

# Decoding linear codes via polynomial systems solving.

## Generalized Newton identities for linear codes

Stanislav Bulygin (joint work with Ruud Pellikaan)

S<sup>3</sup>CM: Soria Summer School on Computational Mathematics  
"Algebraic Coding Theory"

July 5, 2008

# Outline

## Outline of the talk

- Quadratic system method
- Generalized Newton identities

# Quadratic system method

## Unknown syndrome

Let  $\mathbf{b}_1, \dots, \mathbf{b}_n$  be a basis of  $\mathbb{F}_q^n$  and let  $B$  be the  $n \times n$  matrix with  $\mathbf{b}_1, \dots, \mathbf{b}_n$  as rows. The *unknown syndrome*  $\mathbf{u}(B, \mathbf{e})$  of a word  $\mathbf{e}$  w.r.t  $B$  is the column vector  $\mathbf{u}(B, \mathbf{e}) = B\mathbf{e}^T$  with entries  $u_i(B, \mathbf{e}) = \mathbf{b}_i \cdot \mathbf{e}$  for  $i = 1, \dots, n$ .

## Structure constants

For two vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$  define  $\mathbf{x} * \mathbf{y} = (x_1y_1, \dots, x_ny_n)$ . Then  $\mathbf{b}_i * \mathbf{b}_j$  is a linear combination of  $\mathbf{b}_1, \dots, \mathbf{b}_n$ , so there are constants  $\mu_l^{ij} \in \mathbb{F}_q$  such that  $\mathbf{b}_i * \mathbf{b}_j = \sum_{l=1}^n \mu_l^{ij} \mathbf{b}_l$ . The elements  $\mu_l^{ij} \in \mathbb{F}_q$  are the *structure constants* of the basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$ .

## MDS matrix

Let  $B_s$  be the  $s \times n$  matrix with  $\mathbf{b}_1, \dots, \mathbf{b}_s$  as rows ( $B = B_n$ ). Then  $\mathbf{b}_1, \dots, \mathbf{b}_n$  is an *ordered MDS basis* and  $B$  an *MDS matrix* if all the  $s \times s$  submatrices of  $B_s$  have rank  $s$  for all  $s = 1, \dots, n$ .

# Quadratic system method

## Unknown syndrome

Let  $\mathbf{b}_1, \dots, \mathbf{b}_n$  be a basis of  $\mathbb{F}_q^n$  and let  $B$  be the  $n \times n$  matrix with  $\mathbf{b}_1, \dots, \mathbf{b}_n$  as rows. The *unknown syndrome*  $\mathbf{u}(B, \mathbf{e})$  of a word  $\mathbf{e}$  w.r.t  $B$  is the column vector  $\mathbf{u}(B, \mathbf{e}) = B\mathbf{e}^T$  with entries  $u_i(B, \mathbf{e}) = \mathbf{b}_i \cdot \mathbf{e}$  for  $i = 1, \dots, n$ .

## Structure constants

For two vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$  define  $\mathbf{x} * \mathbf{y} = (x_1y_1, \dots, x_ny_n)$ . Then  $\mathbf{b}_i * \mathbf{b}_j$  is a linear combination of  $\mathbf{b}_1, \dots, \mathbf{b}_n$ , so there are constants  $\mu_l^{ij} \in \mathbb{F}_q$  such that  $\mathbf{b}_i * \mathbf{b}_j = \sum_{l=1}^n \mu_l^{ij} \mathbf{b}_l$ . The elements  $\mu_l^{ij} \in \mathbb{F}_q$  are the *structure constants* of the basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$ .

## MDS matrix

Let  $B_s$  be the  $s \times n$  matrix with  $\mathbf{b}_1, \dots, \mathbf{b}_s$  as rows ( $B = B_n$ ). Then  $\mathbf{b}_1, \dots, \mathbf{b}_n$  is an *ordered MDS basis* and  $B$  an *MDS matrix* if all the  $s \times s$  submatrices of  $B_s$  have rank  $s$  for all  $s = 1, \dots, n$ .

