The Weight Adjacency Matrix of a Convolutional Code

Heide Gluesing-Luerssen

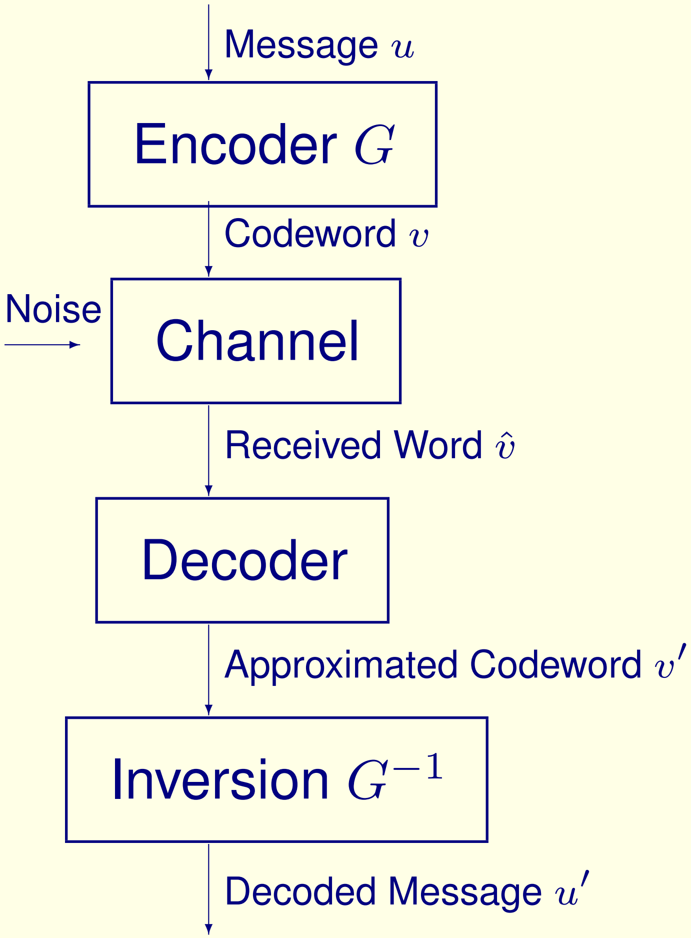
Department of Mathematics
University of Kentucky

April 2007

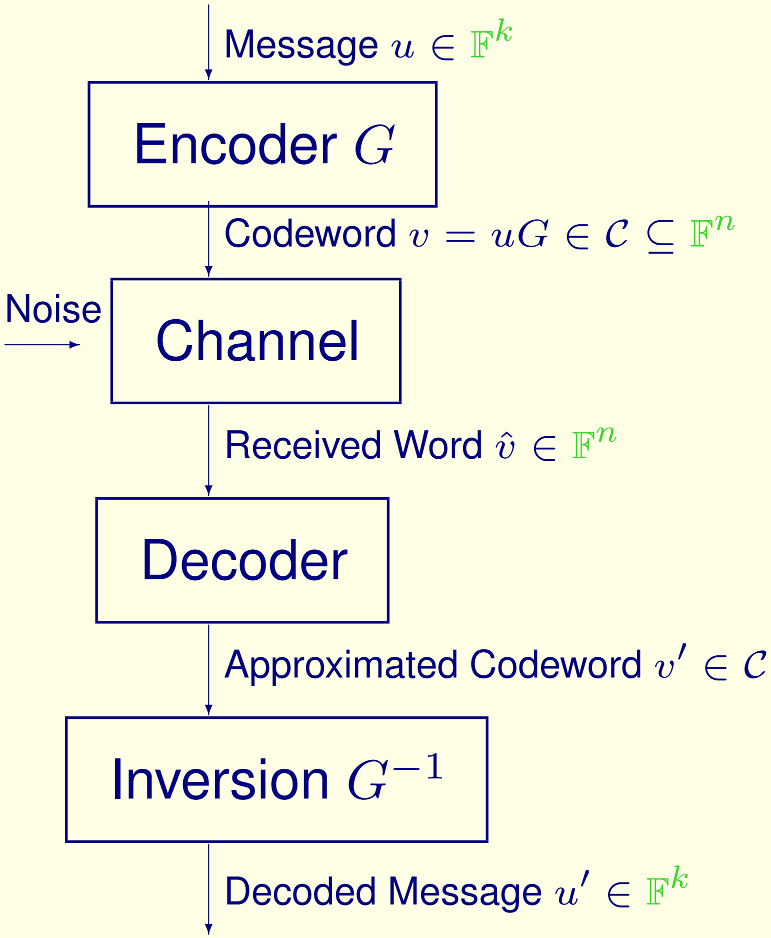
Contents

What is a Convolutional Code?

What is a Convolutional Code?



What is a Convolutional Code?

