



Chains of Invariant Subspaces

Linnea Jones, Maddie Kloud,
Liam Leasure, Max Rodgers

*The problem
we want to
solve*



Example

Database Sequence: 

Database outputs: 

We input: 01010101

Database Sequence: 

Database outputs: 

Behind the Scenes Operations

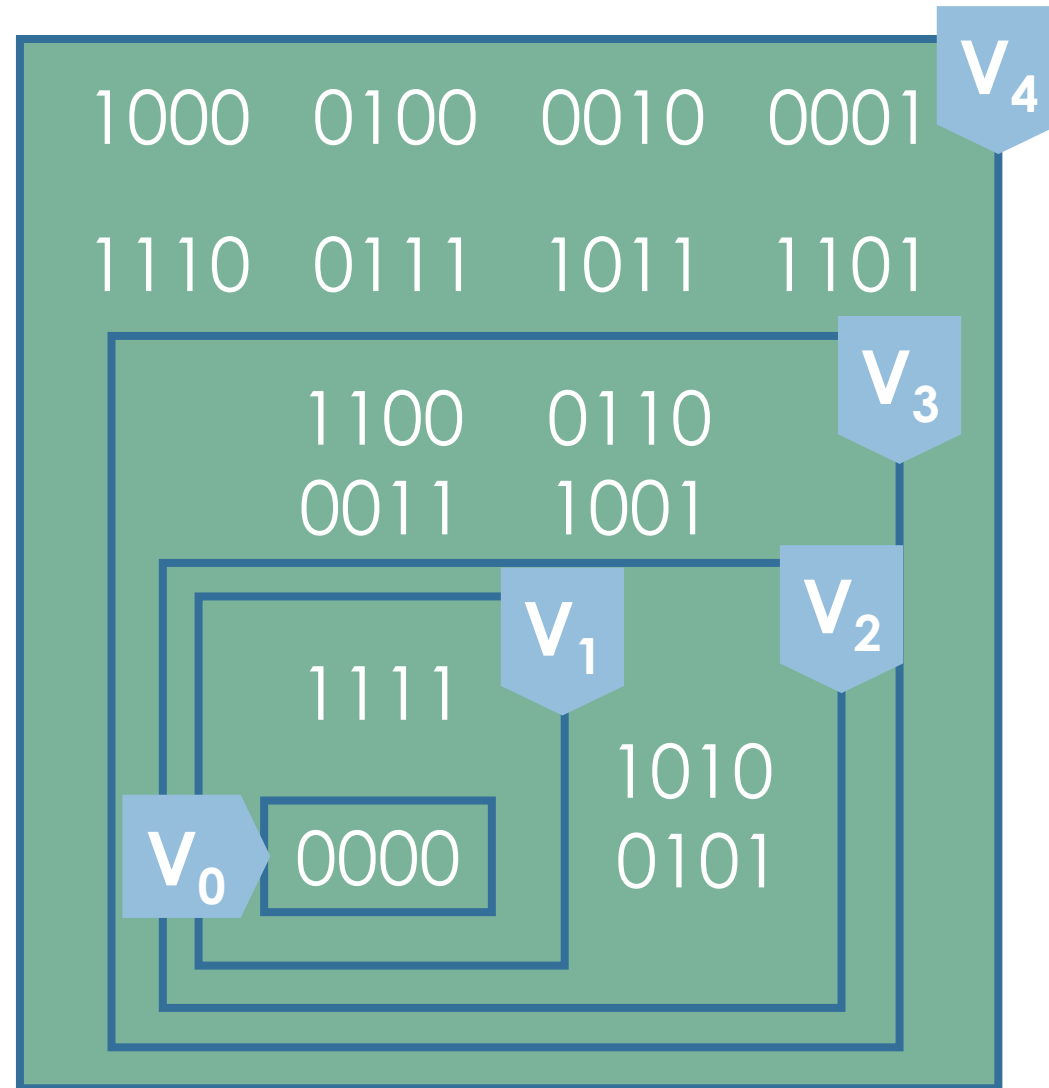
The database takes our input and cycles it some number of times:

