STANFORD

Supplementary Lecture 9C

Reed Muller Decoders

February 3, 2026

JOHN M. CIOFFI

Hitachi Professor Emeritus (recalled) of Engineering

Instructor EE379A – Winter 2026

Announcements & Agenda

- Announcements

- Lattice Cosets and Squaring
- Reed Muller Trellis Descriptions
- Conversion to/from generator

Lattice Cosets and Squaring

Section 7.2

Lattices and Cosets (Appendix B)

- Lattices Λ can be defined over countably infinite fields like $\mathbb{Z}$ or $\mathbb{Z}^2$ ...
- Or as over finite fields like $\mathbb{F}_2 = \{0,1\}$ or $\mathbb{F}_2^2 = \{00, 01, 10, 11\}$.
- Such lattices can be partitioned by a sublattice Λ', so $\mathbb{Z}^2/D_2$ has two subsets (odd squared norms and evens).
- $\mathbb{F}_2^2/D_2$ also has two subsets $D_2 = \{00, 11\}$ and $D_2 + [01] = \{01, 10\}$, so $|\mathbb{Z}^2/D_2| = \left|\mathbb{F}_2^2/D_2\right| = 2$.
  - $D_2 = R_2 \cdot \mathbb{Z}^2$ where $R_2 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, where R_2 is a rotation matrix in $\mathbb{F}_2^2$, also $R_4 = \begin{bmatrix} R_2 & 0 \\ 0 & R_2 \end{bmatrix}$. R_2 doubles free distance.
  - $R_4 \cdot \mathbb{Z}^4 = \{0000, 0011, 1100, 1111\}$, a set of 4 members; while $\mathbb{Z}^4$ is a set of 16 members. $|\mathbb{Z}^4/(R_4 \cdot \mathbb{Z}^4)| = 4$.
- These subsets are **cosets.**
  - The coset leaders $\boldsymbol{c}$ are also a set ([00] and [01] for D_2) that can be added to the sublattice to recreate the entire original lattice.
- The **coset leader set** is written $[\mathbb{Z}^2/D_2]$ or $[\mathbb{F}_2^2/D_2]$.
  - These coset-leader sets are lattices themselves in $\mathbb{F}_2^2$, and in fact characterize RM codes.
  - Unlike $2\mathbb{Z}^2$ for integer-pair lattices, $2\mathbb{F}_2^2 = \{00\}$, while the former is a lattice with all even integer pairs.
  - So binary lattices, which have $2\mathbb{Z}^{2^m}$ as a sublattice, are simply the coset leaders (the RM codes) with binary arithmetic up from $2\mathbb{F}_2^{2^m} = \{00 \; \ldots . \, 00\}$.
- **Partition Squaring** is the double-dimension-size set $[\boldsymbol{\lambda}_1' + \boldsymbol{c}, \boldsymbol{\lambda}_2' + \boldsymbol{c}]$ where $\boldsymbol{c} \in [\Lambda/\Lambda']$, and $\boldsymbol{\lambda}_1' \in \Lambda'$, $\boldsymbol{\lambda}_2' \in \Lambda'$.
  - So when $\Lambda' = 2\mathbb{Z}^{2^m}$, then the squaring construction repeats the coset leader $\boldsymbol{c}$.

Reed Muller Trellis Descriptions

Sections 7.2 and 8.1.3

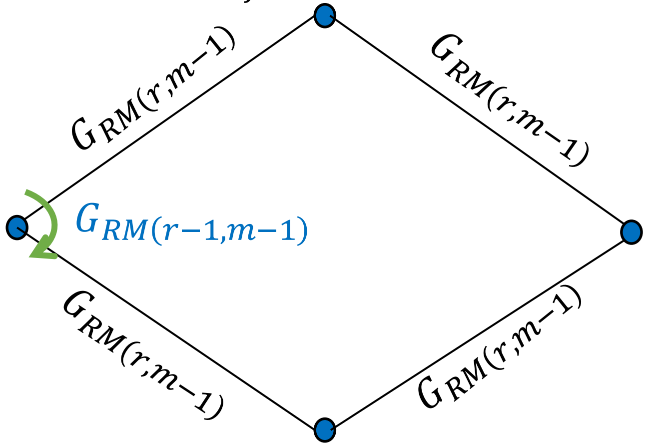
Reed Muller Code Recursion

$$G_{RM(r,m)} = \begin{bmatrix} G_{RM(r,m-1)} & G_{RM(r,m-1)} \\ 0 & G_{RM(r-1,m-1)} \end{bmatrix}$$