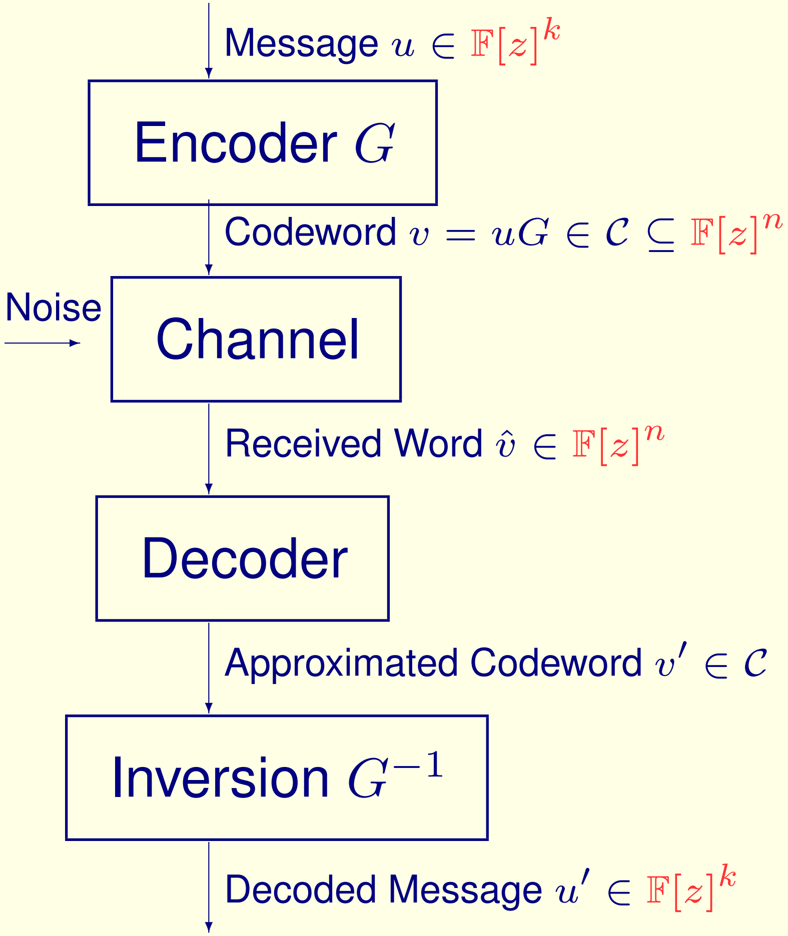


Block Codes:

- Message $u \in \mathbb{F}^k$
- Encoder $G \in \mathbb{F}^{k \times n}$
- Codewords $v = uG \in \mathbb{F}^n$
- Block code $\subseteq \mathbb{F}^n$

where $\mathbb{F}$ is a finite field.

What is a Convolutional Code?



Convolutional Codes:

- Message $u \in \mathbb{F}[z]^k$
- Encoder $G \in \mathbb{F}[z]^{k \times n}$
- Codewords $v = uG \in \mathbb{F}[z]^n$
- Convolutional code $\subseteq \mathbb{F}[z]^n$

where $\mathbb{F}$ is a finite field.

What is a Convolutional Code?

Notation:

$$\mathbb{F}[z]^n = \left\{ (v^{(1)}, \ldots, v^{(n)}) \,\middle|\, v^{(i)} \in \mathbb{F}[z] \right\} = \left\{ \sum_{t=0}^{N} v_t z^t \,\middle|\, N \in \mathbb{N},\ v_t \in \mathbb{F}^n \right\}$$

E. g., in $\mathbb{F}_5[z]^3$

$$(1 + 3z + z^2 + 2z^3,\ z,\ 2 + 4z + 3z^2) = (1, 0, 2) + (3, 1, 4)z + (1, 0, 3)z^2 + (2, 0, 0)z^3.$$

Interpretation

Message: $u \in \mathbb{F}[z]^k$, $u = \sum_{t\geq 0}^{N} u_t z^t$

= sequence of message blocks $u_0, \ldots, u_N \in \mathbb{F}^k$

Encoder: $G \in \mathbb{F}[z]^{k\times n}$, $G = \sum_{j=0}^{m} G_j z^j$, where $G_j \in \mathbb{F}^{k\times n}$

Codeword: $v = uG$

$$= \Big(\sum_{t\geq 0}^{N} u_t z^t\Big)\Big(\sum_{j=0}^{m} G_j z^j\Big) = \sum_{t\geq 0}^{N+m} \sum_{j=0}^{m} u_{t-j} G_j z^t$$

$$= \underbrace{u_0 G_0}_{v_0} + \underbrace{(u_1 G_0 + u_0 G_1)}_{v_1} z + \underbrace{(u_2 G_0 + u_1 G_1 + u_0 G_2)}_{v_2} z^2$$

$$+ \ldots$$

= sequence of codeword blocks $v_0, \ldots, v_{N+m} \in \mathbb{F}^n$

What is a Convolutional Code?

$\mathbb{F}$ finite field, $\mathbb{F}[z]^n := \{(v^{(1)}, \dots, v^{(n)}) \mid v^{(i)} \in \mathbb{F}[z]\}$.

Convolutional Code: $\mathcal{C} \subseteq \mathbb{F}[z]^n$ submodule

Encoder Matrix: $G \in \mathbb{F}[z]^{k \times n}$

$\mathcal{C} := \text{im } G = \{uG \mid u \in \mathbb{F}[z]^k\} \subseteq \mathbb{F}[z]^n$

Encoding: $\mathbb{F}[z]^k \longrightarrow \mathbb{F}[z]^n, \quad u \longmapsto uG$

Degree: $\delta := \deg(\mathcal{C}) = \max\{\deg \gamma \mid \gamma \text{ is a } k\text{-minor of } G\}$.