# Quadratic system method

## Unknown syndrome

Let  $\mathbf{b}_1, \dots, \mathbf{b}_n$  be a basis of  $\mathbb{F}_q^n$  and let  $B$  be the  $n \times n$  matrix with  $\mathbf{b}_1, \dots, \mathbf{b}_n$  as rows. The *unknown syndrome*  $\mathbf{u}(B, \mathbf{e})$  of a word  $\mathbf{e}$  w.r.t  $B$  is the column vector  $\mathbf{u}(B, \mathbf{e}) = B\mathbf{e}^T$  with entries  $u_i(B, \mathbf{e}) = \mathbf{b}_i \cdot \mathbf{e}$  for  $i = 1, \dots, n$ .

## Structure constants

For two vectors  $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$  define  $\mathbf{x} * \mathbf{y} = (x_1y_1, \dots, x_ny_n)$ . Then  $\mathbf{b}_i * \mathbf{b}_j$  is a linear combination of  $\mathbf{b}_1, \dots, \mathbf{b}_n$ , so there are constants  $\mu_l^{ij} \in \mathbb{F}_q$  such that  $\mathbf{b}_i * \mathbf{b}_j = \sum_{l=1}^n \mu_l^{ij} \mathbf{b}_l$ . The elements  $\mu_l^{ij} \in \mathbb{F}_q$  are the *structure constants* of the basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$ .

## MDS matrix

Let  $B_s$  be the  $s \times n$  matrix with  $\mathbf{b}_1, \dots, \mathbf{b}_s$  as rows ( $B = B_n$ ). Then  $\mathbf{b}_1, \dots, \mathbf{b}_n$  is an *ordered MDS basis* and  $B$  an *MDS matrix* if all the  $s \times s$  submatrices of  $B_s$  have rank  $s$  for all  $s = 1, \dots, n$ .

# Quadratic system method

## Check matrix

Let  $C$  be an  $\mathbb{F}_q$ -linear code with parameters  $[n, k, d]$ . W.l.o.g  $n \leq q$ .  $H$  is a check matrix of  $C$ . Let  $\mathbf{h}_1, \dots, \mathbf{h}_{n-k}$  be the rows of  $H$ . One can express  $\mathbf{h}_i = \sum_{j=1}^n a_{ij} \mathbf{b}_j$  for some  $a_{ij} \in \mathbb{F}_q$ . In other words  $H = AB$  where  $A$  is the  $(n-k) \times n$  matrix with entries  $a_{ij}$ .

## Known syndrome

Let  $\mathbf{y} = \mathbf{c} + \mathbf{e}$  be a received word with  $\mathbf{c} \in C$  and  $\mathbf{e}$  an error vector. The syndromes of  $\mathbf{y}$  and  $\mathbf{e}$  w.r.t  $H$  are equal and known:

$$s_i(\mathbf{y}) := \mathbf{h}_i \cdot \mathbf{y} = \mathbf{h}_i \cdot \mathbf{e} = s_i(\mathbf{e}).$$

They can be expressed in the unknown syndromes of  $\mathbf{e}$  w.r.t  $B$ :

$$s_i(\mathbf{y}) = s_i(\mathbf{e}) = \sum_{j=1}^n a_{ij} u_j(\mathbf{e})$$

since  $\mathbf{h}_i = \sum_{j=1}^n a_{ij} \mathbf{b}_j$  and  $\mathbf{b}_j \cdot \mathbf{e} = u_j(\mathbf{e})$ .

# Quadratic system method

## Check matrix

Let  $C$  be an  $\mathbb{F}_q$ -linear code with parameters  $[n, k, d]$ . W.l.o.g  $n \leq q$ .  $H$  is a check matrix of  $C$ . Let  $\mathbf{h}_1, \dots, \mathbf{h}_{n-k}$  be the rows of  $H$ . One can express  $\mathbf{h}_i = \sum_{j=1}^n a_{ij} \mathbf{b}_j$  for some  $a_{ij} \in \mathbb{F}_q$ . In other words  $H = AB$  where  $A$  is the  $(n-k) \times n$  matrix with entries  $a_{ij}$ .

