Course on (algebraic aspects of) Convolutional Codes

Diego Napp

Department of Mathematics, Universidad of Aveiro, Portugal

CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

CIMPA RESEARCH SCHOOL

July 4, 2017

Overview

1. Error-correcting codes: From block codes to convolutional codes
   - Basics: Polynomial encoders
2. Distance properties of convolutional codes
   - Maximum Distance Profile (MDP) and Maximum Distance Separable (MDS)
   - Construction of MDP and MDS: Superregular matrices
3. Decoding of Convolutional codes
   - Viterbi algorithm
   - Decoding of convolutional codes over the erasure channel
4. Network coding with convolutional codes
5. Avenues for further research
   - Motivated by applications: Video streaming and storage systems
   - More theoretical: Multidimensional convolutional codes and convolutional codes over $\mathbb{Z}_{p^r}$

- We assume $G(D)$ is basic and in *row reduced form* with row degrees $\{\nu_1, \ldots, \nu_k\}$
- The set $\{\nu_1, \ldots, \nu_k\}$, called Forney indexes, is the same for all reduced encoders $G(D)$ of $\mathcal{C}$.
- The degree (the size of the memory) is defined as

$$\delta = \sum_{i=1}^{k} \nu_i$$

- The degree δ is also equal to the largest degree of the full size minors of $G(D)$.

- We assume $G(D)$ is basic and in *row reduced form* with row degrees $\{\nu_1, \dots, \nu_k\}$
- The set $\{\nu_1, \dots, \nu_k\}$, called Forney indexes, is the same for all reduced encoders $G(D)$ of $\mathcal{C}$.
- The degree (the size of the memory) is defined as

$$\delta = \sum_{i=1}^{k} \nu_i$$

- The degree δ is also equal to the largest degree of the full size minors of $G(D)$.

Remark

A block code is a convolutional code without memory ($\delta = 0$).

Different points of view

- The Forney indexes are also the same as the Kronecker indexes of the row module

$$\mathcal{M} = \{u(D)G(D) \in \mathbb{F}^n[D] \ : \ u(D) \in \mathbb{F}^k[D]\}$$

when $G(D)$ is basic.

- The Pontryagin dual of $\mathcal{M}$ defines a linear time-invariant behaviors in the sense of Jan Willems, i.e., a linear system. The Forney indexes are the observability indexes.
- $\mathcal{M}$ defines in a natural way a quotient sheaf over the projective line and the Forney indexes are the Grothendieck indexes of the quotient sheaf.

Block codes vs Convolutional codes

- In block coding it is normally considered n and k large.
- Convolutional codes are tipically studied for n and k small and fixed ($n = 2$ and $k = 1$ is common) and for several values of δ.
- Roughly speaking: What matters in block codes is the block length and what matters for convolutional codes is the degree.

Block codes vs Convolutional codes

- In block coding it is normally considered n and k large.
- Convolutional codes are tipically studied for n and k small and fixed ($n = 2$ and $k = 1$ is common) and for several values of δ.
- Roughly speaking: What matters in block codes is the block length and what matters for convolutional codes is the degree.

Convolutional codes

- Decoding over the symmetric channel is difficult.
- The field is typically $\mathbb{F}_2$. The degree cannot be too large so that the Viterbi decoding algorithm is efficient.
- In [Tomas, Rosenthal, Smarandache 2012]:
  - Decoding over the erasure channel is *easy*.
  - Viterbi is not needed, just linear algebra.
- Codes with large field sizes $|\mathbb{F}|$ and degrees δ perform very well.