Upper rows are squaring construction $[\boldsymbol{c}, \boldsymbol{c}]$

Lower rows are elements in Λ'

- Squaring doubles RM codeword length and free distance; $G_{RM(r,m)}$ adds offsets that are codewords of a smaller more powerful (double d_{free}) RM code.



- $G_{(r>m,m)} = G_{(r<0,m)} = \emptyset$
- $G_{(0,0)} = 1$
- $G_{(m,m)} = I_{2^m}$
- $G_{(0,m)} = [1 \;\; 1 \;\; \cdots \;\; 1]$

- The repeated lower branch differs only in 1-to-1 mapping from the zeros, by adding $\boldsymbol{\lambda}_2' - \boldsymbol{\lambda}_1'$ on one side and zeros on the other (since the codes are linear, this does not change the code).

Reed Muller codes

- RM(r, m).
  - $n = 2^m$
  - $k = \sum_{i=0}^{r} \binom{m}{i}$
- $d_{free} = 2^{m-r}$
- Augmented Hadamard has $r = 1$.

Recursively Defined

- Initialize:
  - $G_{RM(0,0)} = 1$; $G_{RM(1,0)} = \emptyset$
  - $G_{RM(r>m,m)} = \emptyset$; $G_{RM(r<0,m)} = \emptyset$
- The RM Recursion
  - $G_{RM(r,m)} = \begin{bmatrix} G_{RM(r,m-1)} & G_{RM(r,m-1)} \\ 0 & G_{RM(r-1,m-1)} \end{bmatrix}$
  - $d_{free(r,m)} = min\left(2 \cdot d_{free(r,m-1)}, d_{free(r-1,m-1)}\right)$

- **Repetition Code** $RM(0, m)$, $r = \frac{1}{2}$

$$G_{RM(0,1)} = G_{1,2} = \begin{bmatrix} G_{RM(0,0)} & G_{RM(0,0)} \\ 0 & G_{RM(-1,0)} \end{bmatrix} = \begin{bmatrix} G_{1,1} & G_{1,1} \\ 0 & \emptyset \end{bmatrix} = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

- **Simple Parity Check** $RM(m-1, m)$, D4 Lattice, $m = 2$

$$G_{RM(1,2)} = G_{3,4} = \begin{bmatrix} G_{RM(1,1)} & G_{RM(1,1)} \\ 0 & G_{RM(0,1)} \end{bmatrix} = \begin{bmatrix} G_{2,2} & G_{2,2} \\ 0 & G_{1,2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} . \quad (8.47)$$

The code $RM(m-1, m)$ is always a parity-check code with rate $r = (2^m - 1)/2^m$ and $d_{free} = 2$. Thus,

$$G_{RM(1,2)} = G_{3,4} = \begin{bmatrix} G_{RM(1,1)} & G_{RM(1,1)} \\ 0 & G_{RM(0,1)} \end{bmatrix} = \begin{bmatrix} G_{2,2} & G_{2,2} \\ 0 & G_{1,2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} . \quad (8.48)$$

The $RM(1, 2)$ code also corresponds to Appendix B's Schlafli D_4 Lattice. Further iteration leads to

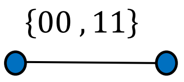
$$G_{RM(2,3)} = G_{7,8} = \begin{bmatrix} G_{RM(2,2)} & G_{RM(2,2)} \\ 0 & G_{RM(1,2)} \end{bmatrix}$$

$$= \begin{bmatrix} G_{4,4} & G_{4,4} \\ 0 & G_{3,4} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} . \quad (8.49)$$