What is a Convolutional Code?

$\mathbb{F}$ finite field, $\quad \mathbb{F}[z]^n := \{(v^{(1)}, \dots, v^{(n)}) \mid v^{(i)} \in \mathbb{F}[z]\}$.

Convolutional Code: $\mathcal{C} \subseteq \mathbb{F}[z]^n$ submodule — direct summand

$\Updownarrow$

Encoder Matrix: $G \in \mathbb{F}[z]^{k \times n}$ — $\exists\, \tilde{G} \in \mathbb{F}[z]^{n \times k} : \quad G\tilde{G} = I_k$

$$\mathcal{C} := \text{im } G = \{uG \mid u \in \mathbb{F}[z]^k\} \subseteq \mathbb{F}[z]^n$$

Encoding: $\mathbb{F}[z]^k \longrightarrow \mathbb{F}[z]^n, \quad u \longmapsto uG$

Degree: $\delta := \deg(\mathcal{C}) = \max\{\deg \gamma \mid \gamma \text{ is a } k\text{-minor of } G\}$.

Error Correction

Distance of a Code

Weight in $\mathbb{F}^n$: $\mathsf{wt}(v^{(1)}, \ldots, v^{(n)}) = \#\{i \mid v^{(i)} \neq 0\}$.

Weight in $\mathbb{F}[z]^n$: $\mathsf{wt}\Big(\sum_{t=0}^{N} v_t z^t\Big) := \sum_{t=0}^{N} \mathsf{wt}(v_t), \qquad v_t \in \mathbb{F}^n.$

Distance in $\mathbb{F}[z]^n$: $\mathsf{d}\,(v, v') = \mathsf{wt}(v - v')$.

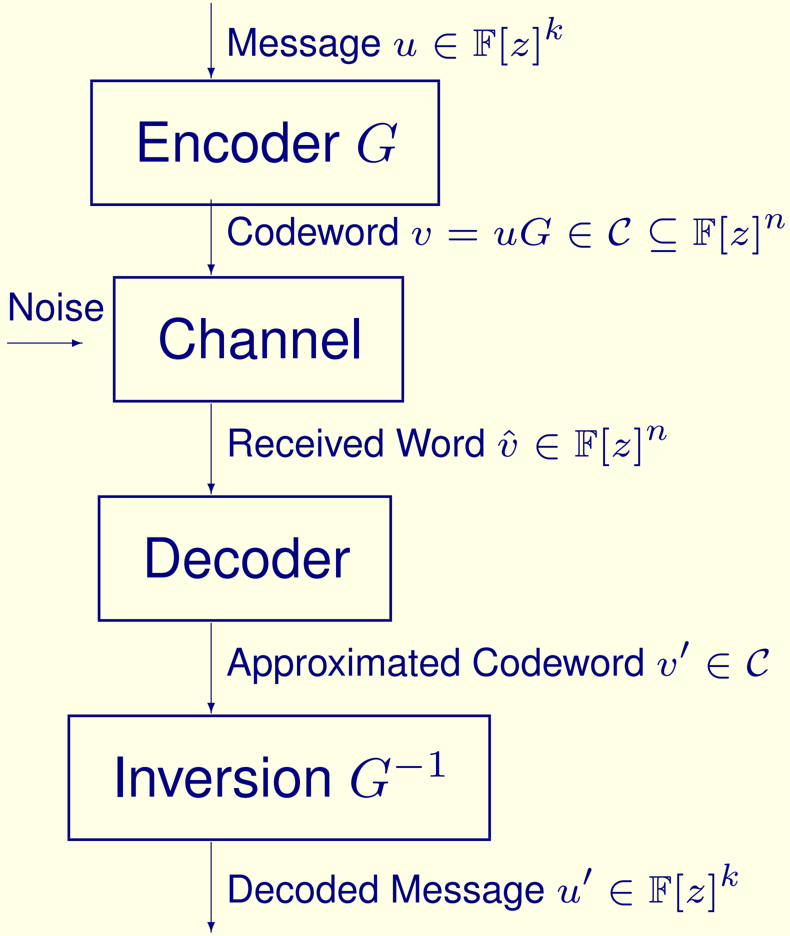
Distance of a code:

$$\begin{aligned} \mathsf{dist}(\mathcal{C}) &= \min\{\mathsf{d}\,(v, v') \mid v, v' \in \mathcal{C},\ v \neq v'\} \\ &= \min\{\mathsf{wt}(v) \mid v \in \mathcal{C},\ v \neq 0\}. \end{aligned}$$

Example: In $\mathbb{F}_5[z]^3$

$$\mathsf{wt}(1{+}3z{+}z^2{+}2z^3,\ z,\ 2{+}4z{+}3z^2) = \mathsf{wt}(1,0,2) + \mathsf{wt}(3,1,4) + \mathsf{wt}(1,0,3) + \mathsf{wt}(2,0,0) = 8.$$

Interpretation



$$\mathrm{d}\,(v, \hat{v}) = \#\{\text{transmission errors}\}$$

Decoding:

Given $\hat{v} \in \mathbb{F}[z]^n$.