Day 2: Distance of convolutional codes

Block codes

The intuitive concept of "closeness" of two words is well formalized through Hamming distance $h(x, y)$ of words x, y. For two words x, y

$$h(x, y) = \text{the number of symbols } x \text{ and } y \text{ differ.}$$

Day 2: Distance of convolutional codes

Block codes

The intuitive concept of "closeness" of two words is well formalized through Hamming distance $h(x, y)$ of words x, y. For two words x, y

$$h(x, y) = \text{the number of symbols } x \text{ and } y \text{ differ.}$$

A code $\mathcal{C}$ is a subset of $\mathbb{F}^n$, $\mathbb{F}$ a finite field. An important parameter of $\mathcal{C}$ is its minimal distance.

$$dist(\mathcal{C}) = \min\{h(x, y) \mid x, y \in \mathcal{C}, x \neq y\},$$

Day 2: Distance of convolutional codes

Block codes

The intuitive concept of "closeness" of two words is well formalized through Hamming distance $h(x, y)$ of words x, y. For two words x, y

$$h(x, y) = \text{the number of symbols } x \text{ and } y \text{ differ.}$$

A code $\mathcal{C}$ is a subset of $\mathbb{F}^n$, $\mathbb{F}$ a finite field. An important parameter of $\mathcal{C}$ is its minimal distance.

$$dist(\mathcal{C}) = \min\{h(x, y) \mid x, y \in \mathcal{C}, x \neq y\},$$

Theorem (Basic error correcting theorem)

1. *A code $\mathcal{C}$ can correct up to t errors if $dist(\mathcal{C}) \geq 2t + 1$.*

Day 2: Distance of convolutional codes

Block codes

The intuitive concept of "closeness" of two words is well formalized through Hamming distance $h(x,y)$ of words x,y. For two words x,y

$$h(x,y) = \text{the number of symbols } x \text{ and } y \text{ differ.}$$

A code $\mathcal{C}$ is a subset of $\mathbb{F}^n$, $\mathbb{F}$ a finite field. An important parameter of $\mathcal{C}$ is its minimal distance.

$$dist(\mathcal{C}) = \min\{h(x,y) \mid x,y \in \mathcal{C}, x \neq y\},$$

Theorem (Basic error correcting theorem)

1. *A code $\mathcal{C}$ can correct up to t errors if $dist(\mathcal{C}) \geq 2t+1$.*

The distance is arguably the single most important parameter determining the performance. The larger the distance, the better the code, as a rule.

Distances

Block Codes

A block code $\mathcal{C}$ of rate k/n satisfies the Singleton bound

$$dist(\mathcal{C}) \leq n - k + 1$$

If achieves the bound is called Maximum Distance Separable (MDS).

Distances

Block Codes

A block code $\mathcal{C}$ of rate k/n satisfies the Singleton bound

$$dist(\mathcal{C}) \leq n - k + 1$$

If achieves the bound is called Maximum Distance Separable (MDS).

There are well-known classes of MDS (e.g. Reed-Solomon) over finite fields $\mathbb{F}$ with $|\mathbb{F}| = n - 1$.

Distances

Block Codes

A block code $\mathcal{C}$ of rate k/n satisfies the Singleton bound

$$dist(\mathcal{C}) \leq n - k + 1$$

If achieves the bound is called Maximum Distance Separable (MDS).

There are well-known classes of MDS (e.g. Reed-Solomon) over finite fields $\mathbb{F}$ with $|\mathbb{F}| = n - 1$.

Conjecture

MDS Conjecture: You cannot do better, i.e., if it is MDS then $|\mathbb{F}| \geq n - 1$.

Distances

Block Codes

A block code $\mathcal{C}$ of rate k/n satisfies the Singleton bound

$$dist(\mathcal{C}) \leq n - k + 1$$

If achieves the bound is called Maximum Distance Separable (MDS).

There are well-known classes of MDS (e.g. Reed-Solomon) over finite fields $\mathbb{F}$ with $|\mathbb{F}| = n - 1$.

Conjecture

MDS Conjecture: You cannot do better, i.e., if it is MDS then $|\mathbb{F}| \geq n - 1$.

Exercise

Show that $\mathcal{C}$ with encoder G is MDS iff all full size minors of G are nonzero iff A is a superregular (all minors are nonzero) matrix where $G \approx [I_k \;\; A]$.