01010101  10101010

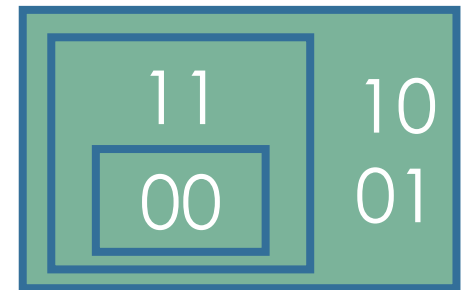
Then it applies the binary exclusive or operator (XOR) to its string and our cycled string:

$$\begin{array}{rcl} 10101010 & \leftarrow & \text{Our Cycled String} \\ \oplus 10101010 & \leftarrow & \text{Database String} \\ \hline 00000000 & & \end{array}$$

Solution for 4-bit Sequences



2-bit
Solution



Expanding basis elements

2 bits

11
01

4 bits

1111
0101
0011
0001

8 bits

1111	1111
0101	0101
0011	0011
0001	0001
0000	1111
0000	0101
0000	0011
0000	0001

16 bits

1111	1111	1111	1111
0101	0101	0101	0101
0011	0011	0011	0011
0001	0001	0001	0001
0000	1111	0000	1111
0000	0101	0000	0101
0000	0011	0000	0011
0000	0001	0000	0001
0000	0000	1111	1111
0000	0000	0101	0101
0000	0000	0011	0011
0000	0000	0001	0001
0000	0000	0000	1111
0000	0000	0000	0101
0000	0000	0000	0011
0000	0000	0000	0001

2ⁿ bits...

Basis for 32 bits:

```
11111111111111111111111111111111
01010101010101010101010101010101
00110011001100110011001100110011
00010001000100010001000100010001
00001111000011110000111100001111
00000101000001010000010100000101
00000011000000110000001100000011
00000001000000010000000100000001
00000000111111110000000011111111
00000000010101010000000001010101
00000000001100110000000000110011
00000000000100010000000000010001
00000000000011110000000000011111
0000000000000101000000000000101
000000000000001100000000000011
000000000000000100000000000001
00000000000000001111111111111111
00000000000000000101010101010101
00000000000000000011001100110011
00000000000000000001000100010001
00000000000000000000111100001111
00000000000000000000010100000101
00000000000000000000001100000011
00000000000000000000000100000001
00000000000000000000000011111111
00000000000000000000000001010101
00000000000000000000000000110011
00000000000000000000000000010001
00000000000000000000000000001111
00000000000000000000000000000101
00000000000000000000000000000011
00000000000000000000000000000001
```

Larger dimensions have the same pattern

- Notice that this matrix is triangular, rows are linearly independent
- So, we can expand the pattern and get an n dimensional chain of nested subspaces
- The subspace generated by the first k rows is invariant

How do we know the subspace is invariant?

