

THE MYSTERIOUS ARITHMETIC OF LEXICOGRAPHIC CODES

John Conway
(Princeton University)

The words of the *integral lexicographic code* of minimal distance d (henceforth *lexicode*) are determined inductively by the condition that each is the lexicographically earliest word $\cdots dcba$ (entries are non-negative integers) that differs in at least d places from all earlier ones. The distance 3 code (C_3) is as follows: $\cdots 000000, \cdots 000111, \cdots 000222, \cdots 000333, \cdots 000444, \dots, \cdots 000nnn, \dots, \cdots 001012, \cdots 001103, \cdots 001230, \cdots 001321, \cdots 001456, \dots, \cdots 002023, \dots, \cdots 010013, \dots$

The **lexicode theorem** asserts that under coordinatewise notions of vector addition and scalar multiplication, all integral lexicones are vector spaces.

However, the addition and multiplication here are **not** the standard ones! Here they are:

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

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

This remarkable arithmetic has many interesting properties – for instance as a field, it is the quadratic closure of $\{0, 1\} = \mathbb{F}_2$.

$$2^2 = 3, \quad 4^4 = 5, \quad 16^{16} = 17, \quad 256^{256} = 257, \quad \dots$$

1, 2, 3 are the cube roots of unity, while 1, 8, 10, 13, 14 are the fifth roots of unity.

$$2^2 = 3, \quad 4^2 = 6, \quad 16^2 = 24, \quad 256^2 = 384, \quad \dots$$

JOHN CONWAY

"The Mysterious Arithmetic of Lexicographic Codes."

The words of the integral lexicographic code of minimal distance d (henceforth "lexicode") are determined inductively by the condition that each is the lexicographically earliest word ... $dcba$ (entries are non-negative integers) that differs in at least d places from all earlier ones. The distance 3 code (b_3) appears at left.

- ...00000
- ...00011
- ...00022
- ...00033
- ...00044
- ...
- ...000nn
- ...
- ...001012
- ...001103
- ...001230
- ...001321
- ...001456
- ...
- ...002023
- ...
- ...010013
- ...
- b_3

The lexicode theorem asserts that under ~~the~~ coordinatewise notions of vector addition and scalar multiplication, all integral lexicones are vector spaces.

However, the addition and multiplication here are not the standard ones! Here they are :-

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

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

This remarkable arithmetic has many interesting properties - for instance $2^2=3$ $4^4=5$ $16^{16}=17$ $256^{256}=257, \dots$
 1, 2, 3 are the cube roots of unity, while 1, 8, 10, 13, 14 are the fifth roots of unity.
 $2=3$, $4^2=6$, $16^2=24$, $256^2=384, \dots$

as a field, it is the quadratic closure of $\{0,1\} = \mathbb{F}_2$

John Conway
 30 Sept 2002