Distance of Convolutional Codes

Main problem

How do we construct convolutional codes of a given rate k/n and degree δ with the largest possible distance???

1. First, we introduce the most common distance measures for convolutional codes, namely:
   - Free distance
   - Column distance
2. Second, we see how to construct convolutional codes with good distance properties.

The Hamming weight of a polynomial vector

$$v(D) = \sum_{i \in \mathbb{N}} v_i D^i = v_0 + v_1 D + v_2 D^2 + \cdots \in \mathbb{F}(D)^n,$$

defined as

$$\mathrm{wt}(v(D)) = \sum_{i \in \mathbb{N}} \mathrm{wt}(v_i),$$

where $\mathrm{wt}(v_i)$ is the number of the nonzero components of v_i.

Definition

The free distance of a convolutional code $(\mathcal{C})$ is given by,

$$d_{\mathrm{free}}(\mathcal{C}) \quad = \quad \min \{ \mathrm{wt}(v(D)) \mid v(D) \in \mathcal{C} \quad \text{and} \quad v(D) \neq 0 \}$$

Theorem

A convolutional code $\mathcal{C}$ can correct all error patterns with up to t errors if and only if $d_{\mathrm{free}}(\mathcal{C}) \geq 2t + 1$

Theorem

Rosenthal and Smarandache (1999) showed that the free distance of convolutional code of rate k/n and degree δ must be upper bounded by

$$d_{\text{free}}(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1. \tag{1}$$

This bound was called the generalized Singleton bound since it generalizes in a natural way the Singleton bound for block codes (when $\delta = 0$). A code achieving (1) is called Maximum Distance Separable (MDS).

Let $g(D) = g_0(D^n) + g_1(D^n)D + \dots g_{n-1}(D^n)D^{n-1}$.

Theorem

(J. Massey) Let p be a prime and $r \in \mathbb{N}$. Let $g(D) \in \mathbb{F}[D]$ generate a cyclic code over $\mathbb{F}_{p^r}$ of length N relatively prime to p and of distance d_g. Let n be any positive divisor of N and $k < n$. If $g(D)$ has at most $n-k$ roots in each n-equivalent class, then the generator matrix

$$G(D) = \begin{pmatrix} g_0(D) & g_1(D) & \cdots & \cdots & g_{n-1}(D) \\ g_{n-1}(D)D & g_0(D) & & \cdots & g_{n-2}(D) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_{n-k-1}(D)D & g_{n-k-2}(D)D & \cdots & \cdots & g_{n-k}(D) \end{pmatrix} \tag{2}$$

is basic and reduced and describes a k/n convolutional code of distance $dist(\mathcal{C}) \geq d_g$

Theorem (Rosenthal, et. al)

They selected a very special $g(D)$ that defines a Reed-Solomon to build the *first* construction of MDS convolutional code.

Theorem (Rosenthal, et. al)

They selected a very special $g(D)$ that defines a Reed-Solomon to build the *first* construction of MDS convolutional code.

But they have several constrains on the parameters...it is not completely general.

Theorem (Rosenthal, et. al)

They selected a very special $g(D)$ that defines a Reed-Solomon to build the *first* construction of MDS convolutional code.

But they have several constrains on the parameters...it is not completely general.

J. Simon and M. Guerreiro

Is it possible to use Abelian codes to build (using these ideas) a more general general class of MDS convolutional codes?

