] \longrightarrow \mathcal{C}^{(2)}/\mathbf{g} * C$$

with kernel the ideal $I_2(\mathcal{Y}) + (f)$, that is the vanishing ideal of $\mathcal{Y} \cap H$ with multiplicities counted. In this situation there is an efficient (polynomial) algorithm that computes a Gröbner basis of $I_2(\mathcal{Y}) + (f)$

Toy Examples

1.- Consider the smallest code that fufills the conditions, i.e. $[4,3,2]$ narrow sense RS code over $\mathbb{F}_5$. $g=0$, $k=3>2$. Its generator matrix in cyclic form is $G=\begin{pmatrix} \xi^3 & 1 & 0 & 0 \\ 0 & \xi^3 & 1 & 0 \\ 0 & 0 & \xi^3 & 1 \end{pmatrix}$ where ξ is a primitive root of $\mathbb{F}_5$. Let us consider the matrix $S=\begin{pmatrix} \xi & 0 & 0 \\ \xi & \xi^2 & 0 \\ \xi & \xi^2 & \xi \end{pmatrix}$.

Let us compute the matrix $G_{Per}=SG=\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & \xi^2 & \xi^2 & 0 \\ 1 & \xi^2 & 0 & \xi \end{pmatrix}$.

Toy Examples (cont.)

Note that it is posible to have a permutation involved, but it makes no difference with the computation of the following ideal.

The linear restrictions on the a_{ij}'s for computing $\mathcal{I}_2(\mathcal{Q})$ where $\mathcal{Q}$ is given by the columns of G_{Per} imply that $a_{22} = a_{33} = 0$ and reducing the two other linear equations relating the coefficients a_{ij}

$$a_{11} + \xi^3 a_{23} = 0, \quad a_{21} + a_{13} + \xi^3 a_{23} = 0$$

and $\mathcal{I}_2(\mathcal{Q}) = \left\langle \xi^3 a_{23} x_1^2 + (a_{13} + \xi^2 a_{23}) x_1 x_2 - a_{13} x_1 x_3 + a_{23} x_2 x_3 \right\rangle$ where $a_{13}, a_{23} \in \mathbb{F}_5$.

Note that this case does not achieve the tight bound but if we take the extended code the bound is achieved since we will be in the case of 5 points in the proyective plain determining a unique conic.

Toy Examples (cont.)

2.- Let us take the extended case (i.e. 5 points) $[5, 3, 3]$ extended RS code over $\mathbb{F}_5$. Its generator matrix is

$$G_e = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \xi & \xi^2 & \xi^3 & 0 \\ 1 & \xi^2 & 1 & \xi^2 & 0 \end{pmatrix}$$

If we use the same S as in the previous example we have that

$$G_{Per_e} = SG_e = \begin{pmatrix} \xi & \xi & \xi & \xi & \xi \\ \xi & 1 & \xi^2 & 0 & \xi^3 \\ \xi & 1 & 1 & \xi^2 & \xi \end{pmatrix}.$$

Toy Examples (cont.)

The linear restrictions on the a_{ij}'s for computing $\mathcal{I}_2(\mathcal{Q}_e)$ where $\mathcal{Q}_e$ is given by the columns of G_{Per_e} imply that $a_{12} = a_{33} = a_{23} = 0$ and reducing the two other linear equations relating the coefficients a_{ij}

$$a_{13} - a_{22} = 0, \quad a_{11} + \xi a_{22} = 0,$$

thus $\mathcal{I}_2(\mathcal{Q}) = \left\langle a_{22}x_1^2 + \xi a_{22}x_1x_3 + \xi a_{22}x_2^2 \mid a_{22} \in \mathbb{F}_5 \setminus \{0\} \right\rangle$ i.e. the unique form $x_1^2 + \xi x_1x_3 + \xi x_2^2$ which is indeed the same as we arrive computing from the columns of matrix G_e without “scrambling” with S.

Indeed, 5 points determine a unique conic!!!!