Find a codeword $v' \in \mathcal{C}$ such that

$$\mathrm{d}\,(\hat{v}, v')) = \min_{\tilde{v} \in \mathcal{C}} \mathrm{d}\,(\hat{v}, \tilde{v}).$$

If at most $\frac{\mathrm{dist}(\mathcal{C})-1}{2}$ errors have occurred during transmission, then $v' = v$.

Efficient Decoding: Viterbi algorithm

Convolutional Codes used in Engineering Practice

- Mobile communication systems often use the industry standard code

$$\mathcal{C} = \text{im}\left(1 + z^2 + z^3 + z^5 + z^6 \quad 1 + z + z^2 + z^3 + z^6\right) \subseteq \mathbb{F}_2[z]^2; \quad \text{dist}(\mathcal{C}) = 10.$$

- Recent deep space missions like Mars Pathfinder (1996), Mars Exploration Rover (2003), and Cassini-Huygens (2004) use a

binary code with $(n = 6,\ k = 1,\ \delta = 14)$ and distance 56.

Weight Enumeration

Weight Enumeration

How many codewords of given weight are in $\mathcal{C}$?

<u>**Weight Enumerator of a block code:**</u> $\mathcal{C} \subseteq \mathbb{F}^n$

$$\mathsf{we}(\mathcal{C}) := \sum_{i=0}^{n} \lambda_i W^i \in \mathbb{C}[W], \quad \text{where } \lambda_i := \#\{v \in \mathcal{C} \mid \mathsf{wt}(v) = i\},$$

$$= \sum_{v \in \mathcal{C}} W^{\mathsf{wt}(v)} \; .$$

MacWilliams Identity Theorem for Block Codes

Let $\mathcal{C} \subseteq \mathbb{F}^n$ be an (n, k) block code.

Dual Code:

$$\mathcal{C}^{\perp} := \big\{ w \in \mathbb{F}^n \,\big|\, \langle w, v \rangle = wv^t = 0 \ \text{ for all } v \in \mathcal{C} \big\}.$$

MacWilliams Identity Theorem '62: Let $\mathbb{F} = \mathbb{F}_q$. Then

$$\text{we}(\mathcal{C}^{\perp}) = q^{-k}\mathbf{M}\big(\text{we}(\mathcal{C})\big),$$

where

$$\begin{aligned} \mathbf{M} : \mathbb{C}[W]_{\leq n} &\longrightarrow \quad \mathbb{C}[W]_{\leq n} \\ f &\longmapsto \big(1 + (q-1)W\big)^n f\big(\tfrac{1-W}{1+(q-1)W}\big). \end{aligned}$$

MacWilliams Identity Theorem for Block Codes

Relevance of the Identity Theorem:

- Practical computation of the weight enumerator for high dimensional codes, e. g. Hamming codes.
- Theoretical consequence:
  All (n, k) MDS block codes over $\mathbb{F}_q$ have the same weight enumerator.
- Weight enumerators for self-dual codes.

Extensions to Block Codes over Rings:

Wood (1999), Mittelholzer (1999), Dougherty (2005), ...

Is there a MacWilliams Identity for Convolutional Codes?

Dual Codes

Definition: The dual of $\mathcal{C} \subseteq \mathbb{F}[z]^n$ is defined as

$$\mathcal{C}^\perp := \{w \in \mathbb{F}[z]^n \mid wv^\mathsf{T} = 0 \text{ for all } v \in \mathcal{C}\}.$$

Then

- $\deg(\mathcal{C}) = \deg(\mathcal{C}^\perp)$.
- $\mathcal{C}^{\perp\perp} = \mathcal{C}$ (since $\mathcal{C}$ is a direct summand of $\mathbb{F}[z]^n$).

Weight Enumerator for Convolutional Codes

$$\mathcal{C} \subseteq \mathbb{F}[z]^n$$

Classical weight enumerator:

$$\text{we}(\mathcal{C}) \in \mathbb{C}[\![W,\ L]\!] \quad (W \equiv \text{ weight},\ L \equiv \text{ degree})$$

Weight Enumerator for Convolutional Codes

$$\mathcal{C} \subseteq \mathbb{F}[z]^n$$

Classical weight enumerator:

$$\text{we}(\mathcal{C}) \in \mathbb{C}[\![W, L]\!] \quad (W \equiv \text{ weight}, \; L \equiv \text{ degree})$$

There is no MacWilliams Identity!