There are more notions of distances, such as the active distances, but the most *fundamental* notion of distance for convolutional codes is the following:

There are more notions of distances, such as the active distances, but the most *fundamental* notion of distance for convolutional codes is the following:

Definition

Let $\mathcal{C}$ be a convolutional code. The jth column distance of $\mathcal{C}$, $d_j^c(\mathcal{C})$, (introduced by Costello), given by

$$d_j^c(\mathcal{C}) = \min\left\{\mathrm{wt}(v_{[0,j]}(D)) \mid v(D) \in \mathcal{C} \text{ and } v_0 \neq 0\right\}$$

where $v_{[0,j]}(D) = v_0 + v_1 D + \ldots + v_j D^j$ represents the j-th truncation of the codeword $v(D) \in \mathcal{C}$

The column distances are invariants of the code and satisfy

$$d_0^c \leq d_1^c \leq \cdots \leq \lim_{j \to \infty} d_j^c(\mathcal{C}) = d_{\mathrm{free}}(\mathcal{C}).$$

The column distances are invariants of the code and satisfy

$$d_0^c \leq d_1^c \leq \cdots \leq \lim_{j\to\infty} d_j^c(\mathcal{C}) = d_{\mathrm{free}}(\mathcal{C}).$$

The j-th column distance is upper bounded as following

$$d_j^c(\mathcal{C}) \leq (n-k)(j+1)+1, \tag{3}$$

The column distances are invariants of the code and satisfy

$$d_0^c \leq d_1^c \leq \cdots \leq \lim_{j\to\infty} d_j^c(\mathcal{C}) = d_{\text{free}}(\mathcal{C}).$$

The j-th column distance is upper bounded as following

$$d_j^c(\mathcal{C}) \leq (n-k)(j+1)+1, \tag{3}$$

Since no column distance can achieve a value greater than the generalized Singleton bound, there must exist an integer L for which the bound (3) could be attained for all $j \leq L$; this value is

$$L = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lfloor \frac{\delta}{n-k} \right\rfloor .$$

and the earliest time instant that can achieve the Singleton bound is

$$M = \left\lfloor \frac{\delta}{k} \right\rfloor + \left\lceil \frac{\delta}{n-k} \right\rceil .$$

Definition (Gluesing-Luerssen, Rosenthal, Smadandache (2006))

A convolutional code $\mathcal{C}$ of rate k/n and degree δ with every $d_j^c(\mathcal{C})$ maximal, for each $j \leq L$ is said to have a maximum distance profile (MDP), i.e., if

$$d_j^c = (n-k)(j+1)+1, \ \text{ for } j = 0, \ldots, L.$$

And it is called strongly MDS (sMDS) if it is MDS at time M.

Definition (Gluesing-Luerssen,Rosenthal,Smadandache (2006))

A convolutional code $\mathcal{C}$ of rate k/n and degree δ with every $d_j^c(\mathcal{C})$ maximal, for each $j \leq L$ is said to have a maximum distance profile (MDP), i.e., if

$$d_j^c = (n-k)(j+1)+1, \text{ for } j = 0, \dots, L.$$

And it is called strongly MDS (sMDS) if it is MDS at time M.

Remark

MDS $\not\Rightarrow$ sMDP and sMDS $\not\Leftarrow$ MDP

Remark

When $(n-k)|\delta$ (i.e. all Forney indices are equal), then

$$\text{MDS} \Leftrightarrow \text{sMDP}$$

Yet another interesting notion

Let $\mathcal{C}$ with parity-check $H(D) = H_0 + H_1 D + \cdots H_\nu D^\nu$. Then $\overline{H}(D) = H_\nu + H_{\nu-1} D + \cdots + H_0 D^\nu$ defines a (reverse) conv. code $\overline{\mathcal{C}}$ with the property that

$$v_0 + v_1 D + \cdots v_s D^s \in \mathcal{C}$$

if and only if

$$v_s + v_{s-1} D + \cdots v_0 D^s \in \overline{\mathcal{C}}$$

A MDP convolutional code $\mathcal{C}$ if called reverse-MDP if $\overline{\mathcal{C}}$ is also MDP.