## Known syndrome

Let  $\mathbf{y} = \mathbf{c} + \mathbf{e}$  be a received word with  $\mathbf{c} \in C$  and  $\mathbf{e}$  an error vector. The syndromes of  $\mathbf{y}$  and  $\mathbf{e}$  w.r.t  $H$  are equal and known:

$$s_i(\mathbf{y}) := \mathbf{h}_i \cdot \mathbf{y} = \mathbf{h}_i \cdot \mathbf{e} = s_i(\mathbf{e}).$$

They can be expressed in the unknown syndromes of  $\mathbf{e}$  w.r.t  $B$ :

$$s_i(\mathbf{y}) = s_i(\mathbf{e}) = \sum_{j=1}^n a_{ij} u_j(\mathbf{e})$$

since  $\mathbf{h}_i = \sum_{j=1}^n a_{ij} \mathbf{b}_j$  and  $\mathbf{b}_j \cdot \mathbf{e} = u_j(\mathbf{e})$ .

# Quadratic system method

## Linear forms

Let  $B$  be an MDS matrix with structure constants  $\mu_l^{ij}$ . Define  $U_{ij}$  in the variables  $U_1, \dots, U_n$  by

$$U_{ij} = \sum_{l=1}^n \mu_l^{ij} U_l.$$

## Quadratic system

The ideal  $J(\mathbf{y})$  in  $\mathbb{F}_q[U_1, \dots, U_n]$  is generated by

$$\sum_{l=1}^n a_{jl} U_l - s_j(\mathbf{y}) \quad \text{for } j = 1, \dots, r$$

The ideal  $I(t, \mathcal{U}, V)$  in  $\mathbb{F}_q[U_1, \dots, U_n, V_1, \dots, V_t]$  is generated by

$$\sum_{j=1}^t U_{ij} V_j - U_{it+1} \quad \text{for } i = 1, \dots, n$$

Let  $J(t, \mathbf{y})$  be the ideal in  $\mathbb{F}_q[U_1, \dots, U_n, V_1, \dots, V_t]$  generated by  $J(\mathbf{y})$  and  $I(t, \mathcal{U}, V)$ .

# Quadratic system method

## Linear forms

Let  $B$  be an MDS matrix with structure constants  $\mu_l^{ij}$ . Define  $U_{ij}$  in the variables  $U_1, \dots, U_n$  by

$$U_{ij} = \sum_{l=1}^n \mu_l^{ij} U_l.$$

## Quadratic system

The ideal  $J(\mathbf{y})$  in  $\mathbb{F}_q[U_1, \dots, U_n]$  is generated by

$$\sum_{l=1}^n a_{jl} U_l - s_j(\mathbf{y}) \quad \text{for } j = 1, \dots, r$$

The ideal  $I(t, \mathcal{U}, V)$  in  $\mathbb{F}_q[U_1, \dots, U_n, V_1, \dots, V_t]$  is generated by

$$\sum_{j=1}^t U_{ij} V_j - U_{it+1} \quad \text{for } i = 1, \dots, n$$

Let  $J(t, \mathbf{y})$  be the ideal in  $\mathbb{F}_q[U_1, \dots, U_n, V_1, \dots, V_t]$  generated by  $J(\mathbf{y})$  and  $I(t, \mathcal{U}, V)$ .

# Quadratic system method

## Main result

Let  $B$  be an MDS matrix with structure constants  $\mu_i^{jj}$ . Let  $H$  be a check matrix of the code  $C$  such that  $H = AB$  as above. Let  $\mathbf{y} = \mathbf{c} + \mathbf{e}$  be a received word with  $\mathbf{c} \in C$  the codeword sent and  $\mathbf{e}$  the error vector. Suppose that  $\text{wt}(\mathbf{e}) \neq 0$  and  $\text{wt}(\mathbf{e}) \leq \lfloor (d(C) - 1)/2 \rfloor$ . Let  $t$  be the smallest positive integer such that  $J(t, \mathbf{y})$  has a solution  $(\mathbf{u}, \mathbf{v})$  over  $\overline{\mathbb{F}_q}$ . Then

- $\text{wt}(\mathbf{e}) = t$  and the solution is unique and of multiplicity one satisfying  $\mathbf{u} = \mathbf{u}(\mathbf{e})$ .
- the reduced Gröbner basis  $G$  for the ideal  $J(t, \mathbf{y})$  w.r.t any monomial ordering is

$$\begin{cases} U_i - u_i(\mathbf{e}), i = 1, \dots, n, \\ V_j - v_j, j = 1, \dots, t, \end{cases}$$

where  $(\mathbf{u}(\mathbf{e}), \mathbf{v})$  is the unique solution.