Use Table, look at Λ column

- Section of RM Table

r	m	$\frac{k}{n}$	d_{free}	$M(r,m)$	# of states (middle) $2^{M(r,m-1)}$	Λ
0	0	1	1	1	0	$\mathbb{Z}$
0	1	$\frac{1}{2}$	2	1	1	D_2
1	1	$\frac{2}{2}$	1	1	1	$\mathbb{Z}^2$
0	2	$\frac{1}{4}$	4	1	2	$D_4^\perp$
1	2	$\frac{3}{4}$	2	2	2	D_4
2	2	$\frac{4}{4}$	1	1	0	$\mathbb{Z}^4$



D_2

D_{2^m} = simple parity code

$D_{2^m}^\perp$ = repetition code

Λ' $[\mathbb{Z}^2/D_2] = \{00\ ,01\}$ = possible cosets (2)

Λ $\mathbb{Z}^2 = D_2 \oplus [\mathbb{Z}^2/D_2]$

$\boxed{RM(0,1)}$

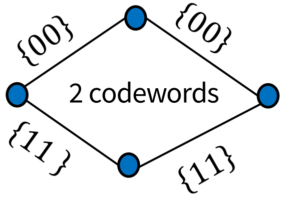
$D_4^\perp = [D_2/\emptyset]^2$

$D_4 = [\mathbb{Z}^2/D_2]^2$

$\boxed{RM(1,2)}$

- $RM(1,2)$ or more generally $RM(m-1,m)$ codes have distance 2 and $r = {}^{2^m-1}/_{2^m}$ and have one parity bit
  - Selects "every other point" (so like 32SQ from 64SQ, but binary and multidimensional)

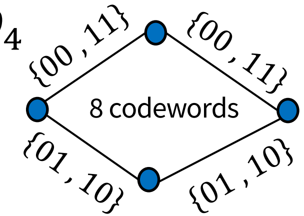
$D_4^\perp$



$G_{1,4} = [1\ 1\ 1\ 1]$

partition squaring of $D_2/\emptyset$ into $D_4^\perp$
repetition code trellis

D_4



$[\mathbb{Z}^2/D_2]^2$ has 8 (4D) elements

$G_{3,4} = \begin{bmatrix} I_2 & I_2 \\ 0\ 0 & 1\ 1 \end{bmatrix}$

partition squaring of $\mathbb{Z}^2/D_2$ into D_4
Simple parity code trellis

Basic D_{2m} Root Trellises & Squaring

0	2	$\frac{1}{4}$	4	1	2	$D_4^{\perp}$
1	2	$\frac{3}{4}$	2	2	2	D_4
2	2	$\frac{4}{4}$	1	1	0	$\mathbb{Z}^4$
0	3	$\frac{1}{8}$	8	1	2	$D_8^{\perp}$
1	3	$\frac{4}{8}$	4	3	4	E_8
2	3	$\frac{7}{8}$	2	3	2	D_8
3	3	$\frac{8}{8}$	1	1	0	$\mathbb{Z}^8$

# of states (middle)

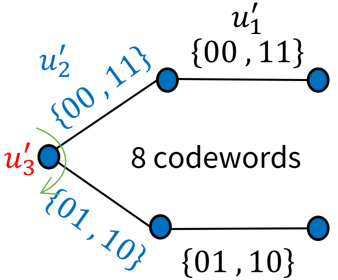
$G_{1,8} = [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1]$