Yet another interesting notion

Let $\mathcal{C}$ with parity-check $H(D) = H_0 + H_1 D + \cdots H_\nu D^\nu$. Then $\overline{H}(D) = H_\nu + H_{\nu-1} D + \cdots + H_0 D^\nu$ defines a (reverse) conv. code $\overline{\mathcal{C}}$ with the property that

$$v_0 + v_1 D + \cdots v_s D^s \in \mathcal{C}$$

if and only if

$$v_s + v_{s-1} D + \cdots v_0 D^s \in \overline{\mathcal{C}}$$

A MDP convolutional code $\mathcal{C}$ if called reverse-MDP if $\overline{\mathcal{C}}$ is also MDP.

Fundamental Questions

Come up with constructions of sMDS and (reverse) MDP convolutional codes.

- Allen conjecture (1999) the existence of convolutional codes that are both sMDS and MDP when $k = 1$ and $n = 2$.

- Allen conjecture (1999) the existence of convolutional codes that are both sMDS and MDP when $k = 1$ and $n = 2$.
- Smarandache et. al (2001), provided the first concrete construction of MDS convolutional codes with some restrictions on the rates and degrees.

- Allen conjecture (1999) the existence of convolutional codes that are both sMDS and MDP when $k = 1$ and $n = 2$.
- Smarandache et. al (2001), provided the first concrete construction of MDS convolutional codes with some restrictions on the rates and degrees.
- Rosenthal et. al (2005), provided a non-constructive proof (using algebraic geometry) of the existence of MDP convolutional codes.

- Allen conjecture (1999) the existence of convolutional codes that are both sMDS and MDP when $k=1$ and $n=2$.
- Smarandache et. al (2001), provided the first concrete construction of MDS convolutional codes with some restrictions on the rates and degrees.
- Rosenthal et. al (2005), provided a non-constructive proof (using algebraic geometry) of the existence of MDP convolutional codes.
- Gluessing-Luerssen et. al (2006), provided the first concrete construction of MDP convolutional codes for all parameters. And conjectured the existence of sMDS convolutional codes that are also MDP (proved in the case $(n-k)|\delta$).

- Allen conjecture (1999) the existence of convolutional codes that are both sMDS and MDP when $k = 1$ and $n = 2$.
- Smarandache et. al (2001), provided the first concrete construction of MDS convolutional codes with some restrictions on the rates and degrees.
- Rosenthal et. al (2005), provided a non-constructive proof (using algebraic geometry) of the existence of MDP convolutional codes.
- Gluessing-Luerssen et. al (2006), provided the first concrete construction of MDP convolutional codes for all parameters. And conjectured the existence of sMDS convolutional codes that are also MDP (proved in the case $(n-k)|\delta$).
- Hutchinson (2008) gave a non-constructive proof of the existence of conv. codes both MDP and sMDS for all rates and degrees.

- Allen conjecture (1999) the existence of convolutional codes that are both sMDS and MDP when $k = 1$ and $n = 2$.
- Smarandache et. al (2001), provided the first concrete construction of MDS convolutional codes with some restrictions on the rates and degrees.
- Rosenthal et. al (2005), provided a non-constructive proof (using algebraic geometry) of the existence of MDP convolutional codes.
- Gluessing-Luerssen et. al (2006), provided the first concrete construction of MDP convolutional codes for all parameters. And conjectured the existence of sMDS convolutional codes that are also MDP (proved in the case $(n-k)|\delta$).
- Hutchinson (2008) gave a non-constructive proof of the existence of conv. codes both MDP and sMDS for all rates and degrees.
- Napp and Smarandache (2016) provided the first concrete construction of convolutional codes that are both sMDS and MDP for all rates and degrees.

Problem

They all require huge finite fields.

Problem

They all require huge finite fields.

Another constructions with excellent distance properties

- Cyclic convolutional codes, Gluesing-Luerssen et al. (2008) which rely on a nontrivial automorphism of the algebra $\mathbb{F}[D]/(D^n - 1)$.
- Goppa convolutional codes, Muñoz Porras et. al. (2013). Convolutional Goppa Codes over algebraic curves. Examples over the projective line and over elliptic curves are provided.