# Quadratic system method

## Features

- No field equations.
- Similar result holds for the complete decoding.
- The solution lies in the field  $\mathbb{F}_q$ .
- The equations are at most quadratic.
- After solving  $J(t, \mathbf{y})$  decoding is simple:

$$B^{-1}\mathbf{u}(B, \mathbf{e}) = B^{-1}B\mathbf{e}^T = \mathbf{e}^T.$$

# Quadratic system method

## Analysis

From  $J(\mathbf{y})$  one can express some  $n - k$   $U$ -variables via  $k$  others. Substitution of those in  $I(t, \mathcal{U}, V)$  yields a systems of  $n$  quadratic equations in  $k + t$  variables, thus obtaining *overdetermined* system. Easier to solve when

- With constant  $k$  and  $t$ ,  $n$  increases.
- With constant  $n$  and  $t$ ,  $k$  decreases.

## Simulations

For example for random binary codes with  $n = 120$  and  $k = 10, \dots, 40$  one can correct 5 – 20 errors in  $\leq 1000$  sec. via computing the reduced Gröbner basis in SINGULAR or MAGMA.

# Quadratic system method

## Analysis

From  $J(\mathbf{y})$  one can express some  $n - k$   $U$ -variables via  $k$  others. Substitution of those in  $I(t, \mathcal{U}, V)$  yields a systems of  $n$  quadratic equations in  $k + t$  variables, thus obtaining *overdetermined* system. Easier to solve when

- With constant  $k$  and  $t$ ,  $n$  increases.
- With constant  $n$  and  $t$ ,  $k$  decreases.

## Simulations

For example for random binary codes with  $n = 120$  and  $k = 10, \dots, 40$  one can correct 5 – 20 errors in  $\leq 1000$  sec. via computing the reduced Gröbner basis in SINGULAR or MAGMA.

# Generalized Newton identities

## GNI for cyclic codes

GNI give rise to several decoding algorithms:

- Polynomial-time up to designed minimum distance: APGZ, Berlekamp-Massey
- Exponential up to true minimum distance: Chen *et.al.*, Augot *et.al.*

It is of interest to find some analogue for arbitrary linear codes.

# Generalized Newton identities

## RS matrix as a special case of MDS

Suppose  $n \leq q$ . Let  $\mathbf{x} = (x_1, \dots, x_n)$  be an  $n$ -tuple of mutually distinct elements in  $\mathbb{F}_q$ . Define  $\mathbf{b}_i = (x_1^{i-1}, \dots, x_n^{i-1})$ . Then  $\mathbf{b}_1, \dots, \mathbf{b}_n$  is an MDS basis. Such a basis is called *Vandermonde basis*. In particular, if  $a \in \mathbb{F}_q^*$  is an element of order  $n$  and  $x_j = a^{j-1}$  for all  $j$ , then  $\mathbf{b}_1, \dots, \mathbf{b}_n$  is called a *Reed-Solomon (RS) basis* and the corresponding matrix is called a *RS matrix* and denoted by  $B(a)$ .

## Structure relations for RS

The above construction gives an RS basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  of  $\mathbb{F}_q^n$  over  $\mathbb{F}_q$  such that  $\mathbf{b}_i * \mathbf{b}_j = \mathbf{b}_{(i+j-1) \bmod n}$ . So

$$\begin{aligned}\mu_l^{ij} &= 1, l = i + j - 1 \bmod n, \\ \mu_l^{ij} &= 0, l \neq i + j - 1 \bmod n\end{aligned}$$

# Generalized Newton identities

## RS matrix as a special case of MDS

Suppose  $n \leq q$ . Let  $\mathbf{x} = (x_1, \dots, x_n)$  be an  $n$ -tuple of mutually distinct elements in  $\mathbb{F}_q$ . Define  $\mathbf{b}_i = (x_1^{i-1}, \dots, x_n^{i-1})$ . Then  $\mathbf{b}_1, \dots, \mathbf{b}_n$  is an MDS basis. Such a basis is called *Vandermonde basis*. In particular, if  $a \in \mathbb{F}_q^*$  is an element of order  $n$  and  $x_j = a^{j-1}$  for all  $j$ , then  $\mathbf{b}_1, \dots, \mathbf{b}_n$  is called a *Reed-Solomon (RS) basis* and the corresponding matrix is called a *RS matrix* and denoted by  $B(a)$ .

