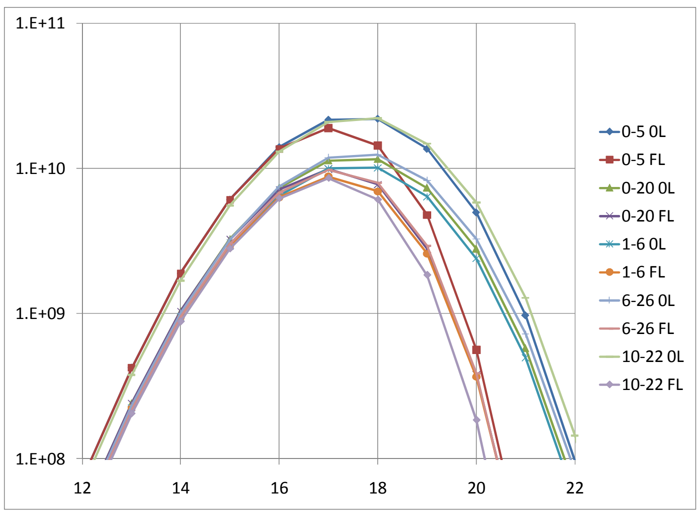
CISS 2010

Costas array search technique that maximizes backtrack and symmetry exploitation



James K Beard
Life Senior Member, IEEE
jkbeard@ieee.org

March 17, 2010 ,11:00 AM

The Last Costas Array

- Costas array of order 27
- Here it is

11	10	4	24	7	23	3	18	21	9	26	16	5	1	15	27	2	25	17	22	19	6	8	12	20	13	14
12	17	10	24	22	8	19	3	7	20	9	16	13	1	2	4	27	26	18	5	23	6	15	25	21	11	14
14	11	21	25	15	6	23	5	18	26	27	4	2	1	13	16	9	20	7	3	19	8	22	24	10	17	12
14	13	20	12	8	6	19	22	17	25	2	27	15	1	5	16	26	9	21	18	3	23	7	24	4	10	11
14	15	8	16	20	22	9	6	11	3	26	1	13	27	23	12	2	19	7	10	25	5	21	4	24	18	17
14	17	7	3	13	22	5	23	10	2	1	24	26	27	15	12	19	8	21	25	9	20	6	4	18	11	16
16	11	18	4	6	20	9	25	21	8	19	12	15	27	26	24	1	2	10	23	5	22	13	3	7	17	14
17	18	24	4	21	5	25	10	7	19	2	12	23	27	13	1	26	3	11	6	9	22	20	16	8	15	14

Properties of Finite Fields

CISS 2010

- Finite fields of order q, denoted by $GF(q)$
- Any implementation of $GF(q)$ is isometric to all other implementations
- $GF(q)$ exists when $q=p^k$, p a prime, k>0
- Commutative and associative addition, subtraction, multiplication, division
- In every $GF(q)$ there is a zero and a one
- Every element x has the properties $x^q=x$ and $p \cdot x=0$
- Other than zero and one, magnitude is not a meaningful concept
- There exist $\Phi(q-1)$ primitive elements α_i
  - Where $\Phi(q-1)$ is the Euler totient function
  - Powers of each α_i cycle through all the nonzero elements

The Vandermonde Matrix

CISS 2010

$$M_{N-1} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2\cdot(N-1)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{N-1} & \alpha^{2\cdot(N-1)} & \cdots & \alpha^{(N-1)\cdot(N-1)} \end{bmatrix}$$

$$\left|M_{N-1}\right| = \prod_{0 \le i < j < N} \left(\alpha^i - \alpha^j\right) \ne 0, \;\; N \le q-1$$

The Order *q-1* Vandermonde Matrix

CISS 2010

$$M = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2\cdot(q-2)} \\ \vdots & & & & \vdots \\ 1 & \alpha^{q-2} & \alpha^{2\cdot(q-2)} & \cdots & \alpha^{(q-2)\cdot(q-2)} \end{bmatrix}$$

$$|M| = \prod_{0 \le i < j < q} \left(\alpha^i - \alpha^j\right) \neq 0$$

Generating Polynomials for a Golomb-Generated CA

CISS 2010

0	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	-99	5	-99	-99	-99	-99	-99	-99	-99	Row 10,29
9	11	0	2	0	23	18	6	11	16	9	15	17	6	5	29	17	-99	19	7	24	8	3	24	1	24	20	Row 10, 31
7	10	4	1	31	34	26	0	35	33	8	0	31	25	20	17	3	17	20	35	5	6	0	30	9	27	29	Row 10, 37
17	0	16	10	23	1	8	6	8	26	28	7	8	38	0	7	0	4	1	38	6	6	21	15	15	7	33	Row 10, 41