The $G(D)$ be an encoder and $H(D)$ a parity-check of $\mathcal{C}$, i.e.,

$$\begin{aligned}\mathcal{C} &= \mathrm{Im}_{\mathbb{F}[D]} G(D) = \left\{ u(D)G(D) : \ u(D) \in \mathbb{F}^k[D] \right\} \\ &= \ker_{\mathbb{F}[D]} H(D) = \{ v(D) \in \mathbb{F}^n[D] : \ v(D)H(D) = 0 \}\end{aligned}$$

H_j^c, called the sliding parity-check matrix, is defined as

$$H_j^c = \begin{pmatrix} H_0 & & & \\ H_1 & H_0 & & \\ \vdots & \vdots & \ddots & \\ H_j & H_{j-1} & \cdots & H_0 \end{pmatrix} \in \mathbb{F}^{(j+1)(n-k) \times (j+1)n},$$

where $H_j = 0$, for $j > m$. Then

$$\begin{aligned} d_j^c(\mathcal{C}) &= \min \left\{ \mathrm{wt}(v_{[0,j]}(D)) \ \middle| \ v(D) \in \mathcal{C} \ \text{ and } \ v_0 \neq 0 \right\} \\ & \min \left\{ wt(\hat{v}) \ \middle| \ \hat{v} = (v_0, \ldots, v_j)^\top \in \ker H_j^c \subset \mathbb{F}^{(j+1)n}, \ v_0 \neq 0 \right\} \end{aligned}$$

LT-Superregular matrices

Definition [Gluesing-Luerssen,Rosenthal,Smadandache (2006)]

A lower triangular matrix

$$B = \begin{pmatrix} a_0 & & & \\ a_1 & a_0 & & \\ \vdots & \vdots & \ddots & \\ a_j & a_{j-1} & \cdots & a_0 \end{pmatrix} \tag{4}$$

is *LT-superregular* if all of its minors, with no zeros in the diagonal, are nonsingular.

Remark

Note that due to such a lower triangular configuration the remaining minors are necessarily zero.

Example

$$\beta^3+\beta+1=0 \;\Rightarrow \begin{pmatrix} 1 & & & & \\ \beta & 1 & & & \\ \beta^3 & \beta & 1 & & \\ \beta & \beta^3 & \beta & 1 & \\ 1 & \beta & \beta^3 & \beta & 1 \end{pmatrix} \in \mathbb{F}_{2^5}^{5\times 5} \text{ is superregular}$$

Example

$$\epsilon^5+\epsilon^2+1=0 \;\Rightarrow \begin{pmatrix} 1 & & & & & & \\ \epsilon & 1 & & & & & \\ \epsilon^6 & \epsilon & 1 & & & & \\ \epsilon^9 & \epsilon^6 & \epsilon & 1 & & & \\ \epsilon^6 & \epsilon^9 & \epsilon^6 & \epsilon & 1 & & \\ \epsilon & \epsilon^6 & \epsilon^9 & \epsilon^6 & \epsilon & 1 & \\ 1 & \epsilon & \epsilon^6 & \epsilon^9 & \epsilon^6 & \epsilon & 1 \end{pmatrix} \in \mathbb{F}_{2^5}^{7\times 7} \text{ is superregular}$$

Theorem

Let $\mathcal{C} = \{v(D) \in \mathbb{F}((D))^n \mid H(D)v(D) = 0\}$

$$H(D) = \sum_{i=0}^{m} H_i D^i = \sum_{i=0}^{m} \begin{bmatrix} A_i & B_i \end{bmatrix} D^i = \begin{bmatrix} A(D) & B(D) \end{bmatrix} \in \mathbb{F}[D]^{(n-k)\times n},$$

where $m = \lceil \frac{\delta}{n-k} \rceil$. *Assume in addition that* A_0 *is invertible and let*

$$A(D)^{-1}B(D) = \sum_{i=0}^{\infty} P_i D^i \in \mathbb{F}((D))^{(n-k)\times k}$$

be the Laurent expansion of $A(D)^{-1}B(D)$ *over the field* $\mathbb{F}((D))$. *Define*

$$\widehat{H}_j^c = \begin{bmatrix} I_{(j+1)(n-k)} & P_j^c \end{bmatrix} \text{ with } P_j^c = \begin{pmatrix} P_0 & & & \\ P_1 & P_0 & & \\ \vdots & \vdots & \ddots & \\ P_j & P_{j-1} & \cdots & P_0 \end{pmatrix}.$$

Theorem cont.