Example: (Shearer/McEliece '77)

$$\text{we}(\mathcal{C}_1) = \text{we}(\mathcal{C}_2) \text{ and } \text{we}(\mathcal{C}_1^\perp) \neq \text{we}(\mathcal{C}_2^\perp).$$

Towards an Improved Weight Enumerator

Improved Weight Enumerator

$$\mathcal{C} = \text{im}\, G = \{uG \mid u \in \mathbb{F}[z]^k\} \subseteq \mathbb{F}[z]^n, \quad G \in \mathbb{F}[z]^{k\times n}$$

Systems Theory:

There exist matrices A, B, C, D over $\mathbb{F}$ such that

$$\sum_{t\geq 0} v_t z^t = \Big(\sum_{t\geq 0} u_t z^t\Big) G \iff \begin{cases} x_{t+1} &= x_t A + u_t B \\ v_t &= x_t C + u_t D \end{cases} \quad \text{and } x_0 = 0.$$

Input-State-Output System:

- input = sequence of message blocks
- output = sequence of codeword blocks
- state x_t = memory of the encoder at time t $\quad$ $x_t \in \mathbb{F}^\delta$ where $\delta = \text{deg}(\mathcal{C})$

State Transition Diagram

Example: $G = \begin{pmatrix} 1+z+z^2+z^3, & 1+z^2+z^3 \end{pmatrix} \in \mathbb{F}_2[z]^{1\times 2}$

Input-State-Output System:

$$x_{t+1} = x_t \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} + u_t \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

$$v_t = x_t \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} + u_t \begin{pmatrix} 1 & 1 \end{pmatrix}$$

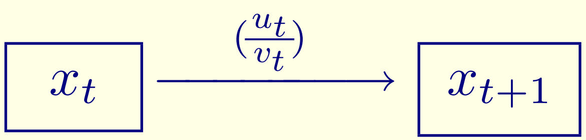
State Transition Diagram

Example: $G = \left(1 + z + z^2 + z^3, \quad 1 + z^2 + z^3\right) \in \mathbb{F}_2[z]^{1\times 2}$

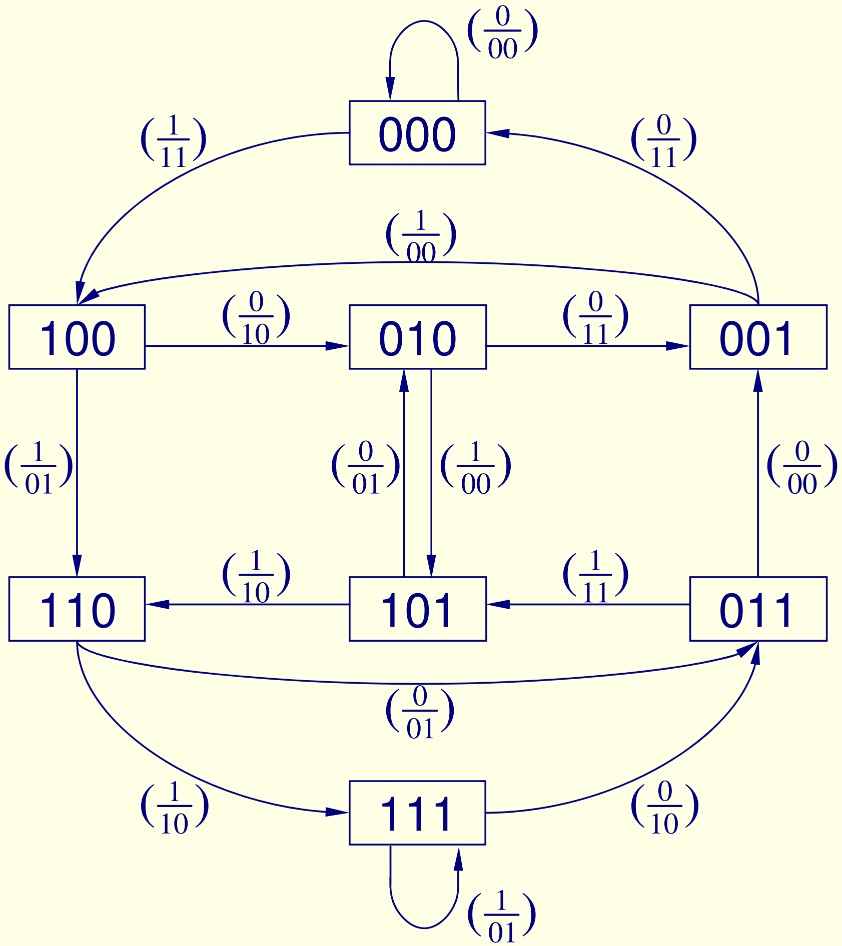
Input-State-Output System:

$$x_{t+1} = x_t \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} + u_t \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$$

$$v_t = x_t \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} + u_t \begin{pmatrix} 1 & 1 \end{pmatrix}$$