## Structure relations for RS

The above construction gives an RS basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  of  $\mathbb{F}_q^n$  over  $\mathbb{F}_q$  such that  $\mathbf{b}_i * \mathbf{b}_j = \mathbf{b}_{(i+j-1) \bmod n}$ . So

$$\begin{aligned}\mu_l^{ij} &= 1, l = i + j - 1 \bmod n, \\ \mu_l^{ij} &= 0, l \neq i + j - 1 \bmod n\end{aligned}$$

# Generalized Newton identities

## GNI for linear codes

Suppose that  $(n, q) = 1$  and let  $a$  be a primitive  $n$ -th root of unity in  $\mathbb{F}$ , where  $\mathbb{F}$  is splitting field of  $X^n - 1$  over  $\mathbb{F}_q$ . Note that  $\mathbb{F} = \mathbb{F}_{q^m}$ , where  $m$  is the smallest positive integer such that  $n \mid (q^m - 1)$ . As an MDS matrix we choose an RS-matrix  $B(a)$ . Now  $I(t, \mathcal{U}, V)$  is generated by

$$\sum_{j=1}^t U_{i+j-1} V_j - U_{i+t}, 1 \leq i \leq n,$$

where indices are taken modulo  $n$ . So  $I(t, \mathcal{U}, V)$  has the form of GNI up to renumbering of indices.

# Generalized Newton identities

## Consistency with GNI for cyclic codes

For the cyclic code  $C$  and received vector  $\mathbf{y} = \mathbf{c} + \mathbf{e}$  let  $s_i, i \in \mathbb{Z}_n$  be the syndromes (both known and unknown) and let  $\sigma_j, 1 \leq j \leq t$  be the coefficients of  $\sigma(Z)$ . Let  $J(t, \mathbf{y})$  be the ideal that corresponds to  $C$  and  $\mathbf{y}$  constructed w.r.t the RS-matrix  $B(a)$ . Assume  $t \leq (d(C) - 1)/2$ , so that  $J(t, \mathbf{y})$  has a unique solution  $(\mathbf{u}(\mathbf{e}), \mathbf{v})$ . Then the following hold:

$$u_i(\mathbf{e}) = s_{i-1}, v_j = -\sigma_{t-j+1}, \forall i, j,$$

where  $s_0 = s_n$ .

## Linear part

We also have that  $J(\mathbf{y})$  is  $U_{i+1} - s_i, i \in S_C$ .

# Generalized Newton identities

## Consistency with GNI for cyclic codes

For the cyclic code  $C$  and received vector  $\mathbf{y} = \mathbf{c} + \mathbf{e}$  let  $s_i, i \in \mathbb{Z}_n$  be the syndromes (both known and unknown) and let  $\sigma_j, 1 \leq j \leq t$  be the coefficients of  $\sigma(Z)$ . Let  $J(t, \mathbf{y})$  be the ideal that corresponds to  $C$  and  $\mathbf{y}$  constructed w.r.t the RS-matrix  $B(a)$ . Assume  $t \leq (d(C) - 1)/2$ , so that  $J(t, \mathbf{y})$  has a unique solution  $(\mathbf{u}(\mathbf{e}), \mathbf{v})$ . Then the following hold:

$$u_i(\mathbf{e}) = s_{i-1}, v_j = -\sigma_{t-j+1}, \forall i, j,$$

where  $s_0 = s_n$ .

## Linear part

We also have that  $J(\mathbf{y})$  is  $U_{i+1} - s_i, i \in S_C$ .