$$11111111 = b_8$$

$$01010101 = b_7$$

$$00110011 = b_6$$

$$00010001 = b_5$$

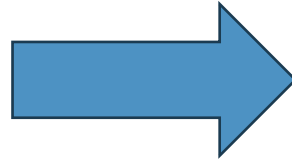
$$00001111 = b_4$$

$$00000101 = b_3$$

$$00000011 = b_2$$

$$00000001 = b_1$$

σ



$$11111111 = b_8$$

$$10101010 = b_7 + b_8$$

$$01100110 = b_6 + b_7$$

$$00100010 = b_5 + b_6$$

$$00011110 = b_4 + b_5$$

$$00001010 = b_3 + b_4$$

$$00000110 = b_2 + b_3$$

$$00000010 = b_1 + b_2$$

Pascal's triangle

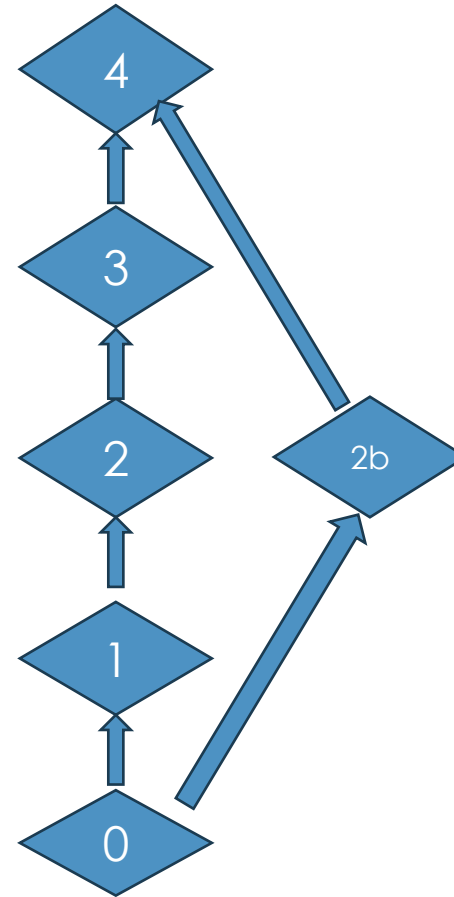
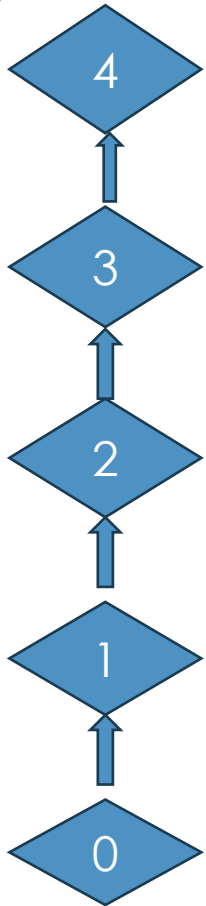
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k},$$

- Take combinations of row n choose k (both nonnegative integers such that $0 \leq k < n$) we get Pascal's triangle.
- We get the same pattern as our basis elements when we convert these values to binary

n=0	1	= 00000001
n=1	1 1	= 00000011
n=2	1 2 1	= 00000101
n=3	1 3 3 1	= 00001111
n=4	1 4 6 4 1	= 00010001
n=5	1 5 10 10 5 1	= 00110011
n=6	1 6 15 20 15 6 1	= 01010101
n=7	1 7 21 35 35 21 7 1	= 11111111

Motivating Fact

The Lattice of invariant subspaces is a chain if and only if V is cyclic and primary.



Cyclic Spaces

A vector space is cyclic or σ -*cyclic*, if it can be generated by a basis of the form $(v, \sigma(v), \sigma^2(v), \dots, \sigma^k(v))$.

The cyclic basis for the fourth dimension is $(0001, 0010, 0100, 1000)$.