- Table entries are “log to the base alpha”
  - Alpha is the principal element “x”
  - Alpha taken to the power of the table entry equals the polynomial coefficient
  - -99 is placeholder for zero
- Polynomial in GF(N+2) is the Golomb generator
- Other polynomials seem unremarkable

Generating Polynomials for the Last Costas Array

CISS 2010

GF(29)

23	14	2	23	11	24	13	7	4	-99	27	19	3	14	13	22	17	17	9	23	24	4	26	17	23	4	24
14	6	18	7	21	21	-99	7	22	9	10	3	0	-99	8	23	10	0	20	19	7	26	1	2	13	8	3
16	20	-99	2	15	15	16	-99	16	24	10	10	13	2	15	6	14	13	5	6	8	8	13	21	7	15	24
16	0	5	18	4	1	7	9	9	10	17	15	5	0	14	8	23	12	2	18	26	25	9	2	11	7	2
14	3	20	25	8	20	27	9	22	27	18	27	15	3	3	19	24	27	27	20	11	8	4	17	18	2	19
0	7	19	18	27	1	21	17	5	9	14	22	9	3	0	26	12	18	0	0	21	24	14	9	-99	-99	-99
8	14	26	21	0	3	0	21	9	24	21	23	26	3	20	22	0	24	5	26	2	5	8	18	23	9	7
8	17	20	17	4	5	0	27	6	24	9	5	8	20	7	25	18	6	14	1	0	-99	12	15	3	25	8

GF(31)

4	3	18	1	28	28	2	20	7	18	-99	15	1	27	17	9	6	26	-99	3	22	12	5	28	17	13	22
10	13	21	17	10	7	28	10	3	29	6	6	1	15	4	18	16	18	17	1	2	18	7	14	0	6	0
8	29	24	20	19	3	18	4	13	12	1	20	1	23	20	-99	23	13	15	20	0	15	5	2	12	11	10
24	21	6	6	23	8	13	0	-99	16	25	11	0	27	28	10	16	22	11	5	2	21	4	0	20	23	24
0	29	11	7	22	22	25	25	20	21	28	4	4	27	25	29	9	2	16	22	20	-99	1	14	26	26	14
15	29	23	12	5	15	-99	13	3	20	16	9	29	8	29	22	18	24	-99	13	23	29	12	22	28	29	7
23	17	4	26	29	22	-99	8	1	11	9	1	25	18	0	19	0	29	17	5	0	8	1	15	11	3	2
1	6	19	15	20	22	27	21	8	28	17	24	5	28	8	18	10	12	25	23	21	6	24	11	9	25	25

Other Methods

CISS 2010

- Augmentation
  - Construct augmented matrix from two Costas arrays
  - Result must satisfy Costas condition
  - Interaction between matrices will almost always result in a violation of the Costas condition
- Interleaving
  - Two Costas arrays with orders differing by at most one
  - Construct checkerboard interleaved matrix

Augmentation Results

CISS 2010

- Operated on database of all known Costas arrays up to order 400
- No success in interleaving equal order Costas arrays
- No success in augmenting 2X2 or 3X3 other than known Taylor/Golomb extensions and one example

Database Extended

- Generated Costas arrays to order 500
- Available on web site by Monday
  - http://jameskbeard.com
- Updated user interface program