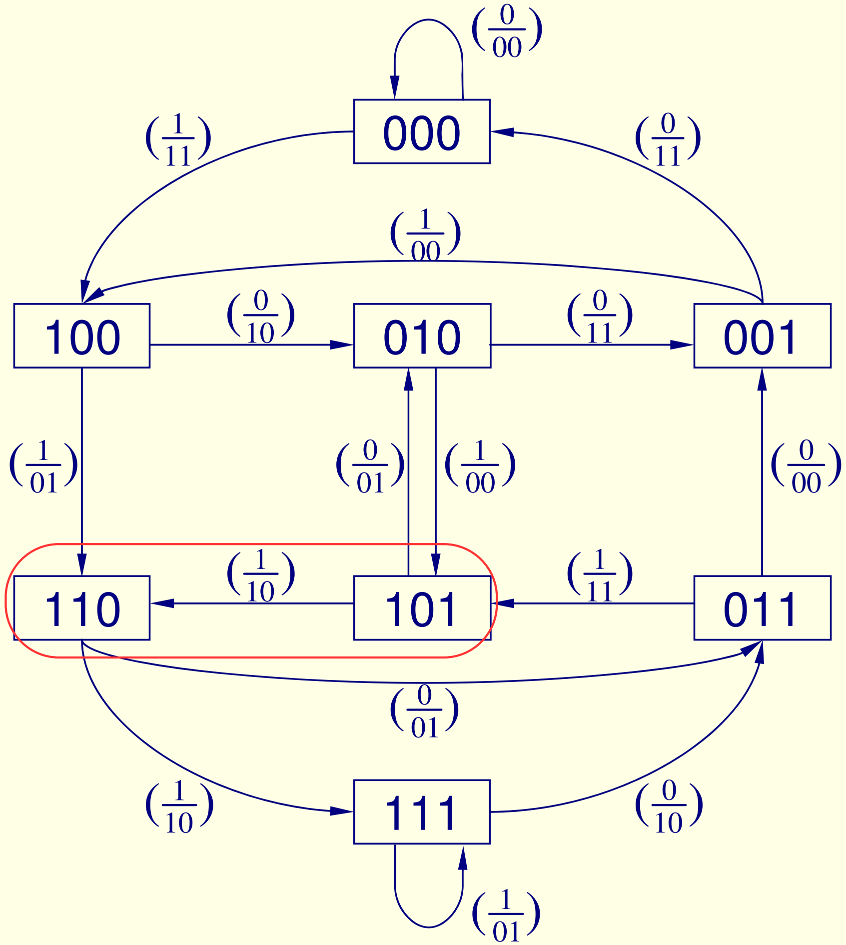


State Transition Diagram:



Weight Adjacency Matrix

State Transition Diagram:

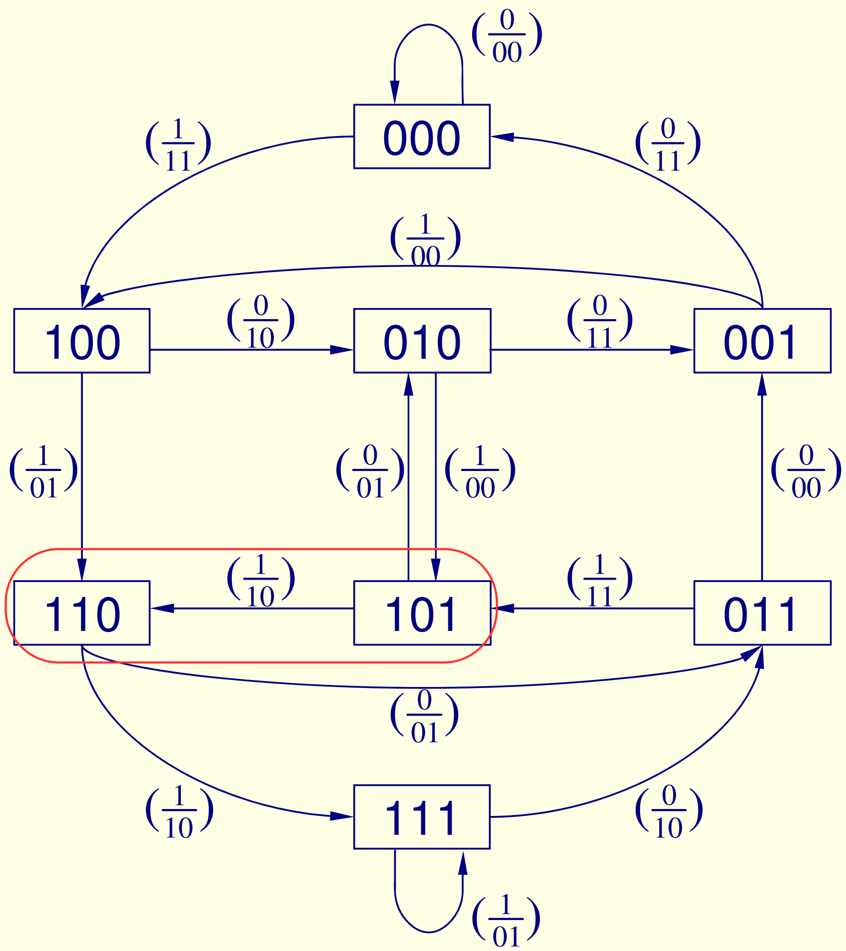


Weight Adjacency Matrix:

	000	001	010	011	100	101	110	111
000	1	0	0	0	W^2	0	0	0
001	W^2	0	0	0	1	0	0	0
010	0	W^2	0	0	0	1	0	0
011	0	1	0	0	0	W^2	0	0
100	0	0	W	0	0	0	W	0
101	0	0	W	0	0	0	W	0
110	0	0	0	W	0	0	0	W
111	0	0	0	W	0	0	0	W

Weight Adjacency Matrix

State Transition Diagram:



Weight Adjacency Matrix:

$$
\begin{array}{c} \\ 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ {\color{red}101} \\ 110 \\ 111 \end{array}
\begin{array}{c}
\begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & {\color{red}110} & 111 \end{array} \\
\begin{pmatrix}
1 & 0 & 0 & 0 & W^2 & 0 & 0 & 0 \\
W^2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & W^2 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & W^2 & 0 & 0 \\
0 & 0 & W & 0 & 0 & 0 & W & 0 \\
0 & 0 & W & 0 & 0 & 0 & {\color{red}W} & 0 \\
0 & 0 & 0 & W & 0 & 0 & 0 & W \\
0 & 0 & 0 & W & 0 & 0 & 0 & W
\end{pmatrix}
\end{array}
$$

Depends on G and $(A,\ B,\ C,\ D)$.