# Generalized Newton identities

## Another Vandermonde basis

In the definition of the Vandermonde basis allow  $a$  to be just the generator of  $\mathbb{F}_q^*$ . Denote the matrix with  $B_V(a)$ . In this case we still have some properties that RS-basis has, namely for  $i$  and  $j$  such that  $i + j \leq n + 1$  holds:

$$\begin{aligned}\mu_l^{ij} &= 1, l = i + j - 1, \\ \mu_l^{ij} &= 0, l \neq i + j - 1.\end{aligned}$$

## Example: Vandermonde code

Consider the binary cyclic code  $C$  of length 39 with defining set  $\{1, 3\}$ ; it is  $[39, 15, 10]$  code.  $d_{BCH} = 7$ , so we may correct 3 errors with linear algebra (e.g. APGZ). Instead of taking RS-matrix for this code which is defined over  $\mathbb{F}_{2^{12}}$  take simply  $\mathbb{F}_{64}$ . Fix  $a$ , a generator of  $\mathbb{F}_{64}^*$  and construct  $B_V(a)$ .

# Generalized Newton identities

## Another Vandermonde basis

In the definition of the Vandermonde basis allow  $a$  to be just the generator of  $\mathbb{F}_q^*$ . Denote the matrix with  $B_V(a)$ . In this case we still have some properties that RS-basis has, namely for  $i$  and  $j$  such that  $i + j \leq n + 1$  holds:

$$\begin{aligned}\mu_l^{ij} &= 1, l = i + j - 1, \\ \mu_l^{ij} &= 0, l \neq i + j - 1.\end{aligned}$$

## Example: Vandermonde code

Consider the binary cyclic code  $C$  of length 39 with defining set  $\{1, 3\}$ ; it is  $[39, 15, 10]$  code.  $d_{BCH} = 7$ , so we may correct 3 errors with linear algebra (e.g. APGZ). Instead of taking RS-matrix for this code which is defined over  $\mathbb{F}_{2^{12}}$  take simply  $\mathbb{F}_{64}$ . Fix  $a$ , a generator of  $\mathbb{F}_{64}^*$  and construct  $B_V(a)$ .

# Generalized Newton identities

## Decoding

Now  $\{1, 2, 3, 4, 5, 6\}$  is one of the "BCH"-intervals of  $C$ , so take the first 6 rows of  $B_V(a)$  as parity-checks for a new code  $C'$  over  $\mathbb{F}_{64}$ . The subfield subcode of  $C'$  over  $\mathbb{F}_2$  is a  $[39, 21, 7]$  code. Note that we have "Newton" structure on the first 6 syndromes, so 3 errors can still be corrected with linear algebra, but now dimension is higher: 21 vs. 15. Some other codes:

cyclic code	Vandermonde code	no.err.corr.with LA
$[39, 15, 10]$	$[39, 21, 7]$	3
$[35, 16, 7]$	$[35, 8, 11]$	2
$[35, 17, 6]$	$[35, 14, 8]$	2
$[39, 24, 6]$	$[39, 32, 4]$	1

Note that the alphabet size is reduced from  $2^{12}$  to  $2^6$ .

# Further research

## Further research

The possible directions of research:

- Study methods of solving  $J(t, \mathbf{y})$  or its equivalents other than Gröbner basis.
- Algorithmic questions connected with the existence of GNI for arbitrary linear codes.
- Adapt an MDS matrix to a given code and try to get something from "almost GNI".
- Generic decoding and the existence of general error-locator polynomial.

# Additional slides: Generalized Newton identities

## Cyclic codes recap

- The code  $C$  is cyclic if for every codeword  $(c_0, c_1, \dots, c_{n-1}) \in C$  the vector  $(c_{n-1}, c_0, \dots, c_{n-2})$  is also in  $C$ .
- The codeword  $(c_0, c_1, \dots, c_{n-1}) \in C$  is represented by a polynomial  $c(x) = \sum_{i=0}^{n-1} c_i X^i$  from the factor ring  $\mathbb{F}_q[X]/\langle X^n - 1 \rangle$ .
- Cyclic codes in  $\mathbb{F}_q^n$  are in one-to-one correspondence with the ideals of  $\mathbb{F}_q[X]/\langle X^n - 1 \rangle$ .

## Defining set

Assume  $(q, n) = 1$ . Let  $\mathbb{F} = \mathbb{F}_{q^m}$  be the splitting field of  $X^n - 1$  over  $\mathbb{F}_q$ . Let  $a$  be a *primitive  $n$ -th root of unity*. Denote by  $S_C = \{i_1, \dots, i_r\} \subseteq \{1, \dots, n\}$  a *defining set* of the cyclic code  $C$ , i.e. the set such that  $c(x) \in C \iff c(a^i) = 0 \forall i \in S_C$ .