Screen Shot


```
Costas arrays from searches of order 3 to 27
Costas arrays of order  27, method: exhaustive search
********************************************************************************
               Order          All      Essential   Symmetrical G-Symmetrical
                  22         2052            259             5           220
                  26           56              8             2             0
Current order:    27          204             29             7             0
               *****        *****          *****         *****         *****
               *****        *****          *****         *****         *****
               *****        *****          *****         *****         *****
********************************************************************************
Current options:

No. Value, Description
1       T, T => all CAs to order 27; F => generated CAs to order 500
2      27, Order of CAs for output
3       F, T => filter by generator method; F => output all
4       0, If previous option is T, filter by generator method 1 to 19
5       1, 1 => All, 2 => Essential, 3 => Symmetrical, 4 => G-Symmetrical
6       0, 0 => Output CAs are row indices from 0 to N-1, 1 => from 1 to N
7 REWIND, APPEND => append to existing output files; REWIND => overwrite
8       T, T => Find generating polynomial in a Galois field.
9      49, Order of Galois field.
10 C:\Data\IEEE\Papers\CISS\CISS2006\CDROM_Image\, Database folder
11 .\Costas_Array_Database_Output.txt, Pathname for output text

Enter option 1-11 to change, 12 for HELP, or 0 to proceed:
```

Screen Shot

CISS
2010

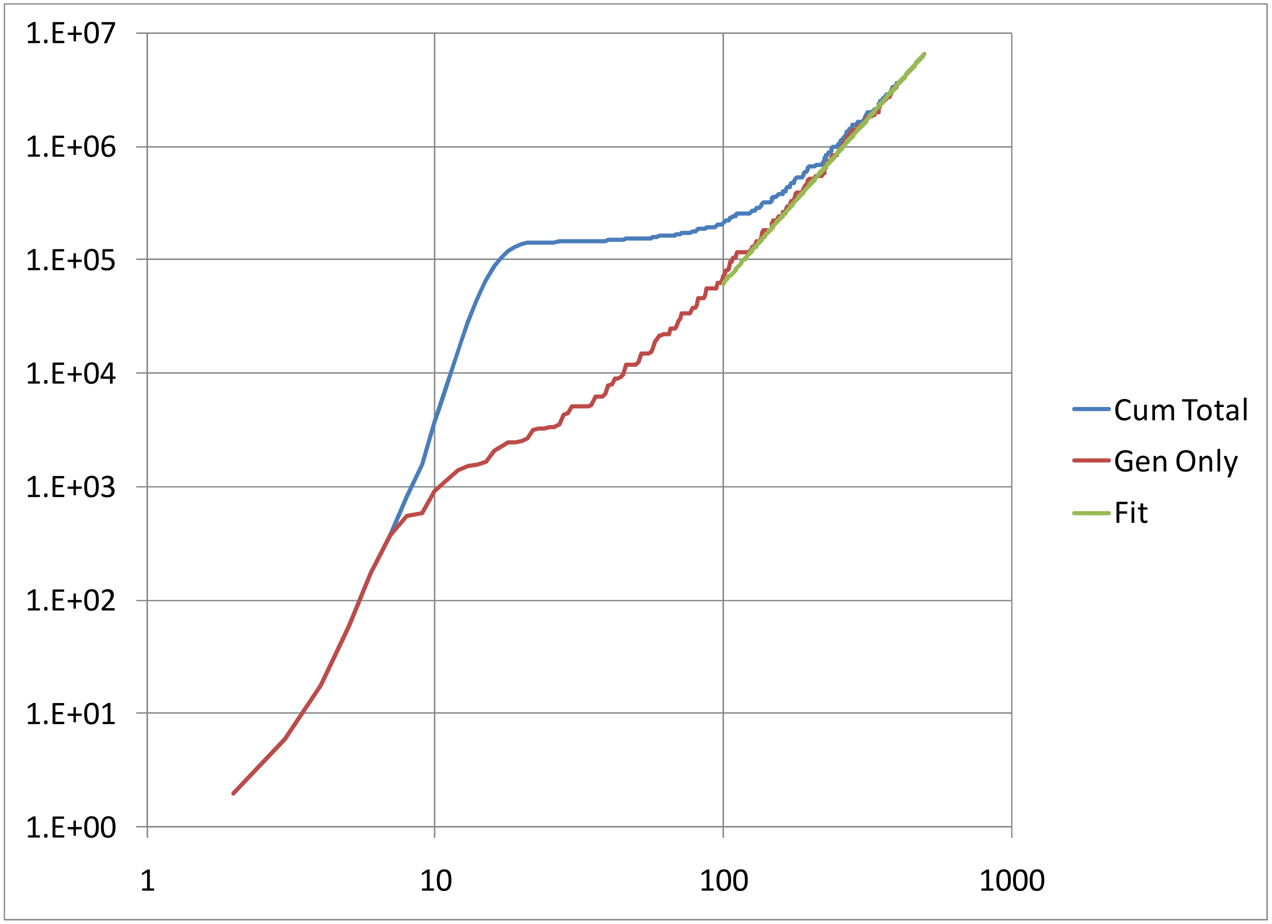
```
******************************************************************************
               Order          All      Essential   Symmetrical G-Symmetrical
                 448       172032          21504             0         86016
                 455        21312           2700            72             0
Current order:   456       131328          16416             0         65664
                 458          276             35             1             0
                 460       162024          20253             0         80960
******************************************************************************
Current options:

No. Value, Description
1      F, T => all CAs to order 27; F => generated CAs to order 500
2    456, Order of CAs for output
3      F, T => filter by generator method; F => output all
4      0, If previous option is T, filter by generator method 1 to 19
5      1, 1 => All, 2 => Essential, 3 => Symmetrical, 4 => G-Symmetrical
6      0, 0 => Output CAs are row indices from 0 to N-1, 1 => from 1 to N
7 REWIND, APPEND => append to existing output files; REWIND => overwrite
8      T, T => Find generating polynomial in a Galois field.
9     49, Order of Galois field.
10 C:\Data\IEEE\Papers\CISS\CISS2006\CDROM_Image\, Database folder
11 .\Costas_Array_Database_Output.txt, Pathname for output text

Enter option 1-11 to change, 12 for HELP, or 0 to proceed:
```