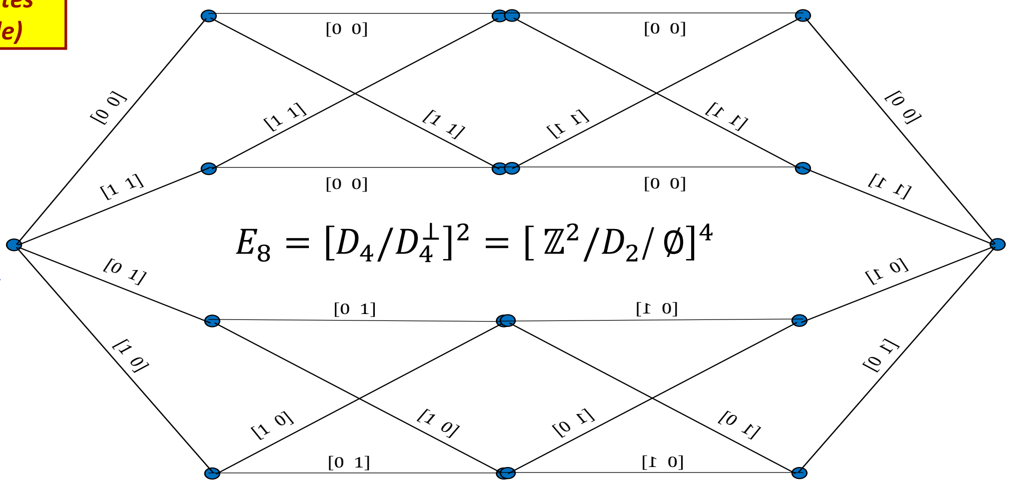
$D_8^{\perp} = [D_4^{\perp}/\emptyset]^2$ — 2 cosets x 1 codeword x 1 codeword

$E_8 = [D_4/D_4^{\perp}]^2$ — $G_{4,8}$ — 4 cosets x 2 codewords x 2 codewords

$D_8 = [\mathbb{Z}^4/D_4]^2$ — $G_{7,8}$ — 2 cosets x 8 codewords x 8 codewords

- Open D_4





$$E_8 = [D_4/D_4^{\perp}]^2 = [\mathbb{Z}^2/D_2/\emptyset]^4$$

Redrawing D_4 into its 2 cosets of $(D_2)^2$; each contains 4 codewords

Viterbi (Trellis) Decode (or BCJR …)

16D Trellises

0	3	$\frac{1}{8}$	8	1	2	$D_8^{\perp}$	1
1	3	$\frac{4}{8}$	4	3	4	E_8	3
2	3	$\frac{7}{8}$	2	3	2	D_8	1
3	3	$\frac{8}{8}$	1	1	0	$\mathbb{Z}^8$	0
0	4	$\frac{1}{16}$	16	1	2	$D_{16}^{\perp}$	1
1	4	$\frac{5}{16}$	8	4	8	Λ_{16}	4
2	4	$\frac{11}{16}$	4	6	8	$\Lambda_{16}^{\perp}$	2
3	4	$\frac{15}{16}$	2	4	2	D_{16}	1
4	4	$\frac{16}{16}$	1	1	0	$\mathbb{Z}^{16}$	0

# of states (middle)

$D_{16}^{\perp} = [D_8^{\perp}/\emptyset]^2$ $\quad G_{1,16}$ 2 cosets x 1 codeword x 1 codeword

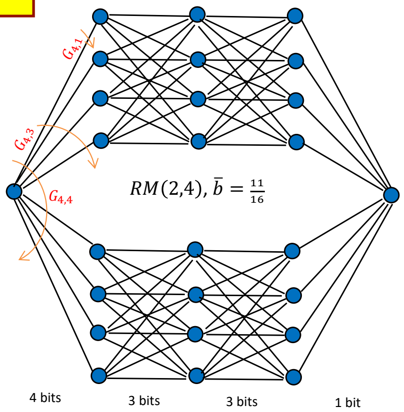
$\Lambda_{16} = [E_8/D_8^{\perp}]^2$ $\quad G_{5,16}$ 8 cosets x 2 codewords x 2 codewords

$\Lambda_{16}^{\perp} = [D_8/E_8]^2$ $\quad G_{11,16}$ 8 cosets x 16 codewords x 16 codewords

$D_{16} = [\mathbb{Z}^8/D_8]^2$ $\quad G_{15,16}$ 2 cosets x 128 codewords x 128 codewords