# Additional slides: Generalized Newton identities

## Background on cyclic codes

If  $S_C$  is a defining set of the cyclic code  $C$ , then a check matrix  $H$  of  $C$  can be represented as a matrix with entries in  $\mathbb{F}$ :

$$H = \begin{pmatrix} 1 & a^{i_1} & a^{2i_1} & \dots & a^{(n-1)i_1} \\ 1 & a^{i_2} & a^{2i_2} & \dots & a^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a^{i_r} & a^{2i_r} & \dots & a^{(n-1)i_r} \end{pmatrix}.$$

# Additional slides: Generalized Newton identities

## Background on cyclic codes

Let  $\mathbf{y} = \mathbf{c} + \mathbf{e}$ , vectors are also seen as polynomials. Define  $s_i = y(a^i)$  for all  $i = 1, \dots, n$ . Then  $s_i = e(a^i) \forall i \in S_C$ , and these  $s_i$  are the known syndromes. If the error vector is of weight  $t$ , then it is of the form

$$\mathbf{e} = (0, \dots, 0, e_{j_1}, 0, \dots, 0, e_{j_l}, 0, \dots, 0, e_{j_t}, 0, \dots, 0),$$

more precisely there are  $t$  indices  $j_l$  with  $1 \leq j_1 < \dots < j_t \leq n$  such that  $e_{j_l} \neq 0$  for all  $l = 1, \dots, t$  and  $e_j = 0$  for all  $j$  not in  $\{j_1, \dots, j_t\}$ . We obtain

$$s_{i_m} = y(a^{i_m}) = e(a^{i_m}) = \sum_{l=1}^t e_{j_l} (a^{i_m})^{j_l}, 1 \leq m \leq n - k.$$

- $a^{j_1}, \dots, a^{j_t}$  and also the  $j_1, \dots, j_t$  are called the *error locations*
- $e_{j_1}, \dots, e_{j_t}$  are called the *error values*.

# Additional slides: Generalized Newton identities

## GNI for cyclic codes

Define  $z_l = a^{j_l}$  and  $y_l = e_{j_l}$ . Then  $s_{i_m} = \sum_{l=1}^t y_l z_l^{i_m}$ ,  $1 \leq m \leq r$ .

*Error-locator polynomial:*

$$\sigma(Z) = \prod_{l=1}^t (Z - z_l) = Z^t + \sigma_1 Z^{t-1} + \cdots + \sigma_{t-1} Z + \sigma_t,$$

where

$$\sigma_i = (-1)^i \sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq t} z_{j_1} z_{j_2} \cdots z_{j_i}, \quad 1 \leq i \leq t,$$

Generalized Newton identities (GNI):

$$s_i + \sum_{j=1}^t \sigma_j s_{i-j} = 0, \quad \text{for all } i \in \mathbb{Z}_n.$$

# Additional slides: Generalized Newton identities

## Eliminating $U$ -variables

For the case of binary codes it is possible to use Waring function to eliminate  $U$ -variables in  $J(t, \mathbf{y})$ . If  $U$ - and  $V$ -variables are connected via GNI, we have

$$U_{i+1} = W_i(V_t, \dots, V_1), 1 \leq i \leq n-1, U_1 = W_n(V_t, \dots, V_1),$$

where  $W_i$  are Waring functions (polynomials). Thus substituting the above to  $J(\mathbf{y})$  we have the system purely in  $V$ -variables ( $j = 1, \dots, n-k$ ):

$$a_{j1} W_n(V_t, \dots, V_1) + \sum_{l=2}^n a_{jl} W_{l-1}(V_t, \dots, V_1) = s_j(\mathbf{y}).$$

## Additional slides: Generalized Newton identities

### General error-locator polynomial

Recall the notion of the *general error-locator polynomial*. Max Sala proved its existence for cyclic codes and some other families of codes. The question of existence of such a polynomial for an arbitrary linear code remains open. Via an RS-extension  $\mathbb{F}_{q^m}$  it is possible to prove the existence of  $L_C$  over  $\mathbb{F}_{q^m}$ , but we need one over  $\mathbb{F}_q$ !