Cumulative Totals versus Order

CISS 2010



Conjecture Probably FALSE

CISS 2010

- The number of Costas arrays of any given order $N>23$ does not exceed N^2. [FALSE]
- Costas arrays of order 556
  - Total of 306,912
  - 383,684 essential Costas arrays
  - No symmetrical Costas arrays
  - 153,456 G-symmetrical Costas arrays, 38,364 of which are unique
- $556^2 = 309,136$; we have 99.3%

Why It's Important

CISS 2010

- A hard limit of N^2 indicates that a universal generator of rank 2 may exist
- Work on linear algebra in Galois fields for CISS 2008 paper
  - Promising
  - The most powerful linear algebra tools are not available
    - Self-annihilating vectors
    - Square roots do not exist for odd powers of principal elements
- Holy Grail is definition of a rank 2 generator

Why It's Probably False

CISS 2010

- Equality is reached in one known case
  - There are 65536 Costas arrays of order 256
  - None of them are symmetrical
  - 32768 of them are G-symmetrical
  - 8192 of them are unique G-symmetrical Costas arrays
- False for every order from 5 through 23
- Near-equality is reached multiple times
  - N(28) = 712 or 91% of 28^2 = 784
  - N(46) = 2044 or 96.6% of 46^2 = 2116
  - See orders 58, 82, 106, 166, 178,226, 256(!), 358, 556
  - Presently running generators over range 501-600
- Orders 256 and 556 strongly indicate that the conjecture is probably false

Final Resolution is Near

CISS 2010

- Two ways to resolve this conjecture
  - Mathematical proof of the existence of a rank 2 generator of all potential Costas arrays
  - Counterexample, or proof of non-existence
- If a counterexample exists
  - One can almost certainly be found between order 501 and 1000
  - This area is being filled out now
- Ongoing work toward a mathematical proof

There Remain Mysteries

CISS 2010

- There are exactly 4 Costas arrays of these orders
  - 3, 55, 67, 75, 127, 175, 187, 235, 247, 307, 355, 375, 415, 427, 435, 475, 487, 495...
- Nearly all of these are found with the Taylor4 or Golomb*4 generators
  - Begin with Lempel-Golomb
  - Remove (1,2) and (2,1), or (1,1) and (2,q-2)

Ongoing Work

- A new look at generators
  - Math is promising
  - Generating polynomial is heuristic, non-unique
  - Formulation is different for Welch, Lempel-Golomb generators
- Extend the database
  - Search uses extensive “spin” that slows the generator program in proportion to N^3
  - “Spin” is essentially a targeted search that is less fruitful as the order increases
  - May drop “spin” for higher order if examination of database justifies this

On the Web Site

CISS 2010

- Available by the end of March, 2010
  - Extended database
  - Updated database extraction program
  - CISS 2010 paper and slides
  - Costas array data for order 556
- A page on my Engineering web site
  - Link on main page of http://jameskbeard.com
  - Don't forget this whole web site: http://www.costasarrays.org/