Primary Vector Spaces

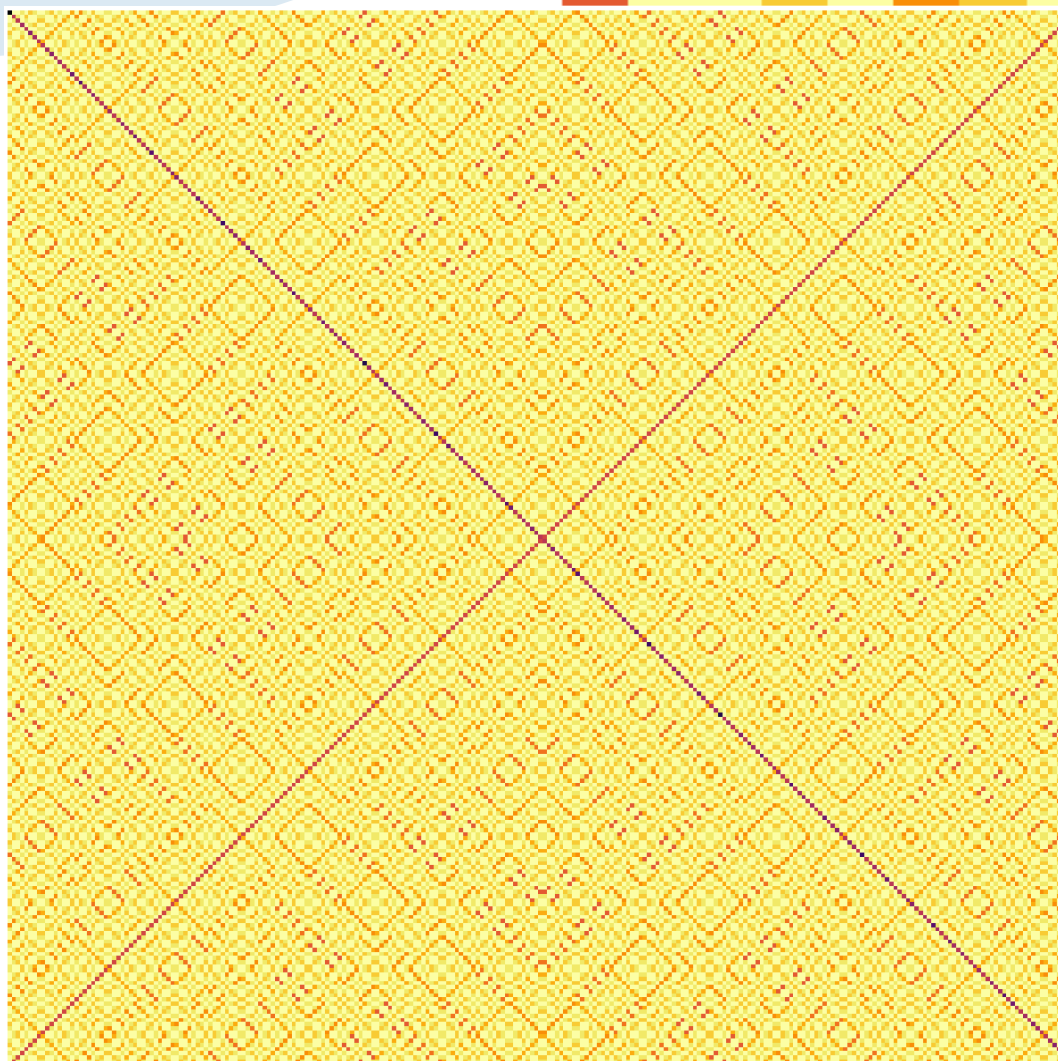
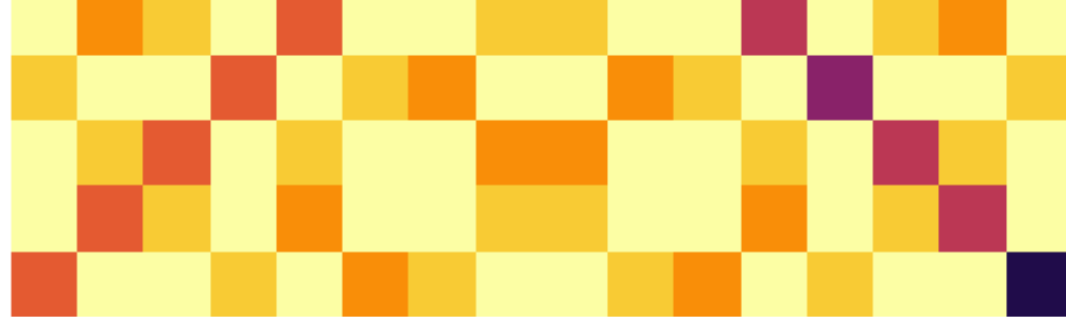
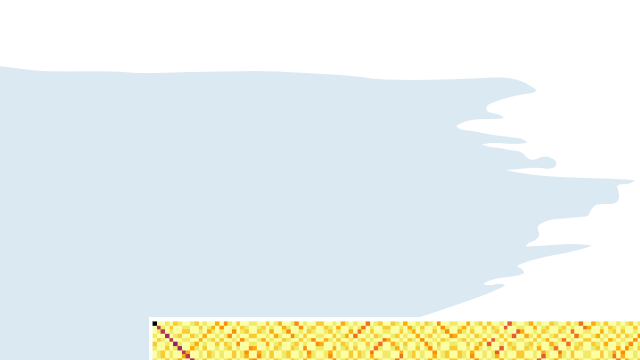
Minimal polynomial of σ : monic polynomial P of minimal degree such that $P(\sigma) = 0$

A vector space is primary if its minimal polynomial is the power of an irreducible polynomial.