Then, the following conditions are equivalent, for all $j \in \{1, \ldots, L\}$:

1. $d_j^c = (n-k)(j+1)+1$;, i.e., $\mathcal{C}$ is MDP;
2. every nontrivial $(n-k)(j+1) \times (n-k)(j+1)$ full-size minor of H_j^c is nonzero.
3. P_j^c is superregular;

Theorem cont.

Then, the following conditions are equivalent, for all $j \in \{1, \ldots, L\}$:

1. $d_j^c = (n-k)(j+1)+1$;, i.e., $\mathcal{C}$ is MDP;
2. every nontrivial $(n-k)(j+1) \times (n-k)(j+1)$ full-size minor of H_j^c is nonzero.
3. P_j^c is superregular;

The construction of MDP convolutional codes boils down to the construction of superregular matrices.

Remarks

- In the context of block codes, the matrices are full, i.e., have all the entries nonzero. Cauchy or Vandermonde matrices are examples of matrices having all their mains nonzero.
- Construction of classes of superregular matrices is very difficult due to their triangular configuration.
- Only two classes exist:

1. Rosenthal et al. (2006) presented the first construction. For any n there exists a prime number p such that

$$\begin{pmatrix} \binom{n}{0} & & & \\ \binom{n-1}{1} & \binom{n}{0} & & \\ \vdots & \ddots & \ddots & \\ \binom{n-1}{n-1} & \cdots & \binom{n-1}{1} & \binom{n}{0} \end{pmatrix} \in \mathbb{F}_p^{n\times n}$$

is superregular. Bad news: Requires a field with very large characteristic.

Remarks

2. Almeida, Napp and Pinto (2013) first construction over any characteristic: Let α be a primitive element of a finite field $\mathbb{F}$ of characteristic p. If $|\mathbb{F}| \geq p^{2^M}$ then the following matrix

$$\begin{bmatrix} \alpha^{2^0} & & & & \\ \alpha^{2^1} & \alpha^{2^0} & & & \\ \alpha^{2^2} & \alpha^{2^1} & \alpha^{2^0} & & \\ \vdots & & \ddots & \ddots & \\ \alpha^{2^{M-1}} & \cdots & & \cdots & \alpha^{2^0} \end{bmatrix}.$$

is LT-superregular. Bad news: $|\mathbb{F}|$ very large.

Construction of Reverve-MDP

In order to construct (n, k, δ) reverse-MDP (for $(n-k)|\delta)$ we need to construct

$$\begin{pmatrix} a_0 & & & \\ a_1 & a_0 & & \\ \vdots & \vdots & \ddots & \\ a_j & a_{j-1} & \cdots & a_0 \end{pmatrix} \text{ and } \begin{pmatrix} a_j & & & \\ a_{j-1} & a_0 & & \\ \vdots & \vdots & \ddots & \\ a_0 & a_1 & \cdots & a_j \end{pmatrix}$$

both LT-superregular.

Reverse-MDP

1. We do not have a characterization in terms of LT-superregular matrices when $(n-k) \nmid \delta$.
2. Although there are some clever ideas and several particular examples, only the construction of Almeida, Napp and Pinto (2013) gives a general construction of reverse superregular.

Fundamental Open Problem

Main problem

Come up with constructions of superregular matrices over *not too large* fields.

Based on many examples (performed with a computer algebra program) it has been conjectured that this is possible.

Exercise

Come up with a 11×11 superregular matrix over a finite field.