Uniqueness of the Weight Adjacency Matrix

Theorem: (G_L'05)
Let Λ, Λ' be the WAMs of the code $\mathcal{C}$ obtained from the systems (A, B, C, D) and (A', B', C', D'). Then

$$\exists\, T \in GL_\delta(\mathbb{F}) :\ \Lambda'_{XT,YT} = \Lambda_{X,Y} \text{ for all } X,\, Y \in \mathbb{F}^\delta.$$

Hence $\Lambda' = P^{-1}\Lambda P$ for some permutation matrix $P \in GL_{q^\delta}(\mathbb{C})$.
If $\delta = 1$ then $\Lambda = \Lambda'$.

Proof:
1) $(A', B', C', D') = (T^{-1}(A - MB)T,\, UBT,\, T^{-1}(C - MD),\, UD)$ for some T, M, U.

2) $$\left.\begin{array}{rcl} Y &=& XA + uB \\ v &=& XC + uD \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{rcl} YT &=& XTA' + (uU^{-1} + XMU^{-1})B' \\ v &=& XTC' + (uU^{-1} + XMU^{-1})D'. \end{array}\right.$$

3) $\delta = 1$, then $T = \alpha \in \mathbb{F}^*$ and $X \xrightarrow{\left(\frac{u}{v}\right)} Y \Longleftrightarrow \alpha X \xrightarrow{\left(\frac{\alpha u}{\alpha v}\right)} \alpha Y$ and $\text{wt}(\alpha v) = \text{wt}(v)$.

Weight Adjacency Matrix of a Code

Factor out the group action induced by $GL_\delta(\mathbb{F})$:

Generalized Weight Adjacency Matrix:

Let $\mathcal{C} \subseteq \mathbb{F}[z]^n$ and Λ be a WAM of $\mathcal{C}$. Then

$$\Lambda(\mathcal{C}) := \left\{\Lambda' \,\middle|\, \exists\, T \in GL_\delta(\mathbb{F})\colon \Lambda'_{X,Y} = \Lambda_{XT,YT} \text{ for all } X,Y \in \mathbb{F}^\delta\right\}$$

is an invariant of $\mathcal{C}$. If $\delta = 0$ (block code), then $\Lambda(\mathcal{C}) = \mathrm{we}(\mathcal{C})$.

Weight Adjacency Matrix of a Code

Factor out the group action induced by $GL_\delta(\mathbb{F})$:

Generalized Weight Adjacency Matrix:

Let $\mathcal{C} \subseteq \mathbb{F}[z]^n$ and Λ be a WAM of $\mathcal{C}$. Then

$$\Lambda(\mathcal{C}) := \left\{ \Lambda' \,\middle|\, \exists\, T \in GL_\delta(\mathbb{F})\colon \Lambda'_{X,Y} = \Lambda_{XT,YT} \text{ for all } X, Y \in \mathbb{F}^\delta \right\}$$

is an invariant of $\mathcal{C}$. If $\delta = 0$ (block code), then $\Lambda(\mathcal{C}) = \mathrm{we}(\mathcal{C})$.

Is there a MacWilliams Identity Theorem for $\Lambda(\mathcal{C})$?

MacWilliams Identity Theorem for $\Lambda(\mathcal{C})$

Theorem: ($\mathrm{G_L}$/Schneider '05/'06)
Let $\mathcal{C}$ be an $(n,\,k,\,\delta)$-code over $\mathbb{F}=\mathbb{F}_q$. Then

$$\Lambda(\mathcal{C}^\perp) = q^{-k}\mathbf{M}\big(\mathcal{H}\,\Lambda(\mathcal{C})^\mathsf{T}\,\mathcal{H}^{-1}\big)$$

where $\mathcal{H}\in\mathbb{C}^{q^\delta\times q^\delta}$ (matrix of characters on $\mathbb{F}^\delta$) and the MacWilliams transformation

$$\mathbf{M}:\mathbb{C}[W]_{\le n}\longrightarrow\mathbb{C}[W]_{\le n},\quad f\longmapsto\big(1+(q-1)W\big)^n f\big(\tfrac{1-W}{1+(q-1)W}\big).$$

is applied entrywise to $\mathcal{H}\,\Lambda(\mathcal{C})^\mathsf{T}\,\mathcal{H}^{-1}$.