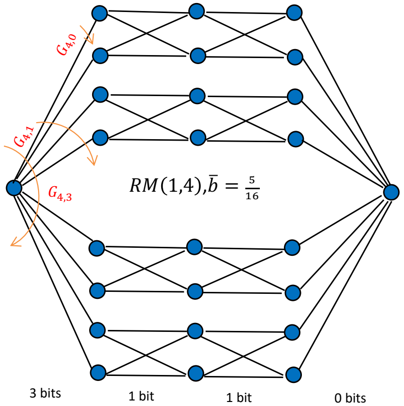
- Best to go to 4-stage trellis diagrams
- Low rate RMs have easy trellises
  - And large free distance
  - Only 8 states (max in middle)
- Decode each stage's metrics
  - Viterbi at higher level on each

$[RM(2,2)/RM(1,2)/RM(0,2)]^4$



$\Lambda_{16}^{\perp} = [\mathbb{Z}^4/D_4/D_4^{\perp}]^4 = [D_8/E_8]^2$

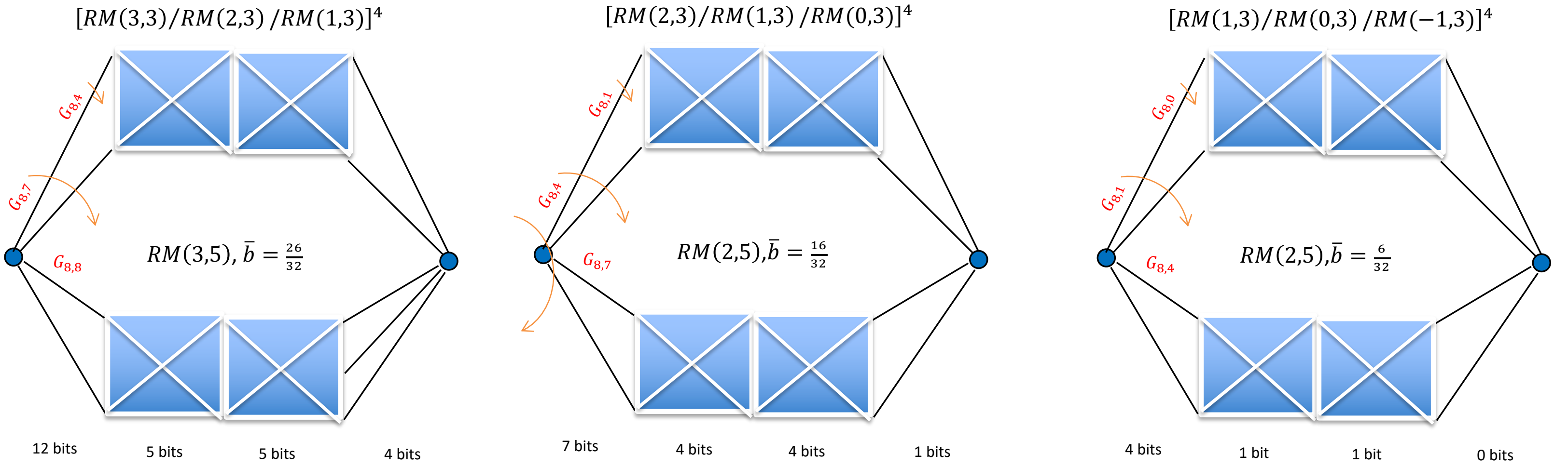
$[RM(1,2)/RM(0,2)/RM(-1,2)]^4$



$\Lambda_{16} = [D_4/D_4^{\perp}/\emptyset]^4 = [E_8/R_8\mathbb{Z}^8]^2$

Major 32 Trellises and RM Codes

- These are 4-stage diagrams, so the blue-crossed boxes need recursive decoding by earlier trellises
  - And their cosets
  - H_{32} has 64 states in middle, but just there, 16 elsewhere