Minimal polynomial of $F_2^{2^n}$ w.r.t $\sigma : x^{2^n} + 1 = (x + 1)^{2^n}$



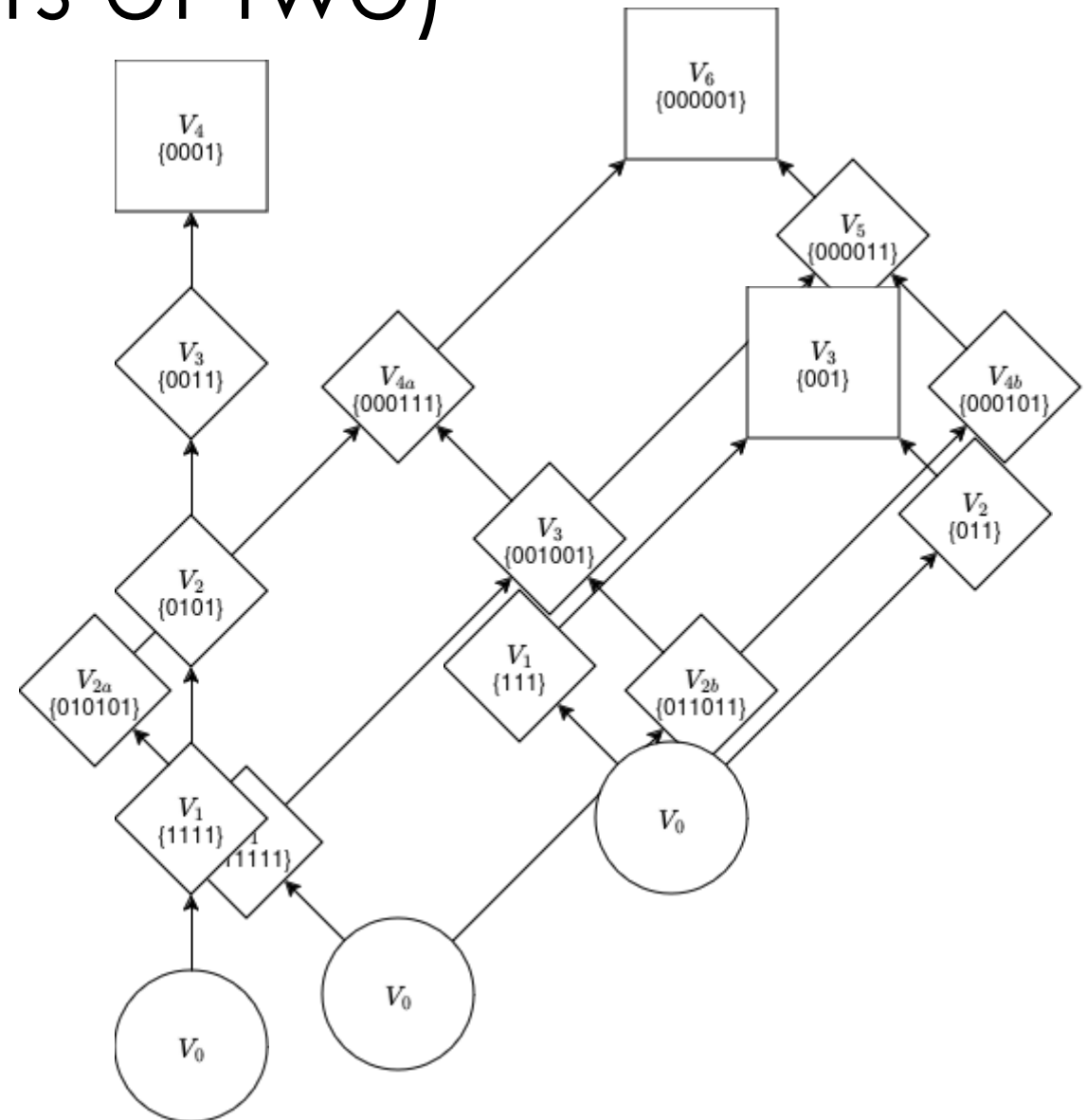
What's Next?



0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Lattices (for non-powers of two)

- Powers of two create chains
- Non-powers of two create lattices that aren't chains
- More complicated to compute



Different Fields

- Same addition and cycling
- Lattices / chains
- Code Jam solutions

+	0	1	X	X+1
0	0	1	X	X+1
1	1	0	X+1	X
X	X	X+1	0	1
X+1	X+1	X	1	0