Abdel-Ghaffar '92 proved the case $\delta=1$ (a different formulation).

$$\mathcal{H}=q^{-\frac{\delta}{2}}\Big(\zeta^{\tau(XY^\mathsf{T})}\Big)_{X,Y\in\mathbb{F}^\delta}\in\mathbb{C}^{q^\delta\times q^\delta}$$

Detailed Formulation

Let $\left\{ \begin{array}{c} \Lambda \\ \hat{\Lambda} \end{array} \right\}$ be the WAMs associated with $\left\{ \begin{array}{ll} (A, B, C, D) & \text{for } \mathcal{C} \\ (\hat{A}, \hat{B}, \hat{C}, \hat{D}) & \text{for } \mathcal{C}^{\perp} \end{array} \right\}$.

Then

$$\Lambda(\mathcal{C}^{\perp}) = q^{-k}\mathbf{M}\big(\mathcal{H}\,\Lambda(\mathcal{C})^{\mathsf{T}}\,\mathcal{H}^{-1}\big)$$

translates into

$$\boxed{\exists\, T \in GL_{\delta}(\mathbb{F}) : \;\hat{\Lambda}_{XT,YT} = q^{-k}\mathbf{M}\big((\mathcal{H}\,\Lambda^{\mathsf{T}}\,\mathcal{H}^{-1})_{X,Y}\big) \text{ for all } (X, Y) \in \mathbb{F}^{\delta} \times \mathbb{F}^{\delta}.}$$

When are two Codes Equivalent?

Isometric Block Codes

Definition:

Two block codes $\mathcal{C}$, $\mathcal{C}' \subseteq \mathbb{F}^n$ are called isometric if there exists a

weight-preserving isomorphism $\phi : \mathcal{C} \longrightarrow \mathcal{C}'$.

Then

$$\mathcal{C},\ \mathcal{C}' \text{ isometric } \underset{\not\Longleftarrow}{\Longrightarrow} \text{we}(\mathcal{C}) = \text{we}(\mathcal{C}').$$

Isometric Block Codes

MacWilliams Equivalence Theorem '62:

$\phi : \mathcal{C} \longrightarrow \mathcal{C}'$ is an isometry $\iff$ $\left\{\begin{array}{l} \mathcal{C}, \mathcal{C}' \text{ are } \underline{\text{monomially equivalent}}, \text{ that is,} \\ \text{there exist a permutation matrix } P \in GL_n(\mathbb{F}) \\ \text{and a diagonal matrix } R \in GL_n(\mathbb{F}) \text{ such that} \\ \qquad \phi(v) = vPR \text{ for all } v \in \mathcal{C}. \end{array}\right.$

Extensions to Block Codes over Rings:

Ward/Wood (1996/1999), Greferath/Schmidt (2000), Dinh/López-Permouth (2004), . . .

Equivalence of Convolutional Codes

Definition: Let $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}[z]^n$.

(a) $\mathcal{C}, \mathcal{C}'$ are (strongly) isometric if there exists a

(degree- and) weight-preserving $\mathbb{F}[z]$-isomorphism $\mathcal{C} \longrightarrow \mathcal{C}'$.

(b) $\mathcal{C}, \mathcal{C}'$ are monomially equivalent if

$\mathcal{C}' = \{vPR \mid v \in \mathcal{C}\}$ for some permutation P and diagonal matrix $R \in GL_n(\mathbb{F})$.

Examples:

- im $(1, 1)$, im $(z, 1)$:
  – isometric – not monomially equivalent – different degrees – different WAMs.
- im $(1, 1+z)$, im $(z, 1+z)$:
  – strongly isometric – not monomially equivalent – same degree – different WAMs.

Equivalence of Convolutional Codes

Properties:

- monomially equivalent $\Longrightarrow$ $\diamond$ strongly isometric,
  $\diamond$ same WAM.
- strongly isometric $\Longrightarrow$ same degree.
- strongly isometric $\not\Longrightarrow$ $\diamond$ monomially equivalent,
  $\diamond$ same WAM.
- Same WAM $\not\Longrightarrow$ isometric.

Equivalence of Convolutional Codes

Theorem: (G$_\text{L}$/Schneider '06)
Let $\mathcal{C},\,\mathcal{C}' \subseteq \mathbb{F}[z]^n$ be two codes such that $\mathcal{C} \cap \mathbb{F}^n = \{0\} = \mathcal{C}' \cap \mathbb{F}^n$. Then

$$\Lambda(\mathcal{C}) = \Lambda(\mathcal{C}') \Longleftrightarrow \mathcal{C},\, \mathcal{C}' \text{ monomially equivalent.}$$

Result is not true if $\mathcal{C} \cap \mathbb{F}^n \neq \{0\}$, in particular for block codes.

Main Arguments:

- For all (X, Y) there is at most one edge $X \xrightarrow{\binom{u}{v}} Y$, thus $\Lambda_{X,Y} \in \{0,\, W^\alpha \mid \alpha \in \mathbb{N}_0\}$.
- Use MacWilliams Equivalence Theorem for block codes.

Equivalence of Convolutional Codes

Open Problems:

- $\big[$ Strongly isometric and $\Lambda(\mathcal{C}) = \Lambda(\mathcal{C}') \Longrightarrow$ monomial equivalence $\big]$?
- Coding-theoretically meaningful notion of equivalence for convolutional codes?
- Should $\Lambda(\mathcal{C})$ be invariant under equivalence?