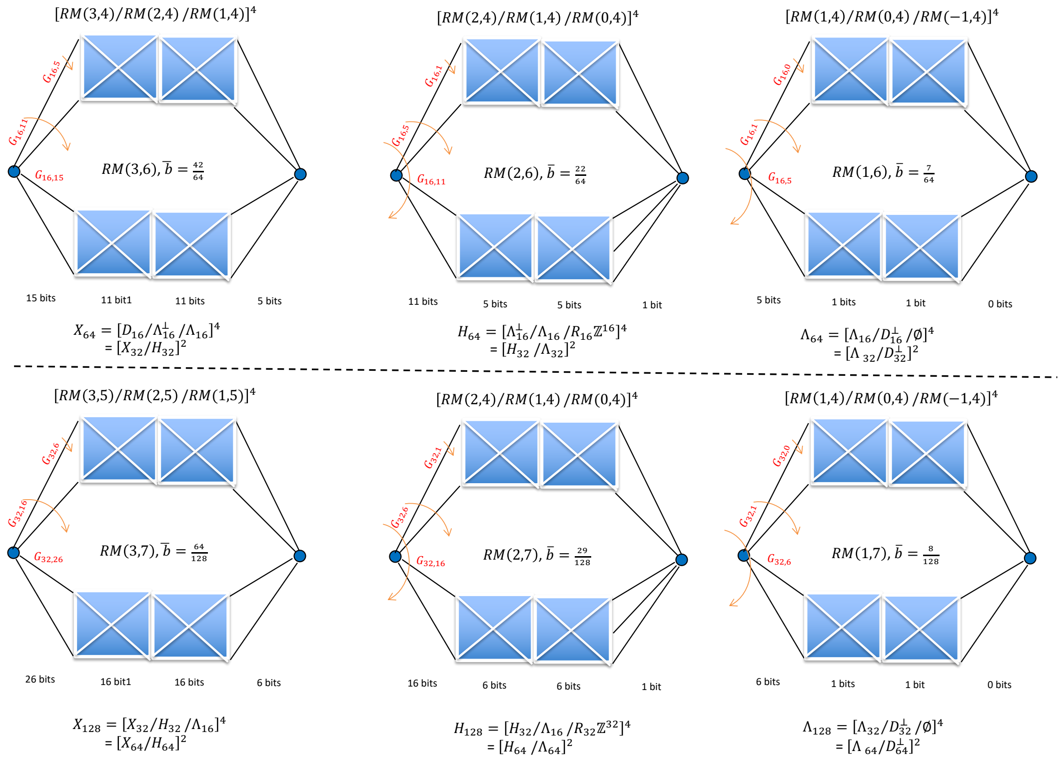


$X_{32} = [\mathbb{Z}^8/D_8/E_8]^4$
$= [D_{16}/H_{16}]^2$

$H_{32} = [D_8/E_8/D_8^{\perp}]^4$
$= [H_{16}/\Lambda_{16}]^2$

$\Lambda_{32} = [E_8/D_8^{\perp}/\emptyset]^4$
$= [\Lambda_{16}/D_{16}^{\perp}]^2$

64D and 128D

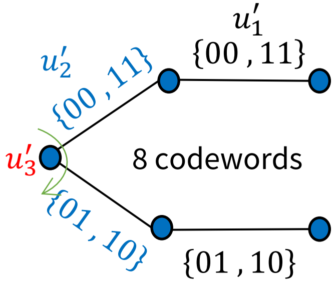


- Can get complex, but not for the low-rate codes or good choice of product code rates to avoid outrageous state counts with iterative decoding.

Conversion to/from Generator

Section 8.1.3

Relating the generators for decoding



$$G'_{4,3} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$G_{4,3} = \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}}_{A_{4,3}} \cdot G'_{4,3}$$

$$G^{-1}_{RM(r,m)} = \begin{bmatrix} G^{-1}_{RM(r,m-1)} & G^{-1}_{RM(r-1,m-1)} \\ 0 & G^{-1}_{RM(r-1,m-1)} \end{bmatrix}$$

$$G^{-1}_{4,3} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$A^{-1}_{4,3} = A_{4,3}$$

- Step 1 – label the trellis with $\boldsymbol{u}'$.
- Step 2 – find the G'
- Step 3 – find the unimodular A matrix that converts $G = A \cdot G'$
- Step 4 – reverse A on trellis decoded bits $\boldsymbol{u}' \cdot G'^{-1} \cdot A^{-1}$

End Lecture S9C